UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

ETSEIB

Desarrollo y aplicación de herramientas de valoración de riesgos tecnológicos en centrales nucleares españolas a partir de la técnica de Análisis Probabilista de Seguridad

Tesis Doctoral presentada por

Pedro Díaz Bayona

para el PhD. en Ingeniería Nuclear y de las Radiaciones Ionizantes

Noviembre 2017

Directores de Tesis:

Dr. Javier Dies Llovera

Dr. Alfredo de Blas del Hoyo

Departament de Física

División d'Enginyeria Nuclear

Universitat Politècnica de Catalunya

UPC ETSEIB

Agradecimientos

A Javier Dies, Alfredo de Blas, y Carlos Tapia, los directores de esta tesis doctoral, por su guía, su apoyo, su consejo, su ayuda, y su ánimo durante este largo trayecto que ha sido esta tesis doctoral. A Manel Martínez, por situarme en este camino, darme los primeros conocimientos de análisis probabilista de seguridad, y su apoyo, pese a la distancia. También a Héctor Hernández, por compartir su conocimiento, por su paciencia, y por su confianza.

A David Aulet, David Lomeña, Carla Formentí, María Celades, Enric Estruch, Bernat Cirera, Gerard Rovira, Matthew Asamoah, Antonio Gómez, Jie Zheng, Nitin Akhade, Mohammed, y Shaikha por su inestimable colaboración y trabajo en todo este proceso. Sin vosotros esta hubiese sido mucho más difícil.

A Eduard Baeza, Roger Garcia, Enric Bargalló, Javier Abal, José Carlos Rivas, y Encarna Alcalde por hacer que el día a día fuese sencillo, divertido, y amigable. A todos los miembros de la otrora llamada *Secció d'Enginyeria Nuclear* por haber tenido siempre la puerta abierta.

A mis padres, Pedro y Loli, por todo, pero principalmente por su paciencia, dedicación, apoyo, y ánimo durante todos estos años. Al resto de mi familia por su apoyo y su ánimo en todo momento. Y a mis amigos, por su paciencia y sus ánimos.

Preámbulo

La tesis doctoral "Desarrollo y aplicación de herramientas de valoración de riesgos tecnológicos en centrales nucleares españolas a partir de la técnica de Análisis Probabilista de Seguridad" ha sido realizada al amparo del programa de doctorado de *Enginyeria Nuclear i de les Radiacions Ionitzants* de la *Universitat Politècnica de Catalunya* (UPC) de acuerdo con el marco del legal establecido por el Real Decreto 99/2011 entre los años 2013 y 2017. Los trabajos y proyectos vinculados a la tesis han sido desarrollados en el seno del *Nuclear Engineering Research Group* (NERG) de la *Divisió d'Enginyeria Nuclear* del *Departament de Física* (DFI) y pertenecen a una de sus diversas líneas de investigación. Concretamente, los trabajos y proyectos que han dado como resultado esta tesis doctoral están vinculados al "Proyecto de Investigación para el desarrollo de métodos de análisis probabilistas de la seguridad en la valoración de riesgos económicos y tecnológicos en centrales nucleares" que el NERG desarrolla en colaboración con una de las empresas operadoras[1] de centrales nucleares españolas desde el año 2007. Debido a la cantidad y variedad de trabajos y proyectos realizados entre 2013 y 2017, esta memoria presenta aquéllos considerados como más relevantes desde el punto de vista científico-técnico. Es necesario destacar que, en beneficio del desarrollo de esta tesis doctoral, la Generalitat de Catalunya ha prestado financiación para su realización a través de la *Secretaria de Recerca i Universitats* en la forma de una beca FI-AGAUR. Es también de importancia indicar que parte del contenido aquí presentado forma parte del alcance del proyecto de I+D+i "Investigación y desarrollo de metodologías de gestión informada por el riesgo en centrales nucleares españolas mediante la aplicación del análisis probabilista de seguridad", incluido en el programa de proyectos I+D+i orientados a los retos de la sociedad del Ministerio de Economía, Industria y Competitividad con referencia ENE2015-67653-R.

El contenido de esta memoria de tesis se divide en tres partes: una, a modo de introducción, en la que se contextualiza la tesis doctoral dentro del campo de la seguridad nuclear, y otras dos partes en las que se presentan sendos proyectos relacionados con la elaboración de herramientas para la toma de decisiones basada en el riesgo asociado a la instalación estudiada. La primera parte, en pos de contextualizar los contenidos de la tesis doctoral, presenta el concepto de seguridad nuclear, analiza la evolución del mismo lo largo del desarrollo de la industria nuclear, desde los años 50 hasta las lecciones aprendidas del accidente de Fukushima, y presenta el estado del arte de la metodología de Análisis Probabilista de Seguridad (APS), y de las técnicas de toma de decisiones informadas por el riesgo.

La segunda parte de la tesis contiene el desarrollo y el análisis de resultados de un modelo piloto de análisis probabilista de seguridad de un almacén temporal individualizado, que se trata de una instalación de almacenamiento de combustible nuclear gastado. El desarrollo de este tipo de análisis consiste en la elaboración de un modelo logico-probabilista que describa la respuesta de la instalación analizada ante sucesos anormales, y que permita cuantificar el riesgo asociado a una consecuencia indeseada. En el momento de su finalización, el modelo aquí presentado era el único existente en la industria nuclear española. En una contribución novedosa al campo de la fiabilidad humana y al campo del APS, esta parte de la tesis doctoral presenta el desarrollo una metodología de análisis de fiabilidad humana de las operaciones a llevar a cabo en el contexto concreto de un almacén temporal individualizado. Se concluye en esta parte de la tesis que la contribución del riesgo del almacén temporal individualizado al riesgo total

[1] El nombre de esta empresa no se puede citar por motivos de confidencialidad.

del emplazamiento es prácticamente nula. Los anexos del A al O de este documento están asociados a esta parte de la tesis.

La tercera parte de la tesis presenta el desarrollo y aplicación de metodologías y herramientas, generadas mediante un análisis probabilista de seguridad de incendios, para incorporar el riesgo inducido por incendio en las prácticas habituales de toma de decisiones respecto a configuraciones de sistemas, componentes, y estructuras, en centrales nucleares. Pese a que la valoración del riesgo incluida en procesos de decisión ha de abarcar todos los aspectos posibles, la valoración del riesgo inducido por incendios se ha llevado a cabo, históricamente, mediante metodologías cualitativas alternativas al análisis probabilista, o se ha menospreciado directamente, a causa, principalmente, de la evolución tardía de la metodología APS de incendios. En consecuencia, las herramientas y metodologías presentadas en esta parte de la tesis doctoral son una contribución novedosa en el campo de la toma de decisiones informada por el riesgo pues precisamente su función es proporcionar una valoración cuantitativa del riesgo de incendios mediante la herramienta que supone el APS de incendios. Específicamente, se proponen y describen dos herramientas novedosas, que se aplican al caso real de una central nuclear española. La primera herramienta desarrollada es la llamada matriz de compatibilidades de indisponibilidades de sistemas contra incendio y funciones clave de seguridad, y la segunda es la llamada matriz de riesgo de incendio de zonas de incendio y funciones clave de seguridad. Tal y como se explica en la memoria de tesis, de la aplicación de estas herramientas a una de las centrales nucleares al amparo de la empresa operadora se ha concluido que todo elemento con impacto en el riesgo inducido por incendios de dicha central está localizado en un grupo reducido de equipos, sistemas contra incendio, y zonas de incendio. Los anexos del P al S de este documento están asociados a esta parte de la tesis.

La difusión científica vinculada al desarrollo de los trabajos y proyectos realizados en el marco esta tesis doctoral se presenta, en un capítulo dedicado a ello, a posteriori de la tercera parte de esta memoria. Se avanza, no obstante, que se han publicado dos artículos en revistas científicas internacionales, que se ha participado, presentando dos ponencias, en un congreso internacional dedicado al análisis probabilista de seguridad, y que se han realizado múltiples colaboraciones, en distintos formatos, en varias reuniones anuales de la sociedad nuclear española.

Índice general

Índice de figuras

Índice de tablas

Nomenclatura

AAA Agua de Alimentación Auxiliar

ABD Accidente Base de Diseño

ACG Analysis Case Group

AEC Atomic Energy Commission

ALARA As Low As Reasonably Achievable

APS Análisis Probabilista de Seguridad

ARI Análisis de Riesgo de Incendios

ASME American Society of Mechanical Engineers

ATHEANA A Technique for Human Error ANAlysis

ATI Almacén Temporal Individualizado

BDG Base de Datos Genérica

BOE Boletín Oficial del Estado

BWR Boiling Water Reactor

CDF Cummulative Distribution Function

CLC Cask Loading Campaign

CLO Condiciones Límite de Operación

CMF Conjunto Mínimo de Fallo

CRUD Chalk River Unidentified Deposit

CSN Consejo de Seguridad Nuclear

DEC Design Extension Condition

DFI Departament de Física

DHFET Detailed Human Failure Event Tree

EFCs Error Forcing Contexts

EFS Estudio Final de Seguridad

EOC Error Of Commission

EOO Error Of Omission

EPIX Equipment Performance Information Exchange System

EPRI Electric Power Research Institute

EPS Effective Plastic Strain

ETF Especificaciones Técnicas de Funcionamiento

FCS Función Clave de Seguridad

FDN Frecuencia de Daño al Núcleo

FGL Frecuencia de Grandes Liberaciones

FGLT Frecuencia de Grandes Liberaciones Tempranas

FMEA Failure Mode and Effects Analysis

HCR Human Cognitive Reliability

HEF High Efficiency Filter

HEP Huamn Error Probability

HEPA High-efficiency particulate arrestance

HFE Human Failure Event

HFET Human Failure Event Tree

HRA Human Reliability Analysis

IAEA International Atomic Energy Agency

INPO Institute of Nuclear Power Operations

INSAG International Nuclear Safety Group

IRIDM Integrated Risk Informed Decision Making Process

LEL Lower Explosive Limit

LOCA Loss of Coolant Accidents

MCS Minimal CutSet

MIT Massachusetts Institute of Technology

MLD Master Logic Diagram

MPC Multi Purpose Canister

NASA National Aeronautics and Space Administration

NEI Nculear Energy Institute

NERG Nuclear Engineering Research Group

NHEP Nominal Human Error Probability

NRC Nuclear Regulatory Commission

NSSS Nuclear Steam Supply System

PCG Piscina de Combustible Gastado

PDF Probability Density Function

PMC (Procedimiento de Manipulación del Contenedor)

PR Protección Radiológica

PSFs Performance Shaping Factors

RADS Reliability and Availability Data System

RAW Risk Achievement Worth

RCS Reactor Coolant System

RDF Risk Decrease Factor

RIF Risk Increase Factor

RMA Risk Management Action

SBLOCA Small Break Loss of Coolant Accident

SBO Station Black-Out

SBO Station Black-Out

SHARP Systematic Human Action Reliability Procedure

SHED Savannah River Site Human Error Database Development for Nonreactor Nuclear Facilities (U)

SPAR-H Standarized Plant Analysis Risk-Human Reliability

SRP Standard Review Plan

SSE Safe Shutdown Earthquake

TECDOC Technical Document

TF Triaxility Factor

THERP Technique for Human Error Rate Prediction

TRC Time Reliability Curve

UA Unsafe Action

UPC Universitat Politècnica de Catalunya

USAEC United States Atomic Energy Commission

WENRA Western European Nuclear Regulators Association

WIPP Waste Isolation Pilot Plant

Parte I

Introducción

Capítulo 1

Sobre seguridad nuclear

1.1. Introducción

El capítulo 1 presenta una introducción a la seguridad nuclear, las temática de mayor jerarquía en la que se enmarca esta tesis doctoral. El objetivo de este primer capítulo es definir el marco de referencia del contenido de esta tesis doctoral y situar, dentro de este marco, los ítems específicos de la seguridad nuclear que son objeto de la tesis, el Análisis Probabilista de Seguridad, capítulo 2, y la toma de decisiones basada en el riesgo, capítulo 3.

En cumplimiento del citado objetivo, en este primer capítulo se presenta el concepto genérico de seguridad nuclear, sección 1.2, que posteriormente se expande mediante los diez principios fundamentales de la seguridad nuclear de la International Atomic Energy Agency[1] (IAEA), sección 1.3. Se extraen cuatro conceptos clave de los diez principios fundamentales de la seguridad nuclear: el marco legislativo, de regulación, y de gestión de la seguridad, presentado en la sección 1.4, las dos filosofías básicas sobre las que se asienta la seguridad nuclear, la defensa en profundidad y la cultura de seguridad, presentadas en la sección 1.5, y el análisis de la seguridad, presentado en la sección 1.6 y objeto de esta tesis doctoral. Finalmente, se presenta la evolución de la seguridad nuclear desde la concepción de la industria nuclear hasta el día de hoy, sección 1.7, para ilustrar el proceso de maduración experimentado.

1.2. El concepto de seguridad nuclear

Toda actividad industrial tiene sus propias ventajas únicas, y sus posibles efectos perjudiciales sobre trabajadores, público, y medio ambiente, entendidos como riesgos, peligros, y daños. En el ámbito industrial, se define el término *seguridad* como la ausencia, o la minimización óptima, de los riesgos, peligros, y daños sobre los trabajadores, el público, y el medio ambiente asociados a una actividad. En consecuencia, el *objetivo de la seguridad* es la protección de los trabajadores, el público, y el medio ambiente, de los efectos perjudiciales asociados a una actividad mediante el adecuado tratamiento de los mismos. La aplicación del objetivo de seguridad en el desarrollo de una actividad industrial es condición *sine qua non* para la aceptación de dicha actividad por parte de la sociedad. Es decir, solo aquellas actividades industriales

[1] La IAEA es una organización que, desde 1955, tiene marcado en sus estatutos el propósito de acelerar e incrementar la contribución de la energía atómica a la paz, la salud y la prosperidad de la humanidad evitando a toda costa su uso militar. Con este objetivo, la IAEA proporciona asistencia multidisciplinar a sus 168 estados miembros. La IAEA es una de las organizaciones de mayor importancia en el marco nuclear debido a su carácter internacional y a su contribución al desarrollo seguro de la tecnología nuclear. El material generado por la IAEA es referencia para la legislación, regulación, desarrollo, y ejecución de la tecnología nuclear en multitud de sus estados miembros.

consideradas como seguras son aceptadas por la sociedad para su explotación y desarrollo. No obstante, el objetivo de seguridad ha de ser alcanzado sin limitar de forma excesiva la actividad de la cual se espera extraer un beneficio, producto, o servicio.

Los efectos perjudiciales de las actividades enmarcadas en el ámbito de la producción de energía eléctrica a partir de energía nuclear, y en otros ámbitos de uso de tecnologías nucleares, van más allá de los tipos convencionales que aplican a cualquier actividad industrial. Concretamente, los posibles efectos perjudiciales asociados a este tipo de actividades nucleares son efectos adversos sobre la salud de los trabajadores y el público causados por la radiación, y la contaminación radioactiva de tierra, aire, mar, y alimentos [11]. Se define *seguridad nuclear* como la ausencia, o la óptima minimización, de estos posibles efectos perjudiciales asociados a las actividades nucleares. El término seguridad nuclear, tal y como está usado en este documento, no incluye los aspectos de seguridad no relacionados con la radiación. En consecuencia, el objetivo general de la seguridad nuclear es (véase las referencias [12][11][13]):

> Proteger a las personas y al medio ambiente de los efectos perjudiciales de las radiaciones ionizantes.

El objetivo general de la seguridad nuclear aplica a todas las instalaciones y actividades nucleares durante todo su ciclo de vida, incluyendo la preparación, la elección del emplazamiento, el diseño, la construcción, la puesta en servicio, y la operación, así como también el desmantelamiento y el cierre. La aplicación del objetivo general de seguridad nuclear no ha de limitar en exceso la operación de las instalaciones ni el desarrollo de las actividades que dan lugar a la radiación y a los riesgos inherentes a la misma. La International Atomic Energy Agency define las medidas que ha de tomar toda instalación nuclear para cumplir el objetivo general de seguridad nuclear [13]:

- Limitar la exposición a la radiación de las personas y la liberación de materiales radioactivos al medio ambiente.
- Limitar la probabilidad de sucesos que puedan causar la pérdida de control sobre un reactor nuclear, una reacción en cadena nuclear, una fuente radioactiva, o cualquier otra fuente de radiación.
- Mitigar las consecuencias de los eventos mencionados si ocurriesen.

El objetivo general de la seguridad nuclear y las tres medidas derivadas de su aplicación indican qué se ha de conseguir, pero no hacen referencia a cómo conseguirlo. Con el objetivo de proporcionar un marco de referencia para definir la forma de cumplir con el objetivo de seguridad, la IAEA define diez principios fundamentales de seguridad [13] (véase sección 1.3 para más detalle). Estos principios proporcionan las bases para el desarrollo de requisitos y medidas a tomar para la protección de las personas y el medio ambiente respecto a los riesgos inherentes la radiación, y para la seguridad de las instalaciones y actividades que dan lugar a los mencionados riesgos de la radiación. La IAEA aplica los principios fundamentales de seguridad en todas sus operaciones y recomienda su aplicación para sus propias actividades a Estados, autoridades nacionales y organizaciones internacionales. Pese a no ser obligatorios, dichos principios y los requisitos que de ellos emanan se incluyeron en los requisitos básicos de seguridad nuclear aplicables a las instalaciones nucleares definidos en la Directiva 2009/71/EURATOM[2] del Consejo de la Unión Europea de 25 de junio de 2009, que establece un marco comunitario para la seguridad nuclear de las instalaciones nucleares en base a documentación de la IAEA y de WENRA (Western European Nuclear Regulators Association)[3] [12].

[2] Esta directiva fue promulgada por la Comunidad Europea de Energía Atómica, llamada EURATOM. EURATOM, que forma parte de la Unión Europea, tiene por objetivo favorecer las condiciones necesarias para la creación de una industria nuclear en el territorio de los Estados Miembros. Entre sus funciones está la de establecer normas en materia de protección radiológica.

[3] WENRA ejerce de marco de encuentro y cooperación para los organismos reguladores de los países de la Europa occidental.

1.3. Principios fundamentales de la seguridad nuclear

En los estatutos de la IAEA, aprobados en octubre de 1956, se explicita que la agencia esta autorizada a establecer o adoptar, y ,cuando sea apropiado, en colaboración con los órganos competentes de las Naciones Unidas y las agencias especializadas interesadas, estándares de seguridad para la protección de la salud y la minimización del peligro para la vida y la propiedad [14]. La agencia también está autorizada a requerir el cumplimiento de estos estándares en cualquier operación en que ella sea una parte, y a requerir el cumplimiento de estos estándares en operaciones y actividades en el campo de la energía nuclear, siempre y cuando el cumplimiento sea requerido por Estados miembros o participantes de la IAEA. Los estándares de seguridad de la IAEA se jerarquizan de la siguiente manera:

1. Principios fundamentales de seguridad: Conceptos, principios, y objetivos básicos para la seguridad.
2. Estándares de seguridad: Requisitos básicos que han de ser cumplidos para garantizar la seguridad en actividades o áreas particulares.
3. Guías de seguridad: Recomendaciones, basadas en la experiencia internacional, respecto al cumplimiento de los requisitos básicos.

La IAEA publica también otros documentos de cariz más técnico, como las Safety Guides, o los Technical Documents (TECDOC) que presentan ejemplos prácticos y métodos detallados para la aplicación de los estándares de seguridad. Pese a que la aplicación de estos principios y estándares no es obligatoria a nivel estatal, ser miembro de la IAEA implica tener el compromiso de cumplir con sus reglas y normas, e, incluso, los países que reciben asistencia de la IAEA están obligados a cumplir con sus requisitos. Aunque es posible regular mediante criterios más estrictos, la mayoría de los países miembros de la IAEA están adoptando los estándares de la IAEA como base para su propia regulación [14]. De hecho,tal y como se ha visto en la sección anterior con el caso de la la Directiva 2009/71/EURATOM, la mayoría de las directivas modernas promulgadas por la Unión Europea reconocen que los estándares y principios de seguridad de la IAEA son una referencia para la regulación. Los principios fundamentales de la IAEA, documentados por primera vez en 1993, están totalmente aceptados a nivel internacional y se presentan en esta Tesis Doctoral como los principios básicos de la seguridad nuclear. En esta tesis se expone, a continuación, la versión actualizada de los principios publicada en 2006.

1.3.1. Principio 1: Responsabilidad sobre seguridad

La máxima responsabilidad sobre seguridad recae sobre el individuo u organización responsable de la instalación y las actividades que dan lugar a los riesgos inherentes a la radiación. El individuo u organización que es autorizado a operar una instalación o llevar a cabo una actividad que pueda dar lugar a los riesgos inherentes a la radiación es conocido como licenciatario. El licenciatario es el máximo responsable de la seguridad durante toda la vida de la instalación o toda la duración de la actividad. Esta responsabilidad no puede ser delegada, pero otros grupos, como, por ejemplo, diseñadores, fabricantes, y constructores, entre otros, también tienen responsabilidad legal, profesional y funcional con respecto a la seguridad. Las responsabilidades del licenciatario para la seguridad, tal y como están definidas en el primer principio fundamental, son las siguientes:

- Establecer y mantener las competencias necesarias para la seguridad.
- Proveer la información y el entrenamiento adecuados.
- Establecer procedimientos y planes para mantener la seguridad bajo cualquier condición.
- Verificar que el diseño y la calidad de las instalaciones, las actividades, y del equipamiento asociado es apropiado.

- Garantizar el control adecuado de todo el material radioactivo usado, producido, almacenado y transportado.
- Garantizar el control adecuado de todo residuo radioactivo generado.

Estas responsabilidades han de cumplirse de acuerdo con los objetivos y requisitos de seguridad establecidos por el organismo regulador competente.

1.3.2. Principio 2: El rol del gobierno

El segundo principio destaca que se ha de establecer y mantener un marco legal y gubernamental para la seguridad que sea eficiente, incluyendo un organismo regulador independiente (véase sección 1.4 para más detalle). El gobierno es responsable de adoptar, dentro del sistema nacional de legislación, aquellas leyes, reglas, y otros estándares y medidas que sean necesarias para cumplir con sus obligaciones nacionales e internacionales en el marco de la seguridad nuclear. Un adecuado marco legal y gubernamental para garantizar la seguridad permite la asignación clara de responsabilidades. El gobierno y el organismo regulador tienen la responsabilidad de establecer los estándares de seguridad y el marco regulador para la protección de las personas y el medio ambiente ante los riesgos inherentes a la radiación. Sin embargo, tal y como establece el primer principio, el licenciatario es el primer responsable de la seguridad.

1.3.3. Principio 3: Liderazgo y gestión para la seguridad

Las organizaciones relacionadas con, y las instalaciones y actividades que dan lugar a, riesgos inherentes a la radiación han de establecer y mantener sistemas de liderazgo y de gestión efectivos para la seguridad. Se destaca en el tercer principio fundamental que el liderazgo en cuestiones de seguridad tiene que manifestarse en los más altos niveles jerárquicos del licenciatario, y que la seguridad debe lograrse y mantenerse por medio de un sistema de gestión efectivo. Se explicita que este sistema debe integrar todos los elementos de la gestión para que los requisitos para la seguridad sean establecidos y aplicados de forma coherente con otros requisitos. De esta manera, la seguridad no se verá comprometida por requisitos o demandas de otros aspectos como la seguridad física o la calidad. El sistema de gestión debe garantizar la promoción dentro de la organización de la cultura de seguridad (véase sección 1.5 para más detalle), el análisis regular del estatus de la seguridad (véase sección 1.6), y la aplicación de las lecciones aprendidas de la experiencia operativa propia y ajena. El sistema de gestión ha de apoyar las buenas prácticas y actuaciones para evitar fallos humanos y organizacionales derivados del factor humano.

1.3.4. Principio 4: Justificación de instalaciones y actividades

El cuarto principio destaca que las instalaciones y actividades que dan lugar a riesgos inherentes a la radiación han de demostrar que proporcionan un beneficio para la sociedad. Los beneficios que proporciona una instalación o actividad deben compensar los riesgos inherentes a la radiación a los que da lugar para que la instalación o actividad se considere justificada. La decisión respecto a la balanza entre beneficios y riesgos de una actividad se toma en muchos casos a nivel gubernamental, como, por ejemplo, la decisión de implantar un programa de energía nuclear. En otros casos es el organismo regulador quien determina si la instalación o actividad propuesta está justificada.

1.3.5. Principio 5: Optimización de la protección

Se ha de optimizar la protección en instalaciones y actividades que dan lugar a riesgos inherentes a la radiación para conseguir que el nivel de seguridad sea el más alto posible. Las medidas de seguridad

aplicadas en instalaciones y actividades que dan lugar a riesgos inherentes a la radiación son óptimas si proporcionan el nivel de seguridad razonablemente más alto posible durante todo el ciclo de vida de la instalación o la actividad. Todos los riesgos inherentes a la radiación relacionados con una instalación o actividad, tanto asociados a operación normal como a condiciones accidentales, han de ser analizados a priori y reanalizados periódicamente durante el ciclo de vida de la instalación o la actividad para determinar si el riesgo es tan bajo como es razonablemente posible. La optimización de la protección requiere juzgar la importancia relativa de varios factores, incluyendo:

- La cantidad de personas (trabajadores y público) que puedan quedar expuestas a la radiación.
- La posibilidad de que estas personas queden expuestas a la radiación.
- La magnitud y la distribución de las dosis de radiación recibidas.
- Los riesgos inherentes a la radiación que podrían ser consecuencia de eventos predecibles.
- Factores económicos, sociales y medioambientales.

La optimización de la protección también implica usar el sentido común y seguir prácticas adecuadas para evitar los riesgos inherentes a la radiación tanto como sea practicable en actividades diarias.

1.3.6. Principio 6: Limitación del riesgo a individuos

Las acciones y medidas tomadas para controlar los riesgos inherentes a la radiación han de asegurar que ningún individuo hace frente a un riesgo inaceptable. Por lo tanto, la dosis y los riesgos inherentes a la radiación han de someterse a y cumplir con límites superiores específicos. Por otra parte, los límites representan la cota superior de aceptabilidad de la dosis y los riesgos inherentes a la radiación, y, por lo tanto, su cumplimiento no es suficiente para garantizar que se aplique la mejor protección posible. La aplicación de los límites ha de apoyarse de la optimización de la protección, el quinto principio, para que la dosis y los riesgos inherentes a la radiación que puedan afectar a los individuos sean lo más bajo posible.

1.3.7. Principio 7: Protección de la generación actual y de las futuras

Los individuos y el medio ambiente, tanto del presente como del futuro, han de estar protegidos frente a los riesgos inherentes a la radiación. Los riesgos inherentes a la radiación pueden trascender las fronteras nacionales y pueden persistir durante un largo periodo de tiempo. Las posibles consecuencias de actuaciones presentes se han de tener en cuenta a la hora de juzgar la idoneidad de las medidas de control de los riesgos de la radiación. Particularmente, los estándares de seguridad aplican tanto a poblaciones locales como a poblaciones que estén lejos de instalaciones o actividades. Además, cuando los efectos de los riesgos de la radiación puedan hacerse notar durante generaciones, las siguientes generaciones han de estar protegidas adecuadamente sin que estas mismas generaciones deban tomar medidas de protección significativas. Este es el caso de los residuos radioactivos, que han de ser gestionados de tal manera que éstos no supongan una pesada carga para las futuras generaciones. Esto implica que las generaciones que produzcan los residuos han de encontrar y aplicar una solución segura, practicable y aceptable desde el punto de vista medio ambiental para la gestión a largo plazo de los mismos.

1.3.8. Principio 8: Prevención de accidentes

Se han de hacer todos los esfuerzos posibles para prevenir y mitigar accidentes nucleares o radioactivos. Las consecuencias más dañinas relacionadas con instalaciones o actividades nucleares han sido resultado de la pérdida de control sobre un reactor nuclear, sobre la reacción nuclear en cadena, sobre fuentes de

radiactividad o similar. En consecuencia, el octavo principio indica que se han de tomar las siguientes medidas para garantizar que la posibilidad de un accidente con consecuencias negativas sea extremadamente baja:

- Impedir la ocurrencia de fallos o desviaciones de la operación normal (incluyendo brechas de seguridad física) que pudiesen dar lugar a una pérdida de control.
- Impedir la escalada de cualquier fallo o desviación que pudiese ocurrir.
- Impedir la pérdida de control sobre una fuente radioactiva o cualquier otra fuente de radiación.

El principal medio de prevenir y mitigar las consecuencias de accidentes es la llamada defensa en profundidad (véase sección 1.5). El concepto de defensa en profundidad se aplica mediante la combinación de niveles de protección consecutivos e independientes que deberían fallar antes de que las personas o el medio ambiente sufrieran los efectos dañinos de la radiación. Si una barrera o un nivel de protección fallara, el siguiente nivel o barrera estaría disponible para impedir la progresión del suceso. Si se aplica adecuadamente, la defensa en profundidad garantiza que ningún tipo de fallo simple, ni técnico ni humano ni organizacional, pueda dar lugar a consecuencias dañinas, y que la probabilidad de ocurrencia de combinaciones de fallos que podrían causar consecuencias negativas es muy baja. La defensa en profundidad es provista por una adecuada combinación de:

- Un sistema de gestión efectivo comprometido con la seguridad y con la implantación de la cultura de seguridad (véase el tercer principio fundamental de seguridad en la página 36)
- Una adecuada selección del emplazamiento y la incorporación de sistemas diseñados para la seguridad con suficientes márgenes de seguridad, y diseñados teniendo en cuenta los conceptos de diversidad, redundancia, calidad, y fiabilidad.
- Guías de accidente severo, procedimientos y prácticas operacionales, exhaustivas.

1.3.9. Principio 9: Respuesta y preparación ante emergencias

Se han de tener preparados planes de emergencia y de respuesta ante incidentes nucleares o radioactivos. Los principales objetivos de la exigencia de preparación y respuesta ante emergencias nucleares o radioactivas son:

- Garantizar que se han tomado medidas para proporcionar una respuesta efectiva ante una emergencia nuclear tanto a nivel local, como regional, nacional e internacional.
- Garantizar que, para incidentes razonablemente predecibles, los riesgos inherentes a la radiación serían menores.
- Tomar medidas prácticas para mitigar cualquier consecuencia para la vida humana, la salud y el medio ambiente en caso de incidente.

El licenciatario, el organismo regulador, y las agencias gubernamentales relacionadas, han de establecer, por adelantado, planes para la preparación y respuesta ante una emergencia nuclear tanto a nivel local, como regional, nacional e internacional. En el desarrollo de los planes de respuesta ante emergencias, se han de considerar todos los eventos que se puedan predecir. Los planes de emergencia se han de ejecutar periódicamente en forma de simulacros para garantizar que las organizaciones que son parte de los planes de emergencia están preparadas para llevarlos a cabo.

El noveno principio indica que, cuando se hayan de tomar acciones urgentes en una emergencia, puede aceptarse que los trabajadores que participen en la emergencia reciban dosis que excedan los límites normales (véase el sexto principio fundamental), siempre y cuando den su consentimiento.

1.3.10. Principio 10: Acciones de protección para reducir los riesgos inherentes a la radiación natural o no regulados

Los riesgos inherentes a la radiación pueden darse en situaciones en las que no son instalaciones o actividades bajo el control regulador las que los producen. En estas situaciones, si el riesgo es relativamente alto, se debe considerar si se pueden llevar a cabo, de forma razonable, acciones de protección que reduzcan la exposición a la radiación o que remedien posibles condiciones adversas. El principio 10 presenta tres tipos de situaciones objetivo:

- Radiación de origen natural, que incluye la exposición a gas radón y sus descendientes, Pb214 y Bi214, en hogares y centros de trabajo, donde se pueden realizar acciones correctivas si es necesario.
- Exposición fruto de actividades humanas llevadas a cabo en el pasado que no estuvieron sujetas a control regulador o que estuvieron sujetas a un control regulador temprano menos riguroso. Un ejemplo son los sobrantes radioactivos de actividades mineras pasadas.
- Acciones de protección realizadas después de una liberación no controlada de radionúclidos a la atmósfera.

En cualquiera de las situaciones postuladas, las acciones de protección que se consideren oportunas tendrán costes económicos, sociales, medio ambientales e implicaran la aceptación de riesgos inherentes a la radiación. Las acciones de protección solo se consideraran justificadas si suponen un beneficio suficiente como para compensar los riesgos inherentes a la radiación y otras desventajas asociadas a ejecutarlas. Además, estas acciones de protección deben optimizarse de tal manera que produzcan el mayor beneficio posible en relación a los costes.

1.4. El marco de aplicación de la seguridad: Legislación, regulación, y gestión

El primer, segundo y tercer principios fundamentales de la IAEA definen el marco de aplicación de la seguridad en instalaciones o actividades nucleares. Este marco de aplicación se divide en tres niveles jerárquicos: la legislación, la regulación, y la gestión y liderazgo en seguridad. Cada nivel es responsabilidad de un actor principal: el gobierno, el organismo regulador, y el licenciatario, respectivamente. Hoy en día, la mayoría de estados con programas nucleares en ejecución mantienen marcos de aplicación de la seguridad similares al promulgado por la IAEA. Tras años de experiencia y tras multitud de países lanzando y ejecutando sus programas nucleares, existe consenso en la comunidad nuclear respecto a que la separación de responsabilidades que promulga el marco de aplicación definido en los tres primeros principios fundamentes de seguridad de la IAEA permite tratar la seguridad de las instalaciones o actividades nucleares de la forma más eficiente y efectiva.

1.4.1. El papel del gobierno

La principal responsabilidad del gobierno en materia de seguridad es establecer leyes y adoptar políticas en las que se enmarque la regulación sobre seguridad y en las que se definan claramente las responsabilidades y funciones de cada ente participante en materia de seguridad nuclear [15]. Una de las leyes a establecer por el gobierno debe ser la de creación del organismo regulador pertinente y definición de sus responsabilidades. En la adopción de sus políticas, el gobierno debe asegurar que el organismo regulador es independiente en la toma de decisiones sobre seguridad, y que esta funcionalmente separado de entidades con responsabilidades o intereses que podrían influenciar exageradamente en la toma de decisiones sobre seguridad. Si otras

autoridades tienen responsabilidades sobre seguridad que coinciden con las del marco regulador para la seguridad establecido por el organismo regulador, el gobierno debe asegurar la correcta coordinación de sus funciones de regulación para evitar omisiones, duplicidades o conflictos.

1.4.2. El papel del organismo regulador

Mientras que el gobierno establece leyes y adopta políticas relacionadas con la seguridad, el organismo regulador desarrolla estrategias y promulga reglas y normas, el marco regulador, en la implantación de esas leyes y políticas. El papel primordial del organismo regulador es el de la creación y mantenimiento de un marco regulador y el establecimiento de estrategias y estándares de seguridad. Es responsabilidad del organismo regulador verificar que las instalaciones y/o actividades al amparo de su marco regulador cumplan con las reglas y estándares del mismo. El organismo regulador debe establecer o adoptar reglas y guías para especificar los principios, los requisitos y los criterios asociados a la seguridad sobre los cuales se basan las acciones, decisiones, y juicios reguladores [15]. Es responsabilidad del regulador asegurar que la supervisión de las centrales nucleares es totalmente independiente. El licenciatario, por su parte, debe proporcionar al regulador toda la documentación e información que requiera este último. El organismo regulador ha de implementar un procedimiento para el reporte de eventos y la gestión de la información que incluya la publicación informes, hallazgos, y otros para el gran público. En materia de emergencias, el regulador es responsable de establecer y mantener un sistema para proveer una coordinación efectiva de los diferentes organismos que toman parte en la respuesta ante una emergencia. También es responsabilidad del operador integrarse en el marco internacional de cooperación para la seguridad.

1.4.3. El papel del licenciatario

El organismo regulador proporciona el marco para el desarrollo de la seguridad de las centrales y es responsable de su verificación, pero la responsabilidad sobre la seguridad recae en el licenciatario u operador. Esta responsabilidad cubre todas las actividades relacionadas con la operación, directa o indirectamente, incluyendo la supervisión de actividades de todos los demás grupos: diseño, suministradores, fabricantes y constructores, subcontratas, y otros. Es responsabilidad del licenciatario el crear y mantener un sistema de liderazgo y de gestión claramente enfocado a conseguir la excelencia en materia de seguridad. Con este objetivo, la estrategia operacional implementada por el licenciatario debe dar a la seguridad la máxima prioridad, por encima de las demandas de la producción [16]. Las características más importantes, en pos de la seguridad, del sistema de gestión a implantar por el operador son:

- El sistema de gestión debe inculcar una fuerte cultura de seguridad, y debe definir con claridad el rol de liderazgo en temas de seguridad del más alto nivel jerárquico de gestión. Los gestores de alto nivel deben hacer llegar las provisiones de la política de seguridad a toda la organización.
- El sistema de gestión ha de ser tal que los aspectos clave de la política de seguridad han de ser trasladados a las subcontratas. Es más, el sistema de gestión ha de proporcionar las herramientas necesarias para consolidar la seguridad en las actividades llevadas a cabo por organizaciones externas de soporte.
- La gestión ha de establecer el compromiso para mejorar la seguridad operacional siempre que sea posible, y debe asegurar que la seguridad no entra en fricción con otros requisitos como puedan ser: producción, protección de la salud, actuación humana, protección del medio ambiente, y otros.
- La auto evaluación ha de ser una parte integral del sistema de supervisión y revisión de la seguridad del sistema de gestión, se han de definir indicadores de actuación (comúnmente conocidos como Performance indicators).
- En el sistema de gestión a aplicar, la estructura del operador y las funciones, roles, y responsabilidades del personal han de ser claras y estar documentadas.

1.5. Los conceptos de defensa en profundidad y cultura de seguridad

La combinación de los conceptos de defensa en profundidad y cultura de seguridad conforma la filosofía básica de seguridad en el diseño y operación de instalaciones nucleares, siendo de especial relevancia en lo que refiere a centrales nucleares [1]. Ambos conceptos han formado parte de la filosofía de seguridad de la industria nuclear desde sus inicios, y han evolucionado con ella (véase sección 1.7 para más detalle). Mientras que la defensa en profundidad ha sido aplicada siempre de forma explícita, la cultura de seguridad era una característica implícita del sistema de gestión del licenciatario hasta que tomó gran relevancia tras el accidente de Chernobyl. A partir de Chernobyl, se insistió, en el seno de la comunidad nuclear, en la aplicación explícita de la cultura de seguridad en las organizaciones responsables de la seguridad [17]. Hoy en día, ambos conceptos forman parte del marco global de aplicación de la seguridad requerido por los principios fundamentales de seguridad de la IAEA. Concretamente, la cultura de seguridad es requerida por el tercer principio fundamental, liderazgo y gestión para la seguridad, y la defensa en profundidad es requerida por el octavo principio fundamental, prevención de accidentes. A continuación se definen los conceptos de defensa en profundidad y cultura de seguridad en su aplicación a la seguridad nuclear de centrales nucleares.

1.5.1. La defensa en profundidad

La defensa en profundidad es una estrategia integral para la seguridad cuyo objetivo es garantizar, con un alto grado de confianza, que las personas y el medio ambiente están protegidas de cualquier peligro asociado al uso de la energía nuclear en la producción de electricidad. La estrategia aplicada en la defensa en profundidad para el cumplimiento de su objetivo es doble: primero, proveer las disposiciones necesarias para prevenir accidentes y, segundo, si la prevención falla, proveer las disposiciones necesarias para limitar las consecuencias y evitar cualquier evolución a peores condiciones. La estrategia de defensa en profundidad está orientada a ofrecer una protección cualificada ante una amplia variedad de transitorios, incidentes y accidentes, incluyendo fallos de equipos y errores humanos, y sucesos externos [1]. Además, la defensa en profundidad abarca todas las actividades relacionadas con la seguridad, incluyendo aquellas que ocurren durante la selección del emplazamiento, el diseño, fabricación, construcción, puesta en funcionamiento, operación, y desmantelamiento de centrales nucleares.

El concepto de defensa en profundidad ha evolucionado sustancialmente desde la idea original, que consistía en interponer varias barreras físicas entre el material radioactivo y el entorno para limitar las consecuencias de un accidente. Actualmente, el concepto incluye una estructura general de múltiples barreras físicas y medios complementarios para proteger a las propias barreras, los llamados niveles de defensa en profundidad. De acuerdo con el documento INSAG-10 [10], la definición actual de defensa en profundidad es la siguiente:

> La defensa en profundidad consiste en el despliegue jerárquico de diferentes niveles de estructuras, sistemas, componentes, y medidas administrativas, es decir, procedimientos y guías, cuyo objetivo es mantener la eficacia de las barreras físicas interpuestas entre el material radioactivo y los trabajadores, el público y el medio ambiente, tanto en operación normal como en transitorios previstos y, para ciertas barreras, también en accidentes.

La defensa en profundidad se divide en 5 niveles [10]. Si un nivel falla a controlar la evolución de una secuencia accidental, el siguiente nivel entra en juego. La tabla 1.1 presenta los 5 niveles de defensa en profundidad, el objetivo de cada uno, y los medios necesarios para logar el objetivo de cada uno.

Los niveles de defensa en profundidad han de ser tan independientes entre sí como sea posible. En la aplicación de la defensa en profundidad se ha de garantizar que un fallo simple, ya sea de equipamiento

Tabla 1.1: Niveles de defensa en profundidad [10]

Niveles de defensa en profundidad	Objetivo	Medios necesarios para logar el objetivo
Nivel 1	Prevenir fallos y desviaciones de la operación normal	Diseño conservador y alta calidad en la construcción y operación
Nivel 2	Control de desviaciones y detección de fallos	Sistemas de control y protección y otras características de supervisión
Nivel 3	Control de accidentes dentro de las bases de diseño	Sistemas para la seguridad y procedimientos de emergencia
Nivel 4	Control de condiciones severas de planta, incluyendo evitar la progresión del accidente y mitigar las consecuencias de accidentes severos	Medidas complementarias y guías de gestión de accidentes
Nivel 5	Mitigación de las consecuencias radiológicas de liberaciones significativas de material radioactivo	Planes de respuesta exterior a emergencias

o humano, en un nivel de defensa, e incluso una combinación de fallos en más de un nivel de defensa, no pone en riesgo a la seguridad propagándose a otros niveles superiores de defensa.

De acuerdo con el objetivo de la defensa en profundidad, se interponen varias barreras físicas para el confinamiento del material radioactivo. La cantidad y el tipo de las barreras que confinan a los productos de fisión dependen de la tecnología del reactor. En el caso de reactores de agua a presión, estas barreras son, de más a menos proximidad a los productos de fisión: la matriz de combustible, las vainas de combustible, la barrera de presión del sistema de refrigeración del reactor, y el edificio de contención. La primera y segunda barreras deberían estar preparadas para evitar entrar en condiciones accidentales como consecuencia de una desviación de la operación normal que sea probable que ocurra durante el ciclo de vida de la central [18]. La figura 1.1 muestra la relación entre los niveles de defensa y las barreras físicas de la defensa en profundidad.

En el marco de la defensa en profundidad se definen las llamadas funciones fundamentales de seguridad, cuyo cumplimiento evita el fallo de las barreras físicas en caso de entrar en condiciones accidentales y/o mitiga las consecuencias en caso de fallo de las barreras. Para mantener un alto nivel de seguridad, estas funciones fundamentales de seguridad han de cumplirse en todo estado operacional de la central, durante y después de un accidente base de diseño y, hasta el extremo practicable, durante y después de condiciones de planta más allá de las bases de diseño. Las funciones fundamentales de seguridad son:

1. Control de la reactividad
2. Extracción de calor del combustible
3. Confinamiento del material radiactivo

El cumplimiento de las funciones fundamentales de seguridad es esencial para la defensa en profundidad y es una medida de evaluación del grado de implementación de la defensa en profundidad en el diseño y la operación de centrales. Las disposiciones de defensa en profundidad implementadas en los diferentes

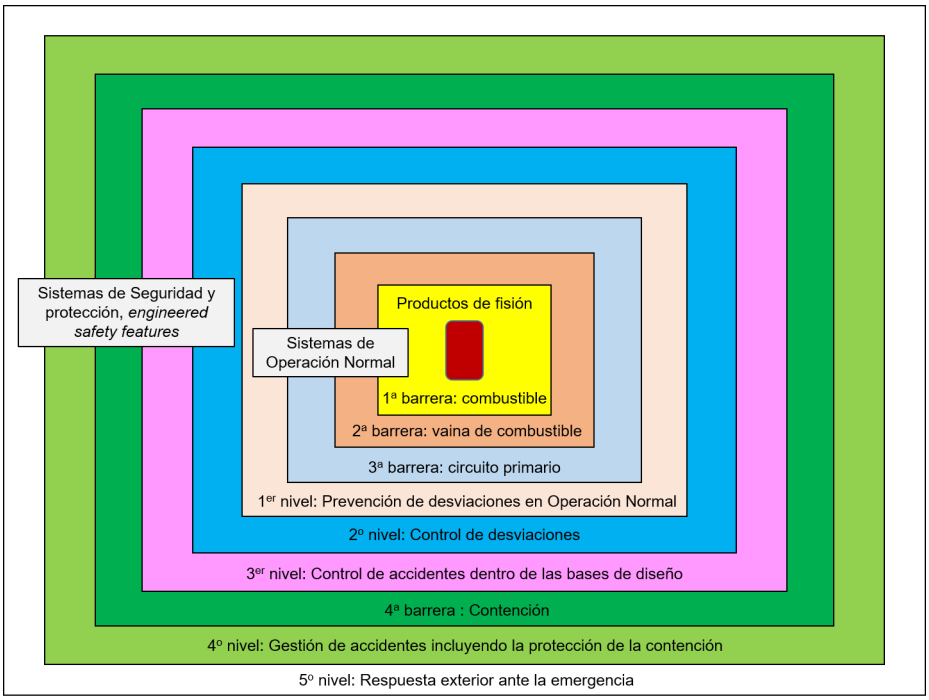


Figura 1.1: Relación entre niveles de defensa y barreras físicas. Fuente: Elaboración propia basada en [1]

niveles de defensa se hacen cargo de los posibles desafíos a las funciones fundamentales de seguridad. Estas disposiciones incluyen características de seguridad intrínseca, márgenes de seguridad, estructuras, sistemas, y componentes, redundancias y separación física, sistemas activos y pasivos, procedimientos y guías, acciones de operador, medidas organizacionales y aspectos de cultura de seguridad.

1.5.2. La cultura de seguridad

El concepto de cultura de seguridad se resume en considerar que la seguridad es el ítem de máxima prioridad en la organización y la realización de cualquiera de las actividades relacionadas con una instalación nuclear. El compromiso de aplicar la cultura de seguridad en la gestión de instalaciones nucleares existe desde los inicios de la industria nuclear [19]. No obstante, no se le dio la relevancia necesaria a la aplicación de la cultura de seguridad hasta que en el accidente de Chernobyl se demostró una flagrante falta de la misma. De hecho, el término cultura de seguridad fue introducido en el primer International Nuclear Safety Group (INSAG) de la IAEA, dedicado al análisis del accidente de Chernobyl. Sin embargo, no se alcanzó un cierto grado de consenso respeto a la definición del concepto hasta el cuarto INSAG de la IAEA, 5 años después del accidente, dedicado a la propia cultura de seguridad. La definición del concepto de cultura de seguridad derivado del cuarto INSAG de la IAEA es la siguiente [17]:

> La cultura de seguridad es el conjunto de características y comportamientos de organizaciones e individuos que establecen que, como prioridad fundamental, los asuntos relacionados con la seguridad de la instalación nuclear reciben una atención acorde a su importancia.

La cultura de seguridad tiene dos principales componentes: el primero, las políticas organizacionales y de gestión que establecen un marco para su aplicación, que son responsabilidad de la jerarquía de la gestión. El segundo es el comportamiento del personal, en todos los niveles, al responder a y beneficiarse de este marco.

La correcta aplicación y definición de la cultura de seguridad en una central nuclear deriva del cumplimiento y realización de ciertos requisitos y prácticas en los diferentes niveles jerárquicos de la misma. Concretamente, para una buena cultura de seguridad se han de cumplir requisitos a nivel de política, de gestión, y de la respuesta de los individuos. Los requisitos a nivel de política y gestión definen el marco de la cultura de seguridad, mientras que los requisitos respecto a la respuesta de los individuos definen cómo se han de comportar éstos al respecto de este marco.

Requisitos a nivel de política

Los requisitos establecidos a alto nivel para el desarrollo de una actividad condicionan la manera en que las personas actúan en la realización de dicha actividad. En el caso de la seguridad nuclear, el más alto nivel es el marco legislativo, en el cual se han de establecer las bases nacionales para la aplicación de la cultura de seguridad. A las organizaciones, incluyendo licenciatarios y organismos reguladores, se les aplica una consideración similar. Las políticas y normas fomentadas en el más alto nivel de la organización modelan el entorno de trabajo y condicionan el comportamiento individual. Las bases a aplicar en el establecimiento o adopción de políticas y normas para la implementación de una cultura de seguridad en una organización son:

- Realizar una declaración de política de seguridad en la cual las responsabilidades de la organización respecto a la seguridad queden definidas.
- Clarificar la responsabilidad en asuntos de seguridad estableciendo lineas de autoridad simples.
- Crear unidades internas e independientes de gestión cuya responsabilidad sea la supervisión de actividades relacionadas con la seguridad nuclear.
- Dedicar a la seguridad los recursos que sean necesarios.
- Tener y aplicar planes de revisión periódicos para aquellas actividades que contribuyan a la seguridad de la planta. Algunos ejemplos de estas actividades son: formación, revisión de experiencia operativa, control de cambios en el diseño, y otros.
- Comprometerse a nivel corporativo respecto a la seguridad. Demostrar y publicitar este compromiso para demostrar la voluntad de la organización de ser abierta en asuntos de seguridad.

Requisitos de gestión

La clave para instaurar una cultura de seguridad eficiente en los individuos se encuentra en que las prácticas, actitudes, y actividades que dan forma al entorno de trabajo acojan actitudes propicias para la seguridad. Es responsabilidad de la gestión el implementar estas prácticas de acuerdo con los objetivos y políticas de seguridad de su organización. Aspectos importantes en la creación del entorno de trabajo son:

- Definir las responsabilidades individuales mediante líneas de autoridad únicas y simples.
- Garantizar que todo trabajo asociado a la seguridad se lleve a cabo de forma rigurosa.
- Garantizar que el personal está totalmente cualificado para llevar a cabo sus tareas. Esto incluye que los trabajadores entiendan la importancia de sus tareas y las consecuencias que pueden tener sus errores.
- Crear un sistema de reconocimientos que premie aquellas actitudes meritorias en materia de seguridad.

- Implementar prácticas de revisión y monitorización como, por ejemplo, revisiones periódicas de los programas de formación.
- La gestión ha de estar comprometida respecto a la seguridad de tal manera que, mediante su actitud y su ejemplo, promuevan que el personal este continuamente motivado para dar lo mejor de sí.

Requisitos en la respuesta de los individuos

El principal requisito que ha de cumplir el personal es responder a y beneficiarse del marco de cultura de seguridad definido en los requisitos anteriores. La siguiente frase define la forma más efectiva de cumplir con el requisito en la respuesta de los individuos [17]:

> Una actitud inquisitiva, un acercamiento prudente y riguroso, y el uso de la comunicación resultarán en una gran contribución para la seguridad.

Una actitud inquisitiva por parte del personal que ha de realizar una tarea relacionada con la seguridad hará que se planteen cuestiones del estilo: ¿Entiendo la tarea? ¿Conozco mis responsabilidades y como se relacionan con la seguridad? ¿Qué puede ir mal? Mediante una actitud inquisitiva el personal ha de ser capaz de identificar si realmente está preparado para realizar con seguridad la tarea que se le ha asignado.

Un acercamiento prudente y riguroso incluye: entender los procedimientos, cumplir con los procedimientos, estar preparado para dar respuesta a sucesos inesperados, buscar ayuda si es necesario, o no tomar atajos. Todas estas prácticas harán que la realización de la tarea sea más segura.

Finalmente, el uso de la comunicación es esencial para la seguridad. La comunicación incluye: obtener información útil de otros, transmitir información a otros, informar y documentar los resultados del trabajo, sean rutinarios o inusuales, y sugerir nuevas iniciativas de seguridad.

1.6. Análisis de seguridad

El primer principio fundamental de seguridad de la IAEA, responsabilidad sobre seguridad, detalla que es responsabilidad del licenciatario verificar que el diseño y la calidad de las instalaciones, las actividades, y el equipamiento asociado es adecuado para mantener un alto nivel de seguridad. En el marco de las centrales nucleares, esta tarea de verificación se realiza mediante la aplicación del llamado análisis de seguridad. Los objetivos generales del análisis de seguridad son:

- Analizar la calidad y el nivel de protección de las disposiciones de seguridad. Este objetivo incluye la evaluación de las bases de diseño, de la aplicación de la defensa en profundidad y de los posibles retos a los que se podría enfrentar, y de la evolución y consecuencias de condiciones accidentales.
- Identificar las maneras en las que se podría incurrir en exposiciones a la radiación normales y potenciales.
- Determinar los niveles esperados de exposición normal, y las probabilidades y niveles de exposiciones potenciales.

El análisis de seguridad se desarrolla y se aplica, en primer término, en la etapa de diseño de la instalación, tal y como indica el requisito 42 sobre el diseño de las centrales nucleares de la IAEA [18]. Del diseño en adelante, el análisis de seguridad se ha de actualizar periódicamente para incluir datos de experiencia operativa, cambios en el diseño, mejoras en el conocimiento sobre seguridad, mejoras en la propia aplicación de los análisis de seguridad, y otros. El análisis de seguridad se ha de aplicar durante todo el ciclo de

vida de la central, y ha de cumplir con requisitos de actualización [20], algunos de ellos mencionados anteriormente, para que siempre represente la central en la forma tal y como está construida.

El análisis de seguridad hace uso de dos métodos complementarios en la verificación de la seguridad de la planta: el método determinista, y el método probabilista, que es objeto de análisis de esta tesis doctoral. A continuación se detallan las principales características de cada uno de los métodos.

1.6.1. Método determinista

El método determinista se caracteriza por la evaluación de situaciones, condiciones, y eventos, previamente postulados, que engloban un rango de posibles sucesos iniciadores[4] con potencial para desafiar la seguridad de la planta. En el desarrollo de análisis deterministas se aplican hipótesis conservadoras para demostrar que la respuesta de la planta y de sus sistemas de seguridad a los eventos postulados está de acuerdo con los objetivos de seguridad. El análisis determinista de seguridad se utiliza principalmente para realizar las siguientes tareas [18, 10]:

- Establecer y confirmar las bases de diseño de todos las estructuras, sistemas, y componentes importantes para la seguridad. Definir los parámetros de diseño de los sistemas para la seguridad.
- Caracterizar los sucesos iniciadores postulados según el emplazamiento y el diseño de la planta.
- Analizar y evaluar las secuencias de eventos resultado de los sucesos iniciadores postulados para confirmar la idoneidad y el cumplimiento de requisitos de seguridad.
- Comparar de los resultados del análisis con los límites de dosis, límites aceptables, y límites de diseño.
- Demostrar que la gestión de sucesos operacionales previstos y accidentes base de diseño es posible mediante la actuación automática de sistemas para la seguridad combinada con acciones humanas procedimentadas.
- Demostrar que la gestión de condiciones que van más allá del diseño es posible mediante la actuación automática de sistemas para la seguridad en combinación con acciones humanas esperadas y/o de recuperación.

1.6.2. Método probabilista

El principal rasgo que define al método probabilista es la inclusión en el modelo de análisis de seguridad de la frecuencia de los sucesos iniciadores, y la inclusión de la probabilidad de fallo o indisponibilidad de todos los sistemas, componentes, y estructuras que participan, o cuya participación puede ser demandada, en la respuesta de la planta a un suceso iniciador. El análisis probabilista de seguridad, resultado de la aplicación del método probabilista, proporciona una valoración del riesgo global de la instalación, entendido como la combinación de la frecuencia de una consecuencia no deseada y la propia consecuencia, así como la identificación de todas las secuencias accidentales que pueden llevar a la consecuencia no deseada (véase el capítulo 2 para más detalle). Por contra, en el análisis determinista, la secuencia accidental analizada está definida previamente, y los resultados que se proporcionan están en términos de variables como la temperatura y la presión. El análisis probabilista de seguridad se utiliza principalmente para llevar a cabo las siguientes tareas [18, 10]:

[4] Un suceso iniciador es un evento que podría acabar en daño al núcleo del reactor directamente, o que desafía la operación normal, de tal forma que ha de ser mitigado exitosamente mediante sistemas relacionados con la seguridad para evitar que se dañe el núcleo del reactor [21]

- Identificar vulnerabilidades en el diseño y en las prácticas operacionales. Demostrar que se ha conseguido un diseño equilibrado de tal manera que ningún suceso iniciador contribuya de manera desproporcionada al riesgo global de la central.
- Demostrar que los niveles de defensa en profundidad son tan independientes como sea posible.
- Demostrar que se evitan aquellas pequeñas desviaciones de parámetros de planta que pudiesen dar lugar a grandes variaciones de las condiciones de planta.
- Comparar los resultados del análisis con criterios de aceptación para el riesgo allá donde estos estén definidos. Dar soporte a la toma de decisiones (véase el capítulo 3 para más detalle).
- Analizar hallazgos o transitorios de planta, y justificar modificaciones de diseño, mediante el análisis del incremento del riesgo asociado. Evaluación del incremento del riesgo en un marco regulador [22] (véase el capítulo 3 para más detalle).

1.7. Evolución histórica de la seguridad nuclear aplicada a centrales nucleares

La seguridad de las centrales nucleares y los estándares y normas asociados a ella han evolucionado considerablemente desde el diseño de las primeras centrales en los años 50 [23]. La industria nuclear ha llevado a cabo un excepcional proceso de maduración en el que la mejora de la seguridad nuclear ha sido una de sus características más importantes. El incremento de la seguridad de las centrales nucleares y de los niveles y objetivos ligados a ella responde a las siguientes causas [19]:

- Asimilación de las lecciones aprendidas de la experiencia (experiencia operativa, experiencia en el diseño, cuasi incidentes, accidentes, e identificación de posibles secuencias accidentales no consideradas con anterioridad, entre otros).
- Investigación y desarrollo de la ingeniería asociada aplicada a la consecución del objetivo de seguridad en las centrales nucleares.
- Adaptación al aumento de escala (es decir, potencia generada) de las centrales nucleares.

El incremento de los niveles y objetivos de seguridad ha afectado tanto a los nuevos diseños de reactor desarrollados a lo largo del proceso de maduración de la industria nuclear como a las centrales ya construidas y en operación puesto que la mayoría de las centrales nucleares existentes fueron diseñadas para operar durante un periodo de 30 a 40 años. En consecuencia, ha sido inevitable que los estándares y normas de seguridad y la ingeniería aplicada en el diseño de las centrales existentes se hayan visto superados por el propio desarrollo de la industria. La mayoría de licenciatarios de estas centrales nucleares en operación han sido requeridos a aplicar mejoras de seguridad para aumentar el nivel de seguridad del diseño original y equipararlo con los estándares y objetivos vigentes en todo momento. Valga como ejemplo el estudio y aplicación de medidas post-Fukushima requerido por el Consejo de Seguridad Nuclear (CSN) a las centrales españolas, así como por otros organismos reguladores a las centrales bajo su supervisión.

Se presenta a continuación un repaso de la evolución histórica de la seguridad nuclear en el que se destacan aquellos hitos, desarrollos, y lecciones aprendidas que han supuesto un avance considerable de los estándares y objetivos de la seguridad nuclear. La figura O.1 en el anexo O resume la información proporcionada en esta sección, situando los hitos más importantes al respecto de la seguridad nuclear en un eje temporal y enfrentándolos al desarrollo de la industria nuclear, que se representa mediante la potencia instalada (MW), la cantidad de reactores en operación, y la generación de reactores.

1.7.1. La seguridad en los inicios de la industria nuclear

La posibilidad de que el uso pacifico y beneficioso de las aplicaciones de la energía nuclear pudiese estar asociado a peligros inusuales fue reconocida en la etapa inicial de la investigación y desarrollo de estas aplicaciones. En consecuencia, los futuros desarrolladores de centrales nucleares se comprometieron, incluso antes de que se pusiese la primera piedra de la primera central, a marcarse como objetivo primordial el conseguir niveles excepcionalmente altos de seguridad [19]. Como resultado, poco después de la segunda guerra mundial, la United States Atomic Energy Commission (USAEC), antecesora de la Nuclear Regulatory Commission (NRC) actual, formó el Advisory Committee on Reactor Safeguards para analizar la seguridad de los reactores nucleares que existían en aquel momento. Este comité, aún en funcionamiento, y que está formado por expertos en seguridad no vinculados al desarrollo de centrales nucleares, ha revisado la seguridad de todas las centrales nucleares comerciales de los Estados Unidos. En 1952, en Estados Unidos, se llegó a la conclusión que la probabilidad de accidente en una central nuclear era distinta a 0, y que, por lo tanto, se debía incluir en las centrales nucleares sistemas de protección especial contra las consecuencias de accidentes severos. Concretamente, las conclusiones respecto a las consecuencias de un accidente severo en un reactor sin contención fueron similares a las que se extraerían del accidente de Chernobyl en 1986 [19]. A raíz de la conclusión del estudio del 1952, el Advisory Committee on Reactor Safeguards introdujo el siguiente requisito [19]:

> Las centrales nucleares se han de alojar en edificios robustos y estancos que han de servir como barrera de protección última ante el escape de material radioactivo de la central en el caso de que ocurra un accidente a pesar de todas las precauciones tomadas.

Este requisito fue rápidamente adoptado por la mayoría de desarrolladores de centrales de agua ligera y agua pesada del mundo. Sin embargo, los primeros reactores de agua ligera de la URSS y de países de la Europa del Este contaban únicamente con edificios de contención parciales. Los nuevos reactores de agua ligera de Europa del Este se siguieron construyendo con edificios de contención parcial hasta mediados de los años 70. La decisión de requerir un sistema de contención se ha convertido en un pilar fundamental de la estrategia para el cumplimiento del objetivo de seguridad de reactores de agua ligera y pesada. Concretamente, se considera el primer paso del desarrollo de la estrategia de defensa en profundidad, en la que el edificio de contención es la última barrera contra la liberación de productos de fisión.

Una de las prácticas habituales en el diseño de sistemas de seguridad de una central nuclear es el análisis de accidentes base de diseño (ABD) , definidos como aquellos transitorios accidentales a los que la central debería hacer frente sin que se generase ningún tipo de consecuencias negativas para las personas o el medio ambiente. La primera aplicación del diseño de sistemas desde el punto de vista de la seguridad a partir de análisis de transitorios se remonta también a la primera etapa del desarrollo de centrales nucleares. En concreto, el transitorio que era motivo de preocupación en los primeros pasos del desarrollo de las centrales nucleares era la excursión de potencia[5]. La investigación en los años 50 y principios de los 60 al respecto de este transitorio llevó al descubrimiento de formas de diseñar el núcleo de reactor que ayudaban a evitar este tipo de accidentes [19].

1.7.2. Evolución hacia la segunda generación de centrales nucleares

El desarrollo de métodos para convertir a las centrales nucleares en instalaciones más seguras se enfocó tanto en la comprensión del modo de fallo de los sistemas presentes en la central, como en el desarrollo de métodos para evitar las consecuencias del fallo [19]. Se pasó de conceptos de seguridad simples, como, por ejemplo, la construcción de un edificio de contención, a la aplicación de metodologías complejas como la estrategia de defensa en profundidad, que propició la introducción del diseño de sistemas para la seguridad

[5] Crecimiento incontrolado de la potencia del reactor que llevaría a una pronta fusión del núcleo y a la creación de grandes cantidades de hidrógeno.

mediante el análisis de sucesos extremos. Por otra parte, el proceso de desarrollo e implantación de una seguridad más avanzada en las centrales tuvo que lidiar con la rápida evolución en tamaño y complejidad de los reactores comerciales.

La adopción de una barrera definitiva, un edificio robusto y estanco, para evitar la liberación de material radioactivo en caso de accidente supuso el primer paso en el desarrollo de la estrategia de defensa en profundidad que se comenzó a aplicar en las centrales nucleares de la segunda generación. La defensa en profundidad, véase sección 1.5 para más detalle, consiste en la implementación de diversas barreras de protección sucesivas, y de medios para asegurar la integridad de estas barreras. Las diferentes barreras y sistemas de protección de las barreras han de estar concebidos de tal manera que si una barrera fallase, otras continuarían ejecutando su labor de protección. Además, en caso de que no se pueda evitar el accidente, la estrategia de defensa en profundidad incluye medidas para evitar consecuencias negativas en la medida de lo posible.

Las autoridades de seguridad de aquella etapa asumían que la protección contra los accidentes más extremos de cualquier tipo también protegería contra accidentes del mismo tipo de menor calado. Por lo tanto, se añadieron sistemas diseñados para la seguridad (engineered safety features) con el objetivo de proteger las centrales en caso darse accidentes extremos. A los accidentes extremos se les pasó a llamar accidentes base de diseño porque se utilizaban para definir las características límite del diseño de sistemas. El uso de sistemas diseñados para la seguridad en la aplicación de la estrategia de defensa en profundidad fue utilizado en el diseño de la mayoría de reactores de segunda generación y se convirtió en uno de los medios principales de protección de centrales nucleares ante cualquier tipo de accidente.

El desarrollo de la estrategia de defensa en profundidad y de los sistemas diseñados para la seguridad no hubiese sido posible sin la mejora del entendimiento de las bases técnicas aplicadas en el cumplimiento del objetivo de la seguridad nuclear. Los principales contribuyentes al desarrollo del entendimiento de las bases técnicas de la seguridad fueron programas de investigación enfocados a los aspectos ingenieriles de la seguridad y la experiencia adquirida con los reactores de la primera generación.

1.7.3. Aparición del Análisis Probabilista de Seguridad

En 1975 la NRC publicó el estudio Reactor Safety Study: An Assessment of Accident Risks in US Commercial Nuclear Power Plants [24], que se considera el primer análisis de riesgo aplicado a centrales nucleares comerciales americanas. El estudio WASH-1400 utilizó por primera vez una técnica probabilista, herencia de la industria aeroespacial, para la estimación simultánea de las probabilidades y las consecuencias de los accidentes más allá de las bases de diseño. A esta técnica se la acabó llamando Análisis Probabilista de Seguridad (véase sección 1.6 para más detalle). El APS traza las posibles secuencias de accidente que originaría un suceso iniciador accidental. Estas secuencias incluyen el fallo de los sistemas diseñados para la seguridad, estimando la probabilidad de fallo en cada etapa de la secuencia y combinando las probabilidades de fallo individual de cada etapa de la secuencia en la probabilidad total de que la secuencia en cuestión pueda ocurrir. El APS permite identificar dependencias entre sistemas, como por ejemplo la dependencia de varios sistemas de seguridad diferentes con sistemas soporte comunes. En el estudio WASH-1400, por ejemplo, se identificó la dependencia de varios sistemas de las centrales estudiadas con sistemas de alimentación comunes y con sistemas de refrigeración comunes. Se concluyó mediante el WASH-1400 que los accidentes más allá de las bases de diseño no eran tan improbables como se creía pero que, por contra, sus consecuencias serían mucho menos dañinas de lo que se había pensado.

El principal hándicap del APS ha sido y es la precisión de los resultados, que siempre van asociados a una banda de incertidumbre. A pesar de ello, la aplicación del APS ha permitido identificar y evaluar nuevas características de seguridad de las centrales y ha sido y es de gran valor en el diseño de sistemas de seguridad y de prácticas relacionadas con la seguridad. Tal y como se describe en la sección 2.2, la metodología APS ha evolucionado notablemente desde su primera aplicación en 1975, hasta el punto que la NRC adoptó la siguiente política en 1995 [22]:

El uso del APS debería verse incrementado en el marco regulador, hasta el punto que el estado del arte lo permita, de tal forma que complemente el acercamiento determinista y de soporte a la filosofía tradicional de defensa en profundidad.

El APS y análisis asociados deberían utilizarse en el marco regulador, siempre que sea práctico, para reducir innecesarios conservadurismos asociados con requisitos regulador, RGs, licenciamiento, etc, actuales. El APS debería utilizarse para dar soporte a la propuesta de requisitos reguladores adicionales en concordancia con el 10 CFR 50.109.

1.7.4. El accidente de Browns Ferry

El 22 de marzo de 1975 se declaró un extenso incendio en la central nuclear estadounidense de Browns Ferry que puso en jaque la integridad del reactor nuclear. El incendio fue causado por el uso de una vela para la identificación de fugas en las penetraciones de la sala de cables que se encontraba bajo la sala de control. El operario acercó demasiado la vela que sostenía a la gomaespuma que estaba utilizando para sellar las fugas y ésta empezó a arder. El uso de la llama de una vela para identificar fugas en sellos era práctica habitual en las centrales de carbón en aquel tiempo. El incendio resultante inutilizó varios de los sistemas de seguridad de la central, incluyendo el sistema de refrigeración de emergencia del reactor, poniendo en jaque la progresión a parada segura de la central.

Las lecciones aprendidas del incendio de Browns Ferry llevaron a la concepción de las siguientes mejoras en materia de seguridad:

- Mejora de los sistemas de prevención contra incendios de las centrales nucleares. Adaptación a la complejidad de una central nuclear [19].
- Percepción de la separación física y de la redundancia entre equipos y sistemas, específicamente en cuanto a cableado eléctrico, como dos rasgos altamente importantes de la defensa en profundidad.

Adicionalmente, el accidente de Browns Ferry espoleó a la NRC en el desarrollo e incorporación del análisis de riesgo en su programa de seguridad nuclear.

1.7.5. El accidente de Three Mile Island

El 28 de marzo de 1979 la unidad 2 de la central nuclear de Three Mile Island (TMI-II) experimentó un suceso de pérdida de refrigerante de pequeño caudal del sistema primario (los llamados SBLOCA) que progresó de tal manera que acabó causando la fusión de un 30 a 40 % del núcleo del reactor [25]. A pesar de la gravedad del suceso, las consecuencias para las personas y el medio ambiente fueron despreciables gracias, en gran parte, al edificio de contención. El transitorio se originó en la pérdida del sistema de agua de alimentación principal y la posterior señal de apertura de las válvulas de alivio del primario. Una vez se produjo el SCRAM y descendió la presión del primario, el origen del suceso SBLOCA se dio al fallar inadvertidamente al cierre la válvula de alivio del primario tras señal de cierre de la misma. Además, el sistema de agua de alimentación auxiliar, que había sido requerido tras la pérdida del sistema de agua de alimentación principal, no entró en funcionamiento porque sus válvulas estaban manualmente cerradas producto de un fallo humano en un mantenimiento anterior. Sin embargo, la principal causa de la progresión del accidente hasta la fusión del núcleo fue el fallo del personal de sala de control a diagnosticar la situación en la que se encontraba el reactor. Pese a las diferentes señales que podían sugerir la existencia de un SBLOCA, como, por ejemplo, la señal de alta temperatura en la línea de alivio del presionador, o la puesta en funcionamiento de la inyección de seguridad, los operarios de sala de control no diagnosticaron la existencia del SBLOCA hasta transcurridos 142 minutos desde el inicio del transitorio. El descubrimiento del núcleo y la oxidación de las vainas de combustible comenzó 100 minutos después del inicio del transitorio[25]. Aunque la principal causa de la progresión del accidente fue el fallo

a diagnosticar el propio accidente, otras causas que facilitaron su progresión estuvieron relacionadas con el mantenimiento (el cierre manual de las válvulas del sistema de alimentación auxiliar es un ejemplo), la mecánica, la operación, y el diseño.

El accidente de Three Mile Island confirmó las conclusiones extraídas del estudio WASH-1400 en cuanto a que la probabilidad de accidentes severos más allá de las bases de diseño era más elevada de lo que se creía hasta el momento. El accidente puso de manifiesto la importancia del fallo humano, y que combinaciones de pequeños fallos y errores podían llevar al reactor a situaciones no deseadas. Además, el accidente puso el foco sobre la preparación ante emergencias de las centrales nucleares. Las lecciones aprendidas del accidente de TMI-II que dieron lugar a mejoras en el campo de la seguridad fueron las siguientes:

- El accidente de TMI-II reforzó el valor del APS como herramienta para revelar deficiencias y vulnerabilidades en el cumplimiento del objetivo de seguridad. El tipo de accidente acaecido, SBLOCA, había sido identificado como uno de los más probables en el WASH-1400. La confirmación de las conclusiones del estudio WASH-1400 supuso el empujón definitivo para la aplicación del APS en los análisis de seguridad de centrales nucleares.
- El factor humano no estaba adecuadamente incluido en los principios y análisis de seguridad. Se incorporó el análisis de fiabilidad humana en los análisis de seguridad y se cambió la concepción del diseño y las practicas operativas en algunos aspectos de las centrales para tener en cuenta el factor humano.
- Falta de preparación ante emergencias. A raíz de TMI-II se reforzó la preparación ante emergencias de los equipos de operación de las centrales y, más importante, se rediseñaron los procedimientos de operación en emergencia para que estuvieran basados en síntomas. Hasta TMI-II los procedimientos de emergencia se basaban en la capacidad de diagnosis de los operarios de sala de control.
- Optimización de las señales disponibles en sala de control. Se llegó a la conclusión de que en sala de control deberían existir señales de apertura (encendido) y cierre (apagado) de equipos, a parte de las señales de orden de apertura (encendido) y orden de cierre (apagado).
- El descubrimiento de que sucesos tipo LOCA podían ocurrir en realidad llevó al desarrollo de modelos deterministas Best Estimate para el análisis de este tipo de transitorios así como al diseño de experimentos para mejorar el entendimiento sobre este tipo de fenómenos.
- La importancia de implementar un análisis efectivo de la experiencia operativa para identificar y eliminar posibles debilidades en la aplicación de la defensa en profundidad.

1.7.6. El accidente de Chernobyl

El 26 de abril de 1986 la unidad 4 de la central nuclear de Chernobyl de diseño ruso RBMK sufrió un devastador accidente de excursión de potencia durante la realización de un experimento. El accidente provocó la liberación al medio ambiente de grandes cantidades de material radioactivo. El objetivo del experimento era demostrar que la potencia residual del rotor de inercia de la turbina se podía considerar como una fuente de alimentación auxiliar para las bombas del RCS (Reactor Coolant System) hasta el arranque de los generadores diésel en caso de disparo de turbina. El desarrollo del experimento incluía la toma de decisiones en contra de la seguridad, como, por ejemplo, la desactivación del sistema de emergencia de refrigeración del reactor, o la desactivación de las señales de bajo nivel, y de presión. Problemas durante el transitorio del experimento llevaron a los operarios a tomar más acciones en contra de la seguridad, como la vulneración del margen de reactividad en operación[6] para poder continuar con el experimento. El cúmulo de acciones en contra de la seguridad dejó al reactor en un estado inestable

[6] Margen de reactividad en operación: la cantidad de barras de control que permanecen en el núcleo del reactor. Si la cantidad era menor que 15 se producía el SCRAM [REF WEB NEA].

y difícilmente gobernable en caso de perturbación positiva de la criticidad, hecho que acabó ocurriendo. Se produjeron dos explosiones a causa de la excursión de potencia. La primera, una explosión de vapor derivada de la desintegración del combustible y la rotura masiva de los ensamblajes de combustible, causó el desplazamiento del bloque de hormigón que rodeaba el reactor. La segunda, una explosión de hidrógeno causada por la oxidación del zircalloy y la entrada de aire, provocó un incendio e hizo volar parte del edificio del reactor, dejando parte del núcleo a la intemperie [26] pues los reactores RBMK no contaban con edificios de contención. Las consecuencias radiológicas del accidente fueron nefastas. Alrededor de 50 personas murieron y 134 personas sufrieron problemas de salud severos por causas radiológicas, aunque ninguno de ellos era miembro del público. No obstante, los efectos en la salud del gran público se hicieron notar en un aumento sustancial de casos de cáncer de tiroides [26]. Cabe destacar que unos cinco millones de personas de zonas ligeramente contaminadas recibieron una dosis media de 10 a 20 mSv[7] [26].

El accidente de Chernobyl no supuso una gran revelación en cuanto a técnicas o sistemas de seguridad se refiere. El accidente puso de manifiesto que la seguridad es mucho mayor cuando los reactores se alojan en edificios robustos y estancos capaces de retener productos de fisión en su interior. Si el diseño RBMK hubiese tenido un edificio de contención, las consecuencias del accidente podrían haber sido similares a las del accidente de TMI-II [19]. Se demostró también que diseñar el núcleo del reactor con enfoque a evitar accidentes de pérdida de control de la reacción en cadena es esencial. No obstante, la industria occidental ya había llegado a estas dos importantes conclusiones en la primera etapa del desarrollo de centrales nucleares (véase sección 1.7.1). Sin embargo, el accidente desveló que los requisitos de seguridad para centrales nucleares no habían sido definidos de forma consistente entre diferentes diseños y entre algunos países. Este hecho, sumado a que las consecuencias radiológicas de Chernobyl afectaron a todo el mundo, hizo aumentar la percepción de que la cooperación internacional entre países, organismos, y operadores era necesaria para, entre otras cosas, mejorar la seguridad de las centrales nucleares. Una de las grandes consecuencias del accidente de Chernobyl fue la creación de organismos internacionales, como, por ejemplo, WANO (World Association of Nuclear Operators), para la cooperación y para el intercambio de experiencias, prácticas, problemas, soluciones, requisitos, y otros.

Más allá de las deficiencias de diseño de los reactores RBMK, la característica que define al accidente de Chernobyl fue la toma de decisiones, y la aceptación de las mismas, por parte de los operadores del reactor. Ya sea por desconocimiento o por presión externa, con sus acciones, los operadores pusieron en jaque la seguridad de la planta. Este hecho fue visto como una gran deficiencia de la cultura organizativa de la central pues, los operadores, o bien desconocían su papel en la seguridad de la planta o bien priorizaron otros aspectos en lugar de la seguridad. En la primera reunión del International Nuclear Safety Group [27], en agosto de 1986, se definió como falta de cultura de seguridad el hecho de que los operadores actuasen contra la seguridad. La introducción de este nuevo concepto, sobre el cual se obtuvo consenso en 1991 en la reunión INSAG-4 [17], y la importancia que se le dio y se le da hoy en día en el mantenimiento de un alto nivel de seguridad, es otra de las grandes consecuencias del accidente de Chernobyl.

1.7.7. Características de seguridad de las nuevas generaciones de reactores

Las centrales nucleares en operación en la actualidad pertenecen a la primera o segunda generación de reactores debido al largo ciclo de vida, de 30 a 60 años, en caso de extensión, de las centrales nucleares. Sin embargo, muchas de ellas , las construidas entre finales de los sesenta y finales de los ochenta, han llegado o están llegando al final de su vida operativa. En consecuencia, la mayoría de países en posesión de centrales nucleares tendrán que replantearse su programa nuclear en los años venideros, y decidir si continúan apostando por la energía nuclear como fuente de producción de energía eléctrica. En caso afirmativo, una de las opciones es proceder a la construcción de reactores de generación tres o generación tres plus, como, por ejemplo, los diseños EPR® de la francesa AREVA® o AP1000® de la americana Westinghouse®. Ambos diseños de reactor entraron en fase de aprobación del diseño por parte de la NRC

[7] El límite de dosis anual para una persona del público general es de 1 mSv.

a mediados de la década del 2000. De hecho, ocho reactores de diseño AP1000 y cuatro de diseño EPR están actualmente en fase de construcción.

Los diseños de nuevos conceptos de reactor han incorporado características y medidas de seguridad acordes con la evolución de la seguridad nuclear. En el diseño e incorporación de estas características se han tenido en cuenta, en su mayoría, las lecciones aprendidas de la experiencia con reactores de generación dos, y las lecciones aprendidas derivadas de situaciones accidentales. Específicamente, destaca la incorporación de medidas de seguridad para dar respuesta a todas aquellas lecciones aprendidas de la experiencia operativa que no han podido ser aplicadas en centrales de generación dos por incompatibilidad con la concepción y diseño originales. Algunas de las características de seguridad incluidas en el diseño de los reactores de generación tres y tres plus son:

- Equilibro adecuado entre elementos de seguridad activa y elementos de seguridad pasiva. Se han incrementado los sistemas y elementos de seguridad pasiva.
- Implementación de sistemas de seguridad de actuación automática que no necesitan de la actuación de operadores en los instantes posteriores a una desviación de la operación normal: Reducción del factor humano. En el caso del diseño AP1000, la planta puede hacer frente durante 72 horas a una pérdida de refrigeración del núcleo sin que actúe ningún operador.
- Diseño de sistemas para que sean intrínsecamente seguros.
- Reducción de la complejidad de los sistemas. En el caso del AP1000, se han reducido los metros de tubería del sistema de refrigeración del reactor conectando las bombas del sistema directamente a los generadores de vapor.
- Aplicación de los conceptos de redundancia y separación física. El EPR, por ejemplo, cuenta con cuatro sistemas de refrigeración de emergencia del núcleo independientes.
- Introducción de sistemas y/o elementos para hacer frente a la fusión del núcleo. Por ejemplo, recombinadores de hidrógeno o el sistema de captura del núcleo del diseño EPR.
- Frecuencias de daño al núcleo del orden de magnitud de 10^{-7}[28, 29].

1.7.8. El accidente de Fukushima Dai-Ichi

El 11 de marzo de 2011 la central nuclear de Fukushima Dai-Ichi, de seis unidades tipo BWR, de las cuales cinco tienen contención MARK-I y una tiene contención MARK-II, padeció los efectos de un terremoto de magnitud 9.0 y fue golpeada posteriormente por un tsunami cuyas olas superaron los 12 metros de altura. Como resultado, se perdió la capacidad de refrigerar cuatro de los seis reactores, y sus respectivas piscinas de combustible. Los reactores de las unidades 1, 2, y 3 se degradaron severamente, causando una sustancial liberación de productos radioactivos e hidrógeno (el reactor de la unidad 4 estaba en parada y, por lo tanto, los elementos de combustible se encontraban en la piscina de combustible y no en el reactor). Se produjeron explosiones de hidrógeno que causaron el grave deterioro de los edificios de reactor de las unidades 1, 3 y 4, contribuyendo así a una mayor liberación de productos radioactivos al medio ambiente. La pérdida de la capacidad de refrigerar las unidades 1, 2, y 3 fue causada por la pérdida total de alimentación de energía eléctrica. Los generadores diésel de emergencia[8], situados en el subsuelo, se inundaron por efecto del tsunami, y las baterías de corriente continua[9] dejaron de funcionar pasado un tiempo, con lo cual se perdió toda capacidad de refrigeración de emergencia. Debido a la escasa

[8] Los generadores diésel de emergencia son la única fuente de energía eléctrica de corriente alterna en caso de perderse el suministro exterior, como ocurrió a consecuencia del terremoto.

[9] Las centrales nucleares disponen de baterías de corriente continua para alimentar a equipos que requieran este tipo de energía en caso de pérdida del suministro exterior de corriente alterna y/o indisponibilidad de los equipos inversores que transforman la corriente alterna en corriente continua.

preparación ante situaciones de tal magnitud, es decir, la zona devastada por tsunami, la ocurrencia de un suceso de pérdida total de alimentación de corriente alterna (suceso comúnmente conocido como Station Black-Out (SBO), y la existencia de reactores sin ningún tipo de refrigeración, los operadores no fueron capaces de llevar los reactores a una situación segura. No obstante, se estima que la cantidad de material radioactivo liberado en forma de emisiones es 1/10 de lo que se liberó en Chernobyl [30], gracias al control temporal de la liberación. Además, gracias a los planes de contingencia y evacuación en emergencia, y a los estrictos controles radiológicos de los trabajadores, la liberación de material radioactivo no tuvo efectos directos sobre el público ni los propios trabajadores.

Han pasado ya más de cinco años desde el accidente de Fukushima y aún se siguen extrayendo lecciones de lo ocurrido, aunque principalmente en el campo de la gestión y mitigación de las consecuencias de un accidente severo. Respecto a la fenomenología del accidente, y aunque este ha vuelto a poner el foco en temas ya considerados de gran importancia como la cultura de seguridad, la mejora continua de la seguridad, la prevención de fallos de causa común, el beneficio de tener un edificio de contención de gran volumen, y el uso del APS, la conclusión más importante que se ha extraído del accidente de Fukushima es que la central no estaba preparada ni técnicamente ni organizativamente para hacer frente al accidente severo. En respuesta a Fukushima, gran parte de los organismos reguladores ha decidido someter a las plantas bajo su regulación a los denominados Stress Test [31], pruebas y estudios para evaluar hasta qué punto serían las centrales capaces de aguantar accidentes similares al de Fukushima. Además, se ha acuñado el término Design Extension Conditions (DEC), que hace referencia la consideración de una serie de accidentes más allá de las bases de diseño, incluyendo accidentes severos, en el proceso de diseño de una central con el objetivo de mantener la liberación de material radiactivo dentro de unos limites aceptables. Como resultado de los Stress Test y de las Design Extension Conditions, se han implantado mejoras en el quinto nivel de la defensa en profundidad para hacer frente y para gestionar accidentes severos. Algunas de estas medidas son: la mejora de las guías de accidente severo, la instalación de recombinadores de hidrógeno pasivos en la contención, la instalación sistemas de venteo filtrado del edificio de contención, la creación de centros de emergencia, ligados a las centrales, con equipos portátiles y utillaje suficiente para hacer frente a un accidente severo, y la creación de centros de emergencia generales, centralizados, para hacer frente a una emergencia en cualquiera de las centrales bajo su amparo.

1.8. Conclusiones

Ya desde los inicios de la industria nuclear en los años 50, la seguridad de instalaciones y/o actividades relacionadas ha sido, y es, considerada uno de los rasgos de relevancia capital de la industria. La llamada seguridad nuclear siempre ha sido considerada de vital importancia debido a las nefastas y, hasta cierto punto, desconocidas, consecuencias para las personas y el medio ambiente que tendría la liberación masiva de material radioactivo. Uno de los objetivos primordiales de la industria nuclear a lo largo de su historia ha sido, y es, el de lograr excelentes niveles de seguridad en sus instalaciones. Pese al consenso sobre su relevancia, la estrategia y estándares de seguridad en instalaciones nucleares no han sido aplicados de forma consensuada en todas partes del mundo en todo momento. Sirva como ejemplo el caso de los primeros reactores de Rusia y Europa del Este, que no tuvieron edificios de contención total hasta mediados de los años 70. Hizo falta un accidente como el de Chernobyl, para poner de manifiesto que la diversidad de reglas y estándares para la seguridad, bajo ningún tipo de control por parte de organizaciones internacionales dedicadas a velar por la seguridad, suponía una gran debilidad de la industria nuclear. Una de las principales conclusiones que se extrajo del accidente fue la necesidad de cooperar internacionalmente en pos de la armonización en materia seguridad. A posteriori del accidente, se crearon diversos organismos internacionales como WENRA o WANO para el intercambio de experiencias y prácticas, y se instó a los organismos reguladores a participar en reuniones y convenciones de cariz internacional. Hoy en día, la industria nuclear goza de de un marco internacional de intercambio de información e ideas sin comparación posible en el panorama industrial actual, y que proporciona un alto grado de armonía en la aplicación de la seguridad en las instalaciones.

La evolución de la seguridad nuclear a lo largo del desarrollo de la industria nuclear va más allá de la armonización de sus estándares. Paralelamente a la industria, la seguridad nuclear ha experimentado un notable proceso de maduración en el que ha pasado de tener como objetivo la mitigación de las consecuencias en caso de accidente, a tener como objetivo la prevención de accidentes y, en caso de que ésta falle, la prevención y mitigación de las consecuencias de un accidente. En conjunción con la evolución de su objetivo, la seguridad nuclear ha pasado de aplicarse mediante conceptos simples como la construcción de un edificio de contención, a la aplicación de metodologías y filosofías complejas como la defensa en profundidad. Los principales causantes de la evolución de la seguridad nuclear han sido la investigación y desarrollo de la ingeniería asociada a la aplicación de la seguridad, incluyendo aquí la investigación y desarrollo del análisis probabilista de seguridad, y la asimilación y retroalimentación de las lecciones aprendidas de la experiencia operativa, cuasi incidentes, accidentes, y eventos de índole similar. En el presente, la aplicación de la seguridad nuclear se basa en tres pilares fundamentales: la existencia de un marco legislativo y regulador que define con claridad las responsabilidades de todos los participantes, y las filosofías de defensa en profundidad y cultura de seguridad.

En la historia de la industria nuclear han ocurrido tres accidentes con fusión del núcleo, Three Mile Island, Chernobyl, y Fukushima, y varios cuasi incidentes, es decir, sucesos en los que la fusión del núcleo ha estado cerca de ocurrir, a pesar de la atención y los recursos dedicados a la maduración y mejora de la seguridad nuclear. La asimilación de las lecciones aprendidas de estos accidentes ha sido uno de los factores clave en la evolución y mejora de la seguridad en centrales nucleares. No obstante, la ocurrencia de estos accidentes pone de manifiesto que la mejora de la seguridad nuclear se enfrenta a una barrera que no puede ser superada: la probabilidad de accidente nunca será igual a 0. Este límite afecta a la vertiente de la seguridad que se encarga de la prevención de los accidentes, que, históricamente, ha sido la vertiente a la que más recursos se le han dedicado porque también afecta a la productividad de la central.

El accidente de Chernobyl supuso un gran revés para la industria, siendo la causa del parón o desaceleración de la mayoría de programas nucleares activos en aquel momento. De manera similar, el accidente de Fukushima supuso el final del llamado «renacimiento nuclear», causando la cancelación o el replanteamiento de la mayoría de reactores en fases previas a la construcción, y el final del programa nuclear alemán. Siguiendo esta tendencia, es probable que, de darse un accidente similar en el futuro próximo, éste supusiera un obstáculo prácticamente insalvable para la industria nuclear de producción de energía eléctrica. La industria estará siempre expuesta a la ocurrencia futura de accidentes de consecuencias similares porque el ser humano es incapaz de predecir, y defenderse ante, todas las posibles secuencias accidentales. Por lo tanto, y sin que esto suponga el abandono de la prevención de accidentes, es menester que la industria nuclear centre recursos y esfuerzos en la mejora de la prevención y mitigación de las posibles consecuencias negativas de un accidente severo. Las lecciones aprendidas del accidente de Fukushima y nuevas características de diseño de los reactores de tercera generación, como el sistema de captura del núcleo del diseño EPR,indican que ya se trabaja activamente en esta dirección. La supervivencia de la industria nuclear en el futuro próximo está íntimamente ligada a la capacidad de la seguridad nuclear para evitar catástrofes como las de Chernobyl o Fukushima, además de a otros aspectos de cariz económico.

Capítulo 2

Análisis Probabilista de Seguridad

2.1. Introducción

El capítulo 2 presenta la metodología de análisis probabilista de seguridad, que es la metodología de referencia utilizada en el desarrollo de los estudios que forman del contenido de esta tesis doctoral. El objetivo de este capítulo es describir la metodología APS de tal manera que facilite el seguimiento y la comprensión de las siguientes partes de la tesis, así como de cualquier documento que describa el desarrollo o uso de modelos APS.

En cumplimiento de este objetivo, el segundo capítulo de la tesis presenta una revisión del desarrollo histórico de la metodología APS en la sección 2.2, que culmina en la sección 2.3 con la definición de los objetivos y alcances diversos de un proyecto APS. Como punto más relevante del capítulo, la sección 2.4 contiene una descripción detallada de la metodología APS de nivel 1 de sucesos internos a potencia.

2.2. Antecedentes

2.2.1. El origen del Análisis Probabilista de Seguridad

El desarrollo de las primeras metodologías de análisis de riesgo y análisis de fiabilidad de equipos se remonta al programa aeroespacial americano de principios de los años sesenta [32]. De hecho, una de las metodologías desarrolladas en el marco del programa aeroespacial americano fue el análisis mediante árboles de fallo, que es uno de los pilares del análisis probabilista de seguridad. Sin embargo, finalmente la NASA (National Aeronautics and Space Administration) no consideró oportuno utilizar los métodos cuantitativos de análisis de riesgo y análisis de fiabilidad porque los primeros resultados obtenidos, en el marco del programa Apollo, fueron decepcionantes [32]. No fue hasta veinte años después, habiéndose desarrollado y aplicado ya las metodologías de análisis de riesgo de forma rigurosa, cuando la NASA decidió volver a realizar análisis cuantitativos de riesgo.

2.2.2. Los inicios del desarrollo del Análisis Probabilista de Seguridad en la industria nuclear

Fue la industria nuclear la que tomó el relevo en el desarrollo y expansión de las metodologías de análisis de riesgo y análisis de fiabilidad creadas por la NASA, aunque en el marco de la realización de los análisis de seguridad. El primer análisis de seguridad llevado a cabo mediante técnicas probabilistas en

territorio estadounidense fue el estudio *WASH-1400: Reactor Safety Study*, publicado en 1975. El estudio WASH-1400, que fue patrocinado por el organismo regulador americano de la época (la AEC (Atomic Energy Commission)) y fue dirigido por el profesor Norman C. Rasmussen del *Massachusetts Institute of Technology* (MIT), tuvo como objetivo la estimación realista del riesgo para el público que supone la operación de una central nuclear [24]. El estudio comparó el riesgo para el público de cariz nuclear con el riesgo para el público asociado a otras actividades a las que la sociedad y los individuos ya estaban expuestos. La principal conclusión extraída del estudio fue que el riesgo para el público debido a una central nuclear era menor de lo que se creía y, sobre todo, comparativamente menor que el riesgo originado por otras actividades. Adicionalmente, se concluyó que la probabilidad de accidente de un reactor era menor que la de muchos otros accidentes con consecuencias similares, aunque mayor de lo que se pensaba [33]. El estudio WASH-1400 también concluyó que accidentes provocados por múltiples fallos de equipos eran más probables de lo que en un principio se creía.

La publicación del estudio WASH-1400 supuso, en Estados Unidos, un estímulo para el desarrollo del análisis cuantitativo de riesgo de centrales nucleares enfocado a la seguridad. Pese a que se destacaron sus ventajas, como la posibilidad de identificar debilidades del diseño y la operación de las centrales, se consideró que la metodología aún era inconsistente [34] y que se debían centrar recursos y esfuerzos en la investigación y desarrollo de algunas tareas como, por ejemplo:

- Estimación de la frecuencia de sucesos iniciadores.
- Métodos para coleccionar y utilizar datos operacionales de planta.
- Análisis de la fenomenología con el núcleo fundido.
- Metodologías para evaluar el impacto de errores humanos.
- Dependencias y fallos de causa común.
- Tratamiento de incertidumbres.

Estados Unidos no fue el único país que tuvo interés en desarrollar técnicas probabilistas para el análisis de seguridad de centrales nucleares durante los años setenta. En Europa, los organismos reguladores del Reino Unido y de Alemania también desarrollaron sus primeros análisis probabilistas de seguridad de centrales nucleares [35]. Sin embargo, estos análisis son posteriores a la fecha de publicación del estudio WASH-1400.

2.2.3. El desarrollo del APS en la industria nuclear americana a posteriori del accidente de Three Mile Island

El accidente de Three Mile Island - II en 1979 confirmó varias de las conclusiones extraídas en el estudio WASH-1400. Concretamente, el accidente demostró que las consecuencias de un accidente severo no eran tan importantes como se pensaba anteriormente, y que accidentes de pérdida de refrigerante tipo LOCA pequeño podían ocurrir[1]. La confirmación de estas conclusiones puso de manifiesto la utilidad que podían tener los análisis de riesgo hasta el punto que las investigaciones Kemeny[2] y Rogovin [33, 36, 37] recomendaron el uso del análisis probabilista de seguridad como complemento a los métodos tradicionales de evaluación de seguridad. En general, una de las lecciones aprendidas como consecuencia del accidente de TMI-II fue la de utilizar técnicas probabilistas para desarrollar análisis de seguridad complementarios a los obtenidos mediante métodos deterministas tradicionales.

[1] El LOCA pequeño era uno de los accidentes más probables según el estudio WASH. Se trata de una pérdida de refrigerante de el sistema primario de la central cuyo diámetro de fuga se considera pequeño.

[2] Se le dio el nombre de *Kemeny Commission* a la *President's Commission on the Accident at Three Mile Island* porque estuvo presidida por John G. Kemeny.

En los años 80, la tecnología para analizar los procesos físicos asociados a un accidente severo evolucionó rápidamente, culminando en el desarrollo de un nuevo modelo computacional de análisis [33]. Paralelamente, la NRC desarrolló y publicó en 1983 una guía que incluía un procedimiento general para llevar a cabo un análisis APS [38]. Esta guía abordaba y subsanaba, hasta cierto punto, algunas de las vulnerabilidades metodológicas identificadas en el WASH-1400. A causa de los avances en la materia, la NRC aprobó una nueva política de evaluación de los riesgos de un accidente severo. La mencionada política derivó, en 1988, en una demanda de información al respecto de vulnerabilidades ante un accidente severo a toda central nuclear licenciada en Estados Unidos. A esta solicitud de información se la llamó *Individual Plant Examination*, y la NRC estableció que se podía llevar a cabo mediante técnicas APS u otros medios. La mayoría de licenciatarios decidieron dar respuesta a la petición mediante la realización de modelos APS, dando lugar a la primera aplicación voluntaria del APS en la industria nuclear americana más allá de las realizadas por el organismo regulador. Adicionalmente, la NRC desarrolló su propio estudio de accidente severo mediante técnicas APS para tener más elementos de los que extraer conclusiones. El estudio fue llamado *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants* [33], publicado en 1990, y estimaba el riesgo de accidente severo para cinco centrales nucleares comerciales de Estados Unidos, siendo algunas de ellas las evaluadas en el WASH-1400. En la realización del estudio se emplearon las técnicas modernas de análisis de riesgo desarrolladas a partir del estudio WASH-1400 como, por ejemplo, el análisis cuantitativo de incertidumbres.

En 1994, la NRC decidió implementar un plan para incorporar elementos informados por el riesgo (*risk-informed*) y basados en las prestaciones (*performance-based*) en su marco regulador, a la vista del desarrollo y maduración de la metodología APS [22], y en respuesta a la ley «*Government Performamce and Results Act*» del congreso americano [39]. El principal objetivo del plan de implementación del APS en el marco regulador fue el de introducir alternativas al cumplimiento de requisitos y criterios deterministas que estuviesen basadas en un análisis de riesgo para todos aquellos casos en los que fuese posible. Uno de los primeros resultados del plan de implementación del APS fue la adopción por parte de la NRC de la siguiente política (1995) [40]:

> El uso del APS debería verse incrementado en el marco regulador, hasta el punto que el estado del arte lo permita, de tal forma que complemente el acercamiento determinista y de soporte a la filosofía tradicional de defensa en profundidad.
>
> El APS y análisis asociados deberían utilizarse en el marco regulador, siempre que sea práctico, para reducir innecesarios conservadurismos asociados con requisitos reguladores requisitos de licenciamiento, y otros, actuales. El APS debería utilizarse para dar soporte a la propuesta de requisitos reguladores adicionales en concordancia con el 10 CFR 50.109.

El plan de implementación del APS en la regulación sigue en marcha hoy en día, aunque ha sufrido dos reorientaciones. En el año 2000 pasó a centrarse en la regulación informada por el riesgo con el objetivo de desarrollar criterios para seleccionar y priorizar aquellas prácticas y políticas de la NRC que deberían estar informadas por el riesgo, amén de producir guías para implementar los elementos informados por el riesgo. En el año 2007 se introdujo el término *performance-based* y se dedicaron esfuerzos a la introducción de este concepto en la regulación.

Una de las principales conclusiones extraídas en los primeros años de implementación del plan fue que la base práctica de los APS no estaba estandarizada y que, por lo tanto, los APS realizados por los licenciatarios no se asemejaban entre sí en algunos aspectos clave como las hipótesis de modelización de sistemas. Este hecho tenía asociadas grandes desventajas: imposibilidad de comparar resultados, grandes esfuerzos para evaluar la calidad de los APS, pues se debía evaluar cada APS en función del acercamiento utilizado, y la toma de hipótesis inaceptables por parte de algunos licenciatarios, lo que inutilizaba el uso de sus APS. En respuesta a este problema, la ASME (American Society of Mechanical Engineers) y el NEI (Nuclear Energy Institute), en colaboración con la NRC, comenzaron a desarrollar estándares para la realización de análisis probabilistas de seguridad y para la revisión por parte de expertos, *peer review*, de los mismos. En 2003, la NRC puso en marcha un plan, reforzado por el desarrollo y aplicación de dichos

estándares, cuyo objetivo era conseguir un nivel idóneo de calidad en la realización y revisión de los APSs americanos [41, 42]. El plan de implementación de la calidad sigue en periodo de desarrollo hoy en día debido, en gran parte, a la diversidad de alcances y objetivos del APS (veáse sección 2.3 para más detalle) que ha de abarcar el propio plan. Además, la totalidad de los estándares de ASME y NEI aún no habían sido finalizados en el año 2013 [43].

El avance en el desarrollo y aplicación del plan de implementación del APS en la regulación informada por el riesgo ha dado como resultado, aparte de los estándares de ASME y NEI ya completados, la publicación de diversas *regulatory guides* que regulan el desarrollo y uso de aplicaciones basadas en el APS (véase el capítulo 3 para más detalle). Algunos ejemplos de *regulatory guides* son:

- *Regulatory guide* 1.174, sobre aplicaciones que tratan cambios en las bases de licenciamiento de una central nuclear.
- *Regulatory guide* 1.201, sobre aplicaciones para categorizar las estructuras, sistemas, y componentes de una central nuclear respecto a su importancia para la seguridad.
- *Regulatory guide* 1.205, sobre protección contra incendios basada en el riesgo para centrales nucleares existentes con reactores de agua ligera.
- *Regulatory guide* 1.206, sobre aplicaciones de licencia combinada de construcción y operación (comúnmente llamada *combined license* (COL)) de centrales nucleares.
- *Regulatory guide* 1.200, sobre la determinación de la idoneidad técnica de los resultados de un APS para dar soporte a actividades informadas por el riesgo.

Actualmente, cualquier nuevo diseño o petición de *combined license* de una central nuclear estadounidense ha de ir acompañada de un análisis probabilista de seguridad para poder ser aceptada por la NRC. Dicho requisito, definido en el 10 CFR 50.71(h) [44], remarca que los APS han de ser de nivel 1 y 2, y que han de estar listos antes de la primera carga de combustible. Además, el requisito define que los APS han de abarcar todos los sucesos iniciadores para los cuáles existan estándares o guías aceptadas por la NRC un año antes de la primera carga de combustible. En cambio, no existen requisitos que demanden el desarrollo de estudios APS para centrales ya en operación. Éstas, no obstante, se han de ajustar a los requisitos expuestos en las *regulatory guides* mencionadas anteriormente, especialmente los de la 1.200, si quieren utilizar el APS para desarrollar aplicaciones informadas por el riesgo.

2.2.4. La contribución de la IAEA al desarrollo del APS

El desarrollo de la metodología APS no solo ha sido seguido y apoyado con gran interés por parte de la NRC y la industria nuclear americana, sino que otros organismos reguladores y organizaciones internacionales también han dado soporte al desarrollo de la metodología. Este es el caso de la IAEA, que dedicó su sexta reunión *International Nuclear Safety Advisory Group*, celebrada en 1992, exclusivamente al APS. Las conclusiones de la reunión fueron claras: «el APS es una metodología con un gran potencial para analizar la seguridad y dar soporte a decisiones operacionales y reguladoras en centrales nucleares [35], pero es una metodología que necesita un desarrollo mayor para que se considere que se puede aplicar de forma consistente». Concretamente, se destacó la necesidad de estandarizar la metodología para poder comparar resultados y para poder utilizarlos en la toma de decisiones, así como la necesidad de mejorar el tratamiento de algunas tareas como el análisis de fiabilidad humana y el análisis de datos. En respuesta a las necesidades expuestas en el INSAG-6, y considerando el APS como una herramienta básica para la evaluación de la seguridad, la IAEA ha preparado una gran cantidad de documentación relacionada con el APS. En primer lugar y con mayor importancia, la IAEA ha publicado, en sus principios de seguridad, requisitos directamente relacionados con el análisis de seguridad y el APS. De forma adicional, la IAEA ha publicado diversos documentos técnicos cuyo objetivo es guiar en el cumplimiento de estos requisitos. Algunos ejemplos son:

- La guía específica de seguridad SSG-3 *Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants*, que presenta recomendaciones para cumplir con los requisitos de la IAEA. La guía de seguridad SSG-3 también promueve la creación de un marco de trabajo estándar para conseguir que haya consistencia técnica entre modelos APS de nivel 1 y que así las aplicaciones derivadas sean más fiables y su revisión más sencilla.
- El documento técnico TECDOC-1200 *Applications of probabilistic safety assessment (PSA) for nuclear power plants*, que contiene un listado de aplicaciones del APS en diferentes etapas del ciclo de vida de una central nuclear. Contiene una explicación detallada de cada una de las aplicaciones.
- El documento técnico TECDOC-1101 *Framework for a Quality Assurance Programme for Probabilistic Safety Assessmen*t, que contiene, de manera similar a la *regulatory guide* 1.200, un marco para la aplicación y evaluación de la calidad de los APS.
- El documento técnico TECDOC-1138, *Advances in safety related maintenance*, que contiene recomendaciones para el uso del APS en la toma de decisiones relacionadas con el mantenimiento de equipos y sistemas.
- El documento técnico TECDOC-1511, *Determining the quality of probabilistic safety assessment for applications in nuclear power plants*, que presenta una metodología para juzgar la calidad de los APS que se utilizan para dar soporte a la creación de ciertos tipos de aplicaciones.

A día de hoy la IAEA sigue comprometida con el desarrollo de la metodología APS pues la considera uno de los pilares básicos del análisis de seguridad de centrales nucleares.

2.2.5. El APS en España

El marco regulador español creado por el CSN ha estado históricamente inspirado en el propuesto por la NRC por razones de similitud tecnológica, y gracias a acuerdos de investigación y desarrollo entre ambas organizaciones. En el caso del APS el grado de verosimilitud no es total pues han existido y existen ciertas diferencias en cuanto a la integración de los APS en la industria y en cuanto a los requisitos al respecto del alcance de los APS y del uso de las aplicaciones informadas por el riesgo. El primer estudio APS español fue requerido por el CSN, en 1983, a la central Santa María de Garoña. A raíz de la experiencia y los beneficios obtenidos del proyecto, el CSN decidió emitir en 1986 el «Programa Integrado de realización y utilización de los Análisis Probabilista de Seguridad» [45]. Este programa constituyó el primer marco regulador de realización de estudios APS en todas las centrales nucleares españolas. Como su propio nombre indica, el programa integrado tenía dos objetivos principales: por una parte, integrar la realización de estudios APS en la industria nuclear española de forma escalonada y siguiendo requisitos establecidos por el propio CSN, y, por otra parte, apoyar el desarrollo de aplicaciones informadas por el riesgo basadas en el APS. Para llegar a alcanzar ambos objetivos, el Programa Integrado estaba dividido en siete puntos, entre los cuales destacaban: el desarrollo de un banco de datos, la creación de reglamentación y guías, y la participación en programas internacionales. Cabe destacar que el requisito al respecto del alcance de los APS del Programa Integrado era más restrictivo que su homónimo de la NRC vigente en aquel momento[3]. En la revisión del Programa Integrado llevada a cabo una década después de su lanzamiento se concluyó que, si bien la progresión en el cumplimiento del primer objetivo del Programa había sido correcta, el desarrollo de aplicaciones informadas por el riesgo basadas en el APS estaba por detrás de lo requerido por el Programa. Como resultado, la revisión del Programa Integrado puso especial énfasis en el desarrollo de aplicaciones de APS, y dejó en segundo plano el desarrollo final de los propios modelos APS pues éstos ya estaban prácticamente finiquitados.

[3] El alcance requerido por la NRC había sido publicado en la *Generic Letter 88-20*, que contenía la descripción de la *Individual Plant Examination*. El requisito del Programa Integrado al respecto del alcance abarcó lo incluido en la GL 88-20 más el análisis de Otros Modos y el análisis de otras fuentes radiactivas.

Actualmente, la realización y aplicación del APS están reguladas por la instrucción de seguridad IS-25, uno de los productos del Programa Integrado. La instrucción de seguridad Instrucción IS-25 del Consejo de Seguridad Nuclear, publicada en el Boletín Oficial del Estado (BOE) el 24 de junio de 2010, trata sobre criterios y requisitos sobre la realización de los análisis probabilistas de seguridad y sus aplicaciones en centrales nucleares. Los principales requisitos expuestos por la IS-25 son:

- Se exige a los licenciatarios que realizen modelos APS de nivel 1 y 2 tanto a Potencia como en Otros Modos[4] incluyendo sucesos iniciadores internos, externos de generación interna, y otros externos (véase la sección 2.3 para más detalle). Se explicita que los sucesos otros externos (terremotos, tsunamis, y accidentes de avión, entre otros) pueden ser analizados mediante otras metodologías siempre y cuando sean aceptadas por el organismo regulador.
- En el desarrollo de los APS se han de considerar, además, otras fuentes de radiactividad que puedan dar lugar a liberaciones de partículas similares a las del reactor, como, concretamente, la piscina de combustible.
- En el futuro, los APS habrán de extenderse hasta el análisis de las posibles liberaciones radiactivas al exterior de la central en caso de accidente.
- La obligatoriedad de incluir análisis de fiabilidad humana, análisis de fallos de causa común, y análisis de dependencias en todo APS.
- Definición de dos tipos de aplicaciones: las programáticas, como, por ejemplo, los monitores de riesgo (véase el capítulo 3 para más detalle), y las de apoyo a modificaciones, cambios, y decisiones.
- No se pueden utilizar los resultados de un APS como único argumento para la toma de decisiones.

El APS goza de buena salud en la industria nuclear española y es que, hoy en día, toda central nuclear española posee, o tiene en vías de desarrollo, modelos APS de diferentes alcances como consecuencia del Programa Integrado y de la IS-25. Aparte de la IS-25, el CSN también ha publicado, en el marco del Programa Integrado, guías de seguridad para la realización de ciertas tareas relacionadas con el APS. Ejemplos destacados de estas guías son la guía de seguridad 1.15 sobre Actualización y Mantenimiento de los Análisis Probabilistas de Seguridad y la guía de seguridad 1.14 sobre Criterios básicos para la realización de aplicaciones de los Análisis Probabilistas de Seguridad, inspirada en la *regulatory guide* 1.174 americana. Además, el CSN ha desarrollado su propio sistema integrado de supervisión de centrales [46], y diversas metodologías para determinar la significación de equipos y sistemas en diferentes situaciones [47, 48], como, por ejemplo, operación en parada de recarga [49]. No obstante, no se han cumplido todos los objetivos planteados en el Programa Integrado pues, a día de hoy, no se han publicado reglamentos y guías precisos y detallados ni para la realización de estudios APS, ni para todas las posibles aplicaciones de APS.

2.3. Objetivos y alcance del Análisis Probabilista de Seguridad

El APS es una técnica de análisis de riesgos[5] que va dirigida, en el marco de la industria nuclear, a la construcción de modelos lógico – probabilistas para la determinación de la frecuencia de ocurrencia de las posibles secuencias de sucesos que pueden desembocar en situaciones accidentales con graves consecuencias para la instalación nuclear o para el exterior. Se trata de una técnica sistemática mediante la cual se

[4] El término Otros Modos hace referencia a los modos de operación de una central nuclear distintos al modo de producción de energía eléctrica. Por ejemplo, el término Otros Modos hace referencia a la etapa de recarga de combustible.

[5] El concepto de riesgo se define como la combinación de la frecuencia de ocurrencia de un suceso y la severidad de las consecuencias de dicho suceso. En el caso de una central nuclear, la principal figura de riesgo, que es la cuantificada en el APS de nivel 1, es la frecuencia con que puede producirse la consecuencia de daño al núcleo.

analizan los aspectos del diseño, procedimientos, y prácticas operativas de la instalación que pueden originar y/o determinar la evolución de la central hacia situaciones accidentales. En el marco de un análisis APS se definen los escenarios accidentales, las posibles evoluciones de los escenarios, y se estudia de forma detallada la probabilidad de que los sistemas necesarios para la mitigación de esos escenarios accidentales dejen de cumplir, o fallen a cumplir, su función de seguridad (véase la sección 2.4 para más detalle sobre la metodología). A diferencia del análisis determinista tradicional, la metodología APS está preparada para utilizar criterios realistas en la modelización de la respuesta de la planta y la actuación de sus sistemas. Más allá de la estimación del riesgo de la central, y a pesar de que en los últimos 20 años se han desarrollado multitud de aplicaciones derivadas de su utilización (véase el capítulo 3 para más información), históricamente el APS se ha utilizado principalmente para identificar vulnerabilidades y deficiencias de seguridad en el diseño y operación de las centrales.

La característica que mejor define a un análisis probabilista de seguridad es su alcance. El alcance de un APS se caracteriza por lo siguiente:

- La fuente radiactiva considerada (núcleo del reactor, piscina de combustible, instalaciones de almacenamiento de combustible).
- Los sucesos iniciadores[6] analizados.
- Los modos de operación de la planta analizados.
- El nivel de APS, o figura de riesgo, analizado.

Un APS es de alcance total si abarca de forma completa todos los aspectos de todas las características del alcance definidas en la lista anterior. Pese a que es posible realizar un APS de alcance total, no es necesario contar con uno para tener una estimación del riesgo de una central, tal y como se desprende de los requisitos de la instrucción de seguridad IS-25 del CSN. De hecho, es práctica habitual y necesaria realizar modelos de APS diferentes para cada uno de los diversos alcances a tratar. Se realizan modelos APS diferentes para los diversos alcances posibles porque, para cada alcance, las hipótesis de modelización de escenarios y sistemas suelen ser diferentes. Valga como ejemplo la práctica de realizar un modelo APS exclusivamente para el modo de operación a potencia, separado de los otros modos de operación. Como resultado, un APS de alcance total es un conglomerado de modelos APS individuales, cada uno con un alcance diferente. Se detallan a continuación las características de cada uno de los diferentes aspectos del alcance de un APS.

2.3.1. Alcance: Fuente radiactiva considerada

Históricamente, los APS se han diseñado para estimar el riesgo de daño al núcleo pues se consideraba y se considera que el núcleo es la fuente radiactiva con mayor riesgo de liberación en una central nuclear. No obstante, el avance en el desarrollo de la metodología APS y, posteriormente, el suceso de Fukushima, han puesto también el foco de análisis en otras fuentes radiactivas cuya liberación podría suponer graves consecuencias medio ambientales. Es el caso específico de las piscinas de combustible gastado, o equivalentes, y, también, de almacenes temporales individualizados de combustible gastado. En la parte II de esta tesis doctoral se presenta una contribución novedosa en el marco del desarrollo de metodologías de análisis probabilista de seguridad para el análisis del riesgo de fuentes radiactivas diferentes al reactor nuclear. Concretamente, la segunda parte de la tesis incluye el desarrollo y aplicación de una metodología de análisis probabilista del riesgo de un Almacén Temporal Individualizado (ATI).

La elección al respecto de la fuente radiactiva estudiada forma parte de la definición del objetivo primordial del análisis de riesgo. El núcleo, la piscina de combustible, y otras fuentes radiactivas, no se pueden

[6] Un suceso iniciador es un suceso que perturba el funcionamiento normal de la planta y que, a partir del mismo, puede desarrollarse una secuencia accidental [50].

analizar de forma conjunta mediante la metodología APS porque los sucesos iniciadores, las funciones clave de seguridad, los sistemas frontales, y los sistemas soporte asociados a cada una son distintos (véase la sección 2.4 para más detalle). Todos los datos aportados de aquí en adelante hacen referencia a análisis probabilistas de seguridad que analizan el daño al núcleo.

2.3.2. Alcance: Sucesos iniciadores

Un suceso iniciador es un evento que perturba el funcionamiento normal de la planta de tal manera que puede desarrollarse una secuencia accidental [50]. Los sucesos iniciadores se clasifican en tres tipos: sucesos internos, sucesos externos, y otros externos.

- Sucesos internos: sucesos de origen interno debidos a fallos de sistemas, estructuras o componentes, o errores humanos.
- Sucesos externos: suceso de origen interno cuyo origen no está relacionado con la fiabilidad de sistemas, estructuras o componentes, o la actuación humana. Valga el ejemplo de incendios o inundaciones internas.
- Otros sucesos externos: sucesos de origen externo a la instalación. Pueden ser naturales o pueden ser consecuencia de actividades industriales o humanas. Valgan como ejemplo sucesos como terremotos, explosiones o caídas de aviones.

Los tres tipos de sucesos iniciadores se analizan mediante modelos probabilistas independientes debido a que sus consecuencias sobre la evolución de la planta son distintas. Es más, en lo que respecta a los sucesos externos y a los otros externos, las condiciones postuladas para cada uno de ellos son tan diferentes en comparación con las de los demás que se analizan en modelos APS individuales[7]. Por contra, los sucesos internos se analizan conjuntamente en el mismo modelo APS. Un APS de alcance total ha de contar con varios modelos APS, cada uno de ellos dedicado exclusivamente al análisis de sucesos iniciadores diferentes a los de los demás.

2.3.3. Alcance: modos de operación

El funcionamiento de la planta se divide en varios modos de operación según el valor de parámetros como la constante de multiplicación k_{eff}, la temperatura y la presión del reactor, y dependiendo de qué sistemas se encargan del control de presión y de la refrigeración del reactor. De forma genérica, estos modos de operación se llaman a Potencia, baja Potencia, Parada, Recarga, y Arranque, y corresponden a la transferencia de producción de potencia a recarga de combustible, y viceversa. En el marco de los análisis APS, el modo de operación a Potencia se analiza de forma separada a los otros modos de operación porque la disponibilidad de sistemas, la progresión de secuencias accidentales, y los sucesos iniciadores internos son diferentes. En consecuencia, existen dos posibles alcances para un APS en referencia a los modos de operación, el análisis del modo de operación Potencia, y el análisis de los Otros Modos de operación. Un APS de alcance total debe contar con modelos APS a Potencia y Otros Modos para todo tipo de suceso iniciador definido en la sección 2.3.2.

2.3.4. Alcance: niveles de APS, figuras de riesgo

La estimación del riesgo de una central nuclear mediante la metodología APS se divide en tres niveles que guardan relación con el concepto de defensa en profundidad (véase la figura 2.1). Cada uno de los niveles

[7] Es decir, se construye un modelo APS para cada tipo de suceso iniciador

del APS está relacionado con una(s) barrera(s) o nivel(es) de protección de la defensa en profundidad. Genéricamente, a los niveles se les da el nombre de nivel 1, nivel 2, y nivel 3, y para cada uno se estima una figura de riesgo diferente. Los niveles se analizan de forma secuencial, es decir, para estimar el riesgo correspondiente al nivel 2 primero se ha de desarrollar un APS de nivel 1.

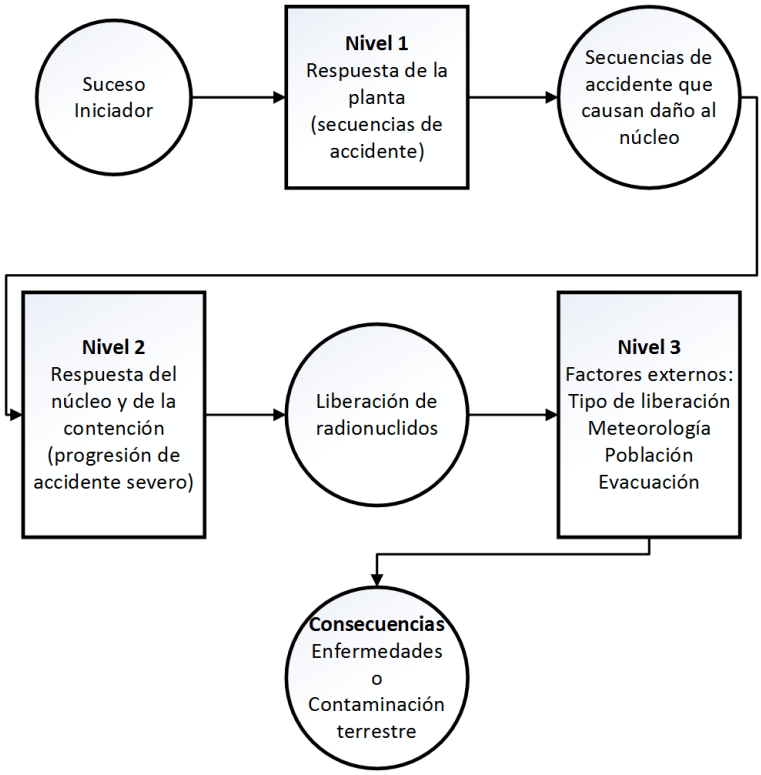


Figura 2.1: Niveles de APS

2.3.4.1. Nivel 1

El alcance de nivel 1 consiste en analizar el diseño y operación de la central con el objetivo de identificar las potenciales secuencias de accidente que pueden dar lugar al daño del núcleo del reactor tras un suceso iniciador. Las barreras físicas de defensa en profundidad evaluadas son la matriz y la vaina de combustible, y el sistema de refrigeración del reactor. Los niveles de defensa en profundidad analizados son los niveles 1, 2, y 3, siendo este último el control de accidentes dentro de las bases de diseño. La figura de riesgo estimada en este nivel de APS es la frecuencia anual de daño al núcleo. Se estima la frecuencia anual de daño al núcleo para toda secuencia accidental. Estas frecuencias se suman para calcular la frecuencia anual total de daño al núcleo. Las secuencias accidentales identificadas y las frecuencias de daño al núcleo asociadas a cada una de ellas son el input para el APS de nivel 2.

2.3.4.2. Nivel 2

El nivel 2 de APS consiste en modelar la respuesta de la planta a las secuencias de accidente cuyo resultado es daño al núcleo según el APS de nivel 1. A estas secuencias de accidente se les acostumbra a llamar accidente severo[8] [51]. En el nivel 2 de APS se analiza la progresión del accidente severo desde el punto de

[8] Accidente que sobrepasa la base de diseño en el que se produce una degradación significativa del núcleo.

vista de cómo las estructuras y sistemas relacionados con la contención responden al accidente (tercera barrera y cuarto nivel de la defensa en profundidad, respectivamente). La respuesta de estas estructuras y sistemas depende de su estado inicial y de su capacidad de soportar las duras condiciones impuestas por el accidente severo. Por lo tanto, en el nivel 2 es importante entender y plasmar la fenomenología accidental ligada a cada secuencia accidental. En cuanto a resultados, el APS de nivel 2 proporciona una estimación del término fuente, es decir, la cantidad de radionucleidos liberados, y de la frecuencia anual de liberación de este término fuente para las secuencias accidentales analizadas. La figura de riesgo estimada en este nivel de APS es o bien la Frecuencia de Grandes Liberaciones Tempranas (FGLT), o bien la Frecuencia de Grandes Liberaciones (FGL). Los términos fuente y las frecuencias anuales de liberación asociadas a cada uno de ellos son los inputs para el APS de nivel 3.

2.3.4.3. Nivel 3

El nivel 3 de APS está relacionado con el último nivel de la defensa en profundidad, la mitigación de las consecuencias radiológicas de liberaciones significativas de material radioactivo, ya que estima las consecuencias de la liberación de material radiactivo causada por los accidentes severos analizados en el nivel 2. Concretamente, se estiman dos tipos de consecuencias:

- Efectos de las dosis de radiación sobre la salud de las personas que viven alrededor de la central.
- Contaminación del suelo a causa del material radiactivo liberado en el accidente.

Las consecuencias dependen de varios factores como, por ejemplo, la cantidad de residentes en los alrededores de la central, las condiciones de evacuación, y la dirección de dispersión de la nube radiactiva en el caso de los efectos sobre la salud. La modelización de los diversos factores que afectan a estas consecuencias es lo que constituye los modelos de APS de nivel 3. El APS de nivel 3 estima las figuras de riesgo mediante la combinación de las consecuencias con sus respectivas frecuencias de ocurrencia. A diferencia de los niveles 1 y 2, no existe consenso al respecto de qué figuras son las mejores para representar el riesgo asociado al nivel 3. No obstante, se considera que figuras tales como la frecuencia anual de cáncer latente y la frecuencia anual de lesión o muerte temprana son buenos indicadores del riesgo asociado al nivel 3. Un APS de alcance total debería estimar los riesgos de nivel 3 en todos los modelos APS que lo forman.

2.4. Metodología APS de nivel 1 para sucesos internos a potencia

En este apartado se describe la metodología de aplicación del análisis probabilista de seguridad de nivel 1 para sucesos internos a potencia. El objetivo es presentar la metodología APS de tal manera que facilite la comprensión del contenido de esta tesis doctoral y de cualquier documento relacionado con la aplicación del APS en centrales nucleares.

Se ha decidido describir la metodología APS de nivel 1 para sucesos internos a potencia porque es la base sobre la que se construye cualquier modelo APS de daño al núcleo de mayor alcance. El principal motivo para ello es que es en el marco de la metodología APS de nivel 1 en la que se analiza el diseño y operación de una central nuclear para evaluar la respuesta de los sistemas de seguridad e identificar las secuencias de accidente que pueden dar lugar a daño al núcleo. Este análisis es necesario para desarrollar todos los posibles alcances de APS que evalúan el riesgo de daño al núcleo, incluyendo tanto los diferentes niveles de APS como diferentes sucesos iniciadores. Además, el APS de nivel 1 de sucesos internos a potencia también es la principal referencia metodológica para la realización de análisis probabilistas que analicen otras fuentes de radiactividad.

La metodologia APS de nivel 1 para sucesos internos a potencia se divide en un conjunto de tareas que se describen en las siguientes secciones (véase la figura 2.2). El desarrollo de un modelo APS es un proceso

iterativo así que el orden en el que se presentan las tareas no se ha de entender como estrictamente cronológico. Algunas tareas de la metodología APS se pueden realizar en paralelo, y otras han de ser revisadas una vez se desarrollen las tareas de cuantificación. Un APS nivel 1 debería desarrollarse hasta que se consiga un modelo lo suficientemente preciso y detallado. Las tareas se listan a continuación en el orden el que son descritas en este apartado:

- Planteamiento y organización del APS
- Familiarización con la planta
- Identificación y agrupación de sucesos iniciadores
- Análisis de secuencias de accidente
- Análisis de sistemas
- Análisis de datos
- Cuantificación
- Análisis de resultados

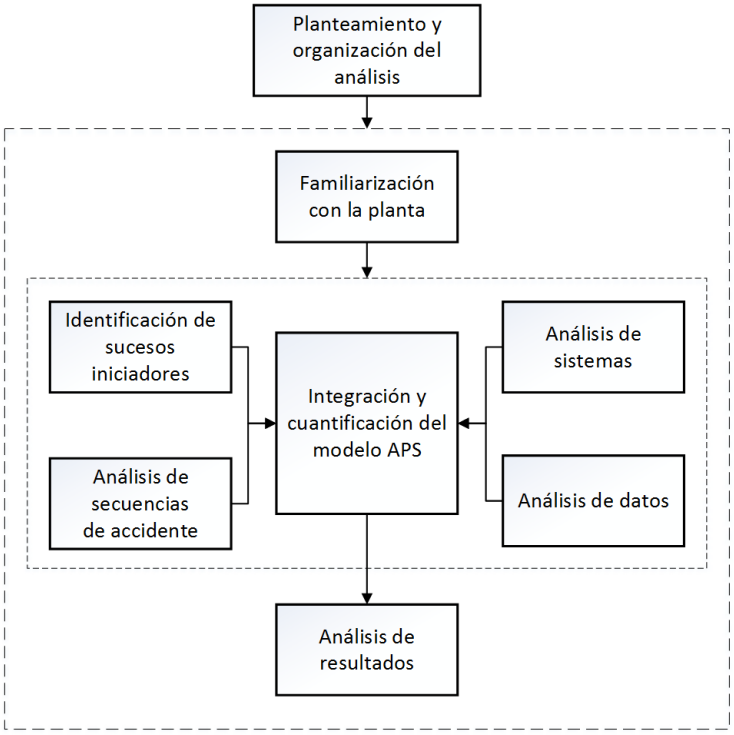


Figura 2.2: Metodología APS de nivel 1 de sucesos internos a potencia

2.4.1. Planteamiento y organización del APS

La primera tarea a realizar en el desarrollo de un APS, sea del alcance que sea, es la de plantear, organizar, y lanzar el proyecto. El planteamiento de los objetivos del proyecto y de los potenciales usos del modelo

APS resultado es condición *sine qua non* para la organización y lanzamiento del proyecto APS. Una vez determinados los objetivos y usos del APS, la organización u organizaciones responsables del proyecto proceden a desarrollar el plan organizativo y de gestión del proyecto, que incluye la toma de decisiones al respecto de las siguientes tareas clave: seleccionar las metodologías y procedimientos a utilizar en el desarrollo del modelo APS, seleccionar el equipo de trabajo que realizará el APS y la organización del mismo, la formación del equipo de trabajo, la preparación del plan de trabajo para la realización del proyecto, la estimación y preparación de la financiación necesaria para desarrollar el proyecto, y el establecimiento de programas de garantía de calidad.

Un proyecto APS puede no ser lanzado o no estar directamente realizado por el licenciatario, ya sea porque sea lanzado por el diseñador o el organismo regulador [21], o porque el licenciatario derive el desarrollo del proyecto a una consultoría, un instituto de investigación, una universidad, u otros. Sea quien sea el responsable de desarrollar el proyecto, el licenciatario siempre ha de ser partícipe del mismo ya que es la principal fuente de información al respecto de la instalación.

Los procedimientos y métodos de trabajo adecuados para desarrollar el proyecto en ciernes han de ser elegidos en la etapa de organización del proyecto. De este modo, se evitan innecesarias iteraciones en el uso de métodos y procedimientos en la etapa de desarrollo que puedan causar la demora del proyecto. En la elección de los procedimientos y métodos a utilizar en el desarrollo del proyecto se han de tener en cuenta los recursos financieros y de personal, las características del equipo de trabajo, y el tiempo postulado para acabar el proyecto. Una vez se hayan seleccionado los métodos y procedimientos a utilizar, las diferentes etapas de los mismos se han de relacionar con tareas de garantía de calidad y preparación del equipo de trabajo para producir un plan de trabajo detallado del proyecto [21]. Este plan de trabajo ha de ajustarse también a la disponibilidad del equipo de trabajo.

El equipo de trabajo que realiza el APS ha de conocer el diseño y operación de la planta y tener experiencia al respecto de las metodologías APS. La participación en el equipo de trabajo de miembros del licenciatario y del responsable del diseño de la central es prácticamente necesaria en algunas de las tareas de la metodología APS. El programa de preparación y formación del equipo de trabajo se ha de desarrollar en función del nivel de conocimiento y experiencia inicial del equipo de trabajo.

El programa de garantía de calidad de un APS incluye la realización de todas las actividades necesarias para conseguir un nivel de calidad adecuado, y la realización de todas aquellas actividades necesarias para verificar que se consiga el nivel adecuado de calidad. El programa de garantía de calidad incluye el desarrollo de un plan de trabajo para mantener y actualizar el modelo APS a lo largo de la vida operativa de la central. Es también objetivo del programa de garantía de calidad garantizar que toda la documentación generada en el marco del proyecto sea clara y trazable para que las tareas de revisión del APS, desarrollo de aplicaciones, y futuras actualizaciones se puedan llevar a cabo de forma sencilla.

2.4.2. Familiarización con la planta

El equipo de trabajo que realiza el APS se ha de familiarizar de forma exhaustiva, si no lo está ya, con la operación y el diseño de la central nuclear objeto de estudio para poder desarrollar el resto de tareas del APS. En la familiarización con la planta, el equipo de trabajo ha de centrarse en identificar y comprender las funciones de seguridad que aseguran el cumplimiento de la filosofía de la defensa en profundidad, así como en identificar y conocer al detalle los sistemas frontales que se encargan de cumplir estas funciones, y los sistemas soporte necesarios para el funcionamiento de los sistemas frontales. También es necesario que el equipo de trabajo identifique posibles amenazas ante las que ciertas ESCs son susceptibles, así como las posibles respuestas de la central a situaciones anormales, accidentales, o de emergencia. Principalmente, la familiarización con la planta se realiza a partir de la revisión de documentación de la propia central y de revisiones *in situ* de estructuras, sistemas, y componentes. A continuación se citan algunos de los documentos más importantes a revisar para llevar a cabo la familiarización con la planta:

- Estudio final de seguridad.

- Documentos de descripción y bases de diseño de sistemas.
- Procedimientos de operación, de operación en fallo de sistemas, de mantenimiento, y de emergencia.
- Diagramas de tuberías e instrumentación, y diagramas de circuitos eléctricos.
- Especificaciones técnicas de funcionamiento.
- Planos del diseño actual de la central, incluyendo planos de tuberías.
- Base de datos de experiencia operativa.

La definición de criterios de daño, criterios de aceptación, y criterios de éxito también forma parte de la tarea de familiarización con la planta. La definición de estos criterios se ha de realizar después de revisar la documentación de la central. Mediante los criterios de daño se postula qué se considera daño al núcleo. Los criterios de daño suelen definirse en forma de valores límite de variables como la presión del sistema de refrigeración del reactor o la temperatura de las vainas de combustible. Mediante los criterios de daño se define cuáles de las secuencias de accidente postuladas (véase sección 2.4.4 para más detalle) llevan a daño al núcleo. Los criterios de aceptación definen el correcto cumplimiento de las funciones de seguridad de la central. Estos criterios suelen definirse con valores límite de variables de proceso tales como el caudal y la presión de refrigerante. Los criterios de éxito de los sistemas frontales y de soporte indican qué componentes, como mínimo, han de estar operables para que se cumplan los criterios de aceptación de la función de seguridad asociada. Los criterios de éxito de sistemas de seguridad deben estar justificados mediante análisis de soporte, es decir, análisis termohidráulicos, neutrónicos, y otros. Estos análisis se realizan una vez se hayan delineado las secuencias de accidente para conocer el estado exacto de la planta a analizar.

2.4.3. Identificación y agrupación de sucesos iniciadores

La primera tarea de la creación del modelo APS es la identificación y agrupación de sucesos iniciadores. Un suceso iniciador es un evento que puede causar daño al núcleo directamente (por ejemplo, la rotura de la vasija) o un suceso que desafía la operación normal de tal manera que se necesita la actuación de sistemas de seguridad para evitar el daño al núcleo [21]. Los sucesos iniciadores son la raíz de la que parte el modelo APS ya que son los que inician las situaciones de las cuáles se estima el riesgo. En consecuencia, la tarea de identificación de sucesos iniciadores ha de realizarse de manera exhaustiva para proveer una lista que sea lo más específica, detallada y amplia posible teniendo en cuenta que es inviable abarcar todos los posibles sucesos iniciadores que puedan ocurrir en una central nuclear. En concordancia con este objetivo, en el proceso de identificación de sucesos iniciadores se aplican diferentes metodologías:

- Aplicación de métodos analíticos como estudios de modos y efectos de fallo (FMEA, Failure Mode and Effects Analysis) en el estudio de los sistemas de seguridad para determinar si el fallo de estos sistemas, ya sea total o parcial, podría generar un suceso iniciador.
- Aplicación de métodos deductivos como diagramas lógicos maestros (MLD, Master Logic Diagram) para identificar los fallos elementales, o combinaciones de fallos, que desafiarían la operación normal de la planta, y, por lo tanto, generarían un suceso iniciador.
- Comparación con la lista de sucesos iniciadores identificados en centrales de diseño similar y con los sucesos iniciadores postulados en guías y estándares de seguridad.
- Identificación de sucesos iniciadores mediante el análisis de la experiencia operativa de la central de estudio y de otras centrales de diseño similar.
- Revisión de los accidentes base de diseño y de los accidentes más allá de las bases de diseño postulados en el estudio final de seguridad.

Además de utilizar diferentes metodologías de identificación de sucesos, las siguientes consideraciones se han de tener en cuenta en la identificación de sucesos iniciadores para que la lista resultante sea lo más completa posible:

- La lista de sucesos iniciadores ha de incluir tanto fallos completos como fallos parciales de componentes y sistemas. Por ejemplo, la lista debería incluir tanto la pérdida de alimentación a todos los generadores de vapor, como la pérdida de alimentación a un generador de vapor, como la reducción de la alimentación a los generadores de vapor [21].
- La identificación de sucesos iniciadores debe abarcar todos los modos de operación a potencia posibles. Por ejemplo, se deben incluir todos los sucesos iniciadores que puedan afectar específicamente a la configuración en la que uno de los lazos de refrigeración se encuentra indisponible.
- Se ha de garantizar que en el listado de sucesos iniciadores se incluyan todos los eventos de muy baja frecuencia pero muy graves consecuencias predecibles.
- La lista de sucesos iniciadores ha de incluir fallos e indisponibilidades de sistemas soporte, como, por ejemplo, el sistema de suministro eléctrico. Se ha de tener un cuidado especial con aquellos sistemas soporte cuyo fallo puede provocar el disparo del reactor y que, además, cumplen una función en el transitorio posterior a un disparo de reactor.

A modo de ejemplo, se presenta a continuación un listado de sucesos iniciadores conceptuales para un APS nivel 1 de sucesos internos a potencia de un reactor de agua a presión:

- Incremento de la evacuación de calor del reactor. Ejemplo: abertura de las válvulas de alivio del sistema secundario.
- Reducción de la evacuación del calor del reactor. Ejemplo: pérdida del agua de alimentación principal a los generadores de vapor.
- Reducción del caudal del sistema de refrigeración del reactor. Ejemplo: disparo de una de las bombas del sistema de refrigeración del primario.
- Anomalías en las distribuciones de potencia y reactividad. Ejemplo: retirada no prevista de barras de control.
- Incremento del inventario de agua del sistema de refrigeración del reactor. Ejemplo: Operación inadvertida de los sistemas de inyección de seguridad.
- Cualquier suceso que cause el disparo del reactor.
- Sucesos de pérdida de refrigerante del sistema de refrigeración del reactor (los comúnmente conocidos como LOCA (*Loss of Coolant Accidents*)).
- Cualquier suceso que provoque la pérdida parcial o total de la potencia eléctrica exterior.

Pese a que el avance de la tecnología informática permite realizar análisis cada vez más complejos, hoy en día se recomienda agrupar los sucesos iniciadores en conjuntos de sucesos iniciadores semejantes para que el tamaño del análisis sea manejable [21]. Dos o más sucesos iniciadores se pueden incluir en el mismo conjunto si cumplen las siguientes condiciones:

- La progresión del transitorio accidental es la misma o muy similar.
- Los criterios de éxito de los sistemas frontales y soporte son los mismos o muy similares. Se escogen los criterios de éxito más restrictivos en el caso que se incluyan en el mismo conjunto sucesos iniciadores que requieran criterios diferentes.

- Las consecuencias de los sucesos iniciadores respecto a la disponibilidad de sistemas frontales y soporte son las mismas.
- La respuesta de los operarios es la misma.

Es posible agrupar sucesos iniciadores cuyas progresiones accidentales y/o criterios de éxito de los sistemas frontales y soporte sean ligeramente diferentes. En estos casos, la secuencia de accidente (véase sección 2.4.4 para más detalle) asociada ha de representar la envolvente de todas las posibles secuencias de accidente y consecuencias de estos sucesos iniciadores.

2.4.4. Análisis de secuencias de accidente

El siguiente paso en la creación del modelo APS es determinar, y plasmar, la respuesta de la planta ante la ocurrencia de los diferentes conjuntos de sucesos iniciadores. La respuesta de la planta se caracteriza a partir de los sistemas de seguridad que han de operar para garantizar el cumplimiento de las funciones de seguridad, y varía en función del conjunto de sucesos iniciadores analizado, y del propio estado de los sistemas de seguridad de la central. Los procedimientos de operación, de fallo, y de emergencia, y las guías de accidente severo son las principales fuentes de información a revisar para determinar las posibles respuestas de la planta. Además, la definición de criterios de aceptación y éxito precisos y detallados en la tarea de familiarización con la planta ayuda sobremanera a determinar la respuesta de la planta.

Las diferentes posibles respuestas de la central ante un conjunto de sucesos iniciadores se plasman mediante una estructura inductiva llamada árbol de sucesos (comúnmente, *Event Tree*). Un árbol de sucesos es una estructura ramificada apaisada que parte de un origen común y en la que cada punto de inflexión, es decir, cada punto de inicio de una nueva rama, se corresponde con una decisión entre dos o más posibles estados. Cada rama del árbol finaliza en un punto singular asociado a ella misma. Es decir, dos ramas no se pueden fusionar. En el contexto de la metodología APS de nivel 1 para sucesos internos a potencia, el origen del árbol de sucesos es el suceso iniciador o conjunto de sucesos iniciadores. Las ramas son cada una de las posibles secuencias de accidente derivadas de la ocurrencia del suceso iniciador. Los puntos de inflexión, que en el caso de la metodología APS en cuestión suelen ser binarios, representan el éxito o el fracaso en la actuación de los sistemas de seguridad que han de operar para garantizar el cumplimiento de las funciones de seguridad. Los arboles de sucesos han de incluir todos las funciones de seguridad, y, por consiguiente, todos los sistemas de seguridad y/o acciones de seguridad relacionados, que han de realizarse en respuesta a los sucesos iniciadores. Los sistemas y acciones de seguridad incluidos en un árbol de sucesos reciben el nombre de cabeceros puesto que su descripción se coloca encima de la estructura ramificada. Cada cabecero tiene asignada una parte de la estructura, en la que se colocan los puntos de inflexión asociados al mismo. La estructura del árbol de sucesos se ha de delinear siguiendo el orden cronológico en el que los cabeceros serían demandados por la planta. Un árbol de sucesos ha de plasmar todas las posibles respuestas de planta relevantes incluyendo tanto las que derivan en daño al núcleo como las que derivan en parada segura. La figura 7.1 presenta un ejemplo de árbol de sucesos.

Cada secuencia de accidente, es decir, cada rama del árbol de sucesos, terminan en un estado final que se asocia a una situación concreta de la central. Generalmente, las secuencias de accidente tienen dos posibles estados finales en el marco de un APS de nivel 1 de sucesos internos a potencia: parada segura, o daño al núcleo. De la definición de los criterios de daño depende, uno, la decisión sobre qué estado final se ha de asignar a cada secuencia de accidente, y, dos, si la consecuencia negativa de daño al núcleo se subdivide en diversos estados finales.

El árbol de sucesos es una metodología de delineación de las diferentes secuencias de accidente que por sí misma no proporciona ninguna información al respecto del riesgo. Ahora bien, la metodología de árbol de sucesos está preparada para acoplarse con otras metodologías que proporcionen información cuantitativa al respecto de los fallos introducidos en el árbol. En el caso del APS, los árboles de sucesos se conectan con otras estructuras de análisis, llamadas árboles de fallos, para poder cuantificar el riesgo de una central

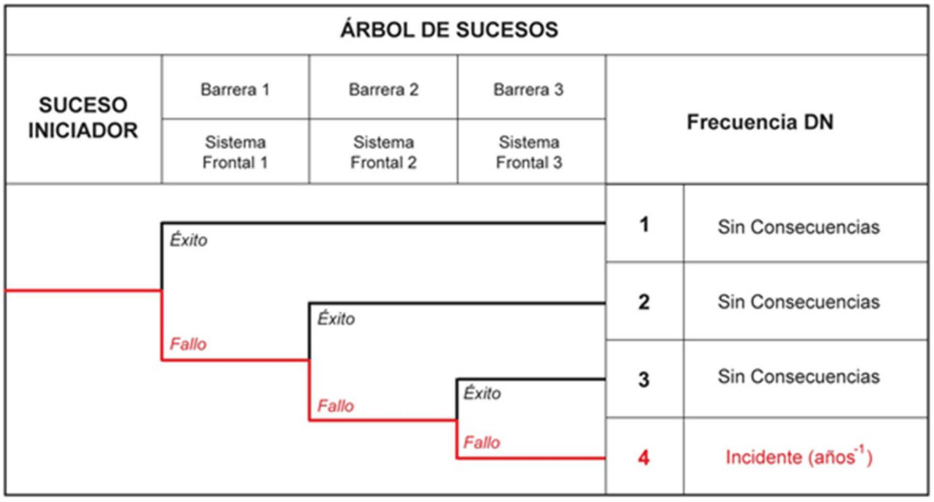


Figura 2.3: Ejemplo de árbol de sucesos

nuclear (véase la sección 2.4.7 para más detalle sobre la cuantificación). Los árboles de fallo son estructuras deductivas que permiten estimar la probabilidad de fallo o indisponibilidad de un sistema. Cada cabecero de un APS de nivel 1 de sucesos internos a potencia, incluidos algunos conjuntos de sucesos iniciadores, está acoplado a un árbol de fallos para introducir la probabilidad de fallo o indisponiblidad de los sistemas de seguridad en la estructura del árbol de sucesos. En la siguiente sección, Análisis de sistemas, se describe la estructura de los árboles de fallo.

2.4.5. Análisis de sistemas

La tarea de Análisis de sistemas consiste en la redacción de descripciones detalladas de todos los sistemas frontales y soporte incluidos en los árboles de sucesos. El ulterior objetivo de la tarea de análisis de sistemas es dar soporte a la modelización de los árboles de fallo de los cabeceros de los árboles de sucesos. En consecuencia, las descripciones de sistemas producto del análisis se caracterizan por proporcionar toda la información necesaria para lo posterior creación de los arboles de fallo. De hecho, la modelización de árboles de fallo se suele incluir como parte del desarrollo de los análisis de sistemas en la división de la metodología APS en diversas tareas. Un análisis de sistemas típico incluye la siguiente información:

- Un descripción detallada y precisa de la función o funciones que puede llevar a cabo el sistema.
- Una descripción detallada de las estructuras y componentes que conforman el sistema.
- Los criterios de diseño del sistema.
- Una descripción de la operación del sistema en todos los diferentes modos en los que pueda operar. Esta descripción ha de incluir valores de las variables de proceso y los motivos por los que se traslada la operación del sistema de un modo a otros.
- Una descripción de la instrumentación del sistema.
- Las especificaciones técnicas de funcionamiento del sistema así como las inspecciones que requiere.
- El plan de mantenimiento del sistema, incluyendo el tiempo que se espera que el sistema esté indisponible por mantenimiento.

- Una descripción de las diferentes configuraciones del sistema. Se han de detallar los sistemas soporte e incluir una matriz de dependencia entre sistemas para cada configuración.
- Una descripción de las interfases entre el sistema estudiado y otros sistemas.
- Un diagrama simplificado del funcionamiento del sistema que incluya todos los componentes clave.
- Las bases e hipótesis de modelización del sistema.

Este último apartado del análisis de sistemas es particularmente importante porque conecta todo el análisis anterior con el desarrollo de la modelización del árbol de fallos correspondiente.

2.4.5.1. Árbol de fallos

La metodología de árbol de fallos es un método de análisis lógico-deductivo que estudia la relación entre la ocurrencia de un suceso no deseado, llamado comúnmente *top event*, y todas sus posibles causas, ya sean sucesos independientes e indivisibles, los llamados sucesos básicos [9] (comúnmente *basic events*), o combinaciones de éstos. La relación entre el suceso no deseado y sus posibles causas se estudia mediante las puertas lógicas XOR, NOR, NAND, y, principalmente, AND y OR. El resultado es una estructura en árbol invertido o piramidal que presenta en la cúspide el *top event* del que cuelgan puertas lógicas hasta llegar a los sucesos básicos. La figura 2.4 presenta un ejemplo de árbol de fallos.

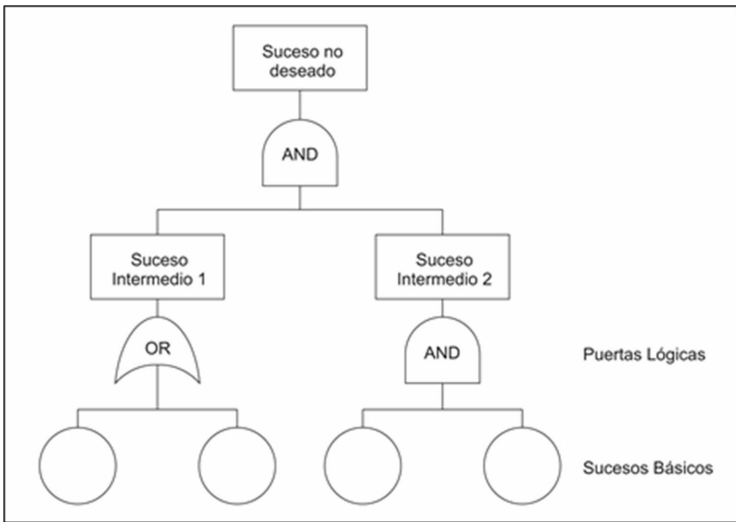


Figura 2.4: Ejemplo de árbol de fallos

En el marco del APS de nivel 1 de sucesos internos a potencia, los árboles de fallo se construyen para determinar las causas de fallo o indisponibilidad de los sistemas de seguridad que conforman los cabeceros de los árboles de sucesos, y, posteriormente, hallar la probabilidad de que estos sistemas estén indisponibles o hayan fallado. Las siguientes consideraciones se han de tener en cuenta al modelizar el árbol de fallos de un sistema de seguridad:

- El criterio utilizado en la modelización del fallo de un sistema ha de ser el inverso del criterio de éxito del sistema tenido en cuenta en la delineación de las secuencias de accidente. Hay casos en los que un mismo sistema de seguridad puede tener diferentes criterios de éxito, que dependen del suceso

[9] Un suceso básico representa un fallo elemental de un componente, es decir, un fallo que no se puede desarrollar en unidades básicas. La probabilidad o frecuencia de los sucesos básicos es conocida o puede estimarse.

iniciador analizado o de la secuencia de sucesos previa a la intervención del sistema. En estos casos, se pueden construir más de un árbol de fallos del mismo sistema o se pueden utilizar los llamados sucesos casa (comúnmente *house events*). Los sucesos casa son interruptores lógicos que activan o desactivan parte del árbol de fallos según el propio estado del suceso casa.

- El árbol de fallos ha de incluir tanto todos los componentes del sistema de seguridad modelizado como todos los componentes de sistemas soporte que se requieran en la operación del sistema. Además, se deben incluir todos aquellos componentes pasivos cuyos fallos podrían derivar en el fallo del sistema.
- El árbol de fallos debe desarrollarse hasta el punto que los sucesos básicos representen fallos independientes de componentes individuales o fallos humanos. Los fallos de componentes pueden ser: fallo en la demanda (arranque, cambio de estado, operación específica en un instante determinado, etc.), fallo en reserva (fallo durante periodo no operacional) o fallo en operación (fallo durante funcionamiento). Los árboles de fallo deben ser lo más completos posibles y deben incluir todos los sucesos básicos que deriven, ya sea de forma directa o en combinación con otros, en la ocurrencia del *top event*.
- Los diferentes tipos de posibles dependencias entre componentes (ver página 58 de la referencia [21]) han de modelarse de forma explícita. Concretamente, los fallos de causa común entre componentes redundantes de un mismo sistema o de diferentes sistemas son particularmente importantes porque pueden derivar en el fallo total del sistema.
- El árbol de fallos ha de incluir sucesos básicos para representar la indisponibilidad de componentes o trenes de componentes debida a actividades de mantenimiento.

El árbol de fallos es una metodología que permite plasmar de forma cualitativa las diferentes causas de un suceso no deseado mediante una estructura piramidal formada por puertas lógicas y sucesos básicos. Además, el árbol de fallos permite utilizar el álgebra de Boole para conocer las diferentes combinaciones de sucesos básicos que derivan en la ocurrencia del suceso no deseado. En consecuencia, se puede estimar la probabilidad de ocurrencia del suceso no deseado, siempre y cuando a los sucesos básicos se les asignen las probabilidades de fallo de los componentes representados. La tarea que se encarga de proporcionar las probabilidades de fallo de los sucesos básicos en el marco del APS de nivel 1 de sucesos internos a potencia es el Análisis de datos.

2.4.6. Análisis de datos

Las representaciones gráficas que resultan del análisis de secuencias de accidente y del análisis de sistemas, es decir, los árboles de sucesos y de fallos, constituyen el denominado modelo APS cualitativo. El modelo cualitativo ha de ser alimentado por datos numéricos para poder obtener resultados en términos de frecuencia de daño al núcleo u otras figuras de riesgo. Estos datos numéricos son, en su mayoría, parámetros de fiabilidad de componentes[10] y frecuencias de ocurrencia de sucesos. Es objeto de la tarea de Análisis de datos el proporcionar los datos numéricos con los que se ha de alimentar el modelo APS para poder estimar la FDN. Concretamente, los datos a proporcionar mediante la realización del Análisis de datos se dividen en dos grupos:

- Frecuencias de sucesos iniciadores.
- Datos representativos de sucesos básicos, que se dividen en:
  - Indisponibilidades por pruebas y mantenimiento.

[10] Entiéndase como parámetro de fiabilidad de un componente la probabilidad de fallo en demanda y/o la tasa de fallo del mismo.

- Sucesos básicos de probabilidad de fallo independiente.
- Sucesos básicos de probabilidad de fallo de causa común.
- Probabilidades de error humano.
- Sucesos especiales [11].

La tarea de Análisis de datos es sumamente exigente y extensa pues abarca el tratamiento de una gran cantidad de datos que, además, provienen de diversas fuentes. Además, la confianza en, y los usos de, los resultados del APS depende en gran medida de la rigurosidad con la que se realice esta tarea, puesto que es la que proporciona la base cuantitativa para la estimación de los resultados en forma de figuras de riesgo y de su incertidumbre. En consecuencia, la tarea de Análisis de datos es una de las más importantes del APS y una de las que más recursos requiere. En el marco de esta introducción a la metodología APS, la descripción de esta tarea se ciñe a presentar la metodología de estimación de la frecuencia de sucesos iniciadores, la metodología de elaboración de la base de datos de probabilidades de fallo independiente, y la metodología de análisis de fiabilidad humana.

2.4.6.1. Estimación de la frecuencia de sucesos iniciadores

Se le ha de asignar un valor de frecuencia anual de ocurrencia a todos los conjuntos de sucesos iniciadores modelados en el APS de nivel 1 de sucesos internos a potencia. A la hora de estimar la frecuencia de los sucesos iniciadores se suelen distinguir cuatro tipos de sucesos:

- Sucesos que nunca han ocurrido en la industria nuclear, como por ejemplo "rotura de vasija" o "rotura múltiple de tubos del generador de vapor". Al no disponer de experiencia operativa, se suele acudir a fuentes de datos genéricas o al juicio de expertos para calcular la frecuencia. Estos sucesos suelen tener un nivel de incertidumbre alto.
- Sucesos que han ocurrido al menos una vez en el marco de la industria nuclear, como por ejemplo "rotura de un tubo de un generador de vapor" o "rotura de líneas de agua de alimentación principal" . En este caso, la frecuencia se calcula teniendo en cuenta el número de sucesos ocurridos y el tiempo de operación de todas las plantas tecnológicamente asimilables a las que han sufrido el suceso.
- Sucesos frecuentes o relativamente frecuentes. Por ejemplo, "disparo del reactor" o "pérdidas de energía eléctrica exterior". Normalmente, la frecuencia se determina mediante la experiencia de la propia central nuclear analizada.
- Sucesos iniciadores relacionados con características singulares de diseño. Abarca aquellos sucesos que dependen del diseño de los sistemas de la propia central, como por ejemplo "pérdida del sistema de refrigeración de componentes" o "pérdida del sistema de agua de servicios esenciales". La frecuencia de estos sucesos iniciadores se estima mediante árboles de fallos. Se ha de revisar que la predicción del árbol de fallos sea consistente con la experiencia operativa.

En aquellos casos en que un grupo de sucesos iniciadores independientes constituya un solo conjunto de análisis, la frecuencia de ocurrencia del conjunto ha de ser la suma de las frecuencias de ocurrencia de los sucesos iniciadores que forman el grupo. Respecto al valor de frecuencia de ocurrencia, en todos aquellos casos en los que sea posible, el valor proporcionado por esta tarea ha de ser un valor promedio acompañado de una distribución estadística que indique el nivel de incertidumbre de la frecuencia de ocurrencia.

[11] Los Sucesos Especiales son aquellos que no se pueden incluir en ninguna otra de las categorías anteriores porque dependen de la evolución dinámica de la planta o de la configuración establecida, o bien, suponen simplificaciones de los modelos APS. Los sucesos de equiprobabilidad son un ejemplo de este tipo de sucesos.

2.4.6.2. Base de datos de probabilidades de fallo

En el desarrollo de la tarea de Análisis de datos se asignan probabilidades de fallo independiente o indisponibilidad a todos los componentes incluidos en el modelo APS. Con este objetivo, se construye una base de datos de probabilidades de fallo independiente en la cual se recopilan datos genéricos de probabilidad de fallo, datos específicos de probabilidad fallo, y las probabilidades de fallo o indisponibilidad de los componentes que definitivamente se utilizan en el APS. La creación de esta base de datos es una de las tareas que más controversia ha generado a lo largo del desarrollo de la metodología APS, convirtiéndose en una de las principales fuentes de desconfianza al respecto de la aplicación de la metodología. El motivo subyacente es que el contenido de la base de datos es la principal fuente de valoración cuantitativa de la incertidumbre epistémica[12] asociada al análisis. Por lo tanto, si el contenido de la base de datos no es fiable, tampoco lo son los resultados del APS.

A cada valor de probabilidad de fallo independiente o indisponibilidad incluido en la base de datos se le ha de asignar una distribución estadística que refleje la incertidumbre respecto al propio valor de probabilidad. Las primeras aplicaciones de la metodología APS fueron recibidas con escepticismo, en parte, por la ausencia de distribuciones de probabilidad, o por el uso de juicio de expertos para estimar distribuciones de probabilidad. Las distribuciones resultado del juicio de expertos de la época tenían una incertidumbre alta y eran difícilmente justificables. En consecuencia, la metodología de creación de la base de datos destacó como una característica importante del APS y se desarrolló sustancialmente a la par que la propia metodología APS. De hecho, una de las conclusiones extraídas del accidente de TMI-II fue la necesidad de desarrollar procedimientos de recopilación de la propia experiencia operativa [25], tanto para dar soporte al APS como para tener un registro de los hechos ocurridos en planta. De TMI hacia delante la industria nuclear ha mejorado ostensiblemente sus procedimientos de recogida de datos, lo que permite que actualmente las centrales tengan a su disposición una gran cantidad de datos de experiencia operativa, tanto propios como ajenos. Como resultado, se han creado multitud de bases de datos genéricas que dan soporte a la tarea de la creación de la base de datos de probabilidades de fallo específica de cada central. La gran cantidad de datos disponible hoy en día permite obtener estimaciones de distribuciones de probabilidad de fallo basadas solamente en la experiencia operativa de centrales nucleares. Por lo tanto, el escepticismo respecto a la metodología APS por causa de la fiabilidad de la base de datos ya no está justificado a día de hoy.

La metodología utilizada actualmente para la creación de la base datos de probabilidades de fallo independiente de componentes se divide en los siguientes pasos:

- Creación de una base de datos genérica.
- Creación de una base de datos específicos.
- Tratamiento de datos y estimación de probabilidad de fallo independiente.

Creación de una base de datos genérica

Uno de los principales objetivos del APS es que sea representativo de la realidad de la planta. Por lo tanto, las probabilidades de fallo de componentes han de reflejar la experiencia operativa de la planta motivo de análisis hasta el extremo posible. Sin embargo, la planta puede no disponer de información suficiente para determinar las probabilidades de fallo independiente de todos los componentes modelados en el APS. Por ello, en función de los tipos de componentes y modos de fallo definidos en el Análisis de sistemas, se elabora una Base de Datos Genérica (BDG) que permite obtener parámetros de partida. La base de datos genérica se construye mediante la consulta a fuentes de datos externas, que se dividen en dos tipos según su procedencia:

[12] La incertidumbre epistémica representa la falta de conocimiento al respecto del valor de un parámetro.

- Fuentes de datos de sucesos ocurridos en diversas plantas, cuyos estimadores puntuales e incertidumbre han sido o deben ser calculados.
- Fuentes de datos cuyas estimaciones se basan en el juicio de expertos.

Para una estimación de datos lo más realista posible se han de elegir fuentes basadas en análisis de datos reales con preferencia sobre las basadas en estimadores de parámetros basados en el juicio de expertos. Hoy en día, existen multitud de bases de datos genéricas basadas en datos reales. Una de las más importantes es la base de datos EPIX, (Equipment Performance Information Exchange System), creada y mantenida por INPO (Institute of Nuclear Power Operations), sobre la que se basa el NUREG/CR-6928 [52][13], la Base de Datos Genérica de las CC.NN.EE [53], desarrollada en el marco del Programa Integrado de 1986, y la aplicación RADS (Reliability and Availability Data System) [54] también de la NRC. La aplicación RADS es una base de datos genérica presentada en aplicación web que se actualiza periódicamente, y que contiene datos desde 1997 hasta el presente.

Para la elaboración de la base de datos genérica, se elige inicialmente una base de datos de referencia que incluya la mayor parte de los componentes modelados en el APS y sus modos de fallo. Mediante el uso de una base de datos de referencia se garantiza que la base de datos genérica sea lo más homogénea posible, ya que en cada fuente de datos se utilizan unos criterios ligeramente distintos para estimar el valor de las probabilidades de fallo. En el caso de que para algún tipo de componente y su modo de fallo no existiesen datos en la fuente de referencia, se toman los valores de otras base de datos siguiendo el criterio de obtener una base de datos genérica que aglutine datos provenientes de experiencia operativa. Si para algún componente no existiese ningún tipo de dato, ni proveniente de experiencia operativa ni de juicio de expertos, se pueden tomar valores de parámetros de distribuciones de probabilidad de otros componentes que se juzgue cubran de forma apropiada la estimación de parámetros deseada al tener características de fallo similares.

Creación de una base de datos específicos

En esta subtarea se analiza la experiencia operativa de la central nuclear con el objetivo de recoger información sobre los componentes relativa a la cantidad de fallos ocurridos y al número de demandas u horas de funcionamiento o espera. Estos datos sirven posteriormente para estimar los parámetros de fiabilidad de los componentes modelados en el APS. Ejemplos de la documentación a revisar para recoger los datos necesarios para la creación de la base de datos específicos son: base de datos de fallos de los equipos, órdenes de trabajo, base de datos de indisponibilidades de equipos, informes de sucesos notificables, e informes sobre incidentes operativos.

Debe remarcarse que para el análisis de fallos sólo se considera fallo completo aquel fallo que impide totalmente a un componente cumplir su función cuando es requerido. Por tanto, se consideran como 'no fallos' todas aquellas situaciones tales como degradaciones o fallos incipientes que puedan afectar al funcionamiento de un componente, cuando es requerido, sin llegar a impedirlo.

La información necesaria para la estimación de los parámetros de fiabilidad es agrupada, según el tipo de componente, de la siguiente forma:

- Número de fallos y número total de demandas para cada componente modelado en demanda, es decir, componentes que se espera que entren en funcionamiento o cambien de estado en una secuencia de accidente.
- Número de fallos y tiempo en espera para cada componente modelado en espera, es decir, componentes que no se encuentran en funcionamiento durante la operación normal, pero que deben estar disponibles en caso de ser requeridos.

[13] El NUREG/CR-6928 es la última base de datos genérica publicada por la NRC. Presenta datos de un periodo aproximado de cinco años, 1998-2002.

- Número de fallos y tiempo total de operación de componentes modelados en misión, es decir, normalmente en funcionamiento y/o que deben funcionar durante un tiempo determinado en una secuencia accidental.

Esta información es necesaria para la estimación de los sucesos básicos de fallo independiente y de fallo de causa común, las indisponibilidades por pruebas y mantenimiento, y la gran mayoría de sucesos especiales. Sin embargo, cada una de las estimaciones se realiza por separado, sólo existiendo un nexo de unión entre los sucesos básicos de fallos de causa común y los de fallo independiente.

En la recopilación de datos específicos se puede dar la situación de que la cantidad de datos disponibles de algunos componentes resulte insuficiente para que se tenga la confianza de que los parámetros de fiabilidad de los mismos representan la realidad de planta. En estos casos, se crean una serie de grupos, llamados grupos bayesianos, para aglutinar datos bajo un mismo nombre y así tener unos parámetros de fiabilidad de componentes con un nivel de representación suficiente. Los criterios para definir estos grupos son:

- Se separan tipos de componentes y modos de fallo distintos.
- Siempre que sea posible, no se agrupan equipos de sistemas distintos.
- Se agrupan componentes con condiciones de operación que los hacen comportarse de forma similar ante la posibilidad de fallo.
- Siempre que sea posible, se agrupan por separado los equipos de seguridad y los de no seguridad.
- Se agrupan únicamente equipos con modos de fallo definidos homogéneos.

Una vez obtenidos los datos específicos de planta y haberse agrupado estos datos en familias, se procede a efectuar el tratamiento de datos. Mediante el tratamiento de datos se analizan de forma conjunta las base de datos genérica y de datos específicos, y se estiman los parámetros de fiabilidad que mejor representan la realidad de la planta para cada componente.

Tratamiento de datos

En los pasos anteriores se han obtenido dos bases de datos de fallo de componentes cuyo contenido proviene de dos fuentes marcadamente distintas. Por una parte, se ha conformado una base de datos genérica cuyo contenido proviene de fuentes externas que reúnen la experiencia operativa de diversas plantas. Por otra parte, se ha creado una base de datos específicos a partir del análisis de la experiencia operativa de la propia central. En consecuencia, se enfrenta una base de datos soportada por una gran cantidad de datos que no representan la realidad de planta, con una base de datos cuyo contenido representa la realidad de planta pero puede no ser suficiente, en cantidad, para estimar con confianza los parámetros de fallo de componentes.

El tratamiento de datos consiste en realizar un análisis de los datos recogidos para cada componente con el objetivo de decidir cuál es la mejor manera de obtener los parámetros de fiabilidad más representativos. En el tratamiento de datos se prioriza la utilización de los datos que representan la realidad de planta para que, a su vez, el modelo APS sea lo más representativo posible. No obstante, los datos reales de planta se utilizan en mayor o menor medida dependiendo de la cantidad de los mismos. Se utiliza, según la cantidad de datos reales existentes, una de estas tres metodologías para obtener los parámetros de fiabilidad del componente en cuestión: tratamiento genérico, tratamiento bayesiano, o tratamiento por estimación directa.

Se utiliza el tratamiento genérico para la estimación de los parámetros de fiabilidad de un componente cuando no existen datos reales de este componente. El tratamiento genérico consiste en utilizar únicamente la información contenida en la base de datos genérica para la estimación de los parámetros de fiabilidad.

Si existen datos reales de planta, pero estos datos no tienen la evidencia estadística suficiente, se utiliza el tratamiento bayesiano. La evidencia estadística es una cualidad poco concreta de los datos reales de fallo de un componente que está ligada a la cantidad de los mismos. Se considera que los datos reales de fallo de un componente tienen suficiente evidencia estadística si existe la cantidad suficiente de datos como para que expertos consensúen que los parámetros de fiabilidad resultantes del tratamiento de estos datos representan fielmente la realidad de la planta. Actualmente no existe ninguna metodología que valore de forma cuantitativa si los datos reales de fallo de un componente tienen suficiente evidencia estadística.

El tratamiento, o ajuste, bayesiano hace uso del Teorema de Bayes [55] para obtener los parámetros de fiabilidad de componentes. El teorema de Bayes permite actualizar el conocimiento que se tiene sobre una distribución de probabilidad (función prior) mediante la incorporación de resultados experimentales (función de verosimilitud) definiendo, de esta manera, una tendencia de comportamiento mediante una función de distribución conocida como función "a posteriori". En la aplicación del teorema de Bayes a la estimación de probabilidades de fallo de componentes de una central nuclear, los datos previos de probabilidad de una variable (función de distribución prior) provienen de la base de datos genérica. La función de verosimilitud empleada proviene de la base de datos específicos. En consecuencia, la función a posteriori obtenida mediante el teorema de Bayes es una combinación de los datos genéricos y los datos específicos en la que la distribución de probabilidad genérica se ajusta según lo ocurrido en planta.

Siempre que se dispone de datos de experiencia operativa con suficiente evidencia estadística se debe utilizar la estimación directa para obtener los parámetros de fiabilidad. De esta manera, los parámetros de fiabilidad describen exactamente el comportamiento histórico del componente. La estimación directa se aplica mediante las siguientes expresiones:

- Tasa de fallos [14]:

$$\lambda = \frac{n^{\text{o}} \text{ de fallos}}{n^{\text{o}} \text{ de horas}} \tag{2.1}$$

- Probabilidad de fallo:

$$p = \frac{n^{\text{o}} \text{ de fallos}}{n^{\text{o}} \text{ de demandas}} \tag{2.2}$$

La frontera entre los diferentes tratamientos de datos es difusa puesto que depende de la evidencia estadística de los datos específicos de los componentes. Hoy en día no existen metodologías que permitan decidir con seguridad cuál es el mejor tratamiento, bayesiano o estimación directa, a utilizar en cada caso. Sin embargo, en la base de datos genérica de las centrales nucleares españolas se incluyen unas directrices para elegir el tratamiento de datos a utilizar:

- Para componentes con cero fallos, se realizará estimación directa si el número de demandas u horas de operación es mayor o igual a tres veces el inverso de la probabilidad o tasa de fallos genérica. En este caso, la estimación directa será el resultado de dividir la unidad entre dos veces el número de demandas u horas de operación. En caso de no cumplirse el criterio, se utiliza el tratamiento bayesiano si existen datos de experiencia operativa de la planta.
- Para componentes con un solo fallo, se realizará estimación directa si el número de demandas u horas de operación es mayor o igual que el inverso de la probabilidad o tasa de fallos genérica, respectivamente. En caso de no cumplirse el criterio, se utiliza el tratamiento bayesiano.
- Para componentes con dos o más fallos, se aplicará estimación directa siempre. En este caso, se podría justificar la desviación de este criterio siempre y cuando se demuestre que no existe suficiente evidencia estadística por la escasez en el número de demandas u horas de operación acumuladas.

[14] La tasa de fallos es el parámetro de fiabilidad principal de los componentes que operan de forma constante. La tasa de fallo de un componente es el cociente entre el número de fallos que ha sufrido el componente y el tiempo durante el cual el componente ha estado operando.

2.4.6.3. Análisis de fiabilidad humana

La experiencia de la industria nuclear demuestra que el error humano ha sido y es uno de los factores que contribuye en mayor medida a la ocurrencia y progresión de accidentes. Así lo pone de manifiesto el hecho de que varias de las causas de los accidentes de TMI-II y Chernobyl fueron acciones o decisiones humanas. En consecuencia, reducir al máximo la probabilidad de ocurrencia de errores humanos ha sido y es uno de los principales objetivos de la industria nuclear. Con este objetivo, a lo largo del avance de la industria nuclear se han desarrollado programas de entrenamiento, procedimientos, cadenas de mando, y estructuras de gestión, entre otros, para reducir la influencia en la seguridad del factor humano. A pesar del desarrollo de estos métodos, la realización de análisis de fiabilidad humana en el marco de análisis probabilistas de seguridad ha demostrado que no se puede obviar la contribución del factor humano al riesgo de la central [24].

El Análisis de Fiabilidad Humana, comúnmente conocido como HRA (Human Reliability Analysis), enmarca todas las técnicas y metodologías utilizadas para analizar sistemáticamente las acciones y operaciones que el personal de planta ha de llevar a cabo en situaciones específicas bajo condiciones específicas. El objetivo del HRA es identificar, describir, evaluar, y cuantificar la probabilidad de ocurrencia de los diferentes errores humanos que puedan ocurrir al realizar estas acciones y operaciones, que no incluyen acciones malévolas. El HRA se aplica en el marco del APS desde la realización del estudio WASH-1400, y hoy en día se incluye como tarea a obligatoria en los estándares y guías de aplicación del APS más importantes [38, 56, 21].

La respuesta del ser humano ante situaciones de emergencia no es fácil de predecir debido a la aleatoriedad intrínseca del comportamiento humano. Desde el nacimiento de la metodología APS, se han desarrollado multitud de metodologías de análisis de fiabilidad humana que, a diferencia de las metodologías de aplicación del APS que surgieron, son sustancialmente diferentes entre sí. Algunos de los métodos desarrollados centran el análisis en la evaluación de la probabilidad de fallo cognitivo[15], mientras que otros basan el análisis en la evaluación de la probabilidad de fallo manual[16]. Otros métodos combinan ambos tipos de fallo mediante árboles de sucesos, e incluyen en el análisis la influencia del contexto en la actuación humana. Hoy en día aún no se ha conseguido llegar a un consenso generalizado al respecto del análisis y cuantificación de la fiabilidad humana, y plantas bajo el mismo marco regulador utilizan metodologías de HRA diferentes [21]. No obstante, la experiencia adquirida en la aplicación de este tipo de análisis a lo largo de los años ha reducido la cantidad de métodos considerados como adecuados. Además, a pesar de cuantificar el error humano de formas diferentes, los métodos que han sobrevivido a la experiencia comparten las bases teóricas de modelización cualitativa del error humano, recogidas en un compendio de buenas prácticas publicado por la NRC [57]. Uno de los métodos de aplicción de HRA, de acceso abierto, más utilizados históricamente es el *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications* que presenta la *Technique for Human Error Rate Prediction* (THERP), incluida en el NUREG/CR-1278.

Las metodologías de análisis de fiabilidad humana han sido desarrolladas tradicionalmente para dar soporte a modelos APS de nivel 1 de sucesos internos a potencia. Esto implica que estas metodologías están especialmente preparadas para cuantificar probabilidades de error humano asociadas a acciones llevadas a cabo en situación de emergencia en el interior de la sala de control. Existe una falta evidente de metodologías para evaluar el fallo humano en situaciones diferentes como, por ejemplo, acciones de movimiento de combustible en el edificio de combustible. Esta tesis doctoral presenta en su segunda parte el desarrollo de una metodología de aplicación de análisis de fiabilidad humana novedosa. La metodología desarrollada es aplicable para el estudio de la actuación humana en el contexto de las operaciones a llevar a cabo para trasladar combustible gastado a un Almacén Temporal Individualizado.

[15] Fallo al tomar una decisión. El tiempo disponible para tomar la decisión influye significativamente en este tipo de fallo.
[16] Fallo de un operario a realizar una acción, ya sea por omisión de la misma o por cometer un error al realizarla.

2.4.7. Cuantificación

El modelo APS está preparado para ser cuantificado una vez la tarea de Análisis de datos se ha completado, es decir, una vez se han asociado frecuencias de ocurrencia a todos los sucesos iniciadores, y parámetros de fiabilidad a todos los sucesos básicos del modelo. La tarea de cuantificación requiere gestionar y utilizar una gran cantidad de datos por lo que se hace necesario realizarla mediante un software informático. El modelo cualitativo definido en tareas anteriores ha de ser, si no lo ha sido ya, volcado en este software, que está preparado para que el usuario pueda delinear y cuantificar modelos APS. De la misma forma, el resultado de la tarea de Análisis de datos también se introduce en el software para poder proporcionar resultados cuantitativos. El software informático utilizado para delinear y cuantificar modelos APS en el marco de esta tesis doctoral es RiskSpectrum® de Lloyd's Register Group.

La tarea de cuantificación tiene dos objetivos principales: obtener las ecuaciones booleanas de daño al núcleo de las secuencias de accidente de interés y de toda la planta, y obtener las frecuencias de daño al núcleo de las secuencias de accidente de interés y la asociada a toda la planta. Las ecuaciones booleanas son el resultado de aplicar el álgebra de Boole al modelo APS cualitativo, y son la base para la posterior cuantificación de las frecuencias de daño al núcleo. Las ecuaciones contienen todas las posibles combinaciones de sucesos iniciadores y sucesos básicos que llevarían a daño al núcleo en caso de ocurrir. Mediante el álgebra de Boole se aplica toda reducción posible a las ecuaciones booleanas para que las combinaciones que las acaben conformando sean las combinaciones mínimas de sucesos que llevan a daño al núcleo. A las combinaciones mínimas de sucesos que llevan a daño al núcleo se les llama Conjuntos Mínimos de Fallo (CMF) (comúnmente, Minimal CutSets (MCS)), y son el producto de la frecuencia de ocurrencia de un suceso iniciador y la probabilidad de fallo de uno o diversos componentes de los sistemas frontales y/o soporte. Una ecuación booleana reducida se expresa como un sumatorio de CMFs. La frecuencia de daño al núcleo asociada a una ecuación se obtiene introduciendo todas las frecuencias de sucesos iniciadores y probabilidades de fallo de componentes en los conjuntos mínimos de fallo, y, posteriormente, resolviendo la ecuación.

La cantidad de CMFs resultante acostumbra a ser considerable debido al detalle y complejidad del modelo APS cualitativo. En consecuencia, la tarea de obtener todos los CMFs y posteriormente cuantificarlos para obtener la frecuencia de daño al núcleo puede llevar una cantidad ingente de tiempo. No obstante, una proporción de los CMFs son combinaciones de sucesos de muy baja probabilidad. Para reducir el tiempo de análisis, se impone un valor de truncamiento para la frecuencia de los CMF. Todo CMF cuya frecuencia sea menor que la del valor de truncamiento no se tiene en consideración en el análisis, lo que también significa su exclusión de la ecuación booleana analizada. El valor de truncamiento se ha de justificar adecuadamente para demostrar que no deja fuera del análisis combinaciones de sucesos cuya contribución al riesgo sea importante.

La cuantificación es habitualmente un proceso iterativo puesto que los CMFs que forman las ecuaciones booleanas que representan el riesgo de la central se revisan en profundidad. Cualquier cambio producto de esta revisión obliga a recuantificar el modelo APS. Las revisiones típicas de CMFs que se llevan a cabo en la tarea de cuantificación son las siguientes:

- Post-proceso de los CMFs para garantizar que todos los incluidos en las ecuaciones booleanas llevan a daño al núcleo.
- Post-proceso para garantizar que no haya CMFs que contengan sucesos básicos que se excluyan mutuamente.
- Identificación de posibles acciones humanas de recuperación para posteriormente introducirlas al modelo.
- Identificación de dependencias entre acciones humanas para tratarlas posteriormente.

2.4.8. Análisis de resultados

El análisis de resultados de un APS tiene por objetivo obtener figuras de interpretación de los resultados que proporcionen información adicional a la representada por las frecuencias de daño al núcleo. Por lo tanto, el análisis de resultados va más allá de una mera ordenación de las frecuencias de daño al núcleo de las secuencias de accidente. Las figuras de interpretación de resultados facilitan la evaluación del diseño y operación de la central, así como del propio modelo APS. El análisis de resultados se divide en tres tareas: análisis de importancia, análisis de incertidumbre, y análisis de sensibilidad.

2.4.8.1. Análisis de importancia

El objetivo del análisis de importancia es la obtención de distintas figuras numéricas, llamadas medidas de importancia, que faciliten la identificación de los principales contribuyentes al riesgo de la central. El análisis de importancia se puede aplicar a sucesos básicos, grupos de sucesos básicos, parámetros de fiabilidad, sucesos iniciadores, y otros conjuntos que se quieran analizar. Las medidas de importancia son figuras cuantitativas que valoran la contribución del ente estudiado a la frecuencia de daño al núcleo o medida de riesgo analizada en el APS. A modo de ejemplo se presentan dos de las medidas de importancia más utilizadas [58]: la importancia *Fussell-Vesely* y la figura *Risk Achievement Worth* (RAW).

La medida de importancia de *Fussell-Vesely* de un suceso básico es el cociente entre la frecuencia de la ecuación booleana referencia (R_{base}) menos la frecuencia que tendría la misma si se asignase cero a la probabilidad del suceso (R_0), dividido por la frecuencia de la ecuación de referencia(R_{base}) . Los valores que adopta esta medida de importancia van de cero a uno y puede interpretarse como la contribución fraccional de los conjunto mínimos de fallo que contienen el suceso básico motivo de análisis a la frecuencia de la ecuación de referencia.

$$FV = \frac{R_{base} - R_0}{R_{base}} \tag{2.3}$$

La medida de importancia RAW de un suceso básico es el cociente entre la frecuencia de la ecuación booleana calculada considerando el suceso básico de análisis como ocurrido[17] (R_1) dividida por la frecuencia de la ecuación booleana referencia (R_{base}) . La medida RAW adopta valores entre 1 e infinito, e indica por cuánto se multiplicaría la FDN, o la medida de riesgo utilizada, si el suceso básico ocurriese.

$$RAW = \frac{R_1}{R_{base}} \tag{2.4}$$

Las medidas de importancia son una de las bases cuantitativas de los estudios de evaluación detallada del diseño y operación de la central y, además, se utilizan en la mayoría de aplicaciones de APS. En consecuencia, el análisis de importancia es una de las tareas más importantes y con mayor valor añadido del APS.

2.4.8.2. Análisis de incertidumbre

Los parámetros de fiabilidad de componentes y las frecuencias de sucesos iniciadores seleccionados en el Análisis de datos están sujetos a incertidumbre epistémica, es decir, incertidumbre respecto al desconocimiento del valor puntual de estos parámetros. Por lo tanto, en la tarea de Análisis de datos se les ha asignado una distribución estadística que representa de la manera más fiel posible esta incertidumbre epistémica. Consecuentemente, se desarrolla el Análisis de Incertidumbre con el objetivo de propagar

[17] Cuando se considera que un suceso básico ha ocurrido se le asigna una probabilidad de fallo igual a 1 o el estado *TRUE*.

la incertidumbre asociada a cada suceso básico en las ecuaciones de conjuntos mínimos de fallo en que intervienen para obtener la distribución estadística de la variable aleatoria que representa la FDN de la ecuación en cuestión. Actualmente, la incertidumbre de los sucesos básicos se propaga haciendo uso de técnicas Monte Carlo.

Conocer la incertidumbre epistémica de los resultados permite valorar su aceptabilidad y su posible uso en aplicaciones de apoyo a la toma de decisiones basada en el riesgo. Frecuencias de daño al núcleo asociadas a incertidumbre significativas no son apropiadas para procesos de toma de decisiones y, además, pueden ser rechazadas como representación del riesgo de la planta.

Además de la incertidumbre epistémica de los parámetros de fiabilidad, existen otros dos tipos de incertidumbre en el APS de nivel 1 de sucesos internos a potencia [21]. El primero de estos tipos de incertidumbre está relacionado con la integridad del modelo y con el hecho de que no se puede asegurar que el modelo incluya todas las secuencias de accidente posibles. El otro tipo deriva de la modelización de sistemas y secuencias, y está relacionado con la falta de conocimiento al respecto de los métodos, modelos, hipótesis, y aproximaciones utilizadas en el APS. La incertidumbre estimada en esta tarea de análisis no incluye estos otros dos tipos, que han de ser valorados mediante otros medios, si es posible, para tenerlos en cuenta en la evaluación de los resultados del modelo.

2.4.8.3. Análisis de sensibilidad

El objetivo del análisis de sensibilidad es evaluar la sensibilidad de los resultados del APS ante las hipótesis y aproximaciones utilizadas en la modelización del APS. Es decir, los análisis de sensibilidad miden cómo cambia la FDN, o la medida de riesgo utilizada, si se modifica alguna de las hipótesis y aproximaciones del modelo. Los análisis de sensibilidad son, por lo tanto, una manera de evaluar el segundo tipo de incertidumbre mencionado en el apartado anterior. De manera similar al análisis de incertidumbre, los resultados de los análisis de sensibilidad se utilizan principalmente para indicar el grado de confianza a depositar en los resultados del APS.

Una análisis de sensibilidad corresponde a un cambio aislado en las hipótesis y aproximaciones del modelo APS. Se ha de evitar el análisis simultaneo de varios cambios de hipótesis para no enmascarar las conclusiones asociadas a cada cambio. Por este motivo, un APS acostumbra a contener una cantidad sustancial de análisis de sensibilidad. Algunos ejemplos de análisis de sensibilidad son:

- Cambio del límite de truncamiento de la cuantificación para comprobar que no quedan CMFs importantes fuera del análisis.
- Variación de las hipótesis de modelización de errores humanos.
- Variación de los tiempos en misión de algunos sistemas de seguridad incluidos en el análisis.

2.5. Conclusiones

La metodología de análisis probabilista de seguridad lleva en estado de desarrollo desde finales de los años sesenta. La complejidad de los modelos generados mediante el APS, la diversidad de alcances, y la adaptación a nuevas tecnologías y enfoques son los principales motivos por los cuales la metodología APS aún sigue en desarrollo. No obstante, que el APS siga en desarrollo no debe entenderse como un aspecto negativo o un estancamiento de la metodología, si no como una señal de la confianza que la industria nuclear tiene depositada en ella. Una clara muestra de esta confianza es que la metodología se ha sobrepuesto al escepticismo con el que fue recibida en sus inicios, especialmente debido a la falta de confianza en los datos de fallo utilizados y en el tratamiento de incertidumbres. El desarrollo del APS avanza de forma consistente y ya se han resuelto, en gran medida, los problemas que eran fuente de

escepticismo. Hoy en día el APS es considerado uno de los pilares del análisis de seguridad y se reconoce su potencial para ser usado en otros campos. Además, organizaciones internacionales de gran peso como el regulador americano, NRC, y la IAEA, tienen en marcha planes de desarrollo e integración de la metodología APS en el campo de la toma de decisiones.

Las principales virtudes del análisis probabilista de seguridad son su capacidad para modelar la planta de forma realista, la posibilidad de identificar debilidades de diseño y operación desde el punto de vista de seguridad, y la posibilidad de crear aplicaciones basadas en los resultados del APS. Si el desarrollo del APS avanza según lo previsto por organismos reguladores y licenciatarios, en un futuro próximo las centrales nucleares utilizaran múltiples aplicaciones APS para dar soporte a la toma de decisiones en varios campos de la gestión de las centrales. Además, los organismos reguladores utilizaran el APS en el diseño del marco regulador, y en el diseño de los criterios y requisitos a cumplir por las centrales. En conclusión, el APS avanza con paso firme hacia su integración total en la industria nuclear mediante un uso intensivo de la metodología que irá más allá del análisis de seguridad. En el siguiente capítulo se repasa el uso del APS en el marco del desarrollo de aplicaciones de soporte a la toma de decisiones destacándose varias de las aplicaciones APS que ya son de uso común en la industria nuclear.

Capítulo 3

Toma de decisiones informada por el riesgo

3.1. Introducción

Ya en su primera aplicación en el marco del estudio WASH-1400, se comprobó que el APS es una herramienta de análisis de seguridad cuya utilidad trasciende la cuantificación del riesgo global de la instalación. Tal y como se ha visto en la sección anterior, el APS destacó en sus inicios por su utilidad para identificar vulnerabilidades y deficiencias de seguridad en el diseño y operación de centrales gracias a la obtención de las ecuaciones booleanas de daño al núcleo de las secuencias de accidente. Tras el desarrollo de la metodología durante los años ochenta, culminado con la realización del estudio *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants*, publicado en 1990, creció el interés en la ampliación de usos del APS en el campo de la toma de decisiones informadas por el riesgo. A raíz de la normalización del APS en la industria, la NRC promulgó en 1995 una política de ampliación de usos del APS [40], y lanzó un plan de implementación del APS en la industria y en el marco regulador que sigue vigente hoy en día. En la actualidad el plan de implementación del APS está dedicado a promulgar y ampliar el uso de aplicaciones APS en la toma de decisiones informadas por el riesgo. Por su parte, la IAEA también ha tenido un papel importante en el desarrollo de aplicaciones de APS para la toma de decisiones basada en el riesgo. Desde que la IAEA dedicase, en 1992, la sexta reunión del grupo INSAG al análisis probabilista de seguridad, ha publicado una gran variedad de documentos dedicados a aplicaciones de APS, entre los que destacan el TECDOC-1200 [56] y la tercera *Specific Safety Guide* [21].

Como resultado de los esfuerzos de la NRC, la IAEA, y otras organizaciones, se han desarrollado, o están en vías de desarrollo, multitud de aplicaciones que utilizan resultados del APS para dar soporte a la toma de decisiones tanto en temas de seguridad y operación, como en temas de gestión o de maximización de beneficios [56]. Es objetivo de este capítulo describir el proceso general de toma de decisiones informado por el riesgo, sección 3.2, y presentar algunas las aplicaciones más importantes desde el punto de vista de seguridad y operación, como, por ejemplo, los monitores de riesgo, las aplicaciones en soporte de la regla de mantenimiento, o las aplicaciones en soporte de la inspección de componentes, en las secciones 3.4, 3.5, 3.6, 3.7, 3.8, 3.9, y 3.10. Además, se describen, en la sección 3.3, las cualidades de un modelo APS que lo hacen apto para su uso en el desarrollo de aplicaciones para la toma de decisiones.

3.2. El proceso integrado de toma de decisiones informada por el riesgo

En los años 90, cuando se consideró que la metodología APS estaba lo suficientemente madura como para aplicarse de manera general [40], nació el concepto de la toma de decisiones basada en el riesgo. En un principio se pensó que bastaba con comparar métricas de riesgo proporcionadas por un APS con criterios de riesgo para tomar una decisión. No obstante, debido a las incertidumbres inherentes al análisis probabilista de seguridad, que podían enmascarar la importancia de algunos aspectos, se decidió incluir datos de otros análisis en la toma de decisiones basada en el riesgo [56]. De este modo, el concepto de proceso de toma de decisiones basado en el riesgo evolucionó al de proceso integrado de toma de decisiones informado por el riesgo.

El proceso integrado de toma de decisiones informado en el riesgo, comúnmente llamado *Integrated Risk Informed Decision Making Process* (IRIDM) [59], es un proceso sistemático de toma de decisiones que, como característica definitoria, integra todos los aspectos importantes de la seguridad de una central nuclear. Aplicando el IRIDM en la decisión al respecto de una cuestión postulada, se valoran las diferentes propuestas desde el punto de vista de cada uno de los aspectos tenidos en cuenta en el proceso. Posteriormente, se comparan dichas valoraciones, y, finalmente, se decide cuál es la mejor propuesta en base a la comparación previa. Uno de los aspectos incluidos en la toma de decisiones del IRIDM es la información relativa al riesgo que pueda proporcionar el APS o aplicaciones APS. Una de las mayores ventajas de la aplicación del proceso IRIDM es que aporta transparencia a la toma de decisiones complejas al implicar la valoración de varios factores clave. De esta manera, las decisiones tomadas mediante el proceso IRIDM pueden ser revisadas y reconsideradas si se consdiera oportuno. La aplicación del proceso IRIDM en la toma de decisiones forma parte de los estándares de seguridad de la IAEA [60], de la guía de seguridad 1.14 del CSN [61], y de la *regulatory guide* 1.174 de la NRC [22]. Actualmente, existen ejemplos de la aplicación del proceso IRIDM en un amplio espectro de cuestiones, que incluyen: diseño, licenciamiento, supervisión, operación, mantenimiento, pruebas, preparación de personal, modificaciones de diseño, extensión de vida, planificación de enmergencias, y otros. La figura 3.1 presenta el diagrama de flujo del proceso IRIDM y los diversos aspectos y análisis que se tienen en cuenta en su aplicación.

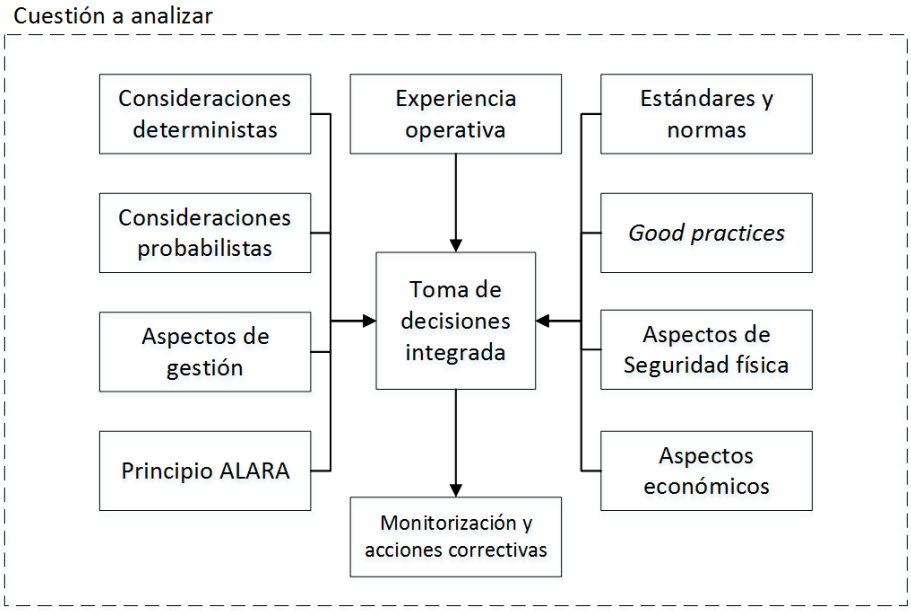


Figura 3.1: Proceso integrado de toma de decisiones informado en el riesgo

Una vez definida la cuestión de análisis, se establecen los aspectos de seguridad a tener en cuenta en el proceso de decisión. Los aspectos de seguridad integrados en el proceso IRIDM acostumbran a ser los siguientes [59]:

- Estándares y normas del organismo regulador.
- Buenas prácticas de la industria nuclear. Incluye la valoración de las decisiones tomadas en casos similares en otras centrales.
- La experiencia operativa de la central y de centrales de diseño similar al respecto de la cuestión de análisis.
- Consideraciones deterministas, incluyendo el concepto de defensa en profundidad, márgenes de seguridad, y análisis de accidentes base de diseño, entre otros.
- Consideraciones probabilistas, que incluyen los resultados y las aplicaciones del APS. El APS y sus aplicaciones proporcionan medidas cuantitativas que son útiles para valorar las consecuencias de cambios y modificaciones. Tener en cuenta el resultado del análisis de incertidumbres integrado en el APS da más valor a cualquier decisión tomada mediante el IRIDM.
- Aspectos organizacionales y de gestión.
- Consideraciones sobre seguridad física.
- El principio ALARA (*As Low As (is) Reasonably Achievable*) para la gestión de la dosis recibida por el personal.
- Aspectos económicos.

Tomar decisiones utilizando el proceso IRIDM puede resultar complicado en algunas situaciones porque los requisitos y consideraciones de los diferentes aspectos de seguridad tenidos en cuenta no están expresados en los mismos términos. Por ejemplo, mientras que las consideraciones probabilistas proporcionan valores cuantitativos, otros aspectos tenidos en cuenta solo proporcionan información en términos cualitativos. En respuesta a este tipo de conflictos, es una buena práctica que el equipo de trabajo encargado de aplicar el proceso IRIDM sea multidisciplinar. Cada miembro del equipo de trabajo ha de ser un experto de, al menos, uno de los aspectos tenidos en cuenta en la toma de decisión. Considerando que la importancia relativa de cada aspecto tenido en cuenta depende de la cuestión analizada, el equipo de trabajo ha de inducir medidas de importancia que permitan valorar todos los aspectos de la decisión de forma conjunta. Este proceso de inducción depende de la cuestión considerada y, por lo tanto, no existe un procedimiento general común a todas las aplicaciones de IRIDM.

El proceso IRIDM es iterativo en tanto que cualquier decisión que se tome es reanalizada desde el punto de vista de todos los aspectos considerados en el proceso para garantizar que se cumplen los requisitos y criterios postulados por todos ellos. La decisión tomada se implementa si supera positivamente el proceso de reanálisis. No obstante, el proceso IRIDM no termina con la implementación de la decisión. Tal y como plasma la figura 3.1, el proceso IRIDM también abarca la monitorización de la solución implementada y toma de cualquier acción correctiva necesaria para conseguir el resultado deseado.

3.3. La calidad de un APS

Desde el punto de vista de las aplicaciones de APS para la toma de decisiones informadas por riesgo, la calidad de un APS se resume en que el modelo utilizado tenga las características suficientes como para poder confiar en los resultados y conclusiones extraídas de la aplicación en el marco del IRIDM. Concretamente, en el plan de implementación de la calidad del APS de la NRC [41], se detalla que la calidad de un APS utilizado para dar soporte a una aplicación se mide en términos de la idoneidad del alcance, el nivel de detalle, y la aceptabilidad técnica del APS.

3.3.1. La idoneidad del alcance

El APS utilizado en el desarrollo de aplicaciones para la toma de decisiones informadas por el riesgo debería ser de alcance total para que la confianza en los resultados fuese máxima [21]. Sin embargo, no disponer de un APS de alcance total no debe implicar la imposibilidad de realizar aplicaciones [61]. Se ha de evaluar, para cada tipo de aplicación, si el alcance del APS referencia es suficiente para permitir la toma de decisiones en el marco del proceso IRIDM. Por ejemplo, un APS de nivel 1 a potencia puede ser suficiente para aplicaciones enfocadas al análisis de sistemas de mitigación de accidentes. En caso contrario, las carencias del APS referencia se pueden suplir mediante ampliaciones del alcance, o bien mediante la utilización de herramientas complementarias que cubran el alcance adicional necesario para que la aplicación sea correcta. Ejemplos de técnicas complementarias son: Análisis de ingeniería, paneles de expertos, y análisis de modos de fallo y efectos [61, 62]. En cualquier caso, si el alcance del APS no es el exigido por el uso de la aplicación existen incertidumbres asociadas a este hecho. Estas incertidumbres deberían estar controladas y, si es posible, cuantificadas mediante la realización de análisis de sensibilidad.

3.3.2. Nivel de detalle

El nivel de detalle del APS requerido depende de los objetivos de la propia aplicación, según se realice un análisis de riesgo a nivel de componente, equipo, o bien, tren o sistema. No obstante, el uso de un APS con un alto nivel de detalle facilita el uso de cualquier aplicación [21]. En casos en los que el nivel de detalle sea insuficiente, la aplicación puede completarse mediante la utilización de otros inputs como, por ejemplo, el juicio de expertos. A continuación se detallan las principales características de un APS que hacen que su nivel de detalle sea suficiente para que su utilización en aplicaciones sea efectiva [21]:

- El APS debe tener en cuenta las dependencias más significativas, tanto funcionales y operacionales como en cuanto a procedimientos.
- El APS debe reflejar de forma realista las características de diseño y operación de la central. En caso de existencia de conservadurismos en un modelo APS que afecten a una aplicación, se deberían realizar análisis de sensibilidad que permitan determina la influencia de éstos en los resultados.
- El APS debe tener elementos que puedan modificarse, de forma sencilla, para representar el cambio que se quiera evaluar mediante la aplicación.

3.3.3. Aceptabilidad técnica del APS

El APS debe haberse diseñado y debe ser mantenido de acuerdo con unos requisitos mínimos para ser técnicamente aceptable en el marco de desarrollo de aplicaciones para la toma de decisiones informada en el riesgo. Los principales requisitos mínimos que ha de cumplir un APS para ser técnicamente aceptable son:

- El modelo APS debe ser mantenido y actualizado con frecuencia para garantizar que continúa reflejando la realidad de la planta [61]. El modelo ha de representar el estado *as-designed*, *as-built*, y *as-operated* de la planta [63].
- El modelo APS se ha de desarrollar en concordancia con la experiencia y las buenas prácticas de la industria [63]. En caso de utilizarse métodos o técnicas innovadoras estos deben apoyarse de análisis que demuestren su idoneidad y sus beneficios.
- Las probabilidades de fallo y frecuencias de sucesos usadas en el modelo APS se han de estimar de forma consistente con las definiciones de los sucesos básicos y los sucesos iniciadores incluidos en el modelo.

- La base de datos ha de estar preparada para permitir la realización de análisis de incertidumbre y sensibilidad.

Además de los aquí mencionados, la *regulatory guide* 1.200 [63] presenta una lista de requisitos técnicos a cumplir en la realización de las tareas que conforman los APS de nivel 1 y nivel 2.

3.4. Monitor de riesgos

Un monitor de riesgos es una herramienta de análisis en tiempo real que proporciona información al respecto del riesgo de la planta mediante el uso de un modelo de análisis probabilista de seguridad. La información cuantitativa proporcionada por el monitor de riesgos depende del alcance del APS referencia, ya sea éste de nivel 1, nivel 2, o nivel 3. La información al respecto del riesgo proporcionada por el monitor representa la configuración actual de la planta, que depende de varios factores:

- El estado operacional de planta (a Potencia u Otros Modos).
- Los componentes que no están disponibles por causa de fallos, mantenimiento, pruebas, o inspección.
- La elección de trenes[1] en operación y trenes en espera para aquellos sistemas que están normalmente en operación.

En el desarrollo de un monitor de riesgos es muy importante que el modelo APS de referencia cumpla con los requisitos de calidad para el nivel de detalle y la aceptabilidad técnica del APS. Es especialmente importante que el APS de referencia, y, en consecuencia, el modelo APS del monitor de riesgos, sean mantenidos y actualizados con la frecuencia adecuada.

Tener en cuenta la configuración de planta en la generación de información al respecto del riesgo obliga a modificar el modelo APS de referencia, que está preparado para proporcionar el riesgo promedio de la planta. Se ha de generar un nuevo modelo APS que permita estimar de forma realista el riesgo de la planta en cualquiera de sus configuraciones posibles. Con dicho propósito, se han de reemplazar o eliminar todas aquellas hipótesis y simplificaciones introducidas en el modelo de referencia cuyo objetivo es facilitar la estimación del riesgo promedio de la planta. Ejemplos de hipótesis y simplificaciones a reemplazar son [21]:

- Sucesos iniciadores asociados a una configuración de planta promedio cuya frecuencia de ocurrencia es la suma de frecuencias de ocurrencia de los mismos sucesos iniciadores en diferentes configuraciones de planta han de ser reemplazados por sucesos iniciadores individuales para cada configuración. Por ejemplo, los sucesos iniciadores LOCA modelados como posibles en un único lazo del sistema de refrigeración del reactor han de ser reemplazados por sucesos iniciadores LOCA en cada lazo del sistema de refrigeración del reactor.
- La alineación de sistemas y la elección de trenes en operación y trenes en espera de sistemas normalmente en operación han de ser modeladas explícitamente.
- Los sucesos básicos incluidos en el modelo de referencia para tener en cuenta el mantenimiento de componentes y equipos han de ser eliminados o bien su probabilidad de ocurrencia ha de ser nula.

[1] Entiéndase por tren de un sistema a un conjunto de componentes que realizan una función específica. Los sistemas de seguridad de una central nuclear tienen varios trenes similares para realizar la misma función (concepto de redundancia) con el objetivo de cumplir con el criterio de fallo simple.

El software de monitor de riesgos es sustancialmente diferente a un software de APS porque el monitor es una herramienta cuyo propósito es ser utilizada por cualquier miembro del personal de la central nuclear. Además, el usuario de un monitor de riesgos ha de ser capaz tanto de informarse al respecto del nivel de riesgo de la planta como de introducir cambios en la configuración de planta que obliguen al modelo a recuantificar el riesgo. El software de monitor de riesgos ha de ser capaz de recuantificar el riesgo en no más de 5 minutos para que la herramienta sea efectiva [56]. La experiencia ha demostrado que la adaptación del modelo APS al software del monitor de riesgos puede requerir la modificación de la lógica del modelo APS [21] para facilitar la introducción de cambios y la cuantificación del propio modelo APS por parte del software del monitor de riesgos. Concretamente, una de los cambios habituales corresponde a reemplazar la estructura de árboles de eventos y árboles de fallos del modelo APS por un gran árbol de fallos equivalente [21].

El monitor de riesgos proporciona información relativa al riesgo, tanto cuantitativa como cualitativa, en un formato adecuado para que pueda ser entendida por la mayoría de usuarios potenciales de la herramienta. Normalmente, los softwares de monitor de riesgos hacen usos de códigos de colores y herramientas visuales como, por ejemplo, termómetros, para ofrecer una indicación visual del nivel de riesgo y el estado de los sistemas y funciones de seguridad. Las figuras de riesgo que se acostumbran a utilizar en monitores de riesgos son la frecuencia de daño al núcleo, el tiempo que la planta puede estar en la configuración actual sin alcanzar niveles elevados de riesgo de daño al núcleo, y la probabilidad condicionada[2] de daño al núcleo acumulada [21].

El monitor de riesgos puede ser utilizado para llevar a cabo diversos análisis aprovechando el hecho de que proporciona el nivel de riesgo de la planta en tiempo real. Algunos ejemplos son:

- El monitor de riesgos se puede utilizar para evaluar el riesgo de sucesos inesperados como, por ejemplo, fallos de equipos.
- Se puede utilizar para hacer un seguimiento del perfil del riesgo de la central a largo plazo y generar indicadores de actuación de las funciones y sistemas de seguridad basados en el riesgo.
- El monitor se puede utilizar para analizar la probabilidad de daño al núcleo acumulada condicionada a configuraciones de planta realistas.
- Se puede utilizar como herramienta para planificar acciones de mantenimiento y como herramienta para dar soporte a la regla de mantenimiento (véase la sección 3.6 para más detalle).

3.5. Especificaciones técnicas de funcionamiento informadas por el riesgo

Las Especificaciones Técnicas de Funcionamiento (ETF) de una central nuclear detallan los límites y condiciones de operación de la planta, el mantenimiento, y las pruebas de vigilancia a las que se han de someter los diferentes sistemas y equipos de la central. Las ETF describen un marco envolvente para la operación segura de la central que es consistente con la hipótesis y resultados de análisis de seguridad basados tradicionalmente en técnicas deterministas. Concretamente, las ETF contienen los siguientes datos:

- Requisitos al respecto de la operabilidad de componentes y sistemas. Las ETF detallan qué componentes han de estar en operación o en estado operable para considerar que un sistema se opera de forma segura. Por lo tanto, las ETF detallan aquellas configuraciones de planta que son aceptables.

[2] La probabilidad condicionada de daño al núcleo se define como la probabilidad de que ocurra daño al núcleo en caso de ocurrir un suceso iniciador. Es decir, si se considera que ha ocurrido un suceso iniciador, la probabilidad condicionada es la probabilidad de que fallen los sistemas de seguridad y mitigación necesarios para evitar el daño al núcleo. La probabilidad acumulada es la integral de la probabilidad a lo largo del tiempo.

- El *allowed outage time*, o tiempo de interrupción permitido, que se define como el máximo periodo de tiempo que un sistema o componente puede estar en mantenimiento, reparación, o en situación no operable. En caso de superarse este tiempo la central ha de tomar acciones correctivas.
- El procedimiento a seguir en las pruebas de sistemas relacionados con la seguridad y el intervalo de tiempo entre estas mismas pruebas. Si se supera el intervalo de tiempo entre pruebas, el componente o sistema se considera no operable.
- Las acciones correctivas que se han de tomar en caso de superar el tiempo de interrupción permitido o en caso de entrar en una configuración de planta no aceptable. Estas acciones correctivas pueden llegar al extremo de reducir la potencia o disparar el reactor.

El análisis probabilista de seguridad se puede utilizar para analizar tanto las condiciones de operación como los *allowed outage times* desde el punto de vista del riesgo . Mediante los modelos APS se pueden reproducir configuraciones aceptables e inaceptables según las ETF, y se pueden calcular tanto las figuras de riesgo asociadas a estas configuraciones como los tiempos de exposición necesarios para alcanzar niveles de riesgo altos. Comparando estos resultados con criterios de valoración del riesgo, se pueden justificar las configuraciones y tiempos de interrupción permitidos, o bien se pueden proponer cambios en los requisitos de los mismos, tanto porque estos fuesen demasiados restrictivos como demasiado laxos. El *Nuclear Engineering Research Group* ha desarrollado una metodología de evaluación de las ETF que ha sido publicada en un artículo de la revista internacional *Nuclear Engineering and Design* [64].

3.6. Optimización del programa de mantenimiento

El propósito de las actividades que conforman el programa de mantenimiento es el de detectar la degradación y prevenir el fallo de equipos y sistemas que realizan funciones de seguridad. Sin embargo, la realización de actividades de mantenimiento tiene la desventaja de que los componentes objetivo quedan indisponibles durante la realización de la mayoría de estas actividades. Es entonces necesario establecer un programa de gestión del mantenimiento que garantice que la fiabilidad y eficiencia de todos los equipos y sistemas de seguridad se mantenga en consonancia con sus criterios de diseño sin que la operación segura de la central se vea afectada por la realización de actividades de mantenimiento.

El análisis probabilista de seguridad es una herramienta particularmente útil para evaluar y optimizar el programa de mantenimiento desde el punto de vista del riesgo gracias a que sus modelos incluyen el fallo o indisponibilidad de componentes y sistemas. De hecho, en los modelos APS se introducen sucesos básicos que representan la probabilidad de que un componente esté indisponible por mantenimiento. Concretamente, en el marco de evaluación y optimización del programa de mantenimiento, el APS puede ser utilizado para:

- Garantizar que las actividades de mantenimiento no incrementan el riesgo de la planta. Por ejemplo, el APS permite identificar situaciones en las que la frecuencia de mantenimiento es tan elevada que la indisponibilidad media de equipos es más alta que en otras situaciones con menor cantidad de mantenimiento.
- Priorizar el mantenimiento de equipos y sistemas según la importancia de los mismos desde el punto de vista del riesgo. Los equipos y sistemas se clasifican en tres grupos: equipos y sistemas que requieren un programa de mantenimiento preventivo exhaustivo, equipos y sistemas que requieren un programa de mantenimiento preventivo reducido, y equipos y sistemas a los que se le aplica mantenimiento correctivo porque su indisponibilidad no causa un aumento del riesgo [56, 65]. En las secciones 3.7 y 3.8 a continuación se exponen casos particulares de actividades de mantenimiento en las que se prioriza según la importancia en el riesgo de componentes y sistemas.

- Planificar las actividades de mantenimiento desde el punto de vista del riesgo. Se pueden incluir las actividades de mantenimiento en el APS para identificar aquellas cuyo impacto sobre la seguridad y el riesgo de la planta es mayor. De esta manera, se puede evitar que la planta entre en situaciones de riesgo elevado por combinación de dos o más actividades de mantenimiento cuyo impacto en el riesgo es importante. La metodología propuesta por la regla de mantenimiento[3] de la NRC [66, 67] es un buen ejemplo de aplicación del APS en la planificación del mantenimiento.
- Monitorizar el impacto en el riesgo de cambios en el programa de mantenimiento para decidir si estos cambios son adecuados o no.
- Decidir en qué modo de operación es más adecuado llevar a cabo las actividades de mantenimiento. Hay actividades de mantenimiento que pueden suponer un incremento del riesgo inaceptable en el modo de operación a potencia o en los otros modos de operación. El APS puede ser utilizado para identificar estas actividades, y para decidir en qué modo operacional una actividad de mantenimiento tiene un impacto sobre el riesgo menor.

La parte III de esta tesis doctoral presenta una contribución novedosa en el marco del uso del análisis probabilista de seguridad en la evaluación y optimización del programa de mantenimiento. Concretamente, la tercera parte de la tesis presenta una metodología para incluir el riesgo de daño al núcleo asociado a incendios en la toma de decisiones al respecto de la planificación del mantenimiento de equipos y sistemas.

3.7. Programa de inspección en servicio informado por el riesgo

El objetivo del programa de inspección en servicio es el de identificar estados de degradación de estructuras, sistemas, o componentes para que éstos puedan ser sometidos a actividades de mantenimiento antes de que el fallo ocurra. Tradicionalmente, el programa de inspección en servicio se ha diseñado y se ha llevado a cabo siguiendo un acercamiento determinista. Sin embargo, los resultados de un análisis probabilista de seguridad pueden utilizarse para complementar el acercamiento determinista de dos maneras diferentes:

- Revisar y optimizar el programa de inspección desde el punto de vista del riesgo. Se pueden modificar parámetros del programa de inspección como, por ejemplo, la frecuencia de inspección, y estimar como afectan estas modificaciones al nivel del riesgo de la central.
- Focalizar el programa de inspección en aquellas estructuras, sistemas, y componentes que sean de mayor importancia para el riesgo de la central e identificar los elementos de baja importancia para el riesgo con el objetivo de reducir la cantidad de sus inspecciones. Esta tarea se puede llevar a cabo mediante un análisis de importancia utilizando como criterios de evaluación de importancia aquellos presentes en la *regulatory guide* 1.201 de la NRC [68].

Una correcta aplicación de los resultados del APS en la inspección en servicio debería resultar en una reducción de la cantidad de inspecciones, una reducción de costes, y una reducción de la dosis del personal que se encarga de las inspecciones, sin incrementar el riesgo de la planta.

[3] La regla de mantenimiento requiere que la actuación de las estructuras, sistemas, y componentes bajo su amparo sea monitorizada. Solo se requieren actividades adicionales o correctivas si la actuación de las ESCs desciende por debajo de un cierto nivel umbral de actuación. Este nivel umbral está relacionado con criterios de riesgo. Siguiendo la regla de mantenimiento, una actividad de mantenimiento solo se puede llevar a cabo si no causa que la actuación de las ESCs bajo el amparo de la regla descienda por debajo del nivel umbral.

3.8. Programa de pruebas en servicio informado por el riesgo

El objetivo del programa de pruebas en servicio es el de determinar qué estructuras, sistemas, y/o componentes han de ser puestos a prueba y con qué frecuencia han de ser puestos a prueba para identificar fallos o indisponibilidades. El programa de pruebas en servicio ha sido tradicionalmente diseñado y puesto en práctica siguiendo el acercamiento determinista del código ASME (sección XI) o equivalentes. De forma similar al programa de inspección en servicio, los resultados del APS se pueden utilizar para revisar y optimizar el programa de pruebas, y para priorizar la prueba de componentes importantes para el riesgo sobre otros menos importantes [69]. La aplicación de un programa de pruebas en servicio informado por el riesgo debería resultar en una reducción de los costes generales de mantenimiento sin disminuir el nivel de seguridad de la central.

3.9. Evaluación de modificaciones de diseño

La experiencia demuestra que es muy probable que se tenga que modificar alguna de las características del diseño de una central nuclear durante su larga vida operacional. Las modificaciones de diseño acostumbran a estar causadas por alguno de los motivos siguientes:

- Adecuación a nuevos estándares y normas de seguridad.
- Aplicación de las lecciones aprendidas de la propia experiencia o de la experiencia ajena. Deseo de mejorar la seguridad por parte del licenciatario.
- Malfunciones de componentes por causas de diseño como, por ejemplo, el caso de los generadores de vapor en diversas centrales nucleares.
- Requisitos del organismo regulador.
- Deseo de mejorar la producción por parte del licenciatario.

Históricamente, las modificaciones de diseño derivadas de alguno de los motivos anteriores han sido defendidas y/o justificadas mediante el desarrollo de análisis deterministas y el propio juicio ingenieril. Sin embargo, en 1998 [70] la NRC publicó la *regulatory guide* 1.174, revisada en mayo de 2011, mediante la cual introducía el uso de métodos probabilistas para defender y/o justificar, de forma complementaria, modificaciones en el diseño de centrales nucleares [22]. Dichos métodos probabilistas, que cuentan con la frecuencia de daño al núcleo y la frecuencia de grandes liberaciones tempranas como figuras de riesgo, se basan en evaluar el incremento del riesgo de la central debido a la modificación de diseño. La modificación es aceptable desde el punto de vista del riesgo si el incremento es negativo o nulo. Aunque sea aceptable desde el punto de vista del riesgo, aún debería ser evaluada mediante métodos deterministas, juicio ingenieril, y otros para ser aceptada definitivamente en el marco del proceso IRIDM. En caso de que el incremento del riesgo sea positivo, la guía reguladora presenta criterios cuantitativos para valorar el incremento y decidir si la modificación es justificable o no lo es. El CSN desarrolló su propia versión de la *regulatory guide* 1.174 en 2007, la llamada Guía de seguridad 1.14, Criterios básicos para la realización de aplicaciones de los Análisis Probabilistas de Seguridad.

3.10. Integración de la toma de decisiones informada por el riesgo en el marco regulador

Tradicionalmente, los organismos reguladores han basado sus programas de regulación de la operación y diseño de centrales nucleares en requisitos resultado de análisis deterministas conservadores. Sin embargo,

las primeras aplicaciones de la técnica de análisis probabilista de seguridad y el accidente de Three Mile Island II demostraron que estos requisitos no abarcaban todos los posibles sucesos que pueden ocurrir en una central y que ciertos riesgos quedaban fuera del amparo regulador. En la década de los noventa, gracias a la generalización del uso de los APS como herramienta de análisis de seguridad, se empezaron a implementar planes para la integración del concepto de riesgo en la regulación [39]. Estos planes, la mayoría aún vigentes por la dificultad de construir estándares de aplicación y calidad del APS, han dado lugar a la regulación informada por el riesgo, que integra conceptos de riesgo con el acercamiento determinista. Expertos de APS y de la regulación en seguridad nuclear como G. Apostolakis consideran que el marco regulador nuclear evolucionará hasta el punto de basarse únicamente en la gestión del riesgo [71].

La regulación informada por el riesgo tiene dos objetivos fundamentales. Por una parte, un objetivo de la regulación informada por el riesgo es la integración de herramientas que permitan extraer conclusiones basadas en el riesgo al respecto de cualquier actividad al amparo del marco regulador. En este sentido, la regulación informada por el riesgo incluye una serie indicadores, niveles, y criterios cuantitativos necesarios para que cualquier decisión tomada en el marco de la regulación pueda apoyarse en resultados de riesgo proporcionados por un APS. De esta manera se cubren los riesgos que no abarca el enfoque clásico determinista y se proporciona una valoración cuantitativa más para la toma de decisiones. Ejemplos de herramientas y criterios de regulación informada por el riesgo son las ya presentadas *regulatory guide* 1.174 de la NRC y guía de seguridad 1.14 del CSN.

El otro objetivo fundamental de la regulación informada por el riesgo es ajustar los requisitos reguladores de manera que sean consistentes con la importancia en el riesgo de los equipos, sucesos, y procedimientos a los cuales aplican. En consonancia con este objetivo, el APS se puede utilizar para identificar aquellas áreas que no están cubiertas por la regulación determinista cuya contribución al riesgo es lo suficientemente importante como para necesitar de la adopción de nuevas reglas. Además, el APS se puede utilizar para determinar la importancia relativa para el riesgo de los requisitos y reglas existentes, de manera que puedan ser mejoradas teniendo cuenta su implicación el riesgo. Es posible que en este último análisis se identifiquen partes de requisitos o reglas que sean innecesarias y que, por lo tanto, puedan ser eliminadas. Por ejemplo, la información relativa al riesgo porporcionada por el APS se puede utilizar para determinar la priorización de actividades en la siguiente tanda de inspecciones reguladoras para que se enfoquen en aquellas zonas de la central que sean significativas para el riesgo de la planta [21]. Mediante la regulación informada por el riesgo, los recursos del licenciatario y del organismo regulador se usan de la manera más eficiente posible al tomar decisiones relacionada con la seguridad de las instalaciones.

3.11. Conclusiones

El proceso IRIDM es altamente beneficioso para la seguridad nuclear porque permite que las decisiones se tomen de manera transparente y rigurosa. Gracias al proceso IRIDM se integran diversos aspectos importantes para la seguridad en la toma de decisiones, evitándose así que se tomen decisiones importantes para la seguridad en base a criterios subjetivos y/o sesgados. Por lo tanto, la aplicación del proceso IRIDM es otro elemento más orientado a reducir el impacto del factor humano en la seguridad de la central pues dificulta la introducción de vulnerabilidades asociadas a la toma de malas decisiones. A causa de sus beneficios, no es descabellado pensar que el IRIDM se convertirá en una de las piedras angulares de la seguridad nuclear. Teniendo en cuenta la gran cantidad de aplicaciones desarrolladas hasta la fecha, de las cuales las presentadas en este capítulo son solo una muestra, es probable que el alcance del proceso IRIDM aumente con el tiempo hasta el punto que la toma de cualquier decisión que se considere relevante pase por este proceso.

El nivel de integración final del proceso IRIDM en el campo de la toma de decisiones dependerá, en gran medida, de la evolución de la metodología APS. De hecho, el propio proceso IRIDM es una consecuencia de la maduración de la metodología APS, y de su integración en los procesos de toma de decisiones. La información al respecto del riesgo es uno de los pilares del proceso IRIDM y, sin ella, el proceso no tendría

sentido. En consecuencia, se podrá ampliar el rango de contextos en los que el proceso IRIDM es aplicable a medida que la metodología APS sea sólida en más contextos. Tal y como se ha visto en el capítulo anterior, el APS sigue en estado de desarrollo y se espera que la metodología de aplicación del APS sea cada vez más solida en contextos hasta ahora poco o nada trabajados. En ese sentido, esta tesis doctoral constituye una contribución a la ampliación del rango de aplicación del proceso IRIDM. Por una parte, se presenta una metodología de aplicación de las técnicas de análisis probabilista de seguridad para la evaluación de la seguridad de los procesos vinculados a un almacén temporal individualizado. A partir de esta metodología, se podrían desarrollar aplicaciones APS para aplicar el proceso IRIDM en el marco de la toma de decisiones en los procesos vinculados a un ATI. Por otra parte, la tesis presenta el desarrollo y ejecución de una aplicación APS para incluir el riesgo de daño al núcleo derivado de incendios en el proceso IRIDM de planificación del mantenimiento. Mediante esta aplicación se amplia el abanico de usos del proceso IRIDM al incluir la valoración del riesgo derivado de incendios en el proceso de decisión.

Parte II

Análisis Probabilista de Seguridad de un Almacén Temporal Individualizado

Capítulo 4

Introducción

En esta segunda parte de la memoria de tesis se presenta el desarrollo y resultados de un modelo piloto de análisis probabilista de seguridad de nivel 2 de un almacén temporal individualizado. Los principales objetivos del proyecto asociado a esta parte de la tesis son: desarrollar una metodología de aplicación de las técnicas de análisis probabilista de seguridad para el estudio del riesgo del ATI, presentar una figura, o figuras, orientativa al respecto del riesgo del ATI que permita comparar el riesgo de la instalación con el de daño al núcleo, y realizar la mencionada comparación para valorar el riesgo del ATI de manera cuantitativa. En el desarrollo y aplicación de la metodología piloto se le ha prestado especial atención a la evaluación de la actuación humana porque tiene el potencial para ser uno de los principales contribuyentes al riesgo asociado a la instalación. El análisis de fiabilidad humana se ha realizado después de desarrollar y analizar un primer modelo APS, llamado Fase I, que no lo contiene. De esta manera, se facilita el análisis de la contribución de la actuación humana al riesgo asociado al ATI una vez los resultados del análisis se introducen en el modelo APS.

Entiéndase como almacén temporal individualizado a una instalación de almacenamiento de residuos de alta actividad que, concretamente, se utiliza para almacenar elementos de combustible gastado provenientes de la Piscina de Combustible Gastado (PCG) en, o cerca de, el emplazamiento de la central. El ATI objeto de estudio es una instalación real que pertenece a una de las centrales nucleares con las que colabora el *Nuclear Engineering Research Group*. La instalación ATI estudiada se describe minuciosamente en el capítulo 5. Cualquier dato o referencia técnica de la instalación ha sido proporcionada por la central nuclear.

La implantación de almacenes temporales individualizados es la principal respuesta a la saturación[1] de piscinas de combustible gastado en aquellos países o estados que no cuentan con almacenes temporales centralizados, o almacenes geológicos profundos, y cuya política actual de tratamiento de combustible gastado no incluye el reprocesamiento. Existen dos motivos principales por los que se han dado casos de saturación de piscinas de combustible gastado. Por una parte, uno de los motivos es la combinación del cambio de la política de tratamiento de residuos durante el transcurso del ciclo de vida de las centrales nucleares[2], y la falta de un almacén temporal, también por razones políticas. En estas circunstancias, si en el diseño original de una central se tenía previsto que el combustible se reprocesaría[3], la piscina de dicha central llegará a saturación durante su ciclo operacional. Por otra parte, en países sin almacenes temporales, la ampliación del periodo de vida útil de una central nuclear más allá de lo estipulado en

[1] Una piscina de combustible gastado no puede operar con su piscina de combustible totalmente llena porque en caso de emergencia no habría lugar para colocar los elementos de combustible que se hallan en el reactor.

[2] Pasando de un ciclo cerrado, que incluye el reprocesamiento del combustible gastado, a un ciclo abierto, que incluye el almacenamiento del combustible gastado, para la gestión del combustible.

[3] El combustible gastado se ha de llevar a otra instalación para llevar a cabo el reproceso. En consecuencia, las dimensiones de piscinas de combustible gastado en casos en los que se prevé reproceso son más pequeñas que en casos en que no se prevé que haya reproceso.

el diseño original ha dado lugar a situaciones de saturación de piscinas. El primer ATI fue instalado en Canadá en 1977, pero la construcción de este tipo de instalaciones no se generalizó hasta la década de los noventa, en la que se construyeron 28 ATIs [72]. Según el *Nuclear Fuel Cycle Information System* [72] de la IAEA, hay 92 ATIs en operación hoy en día[4] en más de 18 países, tres de los cuales están situados en centrales nucleares españolas. En consecuencia, y pese a la relativa juventud de este tipo de instalaciones, el uso de ATIs para el almacenamiento del combustible gastado es hoy en día generalizado, habiendo uno por cada cinco reactores en operación.

El almacenamiento de elementos de combustible gastado en instalaciones ATI implica la extracción de estos elementos del Edificio de Combustible, y su almacenamiento en contenedores que acostumbran a estar al aire libre. En caso de fallo del contenedor, los elementos de combustible pueden quedar expuestos al ambiente, hecho que provocaría liberación de radionúclidos. Por lo tanto, la instalación ATI tiene asociado un riesgo para el público derivado de la posibilidad de que ocurra un episodio de liberación de radionúclidos. Dada la tendencia a utilizar este tipo de instalaciones en los años 90 y posteriores, la NRC y el Electric Power Research Institute (EPRI) lanzaron sendos programas de desarrollo de metodologías de evaluación probabilista del riesgo para el público asociado a un ATI. La metodología piloto desarrollada por la NRC, publicada en el NUREG-1864 de 2007, está preparada para una central de diseño *Boiling Water Reactor* (BWR) específica. En cambio, la metodología desarrollada por EPRI, publicada en el EPRI-1009691 de 2004, está preparada para una central de diseño PWR genérico. Ambas publicaciones son los únicos documentos, hasta la fecha, en los que se puede consultar una valoración cuantitativa del riesgo de un ATI. No obstante, la valoración cuantitativa del riesgo de un ATI proporcionada por los documentos en cuestión no es asimilable por cualquier tipo de planta y cualquier tipo de instalación ATI. La metodología desarrollada en el marco de esta tesis doctoral es una contribución más en el campo de la cuantificación del riesgo asociado a un ATI, siendo la primera metodología desarrollada para la industria nuclear española, con el rasgo novedoso de aplicarse a una central PWR específica utilizando las técnicas de análisis más actuales.

Uno de los principales factores a tener en cuenta en la valoración del riesgo asociado a un ATI es la contribución del fallo humano. A diferencia de la operación de los sistemas de seguridad de una central, que es mayormente automática, en el caso del ATI la mayoría de operaciones requieren la participación activa de un ser humano. En consecuencia, la actuación humana puede tener una influencia significativa sobre el riesgo al público inherente a un ATI. El contexto y tipología de las acciones a llevar a cabo en el marco de una instalación ATI es, no obstante, muy diferente al de las acciones analizadas en el marco de un APS en el que se cuantifica la frecuencia de daño al núcleo (véase capítulo 8 para más detalle). Por lo tanto, las metodologías de análisis de fiabilidad humana tradicionalmente utilizadas en soporte a los APS que cuantifican el daño al núcleo no son adecuadas para cuantificar el fallo humano en el contexto del ATI. A día de hoy, no existe ninguna metodología de análisis de fiabilidad humana para evaluar, concretamente, la actuación humana en el marco de un ATI debido a la poca cantidad de APS realizados hasta la fecha. En una contribución novedosa al campo de la fiabilidad humana y al campo del APS, esta tesis doctoral presenta el desarrollo una metodología de análisis de fiabilidad humana para ser aplicada en el contexto concreto de un ATI cuyos resultados han de ser utilizables en el marco de un análisis probabilista de seguridad de este tipo de instalaciones. La metodología de análisis de fiabilidad humana desarrollada se ha aplicado al caso específico del ATI de la central nuclear española y se han introducido los resultados obtenidos en el modelo APS de la instalación. En el cuerpo de la tesis se presenta la cuantificación del riesgo inherente al ATI tanto teniendo en cuenta el análisis de fiabilidad humana (véase capítulo 8) como no teniéndolo en cuenta (véase capítulo 7), y se proporciona una valoración cuantitativa de la influencia de la actuación humana en el riesgo del ATI .

Con el objetivo de presentar las contribuciones anteriormente mencionadas, la parte 2 de la tesis se divide en los siguientes capítulos: un primer capítulo de descripción de la instalación ATI objeto de estudio, capítulo 5, un segundo capítulo de explicación de la metodología APS utilizada en el que se

[4] El propio sistema avisa de que la lista presentada puede no incluir todas las instalaciones existentes en el mundo por indisponibilidad de datos.

hace hincapié en las particularidades adoptadas por ser la instalación analizada un ATI, capítulo 6, un tercer capítulo de aplicación y presentación de resultados de la metodología APS sin aplicar el análisis de fiabilidad humana, Fase I, capítulo 7, un cuarto capítulo de aplicación y presentación de resultados de la metodología APS incluyendo el análisis de fiabilidad humana, llamado Fase II, capítulo 8, y un último capítulo de conclusiones. Además, la parte 2 de la tesis está asociada a los siguientes anexos...

Capítulo 5

Almacén Temporal Individualizado

5.1. Introducción

La descripción del almacén temporal individualizado, de las estructuras asociadas al manejo y transferencia del combustible, y del proceso de almacenamiento del combustible se presenta en este capítulo. La información aquí dispuesta es producto de la realización de la primera etapa de la tarea de familiarización del análisis probabilista de seguridad del ATI (véase el capítulo 7 para más detalle). Como ya se ha comentado, el almacén temporal individualizado es una instalación de almacenamiento de residuos de alta actividad que, concretamente, se utiliza para almacenar elementos de combustible gastado provenientes de la piscina de combustible gastado de una central nuclear. El ATI está constituido por una zona de almacenamiento, cuya descripción forma parte de la sección 5.2, y por contenedores colocados en esta zona, cuyo diseño se describe en la sección 5.3, que aíslan en su interior los elementos de combustible gastado. Las estructuras y sistemas utilizados para introducir los elementos de combustible gastado en los contenedores, y el utillaje utilizado para trasladar los contenedores hasta la zona de almacenamiento se describen en la sección 5.4. Finalmente, el proceso de almacenamiento, es decir, las diferentes operaciones a realizar para llevar a cabo el traslado de los elementos de combustible gastado desde la piscina de combustible hasta la zona de almacenamiento, se presenta en la sección 5.5.

5.2. Zona de almacenamiento

De entre las diferentes opciones posibles[1], la zona de almacenamiento del ATI está formada por dos losas sísmicas, separadas 8,9 metros, sobre las que descansan, sin anclar, en posición vertical y a la intemperie, hasta 32 contenedores de almacenamiento. Cada una de las losas sísmicas, de 61 centímetros de espesor, puede soportar hasta 16 contenedores de almacenamiento en sus aproximadamente 440 m^2 de superficie. Por lo tanto, en las aproximadamente dos hectáreas que ocupa la zona de almacenamiento se pueden llegar a contener hasta 1024 elementos de combustible gastado.

La zona de almacenamiento está construida sobre una colina en el interior del emplazamiento de la central nuclear. La cima de la colina, lugar de colocación del ATI, está situada 57 metros por encima de la cota de los edificios de seguridad de la central. Esto supone que la instalación ATI esté 70 metros por encima de la vía ferroviaria que atraviesa el emplazamiento de la central y 100 metros por encima del rio que transcurre junto al emplazamiento de la central. La zona de almacenamiento está situada a 630 metros de la carretera más cercana, a 491 m de la vía de ferrocarril y a 305,24 m del edificio de contención .

[1] Otras opciones: Encapsular en posición horizontal, estructura de colmena, los contenedores de almacenamiento en un edifici, o encapsular, en posición vertical, los contenedores en losas sísmicas profundas.

5.3. Contenedores

La principal función de los contenedores es asegurar el buen almacenaje de los elementos de combustible gastado en el contexto nominal y en diferentes condiciones accidentales. Concretamente, los contenedores deben estar diseñados para soportar condiciones de temperatura y presión más allá de las nominales, y deben ser lo suficientemente resistentes como para soportar la tensión y la deformación generadas en posibles accidentes de caída o de golpeo de objetos que pudiesen provocar una brecha en el contenedor. Además, el contenedor debe asegurar subcriticidad tanto en condiciones normales como en posibles accidentes. Finalmente, el contenedor debe estar diseñado para poder evacuar el calor generado por los elementos de combustible sin que estos se calienten de forma excesiva y para que la dosis en el exterior de su superficie sea la mínima posible.

A lo largo del desarrollo e implantación de ATIs en la industria nuclear se han diseñado diferentes tipos de contenedor de diferentes características que cumplen con las funciones de seguridad de los contenedores mencionadas. A pesar de la variedad existente, y aunque existen diferencias conceptuales entre diseños de contenedor, sea cual sea el tipo de contenedor, todas las funciones de seguridad se realizan de manera pasiva. En el caso del ATI de estudio, se utiliza el conjunto de contenedores HI-STORM de Holtec Internaitonal®. La característica principal del HI-STORM es que se utilizan diversos contenedores para asegurar el cumplimiento de las funciones de seguridad durante todo el proceso de almacenamiento. Cada uno de los contenedores utilizados realiza unas funciones de seguridad específicas dentro del conjunto de funciones mencionado anteriormente. Los contenedores que forman el HI-STORM 100 son: el contenedor multi-propósito (MPC), el contenedor de transferencia HI-TRAC 125D, y el contenedor de almacenamiento HI-STORM 100. El anexo O contiene varias figuras e imágenes que acompañan a las descripciones expuestas a continuación.

5.3.1. Contenedor multi-propósito MPC

La función principal del contenedor multipropósito es aislar en su interior los elementos de combustible gastado durante todo el proceso de almacenamiento. Es el contenedor que se encarga de dar integridad estructural a la configuración de elementos de combustible. Para reducir la dosis ocupacional exterior, se utilizan otros contenedores a modo de recubrimiento de éste.

El contenedor MPC del caso de estudio es de 4,8 m de altura y 1,7 m de diámetro. Está constituido por una pared exterior de acero inoxidable y en un principio no está tapado (se tapa una vez el combustible es cargado). La estructura interior en forma de panal de abeja, similar a la camisa del reactor, está sujeta al interior de la pared de acero mediante unos soportes. Ésta también es de acero inoxidable, pero con la característica de que se colocan láminas boradas en cada celda para prevenir criticidad tanto en condiciones normales como de accidente. Además, su diseño promueve la recirculación del gas inerte, Helio, que se coloca en el interior. El Helio se utiliza tanto para prevenir la corrosión de las vainas de combustible como para mejorar la transferencia de calor hacia el exterior mediante convección. En el interior de la camisa se colocan espaciadores en las celdas para que los elementos de combustible se mantengan verticales. Su cierre se realiza mediante la soldadura de dos tapas, dotando al MPC de redundancia y seguridad contra fugas. Además, el tiempo para la soldadura de estas tapas es mínimo, lo que favorece la reducción de la dosis exterior en el procedimiento de soldadura. La generación de calor interior máxima de diseño del MPC es de 36,9 kW y se pueden colocar hasta 32 elementos de combustible gastado PWR en su interior. Cuando está cargado, el MPC puede llegar a pesar 40 toneladas aproximadamente.

5.3.2. Contenedor de transferencia HI-TRAC 125D

El contenedor de transferencia es un contenedor cilíndrico delgado cuyas funciones son proteger el MPC durante la etapa de carga del proceso de almacenamiento y proporcionar blindaje de radiación para los

trabajadores. El HI-TRAC 125D está construido con una estructura acero-plomo-acero, sirviendo el plomo como blindaje, con una tapa inferior que se puede quitar para poner otra y así facilitar el movimiento del MPC entre contenedores. Además, para minimizar la exposición a dosis del personal durante las operaciones de manejo y cierre del MPC, el contenedor de transferencia tiene un recubrimiento de agua adicional. Se necesita que este contenedor sea delgado para que pueda utilizarse en espacios pequeños y para que no se necesiten grandes grúas. El contenedor de transferencia está preparado para que pueda ser transportado de manera sencilla. Concretamente, su parte superior presenta unas articulaciones cuyo objetivo es que el contenedor de transferencia se pueda anclar al yugo de alzamiento, que a su vez está enclavado al puente grúa del edificio de combustible. La tapa inferior asegura que la superficie del MPC no se vea contaminada por agua proveniente de la PCG. En el caso a analizar, el HI-TRAC 125D mide 5 m de altura y 2,3 m de diámetro y pesa aproximadamente 100 toneladas cuando está cargado con el MPC. Un único contenedor de transferencia e puede utilizar en diferentes cargas de MPCs. Es el único contenedor reutilizable.

5.3.3. Contenedor HI-STORM 100

La función principal del contenedor HI-STORM 100 es proteger al MPC durante las etapas de transferencia y almacenamiento ante posibles casos de caída, golpeo, penetración, y otros. Además, también está diseñado para proporcionar blindaje radiológico.

En el caso de estudio, este contenedor está constituido por una lámina exterior de acero y otra interior de acero unidas por placas radiales de acero. El hueco entre láminas es rellenado con hormigón, que es el elemento que proporciona el blindaje radiológico. La tapa del contenedor se ancla a las placas radiales de acero mediante los llamados bloques de anclaje. El diseño del contenedor deja un espacio entre la lámina interior de acero y el MPC para que se produzca la circulación natural de aire. En el caso del ATI de la central nuclear, el cuerpo del contenedor mide 5,9 m de altura y 3,4 m de diámetro. Los conductos de entrada y salida de aire, situados cerca de las partes inferior y superior del módulo respectivamente, están diseñados especialmente para que no se acumulen restos y partículas en el interior del contenedor. La figura 5.1 muestra la disposición del MPC con respecto al HI-STORM 100 y las partes del HI-STORM 100.

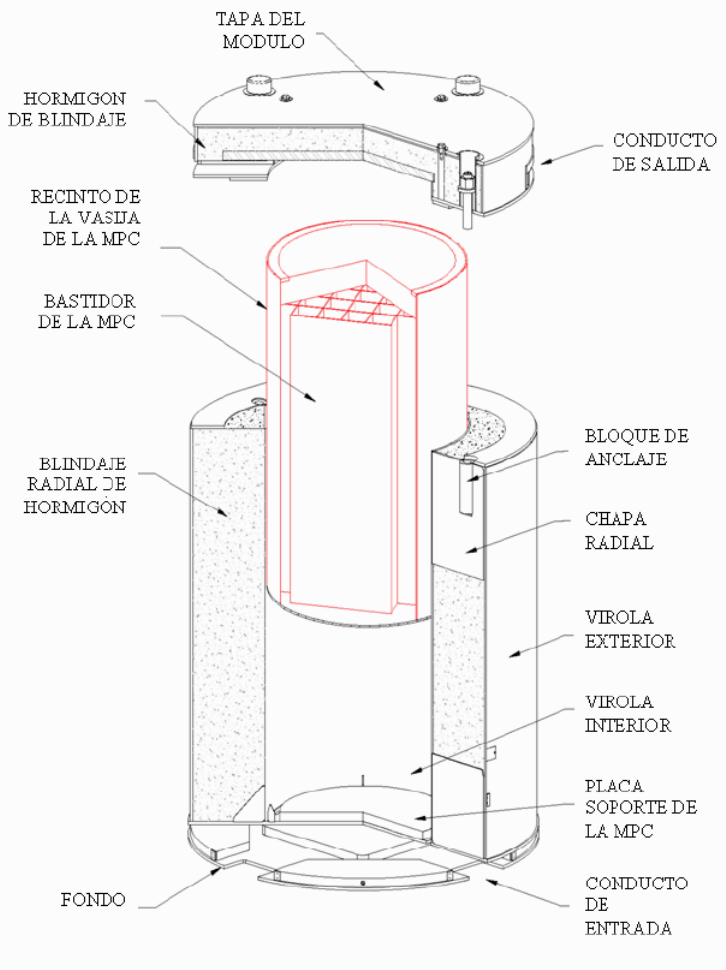


Figura 5.1: HI-STORM 100 y MPC.

5.4. Estructuras y sistemas asociados al manejo y transferencia del combustible y el contenedor

La presente sección incluye la descripción de las principales estructuras y sistemas utilizados en la carga de elementos de combustible gastado en el contenedor y en el traslado del contenedor. Específicamente, se describen el pozo del contenedor, la grúa de manejo de combustible, la grúa puente del edificio de combustible, la plataforma de perfil nulo, y el vehículo de traslado. Las estructuras y sistemas asociados a la soldadura de la tapa del MPC y el posterior rellenado con helio del contenedor (véase la sección 5.5) no se describen en esta sección porque no son sistemas que se analicen en el APS de ATI.

5.4.1. Pozo del contenedor

Cavidad cilíndrica de 13,33 metros de profundidad que se comunica mediante compuertas con la piscina de combustible gastado. En esta cavidad se lleva a cabo el proceso de carga del contenedor con elementos

de combustible gastado, en consecuencia, la altura del pozo es superior a la del contenedor para que exista una capa de agua que blinde a los trabajadores de la radiación en el proceso de carga.

5.4.2. Grúa de manejo de combustible. Herramienta de manejo de combustible gastado

La grúa de manejo de combustible es una grúa pórtico que se desplaza sobre carriles situados a ambos lados de la piscina de combustible gastado y el canal de transferencia. El área de barrido de la grúa pórtico cubre la piscina de combustible gastado, el canal de transferencia, y el pozo del contenedor. Una herramienta de brazo largo, suspendida de un gancho, se conecta a la grúa para mover los elementos de combustible gastado por su área de barrido. El gancho está directamente conectado al dispositivo de izado de la grúa pórtico. El rango del gancho y la longitud de la herramienta de brazo largo están diseñadas para mantener los elementos de combustible a profundidad suficiente como para garantizar la protección de los trabajadores ante la radiación. Las características de seguridad de la grúa pórtico son las siguientes:

- Todos los posibles desplazamientos de la grúa pórtico, y los alzamientos y descensos de la carga suspendida se limitan por medio de enclavamientos y dispositivos final de carrera.
- El gancho tiene dos enclavamientos independientes para limitar su posición inferior y otros dos independientes para limitar su posición superior.
- El motor de alzamiento tiene dos sistemas de frenado independientes. Un sistema de frenado eléctrico automático actúa cuando se pierde el suministro eléctrico del motor y un sistema de frenado mecánico de disco inmoviliza la carga cuando el motor deja de funcionar.
- Tanto la grúa pórtico como el sistema de izado tienen actuadores manuales para almacenar de forma segura el combustible gastado en caso de pérdida de suministro eléctrico.
- La grúa pórtico presenta un sistema de enclavamiento que impide el alzado de una carga que pese más de 908 kg.

La herramienta de brazo largo se usa para manipular el combustible nuevo y el gastado en la zona de la piscina de combustible. Esta herramienta, que se fija al gancho del sistema de izado de la grúa pórtico, se actúa manualmente. Esencialmente, la herramienta de brazo largo es un tubo largo con un sistema de agarre en su extremo inferior.

5.4.3. Grúa puente del edificio de combustible

La grúa puente del edificio de combustible de la central ha sido recientemente modificada para que su diseño sea consistente con los criterios de fallo simple establecidos en el NUREG-0554 y el NUREG-0612. Cumplir con criterios de fallo simple asegura la redundancia de componentes importantes para la seguridad. Por lo tanto, la fiabilidad de la grúa es mayor y su probabilidad de fallo es menor. Esta grúa cubre toda la superficie del edificio de combustible, y está formada por dos elementos principales: El puente birrail, que se mueve en la dirección longitudinal, y el vehículo, que está acoplado al puente birrail y se mueve en la dirección transversal. La grúa pruente tiene dos ganchos, uno principal y uno auxiliar. El gancho principal es doble para estar de acuerdo con el criterio de fallo simple, y es capaz de aguantar cargas de hasta 115 toneladas. El gancho auxiliar es simple y aguanta cargas de hasta 15 toneladas. El gancho principal es el utilizado para mover y alzar los contenedores. La figura 5.2 muestra un dibujo conceptual de la grúa puente.

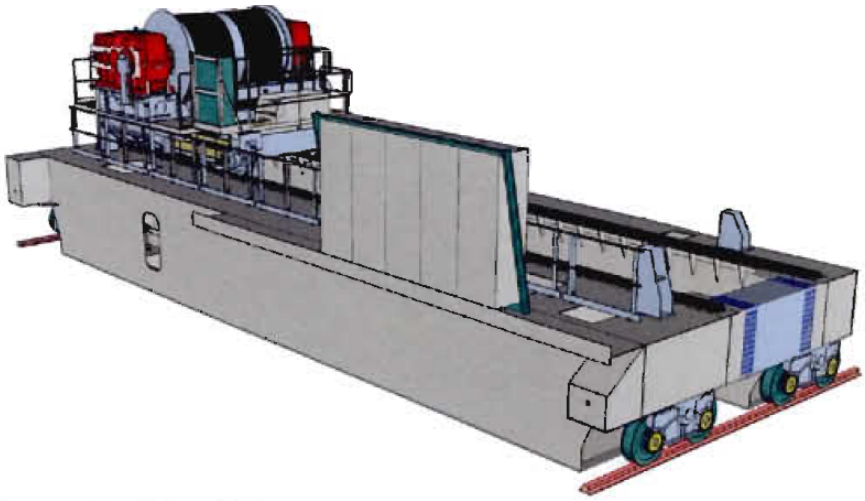


Figura 5.2: Dibujo conceptual de la grúa puente. Fuente:

La grúa puente del edificio de combustible se puede trasladar por encima de la piscina de combustible utilizando el gancho principal gracias a que cumple con los criterios de fallo simple establecido en los NUREGs mencionados anteriormente. Los criterios de fallo simple aplican únicamente al sistema del gancho principal y a los sistemas de frenado del vehículo y del puente. Otros componentes resistentes de la grúa puente, como por ejemplo las vigas, se diseñan aplicando criterios conservadores, pero no necesitan considerarse bajo el criterio de fallo simple.

El vehículo de la grúa puente ha sido reemplazado para que la grúa esté de acuerdo con los criterios de fallo simple. El nuevo vehículo comprende un bastidor sobre el cual se monta el conjunto de todos los mecanismos que forman el sistema de elevación principal, el sistema de elevación auxiliar y el sistema de traslación del vehículo. Los elementos de detección necesarios para asegurar en todo momento el correcto funcionamiento del vehículo y los elementos de control descentralizados del equipo principal también se montan sobre el bastidor.

El gancho de elevación principal se ha diseñado con duplicidad de todos sus mecanismos y con una cadena cinemática cerrada entre todos ellos. En consecuencia, la rotura o fallo de cualquier elemento permite finalizar la maniobra.

El criterio de fallo único está íntimamente relacionado con el concepto de carga crítica, entendiendo carga crítica aquella que, al ser manipulada, puede ser causa directa o indirecta de liberación o fuga de radiactividad. Se considera carga crítica cualquier carga que deba izarse y/o desplazarse que contenga dos o más elementos de combustible gastado, o una carga de peso superior a un elemento de combustible con barras de control más la herramienta de manejo y que deba manejarse por encima de elementos de combustible gastado.

La grúa dispone de dos motores en el mismo eje de accionamiento. Ambos con la capacidad de manejar la máxima carga crítica a una velocidad máxima fijada en 1,524 mpm. Uno de los motores queda en reserva, preparado por si el otro falla. Existe duplicidad completa en el dispositivo de frenada: doble freno de retención a la entrada de cada uno de los reductores, además de un freno de emergencia actuando en el eje de accionamiento, situado entre ambos motores.

La gestión de la grúa puente se realiza mediante un PLC principal o de control que recoge todas las órdenes de manejo y las señales de estado de los distintos elementos, procesa las mismas, y ejecuta las órdenes sobre los dispositivos. De este sistema cuelgan todos los elementos de seguridad secundarios mientras que los primarios (paros de emergencia, finales de carrera de seguridad, y otros) actúan directamente sobre la alimentación del sistema. Toda la gestión y supervisión del sistema de control se realiza mediante

un ordenador personal que visualiza toda la información del estado de la grúa puente y actúa sobre determinados parámetros de configuración. El sistema de control permite manipular la grúa puente desde tres puntos distintos. No obstante, la manipulación de cargas críticas solo es posible desde el puesto de mando principal.

El principal elemento relacionado con la seguridad de la grúa puente es la cadena de seguridad principal. Actúa de manera automática e independiente al sistema de control principal. Puesto que la condición más conservadora y segura de la grúa puente es desenergizada, la actuación de esta cadena provoca la entrada inmediata de todos los frenos y posterior desconexión de la grúa. Se trata de un sistema en serie compuesto de los siguientes elementos relacionados con la seguridad:

- Paros de emergencia de toda la grúa: Cabina de mando, puesto de mando, cabina y panel eléctrico principal.
- Final de carrera de seguridad superior de la elevación principal.
- Final de carrera de seguridad superior de la elevación auxiliar.
- Relé de sobrevelocidad elevación principal.
- Sistema de supervisión entre PLC.

Todos los elementos de esta cadena son redundantes. El estado de cada uno de ellos debe ser coherente con el estado de los demás. Una discrepancia entre ellos comportará el frenado y desenergización de la grúa.

La grúa puente está diseñado para soportar estructuralmente las cargas máximas producidas por el sismo de parada segura. Con ello se impide la caída de la carga suspendida en la grúa puente o de componentes de la misma que pudieran caer sobre la piscina de combustible gastado u otras áreas del edificio de combustible.

La máxima altura a la que se puede elevar el gancho principal es de trece metros sobre la cota cero del edificio de combustible. El yugo de alzamiento es el elemento utilizado para alzar los contenedores. Este yugo se ancla al gancho principal cuando es necesario, y se ancla al contenedor mediante las articulaciones del contenedor y los brazos del yugo. El yugo está especialmente diseñado para cumplir con los requisitos dimensionales necesarios para poder acoplarse a las articulaciones del contenedor. La figura 5.3 presenta el diseño conceptual del yugo y del anclaje al HI-TRAC 125D.

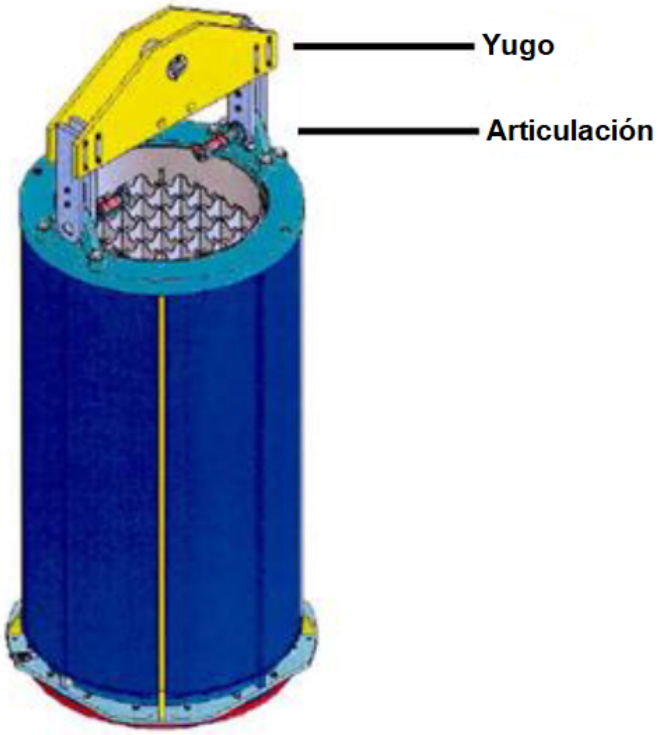


Figura 5.3: Yugo de alzamiento de contenedores.

5.4.4. Plataforma de perfil nulo

La plataforma de perfil nulo es un dispositivo mecánico que se utiliza para desplazar el HI-STORM 100, cargado o vacío[2], entre el interior del edificio de combustible y la zona de transporte, y viceversa. La zona de transporte acoge la etapa de traslado del contenedor entre el vehículo de transporte y la plataforma de perfil nulo, y viceversa. La plataforma se desplaza sobre raíles embebidos en el suelo del edificio de combustible, en línea recta. La carga se posiciona en la plataforma en dirección vertical.

Los componentes principales de la plataforma son un conjunto hidráulico de izado formado por cuatro gatos hidráulicos, un bastidor, cuatro rodillos de transporte y un sistema de guía. El conjunto hidráulico de izado levanta el HI-STORM y consigue que el contenedor esté a la altura correcta para optimizar su manejo en el interior del Edificio de Combustible. El sistema de guía mantiene la orientación de la plataforma durante el movimiento. La plataforma de perfil nulo y todos los componentes asociados tienen un peso conjunto de aproximadamente diez toneladas.

5.4.5. Vehículo de transporte

El vehículo de transporte es de tipo oruga y se utiliza para el manejo y transporte en posición vertical de los contenedores, cargados o vacíos, desde el exterior del edificio de combustible hasta las losas del ATI, o a la inversa. El vehículo no tiene funciones de blindaje, estructurales, de contención, de confinamiento o térmicas asociadas al combustible. En general, el vehículo de transporte se ha diseñado, fabricado,

[2]La plataforma de perfil nulo puede ser usada también para trasladar el HI-TRAC o un MPC vacío a lo largo de una campaña de carga de contenedores.

inspeccionado, mantenido, probado, y se opera de acuerdo con los requisitos estipulados en el NUREG-0612, y el NUREG-0554. Por lo tanto, el vehículo cumple con los criterios de fallo simple establecidos en dichos NUREGs.

Los componentes principales del vehículo de transporte son aquellos miembros estructurales, dispositivos de izado y soportes del mismo, que soportan todo o una parte del peso del HI-STORM en las operaciones de traslado. Concretamente, los componentes principales son: el chasis del vehículo, los conectores de izado del vehículo, que conectan el contenedor con la viga superior del vehículo, el sistema de poleas de trasvase de la MPC, la viga superior, y los brazos de izado, que son unas estructuras tipo viga retráctiles y extensibles que soportan la viga superior y el sistema de poleas de trasvase de la MPC. Además, el vehículo está dotado de los accionadores de acoplamiento, el sistema de sujeción del módulo, el motor, y los sistemas de control. La figura 5.4 presenta un esquema del vehículo de transporte.

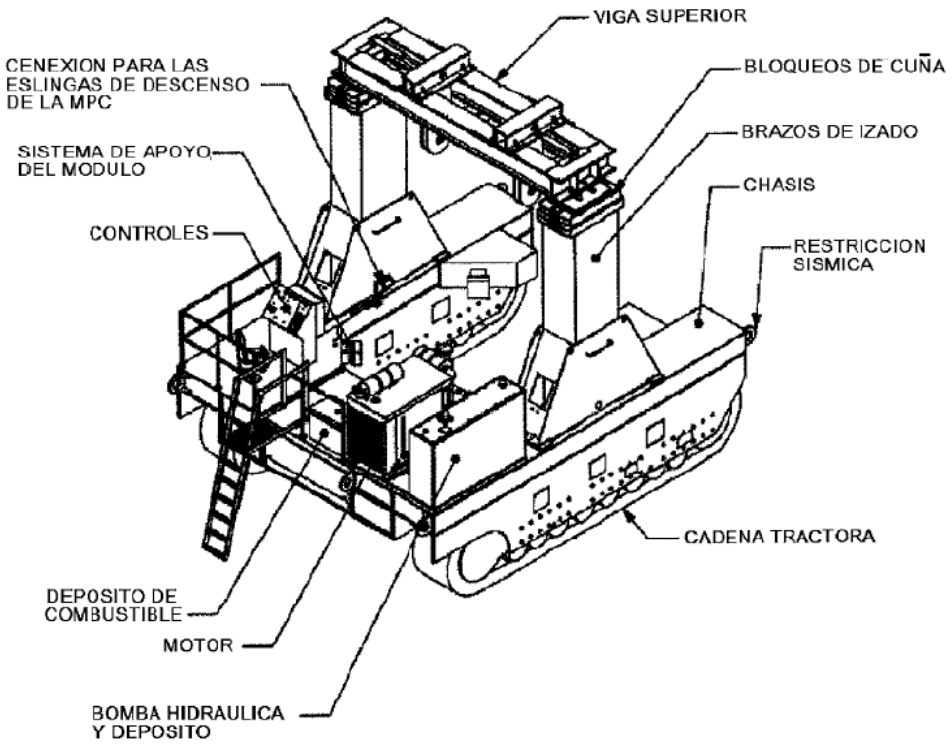


Figura 5.4: Esquema del vehículo de transporte. Fuente:

El HI-STORM se transporta en posición vertical dentro de la huella interna del vehículo. El contenedor se sostiene mediante las fijaciones de los conectores de izado, que están sujetas a la viga superior. Los brazos de izado soportan la viga superior y transfieren el peso al chasis del vehículo. El sistema de sujeción, que consta de una eslinga circular que se ajusta a la circunferencia del contenedor, mantiene el contenedor aferrado al chasis del vehículo durante el traslado horizontal para minimizar posibles efectos de balanceo. Un posible descenso incontrolado de la carga se evita mediante la combinación de componentes redundantes y altos factores de seguridad en el diseño del vehículo.

5.5. Proceso de almacenamiento

Aunque la estancia de los contenedores en la zona de almacenamiento es la etapa más larga del proceso, es necesario describir y analizar todo los pasos seguidos para trasladar los elementos de combustible gastado

hasta dicha zona de almacenamiento. El proceso previo a la etapa de almacenamiento se divide en otras tres etapas: preparación, carga, y transferencia.

5.5.1. Etapa de preparación

La etapa de preparación está compuesta de tres importantes tareas: la inspección de contenedores y grúas, el diseño del plan de movimientos de combustible gastado, y la colocación de los contenedores en su posición inicial. El plan de movimientos determina qué elementos de combustible gastado, y en qué posición, se han de colocar en el interior del contenedor MPC. El contenedor HI-STORM se coloca, mediante la plataforma de perfil nulo, en su posición en el interior del edificio de combustible. El MPC es insertado en el contenedor de transferencia y es llenado con agua tratada específicamente para esta operación. Una vez llenado, se introduce el contenedor de transferencia en el pozo del contenedor. Una vez el contenedor de transferencia está colocado, se retiran las puertas u obstáculos existentes entre la PCG y el pozo, que están por encima del nivel del combustible, para proceder al llenado del MPC.

5.5.2. Etapa de carga

El contenedor de transferencia espera en el fondo del pozo de transferencia anexo a la piscina de combustible gastado. En este punto, la carga del contenedor MPC empieza con la colocación paulatina de los elementos de combustible gastado mediante la grúa de manejo de combustible y su herramienta de brazo largo. Cuando el MPC está lleno, se coloca la tapa superior del MPC por gravedad, sin soldadura, y el contenedor de transferencia se saca del pozo. Una vez fuera, el HI-TRAC 125D se lleva alzado, en posición vertical y a una altura de 0,5 m sobre la superficie, mediante el sistema de grúa puente, gancho y yugo, al área de preparación. En el área de preparación, el MPC es testado, drenado, secado, se le introduce gas inerte Helio y es sellado, es decir, se sueldan las tapas del MPC. El área de preparación del edificio de combustible de la central es una estructura alzada con unas plataformas abatibles sobre las que se coloca el personal. El contenedor reposa sobre el suelo durante todo el tiempo que permanece en el área de preparación. A continuación, el contenedor de transferencia es llevado al lugar donde descansa el contenedor de almacenamiento y es alzado hasta apoyarse en él[3]. Concretamente, la parte inferior del contenedor de transferencia se alza hasta una altura de 5,9 m. Entonces, se quita la tapa inferior del HI-TRAC 125D y el MPC es trasladado del contenedor de transferencia al contenedor de almacenamiento mediante un dispositivo de izado específico[4]. Esta operación supone bajar el MPC una altura de 5,8 m. Cabe destacar que el recorrido por el cual se lleva alzado el contenedor de transferencia en el edificio de combustible es un recorrido preestablecido que evita el paso por encima de la PCG para reducir la altura de una posible caída y las consecuencias de la misma. La descripción aquí expuesta es un breve resumen de las tareas más importantes, para más detalle véase el anexo A.

5.5.3. Etapa de transferencia

La etapa de transferencia comienza una vez el MPC está dentro del HI-STORM 100. En primer lugar, se coloca la tapa del contenedor de almacenamiento. A continuación, el contenedor de almacenamiento se coloca en la huella interna del vehículo mediante la plataforma de perfil nulo, y se alza una altura aproximada de 0,3 m. Al contenedor se le coloca un cinturón de Kevlar[5] para evitar su balanceo mientras es desplazado a la instalación de almacenamiento. Este vehículo puede viajar a una velocidad máxima de 0,56 km/h. Finalmente, una vez el vehículo llega a la instalación ATI, se coloca al lado de la plataforma

[3] Se coloca un dispositivo de acoplamiento entre los contenedores para que el apoyo del HI-TRAC sea perfecto.

[4] A este dispositivo se le llama *hoist blocking device*. Este dispositivo evita que el MPC pueda sacarse del contendor de transferencia, siempre que funcione correctamente. Se evitan de esta manera posibles casos de *two-blocking* y/o un aumento significativo de la dosis en los alrededores del contenedor.

[5] Este cinturón forma parte del sistema de sujeción.

que le corresponde al contenedor que esta transportando. Una vez allí, el contenedor es colocado en la plataforma de hormigón en una posición predeterminada. La etapa de transferencia dura aproximadamente 12 horas [5].

5.5.4. Etapa de almacenamiento

Se corresponde al periodo de almacenamiento, que dura los años que hayan sido estipulados por el organismo regulador. La temperatura, la presión interna, y la dosis exterior del contenedor se monitorizan durante toda la etapa de almacenamiento.

Capítulo 6

Metodología APS adaptada al ATI

6.1. Introducción

El capitulo 6 describe la metodología de Análisis Probabilista de Seguridad utilizada en el estudio de evaluación del riesgo del almacén temporal individualizado de la central nuclear. El proceso de familiarización con las técnicas probabilistas de seguridad a aplicar en el contexto de un ATI se completó con anterioridad al inicio de esta tesis doctoral. La familiarización se llevo a cabo mediante el estudio y comparación de dos metodologías de aplicación de técnicas probabilistas en el contexto ATI provenientes de la industria americana [2], y del regulador americano [5], respectivamente. El proceso de comparación entre metodologías APS de ATI llevado a cabo en la fase de familiarización y las conclusiones extraídas del mismo se presentan en la sección 6.2. La metodología de Análisis Probabilista de Seguridad descrita en el presente capítulo es el resultado del proceso de comparación de ambas metodologías. La metodología APS presentada, y aplicada posteriormente en los capítulos 7 y 8, es de nivel 2. Una metodología APS nivel 1 no permitiría comparar el riesgo inherente al ATI con el de la central nuclear porque las figuras de riesgo que se compararían, daño al combustible en el interior del contenedor y daño al núcleo, son sustancialmente diferentes. En cambio, la metodología APS nivel 2 proporciona las mismas figuras de riesgo: frecuencia de liberación de radionúclidos y término fuente. Debido al alto grado de similitud entre la metodología APS estándar, presentada previamente en la sección 2.4 del capítulo 2, y la metodología APS para el ATI, las descripciones de las tareas de esta última se centran en aquellas características que son específicas de la aplicación al ATI. La descripción de las diferentes tareas de la metodología APS de ATI aplicada en el caso de estudio se incluye en la sección 6.3.

6.2. Comparación de metodologías

El proceso de comparación entre metodologías APS [73], realizado fuera del alcance de esta tesis doctoral, enfrenta los métodos adoptados en dos proyectos diferentes:

- ***Probabilistic Risk Assessment (PRA) of bolted storage casks: Updated quantification and analysis report***: publicado en 2004 por EPRI, el proyecto presenta una metodología APS de nivel 3 aplicada a una central PWR genérica con un ATI que utiliza contenedores de diseño TN-32. Entre otras características, la metodología contiene el análisis de la grúa puente del edificio de combustible y el análisis de fiabilidad humana.
- ***A pilot probabilistic risk assessment of a dry cask storage system at a nuclear power plant. NUREG-1864***: publicado en 2007 por la NRC, el proyecto presenta una metodología APS

de nivel 3 aplicada a una central BWR específica con un ATI que utiliza contenedores de diseño HI-STORM 100. En contraste, esta metodología no presenta análisis de fiabilidad humana.

La comparación entre ambas metodologías se realizó en dos etapas. En primer lugar, se analizaron individualmente ambos documentos, identificando las principales características de las metodologías presentadas en cada uno. A continuación, se enfrentaron ambos métodos con el objetivo de identificar, para cada tarea, el procedimiento de ejecución más adecuado[1] al contexto de esta tesis doctoral. Una detallada descripción del proceso de comparación entre metodologías APS queda fuera de alcance de esta tesis doctoral. No obstante, tanto la siguiente sección como los capítulos 7 y 8 describen los procedimientos utilizados para llevar a cabo cada una de las tareas del APS. Las principales conclusiones extraídas de la comparación de metodologías son:

- La figura de riesgo utilizada en el nivel 2 del APS en ambos casos es la combinación de la frecuencia de liberación de radionúclidos y el término fuente total de un contenedor.
- A excepción del análisis de fiabilidad humana, únicamente presente en el documento de EPRI, ambas metodologías presentan las mismas tareas. El análisis del sistema grúa, perteneciente a la tarea de análisis de datos, solo se realiza en el documento EPRI.
- Las tareas de los APS comparados son similares a las que se encontrarían en un APS de nivel 2 de reactor estándar. Como novedad, los APS de ATI presentan análisis estructurales y termohidráulicos de las barreras de confinamiento, es decir, las vainas de combustible y el contenedor, y el análisis del sistema de ventilación del edificio de combustible. Por contra, los APS de ATI comparados no presentan análisis de sistemas de seguridad y mitigación de la central. Sin embargo, en algunos casos, los procedimientos utilizados para realizar las tareas del APS de ATI son diferentes a los utilizados en un APS estándar.
- Aunque, en general, existe cierto grado de semejanza entre los procedimientos seguidos para llevar a cabo las tareas de ambos APS, hay algunas que destacan por la disparidad de sus acercamientos. Concretamente, destacan las diferencias entre los procedimientos utilizados para realizar los análisis estructural y termohidráulico. Se considera que los procedimientos utilizados en el documento de la NRC son más adecuados para el caso de estudio porque se analiza el mismo tipo de contenedor. En la siguiente sección y en capítulos posteriores, capítulos 7 y 8, se describen los procedimientos utilizados para llevar a cabo cada una de las tareas del APS.

Como ya se ha comentado, las metodologías APS comparadas son muy similares a la metodología APS de nivel 2 estándar. La figura 6.1 presenta la metodología APS estándar de nivel 2. En rectángulos de trazo discontinuo se incluyen las tareas que serían específicas de un APS de ATI en comparación con la metodología de referencia. De esta manera, se muestra de forma visual las pocas diferencias existentes a nivel de tareas a realizar entre un APS de nivel 2 de ATI y uno estándar de reactor.

[1] El procedimiento más adecuado no es necesariamente el que proporciona resultados más realistas sino que es el que mejor se adapta a los recursos disponibles para realizar el APS.

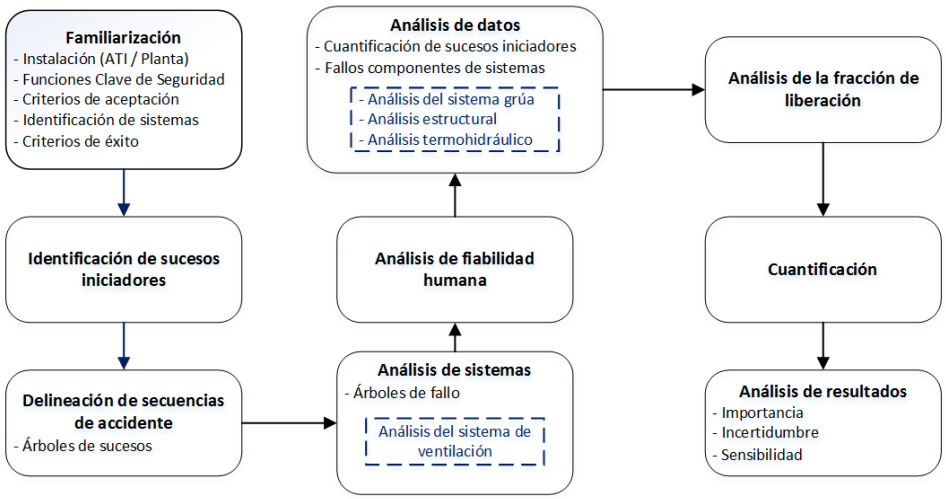


Figura 6.1: Metodología APS de nivel 2 estándar y de ATI.

6.3. Metodología APS adaptada al ATI

El objetivo de aplicar la metodología APS al caso de estudio es obtener una estimación del riesgo inherente al ATI de la central nuclear. La metodología utilizada, de acuerdo con un nivel 2 de APS, proporciona el riesgo en términos de la frecuencia de liberación de radionúcluidos y el término fuente de las secuencias de accidente analizadas. En esta sección, la descripción de la metodología APS utilizada para obtener dichas figuras de riesgo en el caso de estudio, véase la figura 6.1, se divide en las tareas que la conforman. No se debe interpretar el orden en el que se describen las tareas como un orden cronológico o secuencial de realización de las mismas. Hay tareas que se pueden realizar en paralelo o que se pueden realizar más tarde o más temprano respecto a su lugar en la descripción. Además, la realización de estas tareas es un proceso iterativo que requiere revisar algunas tareas a medida que se llevan a cabo algunas de las siguientes. En cualquier caso, la primera tarea a realizar en cualquier APS es la familiarización con la instalación. El software utilizado para crear el modelo APS derivado de la ejecución de la metodología es *RiskSpectrum® PSA*.

6.3.1. Familiarización

La tarea de familiarización tiene por objetivo general la adquisición de información y conocimiento al respecto de la instalación cuyo riesgo se estima en el APS. De acuerdo con este objetivo, la tarea de familiarización se divide en dos etapas: el análisis detallado del diseño y operación de la instalación motivo de estudio, y la definición de funciones clave seguridad, criterios de daño, criterios aceptación, y criterios de éxito asociados a la instalación y a las estructuras, sistemas, y componentes que la conforman. En el caso del ATI, el término instalación hace referencia tanto a la zona de almacenamiento y los contenedores, como a todas las estructuras, sistemas, y componentes que toman parte en el traslado de los elementos de combustible gastado desde la piscina hasta la zona de almacenamiento. Las funciones de seguridad y los diversos criterios a definir son semejantes a los de un APS estándar (véase la sección 2.4.2 del capítulo 2 anterior para más detalle). La tarea de familiarización con la instalación ATI se lleva a cabo a partir de la revisión de documentación. Concretamente, se revisan el estudio final de seguridad del ATI, el estudio final de seguridad de los contenedores HI-STORM 100, planos del edificio de combustible, los procedimientos de manipulación y vigilancia de la carga de contenedores y posterior traslado al ATI, las instrucciones de

operación de la grúa puente del edificio de combustible, y las bases de diseño de los diferentes sistemas que participan en la manipulación de los elementos de combustible y los contenedores.

6.3.2. Identificación de sucesos iniciadores

La identificación de Sucesos Iniciadores se lleva a cabo para determinar aquellos sucesos que pueden representar una amenaza para la integridad contenedor y las vainas de combustible, y que pueden provocar una Liberación de Radionúclidos. A diferencia de los APS estándar, que analizan de forma separada sucesos internos y externos, esta metodología APS considera desde aquellos sucesos generados por la manipulación del contenedor hasta sucesos externos naturales como eventos sísmicos.

En el marco de la tarea de identificación de Sucesos Iniciadores, en primer lugar se obtiene un amplio listado de sucesos iniciadores mediante una búsqueda en literatura disponible (véase el capítulo 7 para más detalle). A continuación, los sucesos iniciadores de este listado se enfrentan a las características de la instalación ATI de estudio para cribar aquéllos cuya ocurrencia sea físicamente imposibles. Los sucesos que superan el cribado cualitativo se agrupan en escenarios de accidente. En el contexto del ATI, los escenarios de accidente hacen referencia a las diferentes etapas en las que se divide una campaña de carga de contenedores.

6.3.3. Delineación de secuencias de accidente

La tarea de delineación de secuencias de accidente tiene por objetivo el desarrollo de árboles de sucesos que plasmen la respuesta de la central ante la ocurrencia de los diferentes conjuntos de sucesos iniciadores. Como ya es conocido, el árbol de sucesos, o *event tree*, es una estructura lógica inductiva que permite modelar las posibles respuestas de una instalación al desafío planteado por un Suceso Iniciador. Cada una de las posibles respuestas de una instalación al desafío planteado por un Suceso Iniciador es una secuencia de accidente. La metodología de desarrollo de los árboles de sucesos del caso de estudio no es diferente a la metodología utilizada en los APS estándar[2] [38]. En el caso de estudio, debido a la simplicidad de la instalación ATI y las operaciones derivadas, los árboles de sucesos combinan únicamente la frecuencia de los Sucesos Iniciadores con la probabilidad de fallo de las distintas barreras de confinamiento, y, en algunos casos, la indisponibilidad o el fallo del sistema de ventilación del edificio de combustible. Los árboles de sucesos generados se introducen en el software *RiskSpectrum® PSA* como parte cualitativa del modelo APS.

6.3.4. Análisis de sistemas

El análisis de sistemas del APS de ATI, a diferencia de un APS estándar, abarca únicamente el sistema de ventilación del edificio de combustible y, en caso de que se considere necesario para estimar la frecuencia de sucesos iniciadores, el sistema de grúas del Edificio de Combustible. Los documentos de análisis de sistemas se realizan siguiendo las directrices empleadas por la propia central, provenientes de las guías de aplicación del APS NUREG/CR-2300 [38] y SSG-3 [21], a partir de la información obtenida de los documentos de familiarización. El análisis del sistema de ventilación incluye la realización del árbol de fallos del sistema, que se conecta con algunos de los árboles de sucesos del APS. El árbol de fallo del sistema de ventilación se introduce en el software *RiskSpectrum® PSA* como parte cualitativa del modelo APS.

[2]Se considera que la metodología estándar o de referencia de APS es la utilizada para llevar a cabo un APS de sucesos internos a potencia.

6.3.5. Análisis de fiabilidad humana

El objetivo de la tarea de análisis de fiabilidad humana es evaluar la probabilidad de fallo al realizar acciones humanas asociadas a la manipulación y monitorización del contenedor durante el proceso de almacenamiento. El análisis de fiabilidad humana es una tarea compleja cuyo desarrollo requiere una gran cantidad recursos. En consecuencia, siguiendo el ejemplo del NUREG-1864, se ha decidido no aplicar el análisis de fiabilidad humana en primera instancia para aligerar la carga de análisis que conlleva el desarrollo desde cero del APS del ATI. No obstante, las conclusiones extraídas de este primer desarrollo del APS de ATI recomiendan la realización del análisis de fiabilidad humana porque el fallo humano podría tener una contribución considerable al riesgo inherente a la instalación (véase el capítulo 7 para más información). Por lo tanto, en segunda instancia, se ha desarrollado el análisis de fiabilidad humana y se han introducido los resultados obtenidos en el APS.

La NRC recomienda utilizar la metodología ATHEANA en el análisis de fiabilidad humana de instalaciones ATI [3]. Sin embargo, la tarea de cuantificación de la metodología ATHEANA se realiza mediante el juicio de expertos. No ha resultado posible reunir un panel de expertos en el marco de esta tesis doctoral [74]. Por lo tanto, se ha desarrollado un nuevo método de cuantificación de la probabilidad de fallo humano que permite obtener resultados sin que el uso de paneles de expertos sea obligatorio. Dicho método de cuantificación se acopla a la parte cualitativa de ATHEANA para cumplir, en parte, con las recomendaciones de la NRC.

La introducción del fallo humano también ha propiciado la introducción del fallo de grúa puente del edificio de combustible en el APS, y la representación de la frecuencia de sucesos iniciadores mediante árboles de fallo. En el contexto de esta tesis doctoral, al desarrollo del APS de ATI sin fiabilidad humana se le llama fase I, y al desarrollo del análisis HRA y su posterior introducción en el APS se le llama fase II.

6.3.6. Análisis de datos

El objetivo de la tarea de análisis de datos es obtener todos los datos numéricos que requiere el modelo APS para cuantificar el riesgo inherente a la instalación analizada. Dichos datos numéricos se introducen en el software *RiskSpectrum® PSA* como parte cuantitativa del modelo APS. En el caso de estudio, los datos cuantitativos a aportar al modelo APS del ATI son: la frecuencia de sucesos iniciadores, las probabilidades de fallo o indisponibilidades de los sucesos básicos incluidos en el árbol de fallos del sistema de ventilación, y la probabilidad de fallo de las barreras de confinamiento. Este último conjunto de datos se obtiene del desarrollo de análisis estructurales y termohidráulicos de las barreras de confinamiento. La realización de estos dos tipos de análisis es una tarea única del APS de ATI. A continuación se describen las subtareas que forman parte del análisis de datos.

6.3.6.1. Estimación de la frecuencia de sucesos iniciadores

En la fase I del desarrollo del APS, los sucesos internos identificados en el APS, que son, básicamente, sucesos de caída del contenedor, se tratan como sucesos que han ocurrido al menos una vez en la industria nuclear. Concretamente, la frecuencia de ocurrencia de estos sucesos se calcula teniendo en cuenta el número de veces que han ocurrido, y el número de operaciones que se han realizado en la industria nuclear en las que potencialmente podían ocurrir los sucesos iniciadores estudiados. En relación con estos datos, la NRC acumula en varios documentos datos de experiencia operativa al respecto de movimientos y caídas de cargas pesadas [75, 76, 77]. Dichos documentos se utilizan en la estimación de la frecuencia de estos sucesos iniciadores. Por contra, debido a la introducción del fallo humano y el fallo de la grúa, la frecuencia de los sucesos iniciadores internos se estima mediante árboles de fallo en la fase II del APS. Las probabilidades de fallo o indisponibilidades de los sucesos básicos presentes en los árboles de fallo de los sucesos iniciadores

se obtienen en el análisis de fiabilidad humana y en el propio análisis de datos. La frecuencia de ocurrencia de los sucesos iniciadores internos se obtiene en términos de por año y por contenedor tanto en la fase I como en la fase II del modelo APS.

Los sucesos externos identificados en el APS se tratan de dos formas diferentes. Para aquellos sucesos que también están presentes en el APS de sucesos externos de la central, que son la mayoría, su frecuencia se estima mediante las metodologías utilizadas en el propio APS de sucesos externos. En la mayoría de casos, el uso de las metodologías del APS de externos se traduce en el ajuste de los resultados de dicho APS teniendo en cuenta la diferencia de cotas y la diferencia de superficies entre el ATI y la central. Para aquellos sucesos externos del APS de ATI que no se tratan en el APS de sucesos externos de la central, se buscan metodologías propias en las guías de tratamiento de sucesos externos de la NRC y la IAEA, y en la documentación de otros APS. La frecuencia de ocurrencia de los sucesos iniciadores externos también se obtiene en términos de por año y por contenedor. A diferencia de la práctica habitual en un APS de reactor, no se ha definido un límite de cribado cuantitativo ni para los sucesos internos ni para los externos.

6.3.6.2. Probabilidades de fallo o indisponibilidad de los sucesos básicos

Las probabilidades de fallo o indisponibilidad de los sucesos básicos que conforman el árbol de fallos del sistema de ventilación se obtienen de la base de datos genérica de parámetros de fallo de componentes del APS de sucesos internos a potencia de la central. Dicha base de datos genérica contiene componentes del sistema de ventilación porque en el marco del APS de sucesos internos a potencia se han de analizar otros sistemas de ventilación de la planta. No se ha aplicado un ajuste bayesiano a los datos genéricos porque no se dispone de datos de experiencia operativa de los componentes del sistema de ventilación del edificio de combustible. En consecuencia, los datos genéricos se introducen directamente en el árbol de fallos del sistema de ventilación del modelo APS de ATI.

La fase II del modelo APS requiere la introducción de probabilidades de fallo o indisponibilidades de sucesos básicos referentes a componentes de la grúa puente del edificio de combustible. En este caso, la base de datos genérica del APS de sucesos internos de la central no contiene ningún dato al respecto de componentes de grúa. Los datos utilizados en el APS provienen, por lo tanto, de bases de datos externas. Concretamente, las probabilidades de fallo introducidas en el APS de ATI provienen de un documento de EPRI [2].

6.3.6.3. Análisis estructural

El objetivo principal del análisis estructural es estimar la probabilidad de fallo de las barreras de confinamiento, es decir, el contenedor y las vainas de combustible, en situaciones en las que están sometidas a los efectos de sucesos iniciadores que suponen un desafío mecánico. Además, el análisis estructural debería incluir la estimación de las superficies de rotura o escape de las vainas y del contenedor para posteriormente utilizarlas en el cálculo de la fracción de liberación de radionúclidos.

Los métodos utilizados en los análisis estructurales de los documentos de referencia son sustancialmente diferentes, aunque coinciden en su naturaleza conservadora. Por ejemplo, en el caso de los sucesos iniciadores de caída, el documento de EPRI utiliza curvas de fragilidad, un acercamiento propio del análisis de eventos sísmicos, para estimar la probabilidad de fallo del contenedor, mientras que el NUREG-1864 utiliza modelos de elementos finitos para calcular la deformación plástica máxima del contenedor y posteriormente enfrentarla a la deformación real de fallo del contenedor. Recuérdese que en el NUREG-1864 se evalúa exactamente el mismo diseño de contenedor que el del caso de estudio.

El análisis estructural es una tarea totalmente ajena al resto de metodologías de análisis probabilista de seguridad y, además, requiere del conocimiento de otras áreas también ajenas al núcleo de la ingeniería nuclear. Por estos motivos, y con el objetivo de no entorpecer la obtención de resultados, se ha decidido no

realizar este análisis desde cero. En su lugar, se utiliza el análisis estructural publicado en el NUREG-1864, adaptándolo a las particularidades del ATI y los Sucesos Iniciadores del caso de estudio. Se considera que, por similitud del diseño del contenedor, los resultados obtenidos de la adaptación del análisis estructural del NUREG-1864 son representativos del caso estudiado.

6.3.6.4. Análisis termohidráulico

El objetivo principal del análisis termohidráulico es estimar la probabilidad de fallo de las barreras de confinamiento, es decir, el contenedor y las vainas de combustible, en situaciones en las que están sometidas a los efectos de sucesos iniciadores que suponen un desafío térmico o térmico y estructural conjuntamente. Además, el análisis termohidráulico debería incluir la estimación de la presión y temperatura internas del contenedor para posteriormente utilizarlas en el cálculo de la fracción de liberación de radionúclidos.

Los sucesos analizados y los métodos utilizados en los análisis termohidráulicos de los documentos de referencia son sustancialmente diferentes, aunque coinciden en su naturaleza conservadora. Por ejemplo, en el caso del suceso de incendio cercano, ambos documentos utilizan condiciones iniciales, pero modelos de simulación diferentes, para estimar la temperatura y la presión interna a la que se vería sometido el contenedor. El análisis termohidráulico depende en gran medida de las características de los contenedores, en especial, del sistema de refrigeración interna. Recuérdese que en el NUREG-1864 se evalúa exactamente el mismo diseño de contenedor que el del caso de estudio.

El análisis termohidráulico es una tarea totalmente ajena al resto de metodologías de análisis probabilista de seguridad y, además, requiere del conocimiento de otras áreas también ajenas al núcleo de la ingeniería nuclear. Por estos motivos, y con el objetivo de no entorpecer la obtención de resultados, se ha decidido no realizar este análisis desde cero. En su lugar, se utiliza el análisis termohidráulico publicado en el NUREG-1864, adaptándolo a las particularidades del ATI y los Sucesos Iniciadores del caso de estudio. Se considera que, por similitud del diseño del contenedor, los resultados obtenidos de la adaptación del análisis termohidráulico del NUREG-1864 son representativos del caso estudiado.

6.3.7. Estimación del término fuente y asignación de consecuencias

La tarea de estimación del término fuente del contenedor y asignación de consecuencias a las secuencias accidente es exclusiva de un APS de nivel 2. La realización de la tarea en cuestión proporciona una de las figuras de valoración del riesgo inherente a la instalación de estudio, el término fuente, y, además, permite valorar cualitativamente el estado final de las secuencias de accidente estudiadas según el propio término fuente asignado a cada una de ellas. El término fuente total del contenedor, que se presenta en unidades de Actividad, es la suma de los términos fuente de cada radionúclido. El término fuente de cada radionúclido se calcula como el inventario de radionúclido existente dentro del contenedor, que se proporciona en unidades de Actividad, por la fracción de liberación de dicho radionúclido. Consecuentemente, la tarea en cuestión se divide en los siguientes pasos: estimación del inventario de radionúclidos, cálculo de la fracción de liberación de radionúclidos, y el propio cálculo del término fuente y la asignación de consecuencias.

6.3.7.1. Inventario de radionúclidos

El inventario de radionúclidos se obtiene mediante simulación con el código ORIGEN-S ejecutado desde el paquete SCALE5.1. Conservadoramente, el elemento de combustible simulado tiene las características límite aceptables para poder ser almacenado en seco (la sección 7.7 del siguiente capítulo proporciona información más detallada la respecto de este elemento de combustible). Se simula la irradiación de este elemento de combustible durante tres ciclos de 18 meses cada uno, separados por periodos de enfriamiento de 40 días, llegando a un grado de quemado de 55000 MWd/TU [3]. Se simula también el posterior

[3] El grado de quemado máximo que puede tener un elemento de combustible para ser aceptado en un contenedor de almacenamiento en seco según el Estudio Final de Seguridad del ATI.

enfriamiento del combustible durante los primeros siete años en piscina. El inventario total de un contenedor se calcula, conservadoramente, como la multiplicación del inventario obtenido para este elemento de combustible pasados 5 años[4] de enfriamiento por 32, que es la cantidad de elementos de combustible que tienen cabida en el contenedor.

6.3.7.2. Fracción de liberación de radionúclidos

La fracción de liberación es la proporción, en tanto por 1, entre la cantidad de radionúclidos que podrían salir del contenedor en caso de darse una secuencia de accidente y el inventario de radionúclidos existente en el contenedor. En el caso específico del ATI, la fracción de liberación se calcula como el producto de la fracción de vainas que fallan, la fracción de material disponible para ser liberado que efectivamente es liberado al interior del contenedor, y la fracción de material que ha sido liberado al interior del contenedor que finalmente acabaría al ambiente.

Los documentos de referencia utilizan diferentes procedimientos para calcular las componentes de la fracción de liberación, aunque coinciden en su naturaleza conservadora. Por ejemplo, ninguno de los documentos calcula ni la fracción de vainas que rompen, ni la cantidad de roturas por vaina, figuras necesarias para estimar la fracción de liberación de forma realista.

Con el objetivo de obtener la fracción de liberación para el caso de estudio deberían realizarse una serie de análisis complejos, haciendo uso de modelos detallados, del estado de las vainas del combustible y del contenedor en condiciones de accidente específicas. Debido a la complejidad inherente a estos análisis y al estado del arte de los mismos, la realización exhaustiva de estos análisis podría ser el motivo de estudio de una tesis doctoral. Por lo tanto, en el contexto de esta tesis, se ha decidido no realizar estos análisis desde cero, sino que se utilizan datos publicados en el NUREG-1864. Concretamente, se utiliza la fracción de liberación de un único caso envolvente publicado en el NUREG-1864.

6.3.7.3. Cálculo del término fuente y asignación de consecuencias

El término fuente de cada secuencia de accidente se calcula, como ya se ha comentado, como el producto del inventario de radionúclidos del contenedor y la fracción de liberación asignada a la secuencia de accidente. A cada secuencia de accidente se la asigna un nivel cualitativo de valoración de su consecuencia, por ejemplo, muy bajo, bajo, y alto, entre otros, que depende de la comparación de su término fuente con los términos fuente de las otras secuencias de accidente.

6.3.8. Cuantificación

El objetivo de la tarea de cuantificación es obtener resultados cuantitativos al respecto del riesgo del ATI mediante el modelo APS. En el caso de estudio, la cuantificación se realiza con el software RiskSpectrum® PSA. Llevando a cabo la tarea de cuantificación se obtienen las ecuaciones booleanas reducidas de las frecuencias de liberación de radionúclidos de las secuencias de accidente, y el propio valor cuantitativo de dichas frecuencias de liberación de radionúclidos. Al igual que la frecuencia de ocurrencia de los sucesos iniciadores, la frecuencia de liberación de radionúclidos estimada mediante el APS se calcula en términos anuales y por contenedor. Para el primer año de manipulación de un contenedor, a diferencia de un APS de nivel 1 estándar, no se calcula un total de la frecuencia de ocurrencia de la consecuencia negativa porque las condiciones a las que se somete el contenedor en las tres etapas del almacenamiento son muy diferentes entre sí. El límite de truncamiento de CMFs del modelo APS de ATI es de 1,0E-15 ((año·contenedor)$^{-1}$). Como referencia, en el APS a Potencia de la central nuclear, de nivel 1 y nivel 2, se utiliza un límite de truncamiento a 1,0E-9 (año^{-1}). El límite de truncamiento de la cuantificación del modelo APS de ATI es

[4] El mínimo tiempo que ha de pasar un contenedor en la piscina de combustible para que sea posible su almacenamiento en seco según el EFS del ATI.

más bajo porque se espera que los resultados de frecuencia de liberación de radionúclidos del APS de ATI sean inferiores a los de un APS de reactor.

La aplicación RiskSpectrum® *PSA* gestiona una base de datos relacional definida de tal forma que toda la información propia del estudio probabilista queda almacenada en unas estructuras o tablas definidas y relacionadas entre sí de una forma establecida a priori (p. ej.: la base de datos no puede contener dos definiciones diferentes de una misma puerta). Por tanto, las bases de datos son únicas en su tratamiento. Debido a que el estudio se ha centrado en el análisis de las tres etapas del ciclo de vida del almacenamiento (etapas de carga, de transferencia y de almacenamiento), con sus respectivas particularidades, se han desarrollado tres bases de datos asociadas a estas configuraciones. Así, partiendo de la base de datos del APS nivel 1 a Potencia de la central se ha desarrollado el estudio piloto probabilista del ATI en la etapa de carga. Debido a que en la manipulación de combustible actúan pocos sistemas activos, la contribución, en términos de cantidad de sucesos básicos, del estudio piloto probabilista de ATI a la base de datos del APS a Potencia es mínima. Para las otras dos etapas, transferencia y almacenamiento, se han creado sendas bases de datos. De la misma manera que en el caso de la etapa de carga, al no utilizarse sistemas activos, las bases de datos son pequeñas en cuanto a número de sucesos introducidos.

6.3.9. Análisis de resultados

La tarea de análisis de resultados, como su propio nombre indica, incluye la realización de diversos análisis para evaluar e interpretar los resultados obtenidos al respecto del riesgo del ATI. Específicamente, el análisis de resultados del APS de ATI se desarrolla en las siguientes tareas: análisis de importancia, análisis de sensibilidad, análisis de incertidumbre, y la comparación con los resultados de nivel 2 del APS de sucesos internos a Potencia de la central nuclear.

6.3.9.1. Análisis de importancia

El principal objetivo del análisis de importancia de los resultados de un APS es la identificación de las principales estructuras, sistemas, y componentes contribuyentes al riesgo. En el análisis de importancia del APS de ATI se calculan, para cada suceso básico presente en el modelo, diversas figuras[5] que valoran la contribución de estos sucesos al riesgo del ATI. Al igual que la cuantificación, el análisis de importancia se ejecuta con el software *RiskSpectrum® PSA*. La figura de importancia elegida para comparar las importancias de los sucesos básicos es la figura Fussell-Vesely.

6.3.9.2. Análisis de sensibilidad

El análisis de sensibilidad se realiza para medir cómo cambiaría la frecuencia de liberación de radionúclidos ante la modificación de alguna de las hipótesis y aproximaciones utilizadas en el modelo APS. En el caso del APS de ATI, el análisis de sensibilidad evalúa, exclusivamente, la influencia del límite de truncamiento de CMFs en la estimación de la frecuencia de liberación de radionúclidos. Concretamente, se rebaja el límite de truncamiento a 1,0E-16 para analizar si el límite de truncamiento utilizado en el proceso de cuantificación criba demasiados CMFs.

6.3.9.3. Análisis de incertidumbre

El software RiskSpectrum® *PSA* posee una herramienta para realizar el análisis de incertidumbre de cualquier árbol de fallo, secuencia de accidente, o consecuencia mediante el método Monte Carlo. Sin

[5] Las figuras de importancia normalmente más utilizadas se han presentado en la sección 2.4.8 de la introducción.

embargo, la incertidumbre de algunos parámetros clave del modelo APS, como, por ejemplo, las probabilidades de fallo de las barreras de confinamiento o las frecuencias de los sucesos iniciadores (tanto en la fase I como en la fase II), no han sido incluidas en el modelo APS, ya sea por desconocimiento de metodologías de estimación o por la complejidad de las mismas[6]. Consecuentemente, a parte de las incertidumbres epistémicas inherentes al modelo, tampoco es posible estimar las incertidumbres aleatorias y epistémicas asociadas a los sucesos iniciadores y a los cabeceros de las barreras de confinamiento. La única incertidumbre estimable es la que proviene de la incertidumbre epistémica de los parámetros de fallo de los sucesos básicos del árbol de fallos del sistema de ventilación. Esta única fuente de incertidumbre se considera insuficiente como para representar la incertidumbre real de los resultados y, por lo tanto, su evaluación no se incluye en la memoria de tesis. No obstante, la no realización del análisis de incertidumbres no supone una carencia del APS porque se trata de un estudio piloto.

6.3.9.4. Comparación con los resultados de nivel 2 del APS de la central

En esta última tarea del análisis de resultados, los resultados al respecto del riesgo inherente al ATI obtenidos en el APS, es decir, tanto la frecuencia de liberación de radionúclidos como el término fuente, se comparan con sus homólogos del APS de nivel 2 de sucesos internos a Potencia de la central nuclear. La comparación se realiza entre los casos predominantes, si los hubiese, o extremos. De esta manera, y a pesar de que el APS de ATI es piloto, se valora el riesgo del ATI en función de su comparativa con el de la central.

[6] En el caso de los árboles de fallo de sucesos iniciadores de la fase II, la base de datos genérica de la que se han extraído los parámetros de fallo de los componentes de grúa no proporciona la incertidumbre epistémica de los mismos.

Capítulo 7

Aplicación piloto de la metodología APS (FASE I)

7.1. Introducción

El capítulo 7 presenta la primera fase (Fase I) de la aplicación piloto de la metodología APS, descrita en el capítulo anterior, en la estimación orientativa del riesgo del ATI. Se define como primera fase a la aplicación de la metodología APS sin incluir el análisis de fiabilidad humana. La aplicación se define como piloto puesto que está enfocada al propio desarrollo de la metodología y a su adaptación al almacén temporal individualizado que es objeto de estudio. En consecuencia, los resultados obtenidos mediante esta aplicación no representan el riesgo asociado al ATI de forma minuciosa y, por lo tanto, no son definitivos. No obstante, los resultados obtenidos sí que son una estimación orientativa del riesgo de la instalación que permiten realizar, por una parte, una valoración cuantitativa del mismo en comparación con el riesgo de otras fuentes radiactivas como, por ejemplo, el núcleo del reactor, y, por otra parte, una valoración cuantitativa de la contribución al riesgo de los diferentes elementos del modelo APS. La primera fase proporciona resultados orientativos que se utilizan, en primer lugar, para realizar una valoración inicial, y menos costosa, del riesgo de la instalación ATI, y, en segundo lugar, para valorar el impacto de la actuación humana en dicho riesgo mediante la comparación con los resultados de la segunda fase.

La metodología de análisis probabilista de seguridad aplicada es de nivel 2. En consecuencia, el modelo APS proporciona el riesgo asociado a la instalación ATI como la combinación de la frecuencia de liberación de radionúclidos al ambiente y la cantidad de radionúclidos liberados en términos de Actividad. La cantidad de radionúclidos liberados es el producto del término fuente de un contenedor y la fracción de radionúclidos que pueden ser liberados al ambiente. Ambas figuras de riesgo son comparables con aquéllas proporcionadas por un APS de nivel 2 sucesos internos a Potencia de una central nuclear.

El capítulo 7 se divide en las secciones listadas a continuación. Cada una de estas secciones hace referencia a una de las tareas de la metodología de análisis probabilista de seguridad explicada en el capítulo anterior. La discusión al respecto del análisis estructural y del análisis termohidráulico se incluye en la sección de Análisis de datos.

- Sección 7.2: Familiarización con la instalación: funciones clave de seguridad y criterios.
- Sección 7.3: sucesos iniciadores y escenarios de accidente.
- Sección 7.4: Análisis de secuencias.
- Sección 7.5: Análisis del sistema de ventilación del edificio de combustible.

- Sección 7.6: Análisis de datos.
- Sección 7.7: Asignación de consecuencias y fracción de liberación de radionúclidos
- Sección 7.8: Cuantificación.
- Sección 15.4: Análisis de resultados.

7.2. Familiarización con la instalación: funciones clave de seguridad y criterios de aceptación y éxito

La fase de familiarización con la instalación incluye, en su primera etapa, el análisis detallado del Edificio de Combustible, del diseño y características del emplazamiento del ATI y del contenedor o contenedores a utilizar, y el análisis del procedimiento de carga del contenedor y del procedimiento de transferencia hasta el ATI, así como todos los elementos de manipulación utilizados. Toda la información al respecto de la instalación ATI extraída del proceso de familiarización ha sido plasmada en el capítulo 5 anterior. La información extraída en la familiarización al respecto de otros ítems como el Edificio de Combustible o el procedimiento de carga del contenedor se ha derivado a los Anexos A, C, y O.

En la segunda etapa de la familiarización, se definen las Funciones Clave de Seguridad (FCS) de la operación y/o instalación cuyo riesgo es objeto de estudio, así como los criterios de aceptación de las mismas y los criterios de éxito de los sistemas encargados de asegurar su cumplimiento. En el caso del ATI, las funciones claves de seguridad a garantizar para el correcto cumplimiento de su objetivo, que es el correcto almacenamiento de elementos de combustible gastado, son:

- Control de criticidad.
- Control de presión.
- Disipación de calor residual.
- Confinamiento.

Teniendo presente cuál es el objetivo del análisis probabilista de seguridad, es decir, estimar el riesgo de liberación de radionúclidos al ambiente, las funciones claves de seguridad han sido reducidas a la función de Confinamiento en el desarrollo del modelo APS. Esto es debido a que el no cumplimiento de cualquiera de las otras tres FCS solo implica una consecuencia indeseable, Liberación de Radionúclidos, si la función de Confinamiento no se cumple a su vez. Si se incluyesen todas las FCS en los cabeceros de los árboles de sucesos, las secuencias de accidente que derivarían en la consecuencia negativa de Liberación de radionúclidos serían todas aquellas en las que el Confinamiento ha fallado, sin importar el estado de las otras FCS. En consecuencia, se ha decidido reducir el análisis de funciones clave de seguridad a la función de Confinamiento en pos de la simplicidad del análisis. De esta manera, los cabeceros de los árboles de sucesos estarán relacionados únicamente con la función clave de seguridad de Confinamiento. Esto no implica que el no cumplimiento de las otras FCS no se estudie, sino que se considera su potencial para afectar al Confinamiento en el análisis de sucesos iniciadores.

El criterio de aceptación de la FCS de Confinamiento es el adecuado almacenamiento de los elementos de combustibles gastado, que se traduce en que la liberación de radionúclidos al ambiente derivada del contenedor se mantenga en los niveles de diseño debidos a fugas. En el caso del ATI objeto de estudio, la función de confinamiento es llevada a cabo por dos barreras físicas pasivas: el sistema de contenedores y las vainas de los elementos de combustible. Respecto al sistema de contenedores, que forman, en conjunto, un sistema pasivo, el criterio de éxito es el adecuado mantenimiento de la integridad estructural del contenedor MPC, que también se puede traducir en que la liberación de radionúclidos al ambiente derivada

del sistema contenedor se mantenga por debajo o igual que los niveles de diseño debidos a fugas. El criterio de éxito hace referencia exclusiva al contenedor MPC porque, en caso de pérdida de su integridad, los radionúclidos tendrían vía libre hacia el entorno por medio del sistema de refrigeración del contenedor de almacenamiento HI-STORM 100. Cabe destacar que en el caso de que alguna de las vainas se rompa y se pierda esta barrera de confinamiento, los radionúclidos seguirán aislados del exterior, y, por lo tanto, la FCS de confinamiento seguiría cumpliéndose. No obstante, la barrera de confinamiento interpuesta por las vainas se incluye en las secuencias de accidente porque el fallo de su integridad estructural provocaría que la Liberación de radionúclidos fuese más importante en caso de perderse también la integridad del contenedor MPC. En el caso del sistema de ventilación, su criterio de éxito se presenta en la sección 7.5, que trata únicamente sobre este sistema.

7.2.1. Alcance del análisis e hipótesis

El análisis probabilista de seguridad de la instalación ATI abarca tres de las cuatro fases del proceso de almacenamiento descrito en la sección 5.5 del capítulo 5. La etapa de preparación queda fuera de alcance del APS porque cualquier desafío a la integridad del contenedor que pueda ocurrir en esta fase no provocaría liberación de radionúclidos. Sin embargo, un fallo o suceso ocurrido en esta etapa podría quedar latente y provocar un fallo o suceso en las posteriores etapas del proceso de almacenamiento que sí podría derivar en liberación de radionúclidos. En este APS se asume, no obstante, que todas las operaciones de la etapa de preparación se llevan a cabo correctamente. Las otras hipótesis principales que se han tomado para la correcta realización del modelo APS son:

- Los sucesos iniciadores relacionados con caídas de elementos de combustible gastado se tratan en el APS de piscina. Por lo tanto, quedan fuera de alcance del APS de ATI.
- Los elementos de combustible están en perfecto estado estructural. Se asume que un elemento de combustible cuyo estado estructural no sea óptimo[1] para su traslado y almacenamiento en contenedores no será almacenado en el ATI.
- La etapa de transferencia no puede verse afectada por fenómenos ambientales y sísmicos porque el personal encargado del movimiento de contenedores decide cuándo llevar a cabo el traslado al ATI. Se entiende que el personal pospondrá la etapa de transferencia si existe la posibilidad de que ocurra un fenómeno ambiental y/o sísmico durante el desarrollo de la misma.
- Se asume que la zona de almacenamiento estará vigilada durante el periodo de tiempo que dure el almacenamiento del combustible en seco y que se llevarán a cabo las pruebas y limpiezas necesarias periódicamente.

7.3. sucesos iniciadores y escenarios de accidente

En el contexto del ATI, se denomina sucesos iniciadores a aquellos eventos (por ejemplo, fallos del sistema grúa del Edificio de Combustible) o accidentes cuya ocurrencia incrementa el riesgo asociado a la manipulación del contenedor y al almacenamiento de los elementos de combustible gastado en contenedores. El objetivo de este apartado es la identificación de sucesos iniciadores, con el mayor grado de extensión posible, que desafíen el cumplimiento de la función de Confinamiento.

El alcance del modelo APS incluye todos aquellos sucesos iniciadores que pueden causar la pérdida de las barreras de confinamiento que mantienen aislado el combustible gastado (vainas y contenedor) ya sea por desafío mecánico, térmico o ambos a la vez. Cabe destacar que se han contemplado incendios y

[1] Por ejemplo, por oxidación o exfoliación de vainas de combustible o por otras causas que debiliten su integridad estructural.

sucesos externos tales como terremotos, inundaciones, u otros, ya que son los únicos sucesos posibles en la etapa de almacenamiento. En cambio, los sucesos de corrosión interna debida a un mal rellenado con Helio, y accidentes de criticidad han sido desestimados debido a que el diseño del contenedor los hace ser prácticamente improbables en comparación con otros sucesos iniciadores [5, 78]. Por último, no se ha dado crédito a la posibilidad de cargar el contenedor con una carga térmica superior a la de diseño, es decir, cargar elementos de combustible con una generación de calor superior a la de diseño, debido a que este hecho es fácilmente detectable [5].

Los sucesos iniciadores a tener en cuenta se han obtenido mediante un análisis de la literatura existente. Concretamente, se han analizado los documentos:

- *Probabilistic Risk Assessment (PRA) of Bolted Storage Casks: Updated Quantification and Analysis Report*, publicado por EPRI [2].
- *Dry Cask Storage Probabilistic Risk Assessment Scoping Study*, publicado por EPRI [79].
- *A Pilot Probabilistic Risk Assessment Of a Dry Cask Storage System At a Nuclear Power Plant.* NUREG-1864, publicado por la NRC [5].
- Estudio Final de Seguridad (EFS). Capítulo 18: Almacén Temporal Individualizado. Propiedad de la central nuclear.
- Documentación del Procedimiento de manipulación del contenedor (PMC). Propiedad de la central nuclear.

Los tres primeros documentos son análisis probabilistas de seguridad piloto de instalaciones similares al ATI de estudio. Todos los sucesos iniciadores analizados en estos APS han sido volcados en una lista, a la que también se han añadido los sucesos iniciadores producto de un análisis lógico del PMC, y los casos analizados en el estudio final de seguridad del ATI objeto de análisis. El listado inicial de sucesos iniciadores obtenido a partir de los documentos mencionados se presenta en la tabla 7.1.

ID	Suceso Iniciador
1	Caída de un elemento de combustible
2	Caída del contenedor de transferencia en el pozo de cofres
3	Volcado del contenedor de transferencia
4	Caída del contenedor de transferencia sobre el suelo del Edificio de Combustible
5	Caída del contenedor de transferencia debido a *two-blocking*
6	Caída del contenedor de transferencia sobre el de almacenamiento
7	Caída del contenedor de transferencia sobre una superficie de hormigón
8	Caída del MPC sobre el contenedor de almacenamiento
9	Caída del contenedor de almacenamiento sobre la superficie de transporte
10	Volcado sobre la superficie de transporte
11	Incendio del vehículo
12	Explosión cercana al vehículo de transporte
13	Inundación del emplazamiento
14	Golpeo de escombros llevados por el agua
15	Terremoto
16	Tsunami
17	Incendio cercano
18	Explosión cercana al emplazamiento ATI
19	Vientos fuertes (tornado)
20	Golpeo de escombros llevados por el viento
21	Meteorito
22	Accidente de avión
23	Bloqueo de la refrigeración por precipitación, nieve o granizo
24	Fallo de las correas de la grúa causando la caída de un EC
25	Error de un operador que lleva a la caída de un EC desde la grúa
26	Pérdida de la disipación de calor por bajada del nivel del pozo del contenedor debido a bajada del nivel de la PCG
27	Fallo de la grúa por sobrepeso
28	Fallo estructural del edificio de almacenamiento
29	Fallo en el proceso de descontaminación
30	Fallo en el control del nivel de la PCG
31	Impacto de un objeto combustible pesado en el vehículo causando volcado

Tabla 7.1: Listado inicial de sucesos iniciadores

Este listado no es definitivo porque algunos de los sucesos iniciadores identificados están fuera del alcance del análisis. Cabe recordar que se analiza desde la carga del primer elemento de combustible hasta el periodo de almacenamiento y que, por ejemplo, no se tienen en cuenta posibles caídas de elementos de combustible. Además, algunos de los sucesos iniciadores listados son imposibles en el contexto específico del ATI objeto de análisis, o bien sus consecuencias son despreciables. Para identificar aquellos sucesos iniciadores de la lista que son imposibles se ha enfrentado el listado completo de sucesos iniciadores con el contenido del PMC y el EFS. Todos aquellos sucesos iniciadores de la lista anterior que o bien estén fuera del alcance del APS, o bien son imposibles, o sus consecuencias son ínfimas, son eliminados de la lista de sucesos iniciadores. En el contexto de un APS, al proceso de eliminación de sucesos iniciadores de un amplio listado por diferentes razones que no incluyen una valoración cuantitativa del riesgo se le llama cribado cualitativo. A continuación se expone qué sucesos iniciadores han sido cribados y las razones que han motivado la criba:

- Caída de un elemento de combustible: La caída por fallo de grúa está fuera de alcance ya que forma

parte del alcance del APS de nivel 1 de la piscina de combustible gastado. La caída de un elemento de combustible por encontrarse en mal estado se encuentra fuera de alcance pues una de las hipótesis realizadas es que los EC están en perfecto estado en el momento de cargarlos en el contenedor.

- Tsunami: La central nuclear se encuentra lejos de la costa, por lo tanto, el riesgo de Tsunami es nulo .
- Fallo de las correas de la grúa causando la caída de un EC: Fuera de alcance por forma de calcular la frecuencia de los SI de Caída (véase la sección 7.6).
- Error de un operador que lleva a la caída de un EC desde la grúa: Fuera de alcance de la primera fase porque no se realiza análisis de fiabilidad humana.
- Pérdida de la disipación de calor por bajada del nivel del foso del contenedor debido a bajada del nivel de la PCG: Fuera de alcance, tratado en el APS de la piscina de combustible gastado.
- Fallo de la grúa por sobrepeso: Se considera improbable porque el peso total del conjunto formado por el contenedor más los elementos de combustible en su interior fue tenido en cuenta en el diseño de la grúa.
- Caída del contenedor de transferencia sobre una superficie de hormigón: Es el mismo suceso iniciador que el de caída del contenedor de transferencia sobre el suelo del Edificio de Combustible.
- Caída del contenedor de transferencia sobre el de almacenamiento: Debido al procedimiento de manipulación, el contenedor de transferencia se coloca justo encima del de almacenamiento sin dejar espacio para una posible caída.
- Fallo estructural del edificio de almacenamiento: Imposible, no existe edificio de almacenamiento.
- Fallo en el proceso de descontaminación: Se considera que las consecuencias son ínfimas [2].
- Fallo en el control del nivel de la PCG: Fuera de alcance, tratado en el APS de PCG de la central nuclear.
- Impacto de un objeto combustible pesado en el vehículo causando volcado: Integrado en el análisis como precursor del suceso iniciador de accidente del vehículo con incendio.

A continuación se presenta, en las tablas 7.2 y 7.3, la descripción resumida de los sucesos iniciadores que han superado el cribado, y que, por lo tanto, son analizados en el modelo APS de ATI. Cabe destacar que el proceso de identificación de sucesos iniciadores es diferente en la fase II porque se incluye la información proporcionada por el análisis de fiabilidad humana.

Suceso iniciador	Descripción
Caída del contenedor de transferencia en el pozo del contenedor	Este Suceso Iniciador describe la caída del contenedor de transferencia en el pozo del contenedor una vez cargado el MPC con elementos de combustible gastado. La caída puede ser debida al fallo de uno o más de uno de los componentes de la grúa, o bien debida a un error humano. En caída, el contenedor caería 0,5 m por aire y 13,3 m por agua. Para el análisis de este suceso se va a considerar una caída de 13 m de altura en aire. Esta consideración conservadora se va a utilizar tanto para el análisis de riesgo de su secuencia de accidente como para el análisis de Liberación.
Volcado del contenedor de transferencia	Este suceso iniciador describe el volcado del contenedor de transferencia en el interior del Edificio de Combustible. Este volcado puede ser causado por el fallo de los brazos que sujetan el contenedor, o bien por choque del contenedor con algún elemento del edificio a causa de llevar el contenedor por un camino diferente al pre-establecido en el PMC.
Caída del contenedor de transferencia sobre el suelo del edificio de combustible	Suceso iniciador que describe una situación similar al primero descrito, pero, en este caso, la caída se produce sobre la superficie del Edificio de Combustible. En este caso hay diferentes alturas de caída posibles: 0,5 m, o 5,9 m. Estas son las alturas a las que se traslada el contenedor según el PMC.
Caída del contenedor de transferencia debido a un caso de *two-blocking*	Este suceso iniciador hace referencia a un evento producido por la combinación del fallo de la grúa y de error humano en el cuál el yugo del contenedor es alzado súbitamente hasta el cuerpo de la grúa causando el fallo de la unión yugo-contenedor y la caída de éste desde la altura máxima posible [2]. Teniendo en cuenta de que la cota máxima del gancho es de 13 m sobre el nivel del Edificio de Combustible, la caída de altura máxima del contenedor de transferencia es de 8 m.
Caída del MPC en el interior del contenedor de almacenamiento	Suceso iniciador que hace referencia a un fallo de la grúa o un error humano en el momento en el que el MPC está siendo introducido en el contenedor de almacenamiento. La caída sería de 5,8 m, la altura del HI-STORM 100.
Caída del contenedor de almacenamiento sobre la superficie de transporte	Suceso iniciador que describe la caída del contenedor de almacenamiento mientras es transportado por el vehículo de transferencia. Se produce por un fallo del dispositivo de alzamiento o por error humano.
Volcado sobre la superficie de transporte	Suceso iniciador similar al anterior, pero, además de caer, el contenedor vuelca.
Incendio del vehículo	Este suceso iniciador describe un evento en el que el vehículo se incendia provocando un fuego que rodea al contenedor.
Explosión cercana al vehículo de transporte	Suceso iniciador que describe una situación en la que, durante el transporte del contenedor de almacenamiento, se produce una explosión cercana en alguno de los depósitos o conductos de sustancias explosivas del exterior o del interior del emplazamiento de la central nuclear provocando una sobrepresión que afecta la contenedor.

Tabla 7.2: Sucesos iniciadores que han superado el cribado (1)

Suceso Iniciador	Descripción
Inundación del emplazamiento	Suceso iniciador que hace referencia a una inundación que llega a la cota de la instalación ATI.
Golpeo de escombros llevados por el agua	Suceso iniciador que hace referencia a la situación en la que una inundación arrastra objetos que pueden golpear a los contenedores situados en la instalación ATI.
Terremoto	Suceso iniciador que describe un terremoto que desafía la estructura de la instalación ATI.
Incendio cercano	Este suceso iniciador hace referencia a un incendio forestal cercano que provoca un aumento de temperatura en la instalación ATI.
Explosión cercana al emplazamiento del ATI	Suceso iniciador similar al presentado para el vehículo de transporte. En este caso el lugar a analizar es la instalación ATI.
Vientos fuertes (tornado)	Suceso iniciador que hace referencia a la existencia de vientos fuertes que provocan altas cargas y presiones sobre los contenedores situados en la instalación ATI.
Golpeo de escombros llevados por el viento	Suceso iniciador que describe la situación en la que un viento fuerte arrastra objetos, misiles, que pueden golpear los contenedores situados en la instalación ATI.
Meteorito	Suceso iniciador en el que la instalación ATI, o algunos contenedores, son golpeados por un meteorito.
Accidente de avión	Suceso iniciador que describe la situación en la que un avión sufre un accidente y cae en la instalación ATI golpeado uno o más de uno de los contenedores.
Bloqueo de refrigeración	Este suceso iniciador describe la situación en la que, debido a precipitación, nieve o granizo, las entradas y salidas de la ventilación de los contenedores quedan bloqueadas, produciéndose un aumento de la temperatura interna del contenedor.

Tabla 7.3: sucesos iniciadores que han superado el cribado (2)

7.3.1. Escenarios de accidente

El listado final de sucesos iniciadores, con 19 sucesos diferentes a considerar, es muy amplio. La metodología APS recomienda agrupar los sucesos iniciadores que representen un mismo tipo de desafío para reducir la cantidad de árboles de eventos a generar en el apartado de secuencias de accidente. No obstante, en este caso no se puede realizar tal agrupación porque las consecuencias que los sucesos iniciadores listados provocan sobre el contenedor son diferentes. Por ejemplo, los sucesos iniciadores de caída del contenedor de transferencia no se pueden agrupar porque en cada caso la altura de caída es diferente. No obstante, los sucesos iniciadores sí que se pueden agrupar según las etapas del proceso de almacenamiento. Pese a que esta agrupación no supone una mejora de la simplicidad del modelo APS, es decir, no se reduce la cantidad de árboles de eventos, sí que permite analizar los resultados de forma más detallada y conocer qué tipo de operaciones son las que tienen un mayor impacto en el riesgo del ATI. Las etapas del proceso de almacenamiento son: la etapa de carga, la etapa de transferencia, y la etapa de almacenamiento.

7.3.1.1. Etapa de carga

La etapa carga es aquella que abarca desde la colocación del primer elemento de combustible en el contenedor hasta la colocación del MPC en el contenedor de almacenamiento. Esta es la única etapa en la que el contenedor es manipulado en el interior del Edificio de Combustible por la grúa del Edificio de Combustible, por lo tanto, todos los fallos relacionados con caídas en el interior del Edificio de Combustible

se agrupan en esta etapa. No se tienen en cuenta los sucesos externos del listado porque el contenedor está protegido en todo momento por el Edificio de Combustible.

Sucesos iniciadores en la etapa de carga
Caída del contenedor de transferencia en el pozo
Volcado del contenedor de transferencia
Caída del contenedor de transferencia debido a un caso de *two-block*
Caída del contenedor de transferencia en el Edificio de Combustible (dos alturas, 0,5 y 5,9 m)
Caída del MPC en el interior del contenedor de almacenamiento

Tabla 7.4: Sucesos iniciadores de la etapa de carga

7.3.1.2. Etapa de transferencia

La etapa de transferencia es aquella que abarca el transporte del contenedor de almacenamiento desde el Edificio de Combustible hasta el emplazamiento de la instalación ATI y su colocación en este último. Bajo esta etapa se agrupan todos los accidentes relacionados con el vehículo de transporte (caídas, volcados, etc.) y todos los accidentes relacionados con la localización del camino de transporte. No se tienen en cuenta sucesos externos porque se considera que se puede elegir el momento en el que realizar el transporte, evitando, de esta manera, realizar el transporte en condiciones externas adversas [5]. La etapa de transferencia dura alrededor de doce horas por contenedor.

Sucesos iniciadores en la etapa de transferencia
Caída del contenedor de almacenamiento sobre la superficie de transporte
Volcado sobre la superficie de transporte
Incendio del vehículo
Explosión cercana

Tabla 7.5: Sucesos iniciadores de la etapa de transferencia

7.3.1.3. Etapa de almacenamiento

Esta etapa se corresponde con el periodo de tiempo de almacenamiento estipulado por el organismo regulador. Debido a que los contenedores están colocados a la intemperie, en esta etapa se agrupan todos los sucesos externos del listado anterior.

Sucesos iniciadores en la etapa de almacenamiento
Inundación en el emplazamiento
Golpeo de escombros llevados por el agua
Terremoto
Incendio cercano
Explosión cercana
Vientos fuertes (Tornados)
Golpeo de escombros llevados por el viento
Meteorito
Accidente de avión
Bloqueo de refrigeración

Tabla 7.6: Sucesos iniciadores de la etapa de almacenamiento

7.4. Análisis de secuencias

El objeto de esta sección es detallar la metodología utilizada para obtener los árboles de sucesos de los escenarios descritos anteriormente, así como presentar los mismos. El árbol de sucesos, o *event tree*, es la principal herramienta analítica utilizada para modelar la respuesta de una instalación al desafío planteado por un suceso iniciador. En el caso de estudio, la instalación se reduce prácticamente al contenedor MPC al analizarse únicamente la FCS de Confinamiento. Los principios usados para desarrollar un árbol de sucesos están bien documentados en la guía reguladora NUREG/CR-2300 "Probabilistic Risk Assessment (PRA) Procedures Guide" [38].

En el caso de estudio se realiza un árbol de sucesos para cada suceso iniciador identificado en la sección 7.3. La construcción de un árbol de sucesos se inicia por su suceso iniciador y posteriormente se bifurca en diferentes ramas, llamadas secuencias de accidente (véase para más detalle la sección 2.4.4 de introducción de la tesis). Las secuencias de accidente son progresiones, o cadenas, de sucesos, es decir, fallos o éxitos de sistemas a realizar una función de seguridad o una acción de mitigación, cuya realización es necesaria para detener o mitigar el accidente iniciado por el suceso iniciador. Las secuencias de accidente quedan definidas por el estado final en el que acaban. La progresión de la situación accidental descrita por cada secuencia de accidente determina si el estado final de éstas es de éxito o fracaso respecto a los criterios de daño, aceptación y éxito marcados. Se les llama cabeceros a cada uno de los sucesos, acciones, o funciones presentes en un árbol de sucesos.

7.4.1. Metodología

La metodología seguida para delinear los árboles de sucesos se divide en los siguientes pasos:

1. Elección del estado final de las secuencias de accidente.
2. Definición de las funciones clave de seguridad a incluir en el árbol de sucesos.
3. Identificación de los cabeceros de las secuencias de accidente de cada suceso iniciador. Delineación de los árboles de sucesos para cada suceso iniciador.
4. Elección de los niveles discretos del estado final.

La aplicación de esta metodología requiere una fase de preparación en la que se ha de adquirir un conocimiento exhaustivo de las posibles respuestas de la instalación ante la ocurrencia de los sucesos iniciadores.

Por ello, en la etapa de familiarización, o llegado este punto, es necesario revisar los procedimientos de operación, especialmente los de emergencia, de la instalación objeto de estudio. Mediante los procedimientos de operación se conoce cuál es la progresión ideal hacia parada segura dada una situación anormal, y las posibles desviaciones de este camino ideal que pueden darse por el fallo de estructuras, sistemas, y/o componentes. Pese a que el grupo de análisis encargado de esta tarea puede aportar sus propias ideas, la precisión y el alcance de los árboles de sucesos depende en gran medida de la disponibilidad de procedimientos de operación correctamente documentados. La fase de preparación es más sencilla en el caso del ATI que en el caso de una central nuclear porque, en comparación con una central, la cantidad de ESCs a tener en cuenta en la delineación de los árboles de sucesos es ínfima.

7.4.2. Elección del estado final de las secuencias de accidente

El estado final de las secuencias de accidente se escoge en armonía con el objetivo del análisis probabilista de seguridad, que es la estimación del riesgo del ATI en términos de frecuencia de liberación de radionúclidos y cantidad de radionúclidos liberados. En consecuencia, las secuencias de accidente de los árboles de sucesos de este APS pueden llegar a dos estados finales: éxito, o Liberación de radionúclidos. Las funciones clave de seguridad y los cabeceros a introducir en el árbol se analizan desde el punto de vista de su potencial para causar, o afectar a, una Liberación de radionúclidos.

7.4.3. Definición de las funciones clave de seguridad a incluir en el árbol de sucesos

Tal y como se ha avanzado en la sección de familiarización, sección 7.2, la única FCS que se tiene en cuenta en el estudio probabilista de seguridad del ATI es la de Confinamiento. Por lo tanto, en el desarrollo de los árboles de sucesos y las secuencias de accidente solo se tiene en cuenta dicha función clave de seguridad. Cabe recordar que el criterio de éxito del sistema contenedor es que la liberación de radionúclidos al ambiente derivada del sistema contenedor se mantenga por debajo o igual que los niveles de diseño asociados a fugas.

7.4.4. Identificación de los cabeceros de las secuencias de accidente de cada Suceso Iniciador. Delineación de los árboles de sucesos para cada Suceso Iniciador

Los cabeceros de las secuencias de accidente son todas aquellas funciones de seguridad que deben ser realizadas por ESCs para alcanzar la parada segura de una central nuclear en el caso de que ocurra un suceso iniciador. Además de las funciones de seguridad, también se consideran como cabeceros acciones recuperadoras o mitigadoras, que recuperan el cumplimiento de una función de seguridad o reducen las consecuencias del accidente, respectivamente. En los APS de central o de PCG, al delinear un árbol de sucesos, los cabeceros se colocan secuencialmente en el orden cronológico en el que serían demandados para llevar la central a parada segura. La figura 7.1 muestra un ejemplo de árbol de sucesos de un APS de piscina.

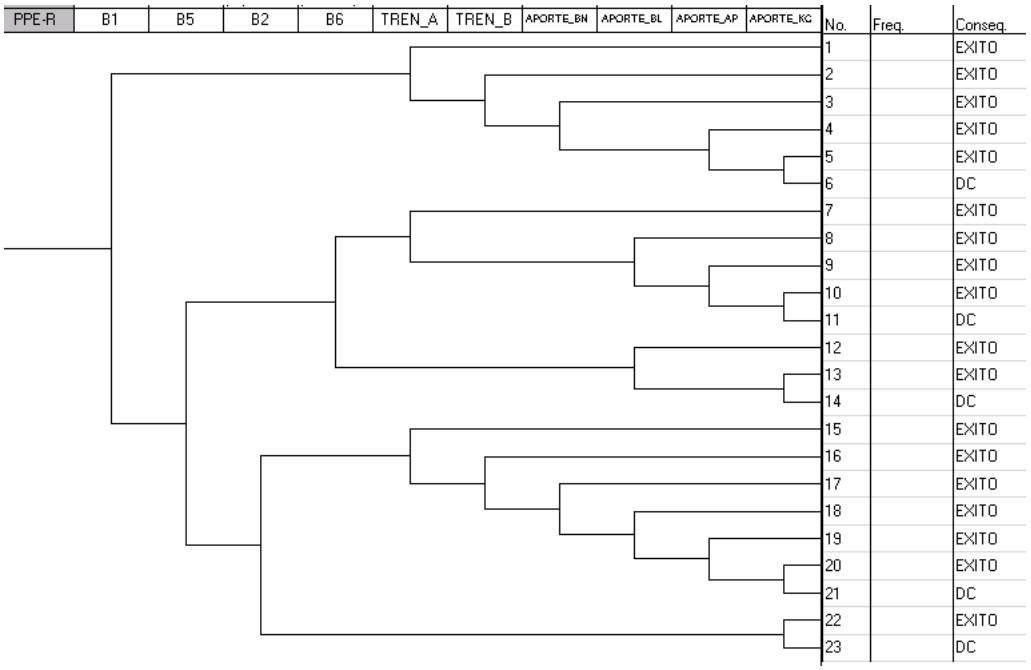


Figura 7.1: Ejemplo de árbol de sucesos de un APS de piscina de combustible gastado.

En el caso del ATI, al ser el contenedor un ente totalmente pasivo, las acciones a realizar y las funciones a asegurar a continuación de cada suceso iniciador son muy diferentes, y muchas menos, a las que se pueden encontrar en un APS de central o de PCG. Específicamente, en el contexto ATI no existen sistemas activos que aseguren la función clave de seguridad de Confinamiento, sino que es el propio diseño del contenedor el que se encarga de que se cumpla. De esta manera, los cabeceros a plasmar en los árboles de sucesos son aquellos que describan el estado de las barreras de confinamiento. Además, en el interior del Edificio de Combustible se da crédito a una acción de mitigación, la del Sistema de ventilación HVAC, con filtros HEPA y de carbón activo, que en el caso de estar activo reduce la Liberación al ambiente hasta un valor prácticamente nulo (su eficiencia está en torno al 99 %, véase la sección 7.5 para más detalle).

El estado de las barreras de confinamiento se describe a partir de su integridad, así que los dos cabeceros que siguen al suceso iniciador son: integridad del contenedor e integridad de las vainas de combustible. Como en todos los sucesos iniciadores la única FCS postulada es la de Confinamiento, estos dos cabeceros están presentes en todos los árboles de sucesos y secuencias de accidente. Esto implica que las secuencias de accidentes sean similares en todos los casos, y que los únicos cambios sean el suceso iniciador y si se da crédito a la acción de mitigación del Sistema de ventilación. Como la acción de mitigación solo es posible durante la etapa de carga, se delinean dos secuencias de accidente genéricas, presentadas en las figuras 14.2 y 14.3.

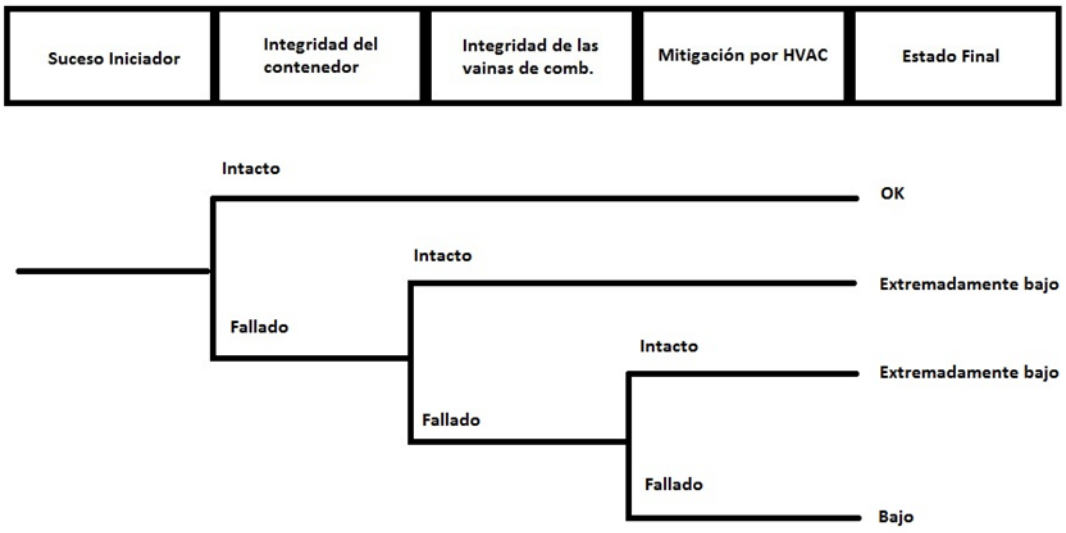


Figura 7.2: Árbol de sucesos para la etapa de Carga.

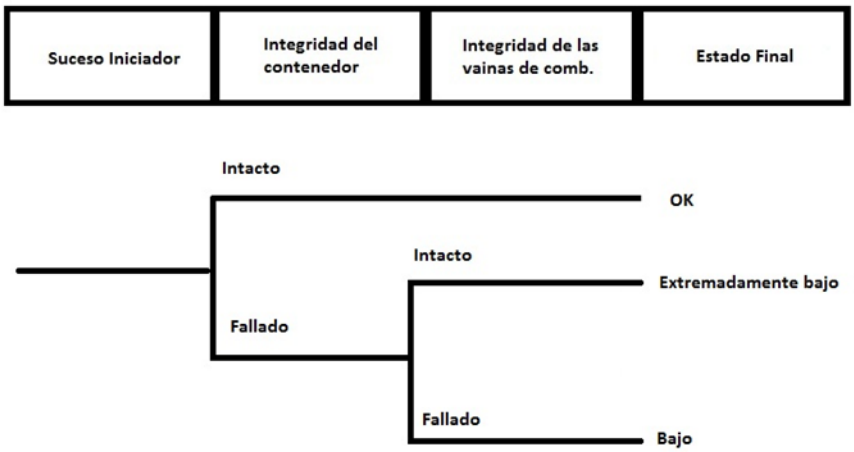


Figura 7.3: Árbol de sucesos genérico para las etapas de Transferencia y Almacenamiento.

Los árboles de sucesos específicos de cada suceso iniciador, presentados en el anexo B, se han introducido en el software *RiskSpectrum*® *PSA* para crear el modelo APS. Los árboles de sucesos obtenidos son similares a los desarrollados en el documento de referencia de EPRI [2], véase la figura 7.4, mientras que el documento de referencia de la NRC [5] no presenta árboles de sucesos. La similitud entre los árboles presentados y los árboles de sucesos desarrollados en el documento EPRI valida positivamente las estructuras de los primeros.

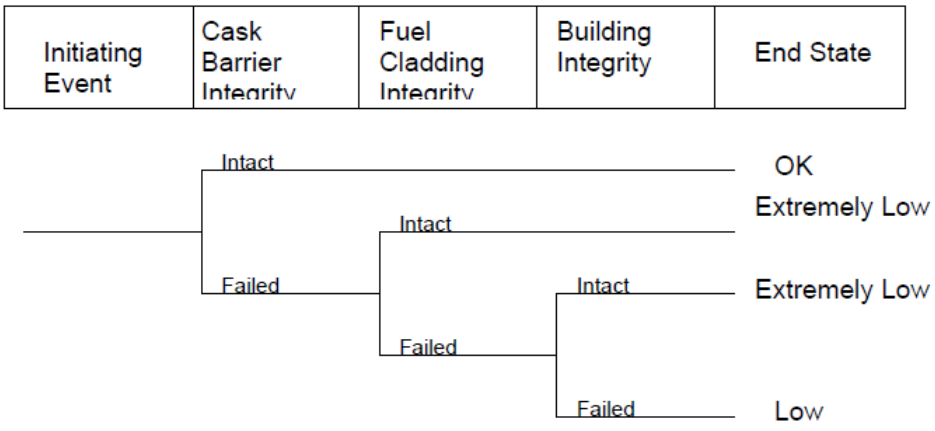


Figura 7.4: Árbol de sucesos de la etapa de carga desarrollado en el documento de referencia de EPRI. Fuente: [2]

7.4.5. Elección de los niveles discretos del estado final

Una vez delineadas las secuencias de accidente, se establecen niveles discretos para describir y valorar cualitativamente el estado final que se alcanzaría en cada una de ellas. En el caso de un APS de nivel 1 de central nuclear, tradicionalmente solo existe un único nivel discreto para valorar la consecuencia negativa: el nivel Daño al núcleo. De forma diferente, en el caso del ATI, si se produce rotura del contenedor, el nivel discreto que representa al estado final, Liberación de radionúclidos, varía según las características del suceso iniciador y de la progresión de la secuencia de accidente. Por lo tanto, a diferencia de un APS de nivel 1 de central nuclear, en el APS del ATI existen diferentes niveles cualitativos de valoración de una misma consecuencia negativa, la liberación de radionúclidos. Para el caso del APS de ATI desarrollado, los niveles discretos que describen el estado final de las secuencias de accidente se basan en el análisis cuantitativo de la fracción de liberación de radionúclidos al ambiente. Por lo tanto, no se presentan hasta la sección 7.7 de análisis de la fracción de liberación de radionúclidos.

7.5. Análisis del sistema de ventilación del Edificio de Combustible

La familiarización con el sistema de ventilación del edificio de combustible se ha llevado a cabo mediante el análisis de los documentos siguientes: Estudio Final de Seguridad del Sistema HVAC del Edificio de Combustible, Diagrama TEI del Sistema HVAC del Edificio de Combustible, Documento Base de Diseño del Sistema HVAC del Edificio de Combustible, Documneto de descripción de Sistemas del Sistema HVAC del Edificio de Combustible, e IOP del Sistema HVAC del Edificio de Combustible.

El documento de análisis del sistema de ventilación del edificio de combustible se ha realizado siguiendo las directrices empleadas por la propia central, y las indicadas en las guías de aplicación del APS NUREG/CR-2300 [38] y SSG-3 [21], a partir de la información obtenida de los documentos de familiarización. El anexo C contiene en su totalidad el documento del análisis del sistema, cuya inclusión en la memoria de la tesis ha sido descartada por motivos de espacio. No obstante, se exponen a continuación las principales conclusiones extraídas del análisis del sistema en cuanto a las funciones del mismo y su papel en el APS, así

como las hipótesis realizadas para la modelización de su árbol de fallos. Se incluye también una sección de modelización en la que se presenta el árbol de fallos del sistema de ventilación del Edificio de Combustible.

7.5.1. Funciones del sistema de ventilación del edificio de combustible

El Sistema de ventilación HVAC del Edificio de Combustible realiza cinco funciones diferenciadas:

- Suministrar aire exterior al Edificio de Combustible para atemperarlo durante la época invernal y distribuir aire por su interior con especial atención a la zona de la PCG. El aire suministrado se filtra antes de su impulsión y distribución.
- Extraer aire captado en diferentes puntos del Edificio de Combustible extrayendo el calor sensible procedente de pérdidas en todos los equipos y tuberías y especialmente el calor latente de evaporación del agua de la PCG.
- Filtrar el aire captado mediante prefiltro, filtro HEPA, filtro de carbón activo y filtro HEPA antes de su transporte y expulsión a través del plénum de descarga del Edificio Auxiliar, durante las condiciones de Operación Normal, Manejo de Combustible y Accidente en el Manejo de Combustible.
- Mantener el Edificio de Combustible en depresión respecto al exterior.
- Aportar calefacción en la época invernal en la zona de ubicación de las unidades de tratamiento de aire.

El sistema de ventilación cuenta con dos unidades de extracción idénticas y redundantes que también realizan la función de filtrado del aire a expulsar del edificio. Ambas unidades de extracción cuentan con los componentes siguientes: Compuertas motorizadas, resistencia eléctrica para calentar el aire, pre-filtro, filtros HEPA, filtro de carbón activo, ventilador y compuerta de regulación. Además, el Sistema HVAC tiene una unidad de suministro de aire que contiene los mismos componentes.

Respecto a su papel en el APS, la correcta actuación del sistema de ventilación del edificio de combustible es la única forma de mitigar la liberación de radionúclidos en caso de darse un accidente en el interior del Edificio de Combustible. Se considera que, en el caso que el Sistema HVAC funcione, la liberación será despreciable debido a la alta eficiencia de retención de los filtros de este sistema , de aquí su importancia. La función de filtrado del aire a expulsar del edificio de combustible es la que se encarga de mitigar la liberación de radionúclidos al medio ambiente. Por lo tanto, el alcance, las bases, y las hipótesis de la modelización del sistema mediante un árbol de fallos se escogen con el objetivo de analizar la actuación de la función de filtrado del aire a extraer.

7.5.2. Alcance de la modelización e hipótesis tenidas en cuenta

Se realiza la modelización del sistema de ventilación del edificio de combustible teniendo en cuenta la no realización de la función de filtrado del aire a extraer como único fallo del sistema. Los sucesos básicos del árbol de fallos representan los fallos independientes de los componentes del sistema. También se incluyen los fallos de los centros de distribución de energía eléctrica que afectan a estos componentes. Las hipótesis utilizadas para la modelización del fallo del sistema son las siguientes:

- En el caso de que exista en el Edificio de Combustible una vía de escape de aire hacia el exterior se considera que la función de filtrado no se cumple y, por lo tanto, que el Sistema ha fallado. Esta hipótesis en particular incumbe a las compuertas de la unidad de suministro de aire.

- En el caso de que el filtrado no sea realizado al 100 % de su capacidad, se considera fallo del sistema de ventilación. Esta hipótesis incumbe a fallos individuales de filtros, fallos de los ventiladores de las unidades de extracción y fallos de las resistencias previas a los filtros.
- En el caso de obturación de la descarga y fallo de las compuertas de alivio, la acumulación de aire provocaría fallo del filtrado.
- Se supone que, en caso de accidente, el sistema de ventilación ha de funcionar durante 24 horas (tiempo en misión de los componentes).
- La fiabilidad humana no entra dentro del alcance de la modelización. Consecuentemente, la única manera de modelizar la detección de un accidente por parte del sistema de ventilación es con los detectores de radiación asociados al sistema. En caso de accidente con liberación de radionúclidos, los trenes de detectores de radiación envían una señal para que el sistema funcione en modo accidente. Si los trenes de detectores fallasen, los propios operarios que realizan la manipulación del contenedor podrían avisar a sala de control del accidente, pero no se van a tener en cuenta en esta modelización. De esta manera, si fallan los trenes de detectores se considera que el sistema ha fallado.
- Se supone que, antes del accidente, el sistema de ventilación estaba en modo Manejo de Combustible. Esta hipótesis afecta al estado de los componentes del sistema previo al suceso iniciador (operación o en espera).
- En todos aquellos componentes que son accionados desde sala de control mediante un interruptor o pulsador se ha desestimado el fallo de éstos últimos. En cambio, se ha tenido en cuenta en todos aquellos componentes accionados mediante contactos de relés.

7.5.3. Modelización: bases y árbol de fallos general

La modelización del Sistema de ventilación se ha basado en la función de filtrado del aire captado en el Edificio de Combustible mediante filtros HEPA y de carbón activo. Realizar esta función implica que el aire en el interior del Edificio de Combustible pase por los filtros de las unidades de extracción, estando estos en perfecto estado, y que no haya vías de fuga de aire en el Edificio de Combustible. Por lo tanto, solo se han considerado aquellos fallos de componentes o unidades que llevan a no filtrar el aire captado en el edificio.

La modelización del fallo al filtrado del Sistema de ventilación se ha realizado considerando las siguientes condiciones:

- El sistema se encuentra en el modo de operación de Manejo de Combustible funcionando tal y como específica el procedimiento de operación del sistema (véase el anexo C para más información sobre el modo de operación mencionado).
- Debido a que al entrar en modo de operación en accidente (véase el anexo C para más información sobre el modo de operación mencionado) una de las unidades de extracción quedará en reserva y no se especifica cual, en ambas unidades se ha de modelar el fallo al arrancar por si es necesario que dicha unidad vuelva a funcionar por fallo de la otra.
- Debido a que solo importa si escapa aire o no, en la unidad de aspiración de aire solo se modeliza el fallo de las compuertas al cerrarse. No importa el fallo del ventilador porque en caso de que este siga funcionando con las compuertas cerradas esto no supondría escape de aire.
- Se considera que si un filtro de una unidad de extracción pierde eficacia por alguna razón la totalidad de la unidad ha fallado.

- No se considera el fallo de los colectores de aspiración de aire puesto que es improbable que fallen todos a la vez al haber una gran cantidad de ellos.

El árbol de fallos del Sistema de ventilación se crea teniendo en cuenta las hipótesis y bases de modelización, y la información al respecto del diseño y operación de los diferentes trenes de componentes que forman el sistema. El anexo C presenta los diferentes sub-árboles que forman el árbol de fallos del Sistema de ventilación. La figura C.1 presenta el árbol de fallos general del sistema. El fallo del Sistema de ventilación a filtrar el aire del edificio se ha modelizado de tal manera que puede ser producto de fallos en los trenes de detectores, o bien fallos en los sistemas de extracción, o bien fallos en la descarga del sistema, o bien fallos en el sistema de suministro de aire (el anexo C describe las causas de cada uno de estos fallos). En el caso de los sistemas de extracción, los dos han de fallar para considerar que el sistema no puede realizar la función de filtrado del aire.

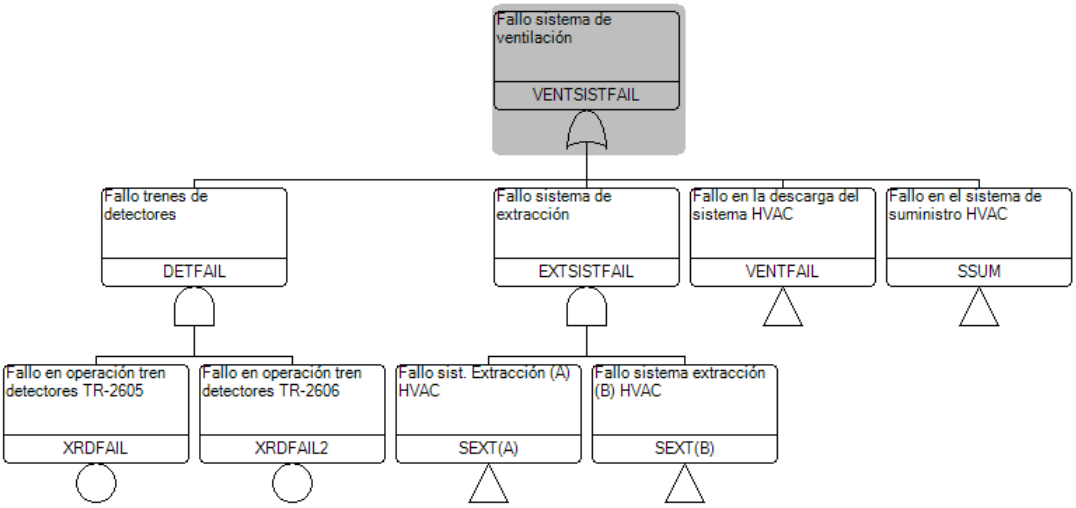


Figura 7.5: Árbol de fallos general del sistema de ventilación

7.6. Análisis de datos

La tarea de Análisis de datos abarca la realización de tres subtareas diferentes en el contexto del APS de ATI. Dos de estas subtareas son comunes a las de un APS de nivel 1 de sucesos internos a Potencia de una central nuclear: estimar la frecuencia de ocurrencia de los sucesos iniciadores, y obtener los parámetros necesarios para modelizar los sucesos básicos incluidos en el modelo de fallo del Sistema de ventilación. La tercera subtarea, en cambio, es única y específica de un análisis probabilista de seguridad dedicado a una instalación ATI. Dicha subtarea consiste en la realización de análisis estructurales y termohidráulicos de las barreras de confinamiento, es decir, el contenedor y las vainas. El objetivo de estos análisis es obtener la probabilidad de fallo de la integridad del contenedor y las vainas en los contextos impuestos por los sucesos iniciadores. Las probabilidades de fallo obtenidas se asignan directamente a los cabeceros de los árboles de sucesos. Se exponen, a continuación, los procedimientos seguidos para realizar cada una de estas subtareas.

7.6.1. Estimación de la frecuencia de ocurrencia de sucesos iniciadores

La estimación de la frecuencia de ocurrencia de sucesos iniciadores, también llamada cuantificación de sucesos iniciadores, se divide en dos bloques. El primer bloque está formado por los escenarios de accidente de las etapas de carga y transferencia, que se denominan sucesos internos, es decir, relacionados

directamente con el procedimiento de manipulación del contenedor. De forma separada se cuantifican los sucesos externos, el segundo bloque, que se podrían dar durante la etapa de almacenamiento, y que están relacionados con sucesos totalmente ajenos a la manipulación del contenedor. El anexo D contiene los cálculos realizados para obtener la estimación de la frecuencia de sucesos iniciadores. En el presente documento se exponen los procedimientos utilizados y los resultados obtenidos en esta subtarea.

7.6.1.1. Cuantificación de sucesos internos

Las tablas 7.4 y 7.5, presentadas en la sección 7.3, contienen los sucesos iniciadores internos analizados en el APS, que son los correspondientes a la etapa de carga y la etapa de transferencia. Todos aquellos que representan la caída del contenedor se tratan conjuntamente.

Sucesos iniciadores de caída

Este caso engloba todos los sucesos iniciadores de la etapa carga y el suceso iniciador de caída del contenedor de almacenamiento durante la etapa de transferencia. La alternativa utilizada en la fase I para estimar la frecuencia de estos sucesos es la de obtener la frecuencia de caída mediante datos de experiencia operativa. Esto es, obtener mediante literatura el número de levantamientos de cargas pesadas que se han realizado en un determinado periodo de tiempo y el número de caídas de cargas pesadas producidas durante este mismo periodo de tiempo. De la división de ambos valores se obtiene la probabilidad de caída de contenedor. En la fase II, se ha realizado un análisis mediante árbol de fallos de la frecuencia de caída en el cual la grúa y la fiabilidad humana son los principales participantes.

Se sigue el procedimiento presentado en el NUREG-1864 para la obtención de datos de levantamientos y caídas de cargas pesadas de la industria nuclear. Los datos de levantamientos obtenidos corresponden a datos de manejo de cargas muy pesadas en las centrales nucleares de Estados Unidos, publicados en el NUREG-1774 [76]. El NUREG-1774 recopila datos de levantamientos de cargas muy pesadas llevadas a cabo durante el periodo de 1968 a 2002. Los datos proporcionados por el NUREG-1774 provienen de nueve plantas estadounidenses de diseño diferente[2], con diferentes diseños de grúa de los edificios de combustible y grupos de trabajo diferentes. Por lo tanto, los datos de levantamiento no son totalmente representativos de la situación específica del ATI objeto de estudio. Además, los datos no están separados según alturas de alzamiento, característica que puede afectar a la probabilidad de caída. Estos hechos permiten valorar el resultado obtenido como una estimación conservadora. A partir de los datos incluidos en el NUREG-1774 (véase el anexo D) se extrapola el número de levantamientos de cargas muy pesadas realizados en las centrales nucleares estadounidenses durante el periodo de 1968 a 2002. Concretamente, se llevaron a cabo aproximadamente 54000 levantamientos.

El número de caídas de cargas muy pesadas en el periodo 1968-2002 se obtiene de informes de sucesos de todas las centrales nucleares de Estados Unidos. El número de caídas en el periodo 1968 a 2002 fue de tres. Conociendo el número de caídas y el número de levantamientos se obtiene una probabilidad de caída de 5,6E-5 (por levantamiento), cociente del número de caídas entre el número total de alzamientos. Debido a que cada suceso iniciador representa un levantamiento del contenedor al año, la frecuencia de caída es de 5,6E-5 caídas por año y por contenedor.

Incendio del vehículo

El documento *Probabilistic Risk Assessment of Bolted Storage Casks: Updated Quantification and Analysis Report* de EPRI presenta un análisis estadístico de incendios en vehículos con duraciones mayores a una

[2]Concretamente, en el NUREG-1774 se hace referencia a diferentes Nuclear Steam Supply System (NSSS). Al tener en cuenta diferentes diseños de NSSS se amplia el rango de usabilidad de los datos. Véase el anexo D para más detalle sobre los diferentes diseños.

hora que estima la frecuencia de este suceso en 4,0E-10 por contenedor y por milla. Utilizando las millas que se recorren por contenedor y por año en el ATI estudiado, es decir, las millas a recorrer entre el edificio de combustible y el emplazamiento del ATI, se podría obtener la frecuencia de incendio de vehículo por año. Ahora bien, en el análisis termohidráulico presentado en la subsección 7.6.3, se demuestra que, en caso de incendio, la integridad del contenedor MPC resiste sin sufrir fallo. En consecuencia, se ha decidido cribar este suceso y no realizar futuros análisis de él.

Explosión cercana

La estimación de la frecuencia de ocurrencia del suceso de explosión cercana en la etapa de transferencia se extrapola de los cálculos realizados para el mismo suceso en la etapa de almacenamiento (véase la subsección 7.6.1.2, que contiene detalles sobre la metodología utilizada). La frecuencia anual de ocurrencia del suceso de explosión cercana es de 1,66E-6 veces por contenedor y por año. La etapa de transferencia dura 12 horas de las 8760 que tiene un año, así que la frecuencia de explosión cercana obtenida en la estimación de la frecuencia anual de ocurrencia para la etapa de almacenamiento se ha de ajustar multiplicándola por el factor 12/8760. El valor obtenido para la frecuencia de explosión cercana en la etapa de transferencia una vez aplicado el ajuste es de de 2,274E-9 por contenedor y por año.

7.6.1.2. Cuantificación de sucesos externos

La tabla 7.6, presentada en la sección 7.3, contiene los sucesos iniciadores externos analizados en el APS, que son los correspondientes a la etapa de almacenamiento. La estimación de las frecuencias de sucesos externos se basa en metodologías diversas, según el caso estudiado. Las metodologías utilizadas provienen de diversos documentos:

- El análisis de sucesos externos de la central nuclear.
- Los documentos de referencia que presentan APS de instalaciones similares al ATI objeto de estudio [5, 2].
- Guías de aplicación de la metodología APS como la NUREG-2300, la NUREG-1407 [80] o el SSG-3 de la IAEA.
- *Regulatory Guides* de la NRC.

A continuación se exponen las metodologías utilizadas y se señala la procedencia de cada una de ellas. Los cálculos específicos de cada caso se presentan en el anexo D.

Inundación y precipitación

El análisis del suceso de inundación y precipitación del análisis de sucesos externos de la central se realiza mediante la metodología presentada en el NUREG-1407. En el análisis de sucesos externos de la central se analizan tres posibles casos de inundación: crecida de rio, inundación por rotura de presas e inundación por precipitación local intensa. Se considera que estos tres mismos casos son los que se deben estudiar para estimar la frecuencia de inundación en la instalación ATI. En consecuencia, en lugar de reproducir la metodología para el caso del ATI, se ha decidido extrapolar los resultados teniendo en cuenta que la cota del ATI está 57 m por encima de la cota de la central.

En el caso de crecida de rio, en el análisis de sucesos externos de la central se evalúa cual es la máxima avenida posible debida a precipitación. Se concluye que la máxima avenida posible llegaría a una cota de 44 m por encima del nivel del rio. Esta crecida no supondría un problema para la central nuclear, puesto

que sus edificios de seguridad están situados en una cota a 50 m por encima del nivel del río. Como el emplazamiento de la instalación ATI está colocado a una cota de 57 m por encima de los edificios de la central, no es posible que sea vea afectado por la máxima avenida posible. En consecuencia, este suceso iniciador es cribado.

Para el caso de inundación por rotura de presas se evalúan diversos estudios relacionados con los posibles fallos y roturas de las presas situadas aguas arriba del emplazamiento de la central. Se concluye que, en el peor caso, definido además como inviable, la cota del agua llegaría al nivel de 51,29 m, que está muy por debajo de la cota del emplazamiento ATI (107 m). En consecuencia, este Suceso Iniciador es cribado. De la misma manera que el suceso de inundación es cribado de futuros análisis, el golpeo de escombros llevados por el agua también es cribado ya que necesita de la inundación para que pueda ocurrir.

El emplazamiento del ATI está colocado en lo alto de una colina. En su diseño se hizo especial hincapié en la construcción de canalizaciones y conducciones para evacuar el agua de precipitación . En consecuencia, se decide cribar también este suceso.

Accidente de avión

En el análisis de sucesos externos de la central se realiza un estudio completo sobre la frecuencia anual de impacto de avión siguiendo la metodología incluida en el *Standard Review Plan* (SRP) de la NRC. Para el cálculo de la frecuencia de impacto, el tránsito aéreo cercano a la central se divide en aerovías y en rutas de llegada o salida a aeropuertos cercanos. Las características de las aerovías cercanas y el tránsito de cada una de ellas es igual para el ATI que para la central, puesto que el emplazamiento del ATI está situado dentro del emplazamiento de la central. Por lo tanto, los resultados presentados en el análisis de sucesos externos de la central se pueden extrapolar para el caso del ATI. El anexo D contiene un resumen de la metodología del SRP utilizada para estimar la frecuencia de impacto de avión.

Los resultados de frecuencia anual de impacto de avión se extrapolan a partir del área efectiva de impacto, al ser ésta la única variable a modificar al analizar el ATI. El valor del área efectiva de la central nuclear es de 0,405 millas^2. Mediante las dimensiones del contenedor HI-STORM 100, se cálcula el área de contenedor que puede ser golpeada por un avión, que es de 72,099 m^2 o bien 2,784E-5 millas^2. Por lo tanto, el factor de corrección a aplicar a la frecuencia de impacto de avión es el cociente entre el área efectiva del contenedor y el área efectiva de la central nuclear. Aplicando el factor de corrección se obtiene una frecuencia anual de impacto de aviones en ruta igual a 6.49E-11 (año·contenedor)$^{-1}$ y una frecuencia anual de impacto de aviones que llegan o salen de aeropuertos de cercanos de 2,12E-12 (año·contenedor)$^{-1}$. El total de la frecuencia anual de impacto de avión suma 6,7E-11 (año·contenedor)$^{-1}$.

Vientos fuertes

En el análisis de sucesos externos de la central se evalúa la capacidad de los edificios de seguridad para resistir las cargas provocadas por vientos fuertes mediante una metodología del SRP. Concretamente, se calcula, con un 95 % de confianza, qué racha de viento, a 30 m de altura y durante 3 segundos, tiene un período de retorno de 1E+6 años (frecuencia = 1E-6), resultando un valor de 104 m/s. A partir de este valor y con las curvas de fragilidad de cada edificio de seguridad se establece la probabilidad de fallo de los edificios.

En el caso del ATI la metodología a seguir es la misma. El primer paso de la metodología utilizada hace referencia a la posibilidad de cribar el suceso si se demuestra que la velocidad de viento máxima de diseño de la estructura analizada tiene un periodo de retorno mayor que 1,0E+6 años. Conociendo que este valor es de 104 m/s para el emplazamiento de la central a 30 m de altura, se calcula cuál sería la velocidad del viento con período de retorno de 1E+6 años en la cota de la instalación ATI utilizando un perfil de velocidades logarítmico.

La velocidad con período de retorno 1,0E+6 en la cota de altura de la instalación ATI es de 114,16 m/s (cálculos recogidos en el anexo D). El análisis estructural del contenedor, subsección 7.6.3, demuestra que es necesaria una velocidad de 179 m/s y otra de 268,3 m/s para deslizar o volcar el contenedor, respectivamente. Por lo tanto, la frecuencia de ocurrencia de estas velocidades sería sustancialmente inferior a 1,0E-06 por año. Además, para calcular la frecuencia de liberación de radionúclidos se debería aplicar la probabilidad de rotura de las barreras de confinamiento, que, en el caso volcado, es de 1,0E-06 (véase el análisis estructural de la sección 7.6.3). En consecuencia, este suceso iniciador es cribado porque su FLR sería despreciable.

De la misma manera que en el caso de golpeo de escombros llevados por agua, en este caso los escombros llevados por viento no se tienen en cuenta debido a que es necesario un viento de mayor velocidad para que los escombros puedan causar daño.

Explosiones

La metodología escogida para estimar la frecuencia de ocurrencia es la propuesta por la *Regulatory Guide* 1.91 de la NRC [81]. La metodología se aplica mediante los siguientes pasos:

1. Estimación de la máxima distancia de seguridad para cada fuente de posible explosión, siendo ésta la distancia a la cual la sobrepresión generada por la explosión es del orden de 1 psi [1 psi = 6894,76 Pa]. En el caso de que la instalación ATI se encuentre más lejos que la distancia de seguridad del punto de la explosión el suceso iniciador se puede cribar.
2. Estimación de la sobrepresión que la explosión generaría en el contenedor. Si la sobrepresión es menor que la de diseño, 10 psi, se criba el suceso iniciador. Si se supera la presión de diseño se supone que el contenedor vuelca.
3. Estimación de la frecuencia anual de explosión de la fuente explosiva analizada.

Existen cuatro posibles casos que podrían dar lugar a una explosión en las cercanías de la central según el análisis de sucesos externos: plantas industriales en un radio de 8 km (8 km es la distancia máxima a analizar según la RG 1.91), sustancias explosivas transportadas por carretera, sustancias explosivas transportadas por ferrocarril y sustancias explosivas almacenadas en el propio emplazamiento de la central. La metodología utilizada y los cálculos realizados para cada caso están en el anexo D.

Solo uno de los cuatro casos estudiados no es cribado en los pasos 1 y 2 de la metodología. Se trata del caso de transporte de sustancias explosivas por ferrocarril, que presenta cinco substancias cuya explosión durante el transporte generaría una sobrepresión en un contenedor del emplazamiento mayor de 10 psi. Concretamente, estas sustancias son: butadienos estabilizados, disulfuro de carbono, metacrilato de metilo inhibido, naftaleno fundido, bebidas alcohólicas. La frecuencia anual de explosión teniendo en cuenta todas las sustancias es de 1,66E-6 por año y por contenedor. Cabe destacar que las sustancias analizadas, y en las cantidades analizadas, datan de 2010. Es probable que en otros años se transporten otras sustancias y en otras cantidades.

Incendio cercano

Igual que en la etapa de transferencia, los resultados del análisis termohidráulico, subsección 7.6.3, demuestran que en caso de incendio el contenedor MPC no sufre daño alguno. En consecuencia, este suceso queda cribado.

Meteorito

La frecuencia de ocurrencia de la caída de un meteorito en un contenedor se obtiene siguiendo la metodología detallada en el documento NUREG-1864. Esta frecuencia es de 2,88E-13 por año y por contenedor. Los detalles de la metodología utilizada por el NUREG-1864 se presentan en el anexo D.

Terremoto

En el estudio final de seguridad del HI-STORM 100 se explicita que la aceleración mínima provocada por un terremoto necesaria para causar el volcado de un contenedor es de 1,35g. Al ser éste un valor elevado de aceleración, se ha decidido, antes de aplicar cualquier metodología, compararlo con el *Safe Shutdown Earthquake* (SSE) de la central, y valorar la posibilidad de cribar este suceso iniciador. En el Informe Final del Consejo de Seguridad Nuclear [31] se expone que el SSE de la central nuclear es de 0,13g. Por lo tanto, la aceleración necesaria para causar el volcado de un contenedor es 10,4 veces más grande que la provocada por el SSE. De esta manera, si ocurriese un terremoto que provocase una aceleración de 1,35g en el emplazamiento, las consecuencias a mitigar en la central serían mucho mayores que las consecuencias en el ATI, las cuales se podrían despreciar. Es por esta razón que se decide cribar este suceso, aunque se emplaza a futuras revisiones de este proyecto el cálculo de la frecuencia de terremoto con aceleración de 1,35 g en el emplazamiento.

Bloqueo de refrigeración por precipitación local intensa

Se ha cribado este suceso por coherencia con el de inundación y precipitación.

7.6.1.3. Resumen de la cuantificación de sucesos iniciadores

La tabla 7.7 contiene el código que se va a utilizar a partir de ahora para nombrar a cada suceso iniciador no cribado, su descripción y su frecuencia de ocurrencia.

Identificador del Suceso Iniciador en el modelo APS	Descripción	Frecuencia de ocurrencia (año·contenedor)$^{-1}$
Etapa de carga		
Caída1	Caída de 0,5 m del contenedor de transferencia durante el traslado	5,6E-5
Caída2	Caída de 8 m causada por *two-blocking*	5,6E-5
Caída3	Caída de 5,9 m del contenedor de transferencia al alzarse por encima del HI-STORM	5,6E-5
Caída4	Caída de 13,5 m sobre el pozo de cofres	5,6E-5
Caída5	Caída de 5,8 m del MPC en el interior del contenedor de almacenamiento	5,6E-5
Volcado	Volcado en el movimiento de alzado	5,6E-5
Etapa de transferencia		
EXPTRANS	Explosión cercana en fase de transferencia	2,274E-9
Etapa de almacenamiento		
ACCAV	Accidente de avión en el emplazamiento	6,69E-11
EXPALM	Explosión cercana en etapa de almacenamiento	1,66E-6
METEO	Golpeo de meteorito	2,884E-13

Tabla 7.7: Tabla resumen de sucesos iniciadores

En el marco de un APS de nivel 1 o de nivel 2 de sucesos internos a Potencia, los sucesos iniciadores cuya frecuencia de ocurrencia es mayor que 1,0E-06 por año son cribados, lo que implica que no son introducidos en el modelo APS. En el caso del ATI, al tratarse de un análisis piloto y de una fuente de radiactividad diferente al reactor de la central, se decide no aplicar ningún criterio de cribado para analizar el riesgo de la instalación en su totalidad.

7.6.2. Obtención de parámetros de fallo para los componentes presentes en el árbol de fallos del sistema de ventilación

Los componentes del Sistema de ventilación del Edificio de Combustible están fuera del alcance de los diferentes APS que ha realizado la central nuclear, por lo tanto, no se tienen datos específicos de fallo de estos componentes. En consecuencia, no se ha podido aplicar el tratamiento bayesiano para obtener los parámetros de fallo. De esta manera, los parámetros de fallo de los componentes presentes en el árbol de fallos del Sistema de ventilación se han obtenido de bases de datos genéricas de componentes de la industria nuclear.

Los parámetros de fallo se obtienen, principalmente, de la base de datos genérica de la central nuclear (véase el capítulo 2 para más detalle sobre este tipo de bases de datos). En caso de que algún componente esté fuera del alcance de la base datos genérica de la central, se obtienen sus parámetros de fallo de las bases de datos IAEA-TECDOC-478 *Component reliability data for use in probabilistic risk assessment* [82], o *Savannah River Site Generic Data Base Development* [83]. Cabe destacar que la base de datos genérica de la central es un conglomerado de las principales bases de datos genéricas de la industria, así que muy pocos componentes quedan fuera de su alcance.

El anexo C presenta, para todos los componentes incluidos en el árbol de fallos del sistema de ventilación, una descripción del componente, que incluye límites físicos, y los parámetros de fallo obtenidos de las bases de datos genéricas.

7.6.3. Análisis estructural y análisis termohidráulico

En el contexto de un análisis probabilista de seguridad de ATI, se llevan a cabo análisis estructurales y termohidráulicos de las barreras de confinamiento (contenedor y vainas de combustible) para evaluar la respuesta de éstas ante los sucesos iniciadores postulados. Concretamente, mediante los análisis estructurales y termohidráulicos se evalúa, en primer lugar, si es posible cribar algún suceso iniciador debido a que sus consecuencias sobre las barreras de confinamiento sean despreciables. En caso negativo, los análisis han de desarrollarse hasta el punto que proporcionen las probabilidades de fallo de las barreras de confinamiento ante el suceso iniciador estudiado. En consecuencia, la realización de estos análisis es una de las tareas clave del estudio probabilista de seguridad de la instalación ATI. Sin embargo, estos análisis son una tarea totalmente ajena al resto de metodologías de análisis probabilista de seguridad y, además, requieren del conocimiento de otras áreas también ajenas al núcleo de la ingeniería nuclear. Por estos motivos, y con el objetivo de no entorpecer la obtención de resultados, se ha decidido no realizar estos análisis desde cero. En su lugar, se utilizan los análisis estructurales y termohidrúalicos publicados en el NUREG-1864, que estudian el mismo tipo de contenedor, adaptándolos a las particularidades del ATI y los sucesos iniciadores estudiados. Se considera que, por similitud del diseño del contenedor, los resultados obtenidos de la adaptación de los análisis del NUREG-1864 son representativos del caso estudiado.

En esta subsección se detalla el procedimiento seguido para adaptar los resultados de los análisis publicados en el NUREG-1864 al caso del ATI estudiado. Cada análisis se divide en los sucesos iniciadores que estudia. Se presenta, para cada suceso iniciador, un resumen de la metodología utilizada en el NUREG-1864, el procedimiento seguido para adaptar los resultados, y los resultados obtenidos. La explicación proporcionada en esta subsección se extiende en el anexo E.

7.6.3.1. Análisis estructural

En el análisis estructural publicado en el NUREG-1864 se estudian, además de otros, los siguientes sucesos iniciadores identificados en el desarrollo del análisis probabilista de seguridad objeto de la tesis: Sucesos de caída (sobre superficie hormigón, en el interior del contenedor de almacenamiento, desde el vehículo de transporte), volcado, terremoto, golpeo de avión, y golpeo de meteorito.

Sucesos de caída sobre superficie de hormigón. Estudio del contenedor

Los sucesos de caída se analizan mediante un modelo de elementos finitos (LS-DYNA) [5] que evalúa la respuesta del contenedor MPC ante caídas de 1,52, 12,2, 21,3 y 30,5 m de altura, respectivamente. Este modelo presenta todos los componentes de los contenedores estudiados y, por simetría, solo necesita evaluar $\frac{1}{4}$ de la configuración real. A partir del análisis se calcula en qué elementos de modelo se produce la máxima deformación en términos de *Effective Plastic Strain*[3] (EPS) (véase el anexo E para más detalle sobre el modelo y los resultados en términos de EPS). El análisis concluye que los elementos de mayor deformación se encuentran en la soldadura que una la base del MPC con su casco cilíndrico. Por lo tanto, en el análisis de los sucesos de caída se evalúa el fallo del contenedor como la fractura de la soldadura en cuestión.

En el análisis estructural del NUREG-1864, el fallo del contenedor MPC por fractura de la soldadura que une el casco cilíndrico con la base del contenedor se valora mediante la comparación de la EPS obtenida

[3] En un escenario de esfuerzo con deformación de un objeto o pieza, la EPS es, exclusivamente, la componente plástica de la deformación generada.

con la *true strain at failure*, es decir, la deformación que, en caso de darse, iniciaría un proceso de rotura. En el anexo E se describen ciertos ajustes a aplicar en la comparación de ambas figuras. Se obtiene la probabilidad de fallo del contenedor MPC a partir de introducir la EPS máxima en la *cummulative distribution function* de la *true strain at failure*. Concretamente, se obtiene la probabilidad de que la *true strain at failure* sea igual o más pequeña que la EPS máxima calculada. Al valor de probabilidad obtenido se le denomina probabilidad de grieta en soldadura. Es importante remarcar que NUREG-1864 puntualiza que el valor calculado ha de ser tomado como conservador pues una grieta no tiene porque llevar a la ocurrencia de una brecha en la soldadura. La tabla 7.8 muestra la EPS máxima y la probabilidad de grieta en soldadura para las alturas de caída evaluadas.

Altura de caída [m]	EPS máxima [cm/cm]	Probabilidad de grieta en soldadura
1,52	0,048	<1E-06
Volcado	0,064	1E-06
12,2	0,213	3,6E-04
21,3	0,285	2,6E-03
30,5	0,385	1,96E-2

Tabla 7.8: Probabilidad de grieta en soldadura para las alturas de caída analizadas en el caso de superficie de hormigón

Los sucesos iniciadores de caída del contenedor sobre superficie de hormigón analizados en el caso de estudio están asociados a alturas de caída diferentes a las estudiadas en el NUREG-1864. Concretamente, las alturas de caída analizadas son: 0,5, 5,9, 8, y 13 m. La altura de caída es la única diferencia entre ambos conjuntos de sucesos, es decir, los del caso de estudio y los del NUREG-1864, porque el contenedor analizado es el mismo y la superficie de impacto es la misma. En consecuencia, se utiliza una función exponencial de cuatro constantes para representar la probabilidad de grieta en soldadura en función de la altura de caída (ver ecuación 15.1). Se utiliza la función exponencial porque es conservadora, ya que proporciona valores de probabilidad más altos que los de una recta segmentada que una los puntos (ver figura 7.6). La función exponencial cuenta con cuatro constantes porque el NUREG-1864 presenta cuatro pares de resultados altura de caída - probabilidad para el caso analizado.

$$P(H) = e^{(A+B*H+C*H^2+D*H^3)} \tag{7.1}$$

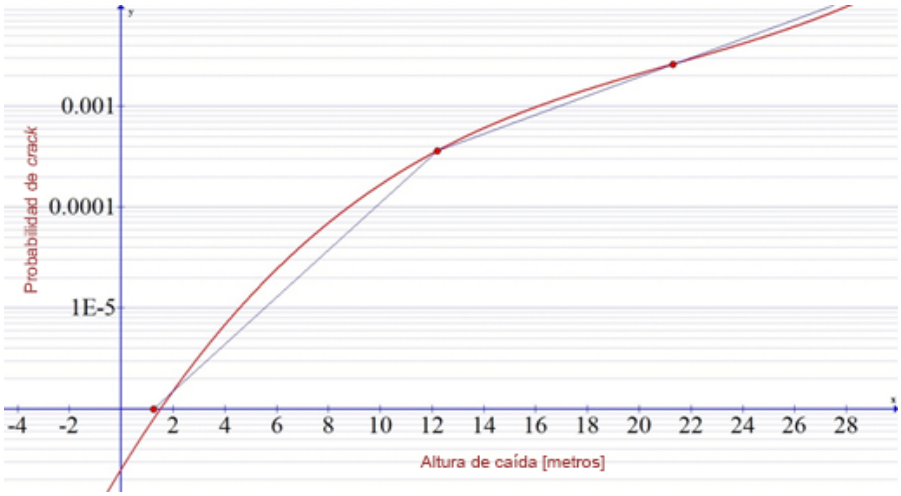


Figura 7.6: Ajuste exponencial de la probabilidad de grieta en soldadura

La tabla 7.9 muestra el valor de las constantes de la ecuación L.5, y las probabilidades de grieta en soldadura para las alturas de caída de los sucesos iniciadores analizados en el APS de ATI.

Constante	Valor	Altura de caída [m]	Probabilidad de grieta en soldadura
A	-15,2	0,5	4,028E-07
B	0,96	5,9	2,285E-5
C	-0,037	8	6,962E-5
D	0,0059	13	4,582E-4

Tabla 7.9: Constantes de la ecuación de adaptación, y valores de probabilidad de rotura para las alturas de caída de los sucesos iniciadores.

Sucesos de caída sobre superficie de hormigón. Estudio de las vainas de combustible

El NUREG-1864 estudia el posible fallo debido a pandeo de las vainas de combustible en los casos de caída mencionados en el análisis del contenedor. El modelo utilizado, que también es determinista, analiza una única vaina como una columna-haz elástica y plástica con una curvatura inicial y bajo un impacto dinámico (véase el anexo E para más información al respecto del modelo). El fallo de las vainas se determina, de forma conservadora[4], comparando la máxima deformación en la vaina con el límite de deformación basado en datos experimentales. El límite de deformación escogido es de 1 % [5], que es la mínima deformación límite atribuible al combustible de alto grado de quemado. En este caso, el análisis no proporciona la probabilidad de fallo de la vaina sino que, si la vaina del modelo falla, se considera, de forma conservadora, que en cualquier escenario similar la vaina siempre fallará y, por extensión, también fallaran el resto de vainas en el interior del contenedor. Se extrae del análisis que la altura de caída que marca la diferencia entre el no fallo y el fallo de vainas es 12,19 m. Por lo tanto, las alturas de caída 0,5 m, 5,9 m, y 8 m del caso de estudio se incluyen en los escenarios en los que las vainas no fallan. En cambio, la altura de caída de 13 m del caso de estudio se incluye entre los escenarios en los que las vainas fallan. Para su introducción en el modelo APS, se le ha asignado una probabilidad de fallo de vainas igual a uno para la caída de 13 m y una probabilidad de 0 para el resto.

[4]Se considera que el modelo es conservador porque, para eventos dinámicos de impacto, como es el caso de las caídas, donde la carga dura del orden de milisegundos, pasar el límite crítico de pandeo no causa, por si mismo, fallo de la vaina. Es la combinación de tiempo y carga la que determina si la vaina llega al fallo por deformación.

Suceso de caída del MPC en el interior del contenedor de almacenamiento

El modelo y el procedimiento utilizados en el estudio de este suceso iniciador es el mismo que en el caso anterior, con la particularidad de que el MPC cae sobre la base del contenedor de almacenamiento, que se considera rígida. En este caso, el punto que recibe la máxima deformación se encuentra en el fondo del MPC, en la superficie exterior, en la misma soldadura que une el casco cilíndrico con la base.

Al ser el diseño del contenedor del caso de estudio el mismo que el del NUREG-1864, la altura de caída evaluada es la misma. En consecuencia, los resultados presentados en el NUREG-1864 se utilizan en el modelo APS desarrollado sin ningún tipo de cambio. La probabilidad de grieta en soldadura obtenida es de 0,282 y las vainas fallan.

Suceso de caída desde el vehículo de transporte

En el análisis estructural del NUREG-1864 se criban tanto la posibilidad de volcado tras caída como la posibilidad de rotura por causa directa de la caída. Respecto al caso de volcado, el análisis estructural demuestra que en el peor caso de caída, caída con la máxima rotación posible, el contenedor puede deslizarse pero en ningún caso volcar debido a que la altura de caída posible es solo de 30,5 cm. Es decir, el contenedor no tiene espacio suficiente para desequilibrarse y volcar debido a la corta altura de caída. En el caso de caída se estudian tres superficies diferentes: hormigón, asfalto, y grava. En este caso se calcula la máxima tensión en el casco del MPC, obteniéndose los valores 53,3 MPa, 50 MPa y 39,7 MPa respectivamente. En el documento se explicita que estos valores son muy inferiores a la tensión de límite elástico del acero inoxidable del MPC.

Volcado

El análisis estructural del caso de volcado concluye que, para que el volcado sea posible con la grúa trasladándose a la máxima velocidad, es necesario que exista un ángulo de 67 grados o menor entre la horizontal y el contenedor. Para que se pueda dar esta condición la altura de caída mínima ha de ser de 40 cm, valor inferior a los 50 cm de altura, como mínimo, a los que se traslada el contenedor. En consecuencia, el volcado es posible en el caso de estudio.

Respecto al daño que causa el volcado sobre el contenedor MPC, la máxima tensión normal causada es de 406,8 MPa, a una altura de 4,53 m, y es debida a una aceleración de 45 g [78]. Esto implica una EPS de 0,0062 cm/cm. Asumiendo que esta EPS se produce en una de las soldaduras axiales o circunferenciales del casco del contenedor, la probabilidad de grieta en soldadura debida al volcado obtenida por comparación con la *cummulative distribution function* de la *true strain at failure* es de 1,0E-06.

Los sucesos iniciadores de explosión cercana se tratan como casos de volcado porque se considera que es la peor consecuencia que puede sufrir un contenedor ante una explosión de este tipo.

Terremoto

El estudio del suceso iniciador terremoto se lleva a cabo mediante dos modelos, uno 2D y otro 3D, en el NUREG-1864. En ambos modelos se calcula la aceleración horizontal necesaria, según el coeficiente de fricción de la losa del ATI, para deslizar y volcar el contenedor. El valor mínimo de aceleración horizontal que, en el peor caso, provocaría deslizamiento según el modelo 3D es de 0,5 g. En el análisis del volcado, se concluye que es necesaria una aceleración horizontal mínima de 1,35 g para causar el volcado del contenedor en el peor caso posible. Teniendo en cuenta que el diseño del contenedor es el mismo se asimilan los resultados de este análisis. Se ha cribado este suceso iniciador por ser esta aceleración mucho mayor que la del SSE de la central.

Golpeo de avión

En el análisis estructural del documento NUREG-1864 se realiza la hipótesis de que la probabilidad de que un accidente de un avión en ruta produzca una brecha en el contenedor MPC es de 1, a causa de la gran velocidad y masa de estos aparatos. En cambio, se concluye que el accidente de un avión que sale o va a aterrizar en un aeropuerto cercano tiene una probabilidad de romper el contenedor MPC de 0 debido a que su velocidad no es suficientemente alta. Esta segunda conclusión depende en gran medida de la localización de los aeropuertos cercanos y de los aviones que los utilizan, así que no es trasladable al caso de estudio. Puesto que se conoce la existencia de un aeropuerto cercano, pero se desconocen los tipos de avión que lo operan, se considera, de forma conservadora, que, en caso de accidente de uno de estos aviones, el contenedor también sufrirá una brecha en su casco. Por lo tanto, la probabilidad de fallo del MPC y de las vainas de combustible por golpeo de avión es de 1.

Meteorito

En la estimación de la frecuencia de ocurrencia de este suceso iniciador ya se tiene en cuenta que el meteorito sea capaz de causar el fallo del contenedor (véase el anexo D para más detalle). En consecuencia, la probabilidad de fallo del contenedor y de las vainas ante este suceso iniciador es de 1.

7.6.3.2. Análisis termohidráulico

Solo uno del total de sucesos iniciadores que han superado el cribado cualitativo del análisis probabilista de seguridad en cuestión, véase las tablas 7.4, 7.5, y 7.6, guarda relación con el análisis termohidráulico. Se trata, concretamente, del caso de incendio cercano. En consecuencia, este suceso es el único expuesto en la memoria de tesis doctoral.

Incendio cercano

El análisis termohidráulico del NUREG-1864 presenta un peor caso de incendio de 82,5 MW durante 3 horas con una temperatura máxima de 1200 °C. En el NUREG se específica, no obstante, que el caso de incendio estudiado es muy conservador puesto que un escenario de incendio creíble duraría mucho menos de 30 minutos. En el escenario postulado, la temperatura máxima del MPC aumenta hasta 352 °C, siendo la normal de 180 °C, y la presión interna aumenta un 12 %. Respecto a las vainas de combustible, su temperatura aumenta hasta los 298 °C, siendo en condiciones normales de 179 °C, muy por debajo del límite 570 °C [84]. Pese a que la temperatura máxima del MPC está muy por debajo de la temperatura de fusión del acero inoxidable[5] de las soldaduras, la combinación de mayor temperatura y mayor presión interna, y, por lo tanto, mayor tensión, podría dar lugar al fallo por superarse los límites de carga[6] del material o al fallo por *creep*[7]. Sin embargo, en el NUREG-1864 se han llevado a cabo sendos análisis Monte Carlo para ambos casos resultando en una probabilidad nula de fallo del contenedor por superar la carga límite o por *creep*. En consecuencia, este suceso iniciador ha sido cribado del modelo APS.

[5] El acero inoxidable austenítico 304 con el que están hechas las soldaduras tiene el punto de fusión entre 1399 y 1454 ºC aproximadamente [85].

[6] La tensión de límite elástico y la tensión de ruptura del acero utilizado en la soldadura se reducen con la temperatura.

[7] El fenómeno *Creep*, o fluencia, es la tendencia de un material sólido a deformarse permanentemente bajo la influencia de una carga que está por debajo de su límite elástico. El ratio de deformación depende de la temperatura, el tiempo de exposición a la carga, la carga aplicada, y las propiedades del material. La ocurrencia de *Creep* es más frecuente cuanto más alta sea la temperatura (por debajo del punto de fusión).

7.6.3.3. Resumen de resultados de los análisis estructural y termohidráulico

La tabla 7.10 presenta la siguiente información: el código que se va a utilizar a partir de ahora para nombrar los resultados útiles de este apartado, la descripción de los sucesos iniciadores asociados, y el valor de probabilidad de fallo del contenedor o vainas asociado.

Código	Descripción	Probabilidad del fallo del contenedor [C] o vainas [V]
MPC1	Caída de 0,5 m del contenedor de transferencia (Caída1)	4,028E-7 [C]
MPC2	Caída de 8 m debida a *two-block* (Caída2)	6,962E-5 [C]
MPC3	Caída de 5,9 m del contenedor de transferencia (Caída3)	2,285E-5 [C]
MPC4	Caída de 13 m sobre el pozo de cofres (Caída4)	4,582E-4 [C]
MPC5	Caída de 5,8 m del MPC en el interior del contenedor HI-STORM (Caída5)	2,82E-1 [C]
VOLCADO	Volcado en movimiento (Volcado)	1E-6 [C]
ACCAV	Accidente de avión (ACCAV)	1 [C]
METEO	Golpeo de meteorito (METEO)	1 [C]
VAINAS0	No se produce rotura de vainas	0 [V]
VAINAS1	Se produce rotura de vainas	1 [V]

Tabla 7.10: Resumen de resultados de los análisis estructural y termohidráulico

Estos resultados se introducen en el modelo APS en *RiskSpectrum® PSA* y se aplican a los cabeceros de integridad de contenedor e integridad de vainas de las secuencias de accidente.

7.7. Estimación del término fuente y asignación de consecuencias

La tarea de estimación del término fuente es una parte fundamental de un APS nivel 2 puesto que proporciona una de las figuras de valoración del riesgo de la instalación, concretamente, la figura que valora las consecuencias de cada escenario. El término fuente total, que se presenta en unidades de Actividad, es la suma de los términos fuente de cada radionúclido. El término fuente de cada radionúclido se calcula como el inventario[8] de radionúclido existente dentro del contenedor, que se proporciona en unidades de Actividad, por la fracción de Liberación de dicho radionúclido. Véase la ecuación 7.2, donde S_T es el término fuente total, I_i es el inventario del radionúclido i, y $F_{L,i}$es la fracción de liberación del radionúclido i.

$$S_T = \sum_{i}^{n} (I_i * F_{L,i}) \tag{7.2}$$

La fracción de liberación representa, en tanto por 1, el cociente entre el inventario de radionúclido que puede salir del contenedor y el inventario de radionúclido total existente en el contenedor. En el caso específico del ATI, la fracción de liberación se calcula como el producto entre la fracción de vainas que

[8]Se entiende como inventario a la cantidad de radionúclido existente. En el marco de los APS nivel 2, el inventario se proporciona en unidades de Actividad en lugar de unidades de masa para calcular el término fuente a partir del inventario.

fallan (F_{rods} en la ecuación 7.3), la fracción de material disponible para ser liberado que efectivamente es liberado al interior del contenedor (F_{rc} en la ecuación 7.3), y la fracción de material que ha sido liberado al interior del contenedor que finalmente pasa al ambiente (F_{ce} en la ecuación 7.3).

$$F_L = F_{rods} * F_{rc} * F_{ce} \tag{7.3}$$

Para el cálculo de estas fracciones son necesarios parámetros como los siguientes:

- Fracción de vainas que rompen y cantidad de roturas por vaina. En el análisis estructural se ha estimado conservadoramente que si rompen vainas de combustible rompen todas y el cálculo de roturas por vaina no se ha realizado.
- Partículas arrastradas por el gas en el interior de las vainas de combustible en caso de accidente. Este parámetro depende del huelgo existente en el interior de las vainas, de la configuración de los productos de fisión y del tamaño de las partículas en el borde exterior de las pastillas de combustible. La obtención de este parámetro requiere un estudio exhaustivo del estado de las vainas de combustible en el contenedor.
- Fracción de deposición de partículas en el interior del contenedor y ratio de despresurización del contenedor. Para ambos parámetros se necesita saber la superficie de brecha del contenedor, dato que no se ha calculado en este estudio.

Con el objetivo de obtener la fracción de liberación deberían realizarse una serie de análisis del estado de las vainas del combustible y del contenedor en condiciones de accidente específicas haciendo uso de modelos detallados de las propias vainas y el contenedor. Debido a la complejidad inherente a estos análisis y al estado del arte de los mismos, la realización exhaustiva de los mismos podría ser el motivo de estudio de una tesis doctoral. Por lo tanto, en el contexto de esta tesis, se ha decidido no realizar estos análisis desde cero, sino que se utilizan datos de otros estudios.

7.7.1. Inventario de radionúclidos

Se presenta en la tabla 7.11 el inventario de radionúclidos de un contenedor MPC cargado con 32 elementos de combustible gastado de diseño Westinghouse® 17x17 PWR como los de la central nuclear a la que pertenece el ATI estudiado. Los contenedores del ATI tienen mayor o menor inventario de radionúclidos dependiendo de características como el enriquecimiento inicial del combustible, el grado de quemado, y el tiempo de almacenamiento en piscina. Dichas características son específicas de cada elemento de combustible, y, por lo tanto, es altamente probable que dos contenedores tengan un inventario de radionúclidos diferente. En el marco de este APS se estudia, conservadoramente, un contenedor que está cargado con 32 elementos de combustible con las características límite para poder ser almacenados en seco según el Estudio Final de Seguridad del ATI: enriquecimiento inicial máximo de 5 %, grado de quemado máximo de 55000 MWd/TU, y tiempo de enfriamiento en piscina mínimo de 5 años. La carga de un contenedor MPC con 32 elementos de características límite es una situación extrema que está prohibida por el propio EFS del ATI, que dictamina que el contenedor se divide en dos regiones, una para elementos de combustible con alto grado de quemado y otra para elementos con grado de quemado inferior. Asimismo, un contenedor cargado con 32 elementos de combustible de características límite supera el umbral de potencia térmica de diseño del contenedor estipulada en su estudio final de seguridad. A pesar de que, salvo error, es imposible que se cargue un contenedor con una configuración de elementos de combustible de características límite, se decide calcular y presentar el inventario de radionúclidos de dicha configuración puesto que es envolvente de cualquier otro estado de carga de un contenedor.

El inventario de radionúclidos del contenedor postulado se ha obtenido mediante simulación con el código ORIGEN-S ejecutado desde el paquete SCALE5.1. Se ha simulado la irradiación de un elemento de

combustible con las características mencionadas anteriormente durante tres ciclos de 18 meses[9][10] cada uno, separados por periodos de enfriamiento de 40 días, llegando a un grado de quemado de 55000 MWd/TU. Se ha simulado también el posterior enfriamiento del combustible durante los primeros siete años en piscina. El inventario del contenedor se ha calculado mediante la multiplicación del inventario obtenido para un elemento de combustible pasados 5 años de enfriamiento por la cantidad de elementos de combustible que tienen cabida en el contenedor, que es de 32. El anexo F contiene las características principales, como, por ejemplo, la composición, del elemento de combustible simulado así como los principales inputs de la simulación realizada. La tabla 7.11 presenta el inventario de radionúclidos para el contenedor MPC postulado.

Radionúclido	Inventario (Bq)	Radionúclido	Inventario (Bq)
Pu-241	8,24E+16	Am-241	8,85E+14
Cs-137	8,41E+16	Co-60	3,54E+14
Ba-137m	7,94E+16	H-3	3,88E+14
Y-90	5,94E+16	Pr-144m	1,09E+14
Sr-90	5,94E+16	Pu-240	3,61E+14
Cs-134	2,83E+16	Sm-151	3,22E+14
Pm-147	2,93E+16	Cm-242	2,79E+13
Rh-106	1,21E+16	Sn-119m	7,46E+13
Ru-106	1,21E+16	Pu-239	2,19E+14
Pr-144	7,77E+15	Mn-54	2,55E+13
Ce-144	7,77E+15	Ag-110m	1,66E+13
Kr-85	6,07E+15	Np-239	2,79E+13
Eu-154	4,52E+15	Am-243	2,79E+13
Cm-244	3,90E+15	Cm-243	2,30E+13
Pu-238	3,82E+15	Tc-99	1,17E+13
Fe-55	1,93E+15	Sn-121m	1,11E+13
Sb-125	1,91E+15	Am-242	9,55E+12
Eu-155	1,24E+15	Am-242m	9,59E+12
Ni-63	7,34E+14	Sn-121	8,63E+12
Te-125m	4,68E+14	Ni-59	5,71E+12

Tabla 7.11: Inventario de radionúclidos para el contenedor MPC estudiado.

La actividad total del contenedor tras 5 años de enfriamiento es de 4,90E+17 Becquerels. La figura 7.7 presenta la evolución de la actividad del elemento de combustible simulado durante los 7 años de enfriamiento estudiados. Se muestra el total y los radionúclidos más importantes.

[9] Los ciclos de operación de centrales nucleares de diseño PWR de generación II duran, aproximadamente, 18 meses. Entre ciclos de operación se llevan a cabo las llamadas paradas de recarga, en las cuales se cambia el combustible y se realizan tareas de mantenimiento durante un periodo de aproximadamente 40 días.

[10] Los elementos de combustible participan en tres ciclos de operación en un reactor de diseño PWR. En cada ciclo de operación se colocan en regiones diferentes del reactor. En cada parada de recarga se cambia un tercio de los elementos de combustible del reactor.

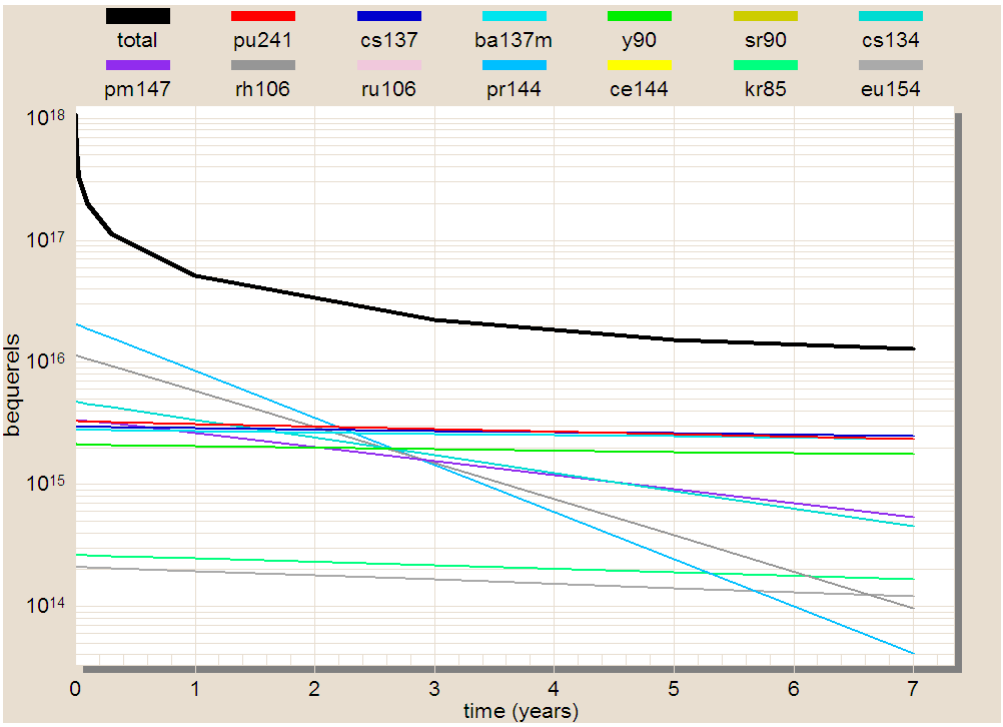


Figura 7.7: Evolución de la actividad, en Becquerels, del elemento de combustible simulado durante los primeros 7 años de postirradiación.

7.7.2. Fracción de liberación

La fracción de liberación utilizada en el marco de este APS se obtiene del documento NUREG-1864 debido a las consideraciones expuestas anteriormente. Concretamente, desde un punto de vista conservador, se elige el peor de los casos estudiados en el NUREG-1864 como caso representativo, y envolvente, de todas las secuencias de accidente de este modelo APS. El peor caso analizado en el NUREG-1864 es el de una caída del contenedor de transferencia, con el contenedor MPC sellado en su interior, de 30,5 m de altura. Dicha altura es mucho mayor que la máxima altura de caída analizada en el APS, que es de 13 m. Se asume que el comportamiento de las vainas de un elemento PWR y el de las vainas de un elemento BWR es el mismo en caídas de altura considerable. Las fracciones de liberación obtenidas, agrupadas por gases nobles, partículas sólidas, y CRUD[11] (*Chalk River Unidentified Deposit*), se presentan en la tabla 7.12.

	Gases Nobles	Partículas	CRUD
Fracción de Liberación	0,12	1,2E-3	1,5E-3

Tabla 7.12: Fracciones de liberación representativas de todas las secuencias de accidente del APS.

7.7.3. Niveles discretos del estado final y término fuente

La elección de los niveles de discretos del estado final de las secuencias de accidente, sección 14.2, depende de la tipología del accidente y de la fracción de liberación asociada al mismo. En este caso, y pese a que

[11] El CRUD es un sedimento, transportado por el agua del sistema primario, que queda enganchando en las vainas de combustible. Se origina en los elementos metálicos del sistema primario y se activa al pasar por el reactor. El isótopo radioactivo mayoritario en el CRUD es el cobalto-60.

solo se presente un resultado en términos de fracción de liberación, se diferencia entre aquellos casos en los que las vainas no fallan y los casos en los que sí fallan. Se aplica únicamente la fracción de liberación del CRUD en aquellos casos en los que, pese a que las vainas no fallasen, se daría liberación de radionúclidos debido al fallo de la integridad del contenedor MPC. Se aplica la totalidad de la fracción de liberación si las vainas fallan. Respecto a las características de los sucesos iniciadores, ya sea en la identificación de sucesos iniciadores o en el Análisis de datos se han cribado aquellos casos, concretamente, incendios y penetraciones del contenedor, cuya influencia sobre la fracción de liberación sería diferente a la de caída o volcado del contenedor. Así pues, se consideran únicamente dos niveles discretos de estado final: el nivel asociado a la única liberación del CRUD, y el nivel asociado a la liberación de todos los tipos posibles de partículas y/o elementos. El primero se considera como Muy Bajo debido al poco inventario de CRUD en el contenedor y a la fracción de liberación de éste. El segundo, que incluye todo, se considera Alto en comparación con el primero. La tabla 7.13 presenta los términos fuente, agrupados por tipos de partículas y/o elementos, de los dos niveles discretos del estado final. Del inventario presentado en la tabla 7.11, se asume conservadoramente que todo el inventario de cobalto-60 es CRUD[12].

Estado final	Gases Nobles	Partículas solidas	CRUD	Término fuente total (Bq)
Muy bajo	X	X	5,31E+11	5,31E+11
Alto	7,28E+14	5,80E+14	5,31E+11	1,31E+15

Tabla 7.13: Término fuente de los niveles discretos del estado final.

7.8. Cuantificación

En el estudio probabilista, de nivel 2, de un Almacén Temporal Individualizado, el objetivo principal de la tarea de cuantificación es obtener las ecuaciones booleanas de las secuencias de accidente, y las Frecuencias de Liberación de Radionúclidos al ambiente asociadas, agrupadas por Suceso Iniciador. A diferencia de un APS de nivel 1 de sucesos internos a Potencia, no es posible obtener la ecuación final de daño representativa de todo el proceso debido a las diferencias en la manipulación del contenedor en las tres etapas del ciclo de vida del almacenamiento. No obstante, es interesante obtener los Conjuntos Mínimos de Fallo (CMF) y la frecuencia asociada a cada secuencia de accidente, consecuencia, y etapa del ciclo de vida de almacenamiento, para poder analizar qué sucesos son los más críticos para la seguridad en la manipulación del contenedor. Los CMF, o *minimal cut-sets,* son combinaciones de sucesos básicos que, junto con un suceso iniciador, provocan Liberación de Radionúclidos.

7.8.1. Descripción de la tarea de cuantificación

La metodología de cuantificación empleada en el estudio piloto probabilista del ATI se basa en la aplicación *RiskSpectrum® PSA*. Se cuantifican las secuencias de accidente de los árboles de sucesos de todos los sucesos iniciadores del proyecto. La cuantificación de las secuencias de los árboles de sucesos tiene en cuenta el estado en éxito o en fallo de los cabeceros que se presentan en su evolución. Los cabeceros contienen como entrada una serie de *Top Events*, que en el caso del estudio probabilista del ATI se relacionan directamente con probabilidades de fallo de las barreras de contención o, en el caso de las secuencias de la etapa de carga, con el árbol de fallos del Sistema de ventilación HVAC del Edificio de Combustible.

[12]Parte del inventario de cobalto-60 proviene de la activación del cobalto presente en las aleaciones que conforman los elementos de combustible.

En la cuantificación de secuencias de accidente se obtienen las ecuaciones booleanas reducidas para todas aquellas secuencias definidas que tengan consecuencia negativa, es decir, que den como resultado Liberación de Radionúclidos. En su forma reducida, una ecuación booleana es un sumatorio de CMFs. No es necesario obtener la ecuación booleana ni la frecuencia de las secuencias que no llevan a consecuencias negativa. La cuantificación se realiza para cada escenario de accidente postulado, y se obtiene la Frecuencia de Liberación y los CMF para cada etapa del ciclo de vida del almacenamiento. Cada ecuación booleana viene definida a nivel de sucesos básicos y contiene las mínimas combinaciones de fallos de componentes que pueden llevar a la ocurrencia de la consecuencia negativa, es decir, los conjuntos mínimos de fallo que conducen a daño.

Se implementan tres bases de datos en el modelo APS: "BDPOTENCIA11.rsd" para la etapa de carga, "FASEDETRANSF.rsd" para la etapa de transferencia y "FASEDEALM.rsd" para la etapa de almacenamiento. Todos los datos contenidos en cada base de datos están documentados en la sección de Análisis de datos y sus anexos de soporte. No es objeto de este documento explicar el funcionamiento y nomenclatura de la aplicación utilizada *RiskSpectrum® PSA*, que puede consultarse en el manual de usuario del mismo.

7.8.2. Especificaciones de la cuantificación

A causa de la complejidad de los modelos APS, en la tarea de cuantificación se define un límite de truncamiento para los conjuntos mínimos de fallo con el objetivo de obtener ecuaciones booleanas manejables. El límite de truncamiento se define en términos de frecuencia de ocurrencia de la consecuencia negativa. Todo CMF cuyo valor de frecuencia de ocurrencia sea superior al límite de truncamiento es incluido en las ecuaciones booleanas reducidas. La elección del límite de truncamiento es importante puesto que determina qué partes del modelo no se tienen en cuenta en la cuantificación. De hecho, uno de los análisis de sensibilidad más aplicados en el campo del APS es el de variar el límite de truncamiento y analizar cómo se ve afectada la frecuencia de consecuencia negativa. Con la mejora de la capacidad y la velocidad de cálculo de las herramientas informáticas, el límite de truncamiento tiende a ser cada vez más bajo para incluir más conjuntos mínimos de fallo en las ecuaciones booleanas.

Como referencia, en el APS de sucesos internos a Potencia, de nivel 1 y nivel 2, de la central nuclear se utiliza un límite de truncamiento de 1E-9 (año^{-1}). No obstante, en el presente estudio se adopta un límite de truncamiento de a 1E-15 ((año·contenedor)$^{-1}$) ya que, al analizarse sucesos iniciadores cuya frecuencia de ocurrencia es mucho menor que el nivel de cribado utilizado habitualmente en los APS (1E-06 (año^{-1})), se espera que los valores de frecuencia de liberación de radionúclidos sean más pequeños que en los estudios de APS de sucesos internos a Potencia. Si se utilizase un limite de truncamiento de 1E-9 (año^{-1}) se correría el riesgo de dejar fuera de la cuantificación una gran parte del modelo APS de ATI.

7.8.2.1. Resultados de la cuantificación

Las tablas 7.14, 7.15, y 7.16 presentan la frecuencia de liberación de radionúclidos y la cantidad de CMF de la ecuación booleana de cada Suceso Iniciador y cada etapa del proceso de almacenamiento de los contenedores. Las frecuencias de liberación de la etapa de carga y la etapa de transferencia se presentan ponderadas por el tiempo de duración de cada etapa en el primer año de almacenamiento de un contenedor, respectivamente. En cambio, las frecuencias de liberación de la etapa de almacenamiento presentadas en la tabla 7.16 son puntuales. Estas frecuencias son representativas del riesgo de la instalación en los años posteriores al de la carga y transferencia del contenedor, pero deberían ponderarse mediante el tiempo de duración de la etapa de almacenamiento en el primer año de vida del contenedor para ser también representativas del riesgo asociado a la etapa de almacenamiento durante este primer año. Sin embargo, la etapa de almacenamiento es predominante también durante el primer año de almacenamiento del contenedor, ya que las etapas de carga y transferencia acostumbran a durar entre 3 y 6 días, con lo que los valores ponderados son prácticamente equivalentes a los puntuales. En el anexo G se tabulan los CMF

de las ecuaciones booleanas obtenida en la cuantificación para cada suceso iniciador. No se presentan los CMF de las secuencias de las etapas de transferencia y almacenamiento porque solo existe un CMF para cada suceso iniciador. El anexo B, que contiene los árboles de sucesos del modelo APS, presenta también las frecuencias de liberación de radionúclidos de cada secuencia de accidente de cada suceso iniciador.

Suceso Iniciador	FLR (año·contenedor)$^{-1}$	# CMF
Caída1	2,03E-14	11
Caída2	3,59E-12	147
Caída3	1,18E-12	43
Caída4	2,38E-11	393
Caída5	1,47E-08	3274
Volcado	5,05E-14	11

Tabla 7.14: FLR y cantidad de CMF para los sucesos iniciadores de la etapa carga.

Suceso Iniciador	FLR (año·contenedor)$^{-1}$	# CMF
EXPTRANS	2,27E-15	1

Tabla 7.15: FLR y cantidad de CMF para los sucesos iniciadores de la etapa de transferencia.

Suceso Iniciador	FLR (año·contenedor)$^{-1}$	# CMF
ACCAV	6,69E-11	1
EXPALM	1,66E-12	1
METEO	2,88E-13	1

Tabla 7.16: FLR y cantidad de CMF para los sucesos iniciadores de la etapa de almacenamiento.

A excepción del Suceso Iniciador Caída5, las frecuencias de liberación de radionúclidos de todos los sucesos iniciadores serían cribadas en un APS nivel 2 de sucesos internos a Potencia. Se pone de manifiesto el bajo nivel de riesgo asociado al ATI, al menos, en términos de FLR en comparación con el riesgo asociado al reactor nuclear.

7.9. Análisis de resultados

Esta sección presenta la tarea de análisis e interpretación de los resultados obtenidos mediante el modelo APS, es decir, la frecuencia de liberación de radionúclidos y el término fuente de cada suceso iniciador. Esta tarea incluye la realización de los análisis de importancia (véase anexo Ñ) , sensibilidad, e incertidumbre de la frecuencia de liberación de radionúclidos. Específicamente para este APS, también se comparan los resultados obtenidos con los del APS de sucesos internos a Potencia de nivel 2 de la central nuclear.

7.9.1. Interpretación de resultados

Las tablas 8.16, 7.18, y 7.19 presentan los resultados obtenidos en el APS para cada Suceso Iniciador y cada etapa del proceso de almacenamiento del contenedor. Las tablas contienen tanto la frecuencia de liberación como el término fuente.

Suceso Iniciador	FLR (año·contenedor)$^{-1}$	Estado final	Término Fuente [Bq]
Caída1	2,03E-14	Muy bajo	5,31E+11
Caída2	3,59E-12	Muy bajo	5,31E+11
Caída3	1,18E-12	Muy bajo	5,31E+11
Caída4	2,38E-11	Alto	1,31E+15
Caída5	1,47E-08	Alto	1,31E+15
Volcado	5,05E-14	Muy bajo	5,31E+11

Tabla 7.17: Resultados obtenidos para la etapa de carga.

Suceso Iniciador	FLR (año·contenedor)$^{-1}$	Estado final	Término Fuente [Bq]
EXPTRANS	2,27E-15	Muy bajo	5,31E+11

Tabla 7.18: Resultados obtenidos para la etapa de transferencia.

Suceso Iniciador	FLR (año·contenedor)$^{-1}$	Estado final	Término Fuente [Bq]
ACCAV	6,69E-11	Alto	1,31E+15
EXPALM	1,66E-12	Muy bajo	5,31E+11
METEO	2,88E-13	Alto	1,31E+15

Tabla 7.19: Resultados obtenidos para la etapa de almacenamiento.

La tabla 7.20 presenta la estimación de la frecuencia de liberación de radionúclidos representativa del primer año del proceso de almacenamiento, es decir, el año en el que se llevan a cabo las etapas de carga y transferencia, y la de los años posteriores. Teniendo en cuenta que durante el primer año del proceso de almacenamiento se dan las tres etapas, la frecuencia representativa de todo el año es la suma ponderada de las frecuencias puntuales de cada etapa, siendo el peso de ponderación el tiempo que dura cada etapa. Sin embargo, las frecuencias de los sucesos iniciadores de la etapa de carga, las caídas, ya han sido calculadas en base anual en trasladar una probabilidad en demanda a una frecuencia anual. De la misma manera, la frecuencia del Suceso Iniciador explosión cercana de la etapa de transferencia ya se ha ajustado, véase la sección 7.6, a la duración de dicha etapa. La FLR de la etapa de almacenamiento es la única frecuencia a ajustar mediante el tiempo de duración de la etapa, pero, debido a la larga duración de esta etapa en comparación con las otras, se utilizan los resultados puntuales de frecuencia como si ya estuviesen ponderados.

FLR [1/(año·contenedor)]	Primer año de almacenamiento	Años posteriores
Etapa de carga	1,47E-8	X
Etapa de transferencia	2,27E-15	X
Etapa de almacenamiento	6,88E-11	6,88E-11
Total	1,48E-8	6,88E-11

Tabla 7.20: FLR del primer año y de los años venideros.

A la vista de las tablas se concluye que existen dos sucesos iniciadores predominantes: el suceso iniciador Caída5 (Caída del MPC en el interior del contenedor de almacenamiento) con una FLR de 1,47E-8 (año·contenedor)$^{-1}$ y consecuencia Alto, y el suceso iniciador ACCAV (accidente de avión) con una FLR de 6,49E-11 (año·contenedor)$^{-1}$ y consecuencia Alto. El Suceso Iniciador Caída5 es el suceso predominante de la etapa de carga y del primer año de manipulación del contenedor, mientras que el suceso iniciador ACCAV gobierna la FLR de la etapa de almacenamiento y, por lo tanto, la FLR de los años venideros. Tomando en consideración que la FLR del primer año es tres órdenes de magnitud superior que la de los años venideros, el suceso más importante, en términos de riesgo, es el suceso iniciador Caída5.

7.9.2. Análisis de importancia

El análisis de importancia aplicado a los resultados del APS de ATI se puede consultar, en su totalidad, en el anexo N. En el estudio piloto probabilista de ATI solo tiene sentido aplicar el análisis de importancia a los resultados de la etapa de carga, puesto que es la única etapa en la que una misma secuencia de accidente se puede dar porque ocurran diferentes combinaciones de sucesos básicos. A la vista de la predominancia del Suceso Iniciador Caída5, el análisis de importancia se ha aplicado exclusivamente a los resultados de este suceso. La tabla 7.22 muestra los sucesos básicos con mayor valor de la figura de importancia Fussell-Vesely para el caso estudiado. Se observa que, a parte del suceso iniciador y las probabilidades de fallo de las barreras de confinamiento, que participan en todas las secuencias de accidente, los sucesos básicos más importantes son los relacionados con la indisponibilidad de las compuertas de los sistemas de extracción y suministro de aire.

Suceso básico[13]	Indisponibilidad o probabilidad de fallo	Fussell-Vesely
CMANT1B	7,79E-03	2,38E-01
CMANT2B	7,79E-03	2,38E-01
CMANT3B	7,79E-03	2,38E-01
1M9GDA38BM	7,79E-03	2,36E-01
CMANT3A	7,79E-03	2,36E-01
CMANT	7,79E-03	2,36E-01

Tabla 7.21: Sucesos básicos más importantes según la figura de Fussell-Vesely.

7.9.3. Análisis de sensibilidad

En el marco del análisis de sensibilidad se evalúa, exclusivamente, la influencia del límite de truncamiento de CMFs en la estimación de la frecuencia de liberación de radionúclidos. Concretamente, se ha rebajado el límite de truncamiento a 1E-16 por año para analizar si el límite de truncamiento utilizado en el proceso de cuantificación criba demasiados CMFs. A la vista de las conclusiones extraídas en el análisis de resultados, se han recuantificado únicamente los dos casos predominantes. Los valores de FLR obtenidos con el nuevo límite de truncamiento para los sucesos Caída5 y ACCAV son:

- FLR (Caída5) = 1,47E-08 (año·contenedor)$^{-1}$
- FLR (ACCAV) = 6,69E-11 (año·contenedor)$^{-1}$

Se observa que la FLR de ambos casos no cambia. Por lo tanto, todos los CMF que contribuyen de manera importante al riesgo ya habían sido incluidos en el proceso de cuantificación.

7.9.4. Análisis de incertidumbre

La incertidumbre de algunos parámetros clave del modelo APS, como, por ejemplo, las probabilidades de fallo de las barreras de confinamiento o las frecuencias de los sucesos iniciadores, no han sido incluidas en el modelo APS. En la mayoría de casos se ha desestimado el cálculo de las incertidumbres asociadas porque la complejidad de cálculo no estaba de acuerdo con la naturaleza piloto del análisis. Consecuentemente, a parte de las incertidumbres epistémicas inherentes al modelo, el modelo APS creado en *RiskSpectrum*® *PSA* tampoco es capaz de analizar las incertidumbres aleatorias y epistémicas asociadas a las frecuencias de ocurrencia de lo sucesos iniciadores y a las probabilidades de los cabeceros de las barreras de confinamiento. Visto de otra manera, la única fuente de incertidumbre que puede valorar el modelo APS es la incertidumbre epistémica de los sucesos básicos empleados en el modelo del árbol de fallos del sistema de ventilación. Esta única fuente de incertidumbre se considera insuficiente como para representar la incertidumbre real de los resultados y, por lo tanto, su evaluación no se incluye en la memoria de tesis. No obstante, el análisis de incertidumbre proporcionado por *RiskSpectrum*® *PSA* se incluye en el anexo H.

7.9.5. Comparación con los resultados de un APS de sucesos internos a Potencia de nivel 2

La tabla 7.22 presenta los peores casos de frecuencia de liberación y término fuente obtenidos del APS[14] de sucesos internos a Potencia de nivel 2. El caso R2[15] es el de mayor actividad total de liberación y el caso R9[16] es el de mayor frecuencia de liberación.

Categoría de liberación	Frecuencia de liberación (por año)	Actividad total de liberación (Bq)
R2	8,30E-10	1,57E+19
R9	1,72E-05	1,19E+17

Tabla 7.22: Frecuencia de liberación y término fuente de la central nuclear de estudio. Peores casos

En comparación, la tabla 7.23 presenta la frecuencia de liberación de radionúclidos y el término fuente de los casos predominantes identificados en el APS de ATI.

Suceso Iniciador	FLR [1/(año·contenedor)]	Actividad total de liberación de un contenedor (Bq)
Caída5	1,47E-08	1,31E+15
ACCAV	6,69E-11	1,31E+15

Tabla 7.23: Frecuencia de liberación de radionúclidos y término fuente del ATI de estudio. Casos predominantes.

El término fuente de los casos predominantes del ATI es cuatro órdenes de magnitud menor que el mayor término fuente calculado en el APS de sucesos internos a Potencia nivel 2 de la central nuclear, dos órdenes de magnitud menor que el término fuente del caso cuya frecuencia de liberación es predominante en el

[14] Versión anterior al año 2002.

[15] La categoría R2 hace referencia a un fallo de la contención anterior o en el momento del fallo de la vasija con el sistema de aspersión indisponible. Es la categoría con mayor Actividad total de liberación.

[16] La categoría R9 hace referencia a la penetración de la losa de hormigón. Es la categoría con mayor frecuencia de ocurrencia.

APS de sucesos internos a Potencia nivel 2 de la central, y un orden y medio de magnitud menor que el caso más favorable[17] calculado en el APS de sucesos internos a Potencia de nivel 2 de la central. Respecto a la frecuencia de liberación del suceso Caída5, ésta es tres órdenes de magnitud menor que la mayor frecuencia calculada en el APS de sucesos internos a Potencia de nivel 2 de la central, y entre uno y dos órdenes de magnitud mayor que la frecuencia de liberación más baja calculada en el APS de sucesos internos a Potencia de nivel 2 de la central, que es la del caso R2. De los 12 casos postulados en el APS de sucesos internos a Potencia de nivel 2 de la central, la FLR del suceso Caída5 es menor que 10 de ellos, y la del suceso ACCAV es menor que las de todos los casos. En consecuencia, mediante la comparación se concluye que el término fuente calculado en el APS de ATI es sustancialmente menor que el de APS de sucesos internos a Potencia de nivel 2 de la central nuclear, y que la mayor frecuencia de liberacción de radionúclidos calculada en el APS de ATI, la del suceso Caída5, no es significativa en relación con las frecuencias de liberación del APS de sucesos internos a Potencia de nivel 2 de la central. Se ha de tener en cuenta, no obstante, que tanto la frecuencia de liberación como el término fuente se han calculado en base a un contenedor del ATI, cuando la zona de almacenamiento de este podría albergar hasta 32 unidades. A la vista de esta comparación, y teniendo en cuenta el notable grado de conservadurismo aplicado tanto en el cálculo de la FLR como del término fuente en el APS de ATI, se concluye que el riesgo asociado a un contenedor del ATI es sustancialmente inferior al inherente al reactor de la central nuclear.

Para dotar de más significado a la comparación y poder enfrentar directamente el riesgo del ATI con el de la central, se ajustan los valores de FLR de los sucesos predominantes del ATI multiplicando su FLR y su término fuente por el número de contenedores esperados en cada caso. Los valores obtenidos son máximos puesto que representan los peores escenarios para casa caso. Multiplicando el valor anterior por cinco[18], se obtiene un valor máximo de FLR de 7,35E-08 por año para el suceso Caída5, que sigue siendo sustancialmente menor, concretamente, más de dos órdenes de magnitud menor, que el máximo valor de frecuencia de liberación del APS de sucesos internos a Potencia de nivel 2 de la central. Respecto al suceso ACCAV, conservadoramente, se obtiene el valor máximo de FLR considerando que la losa de almacenamiento del ATI soporta el mayor número de contenedores posibles, es decir, 32, y utilizando como área efectiva el área de dicha losa de almacenamiento. El valor máximo de FLR del suceso ACCAV obtenido en las condiciones descritas es de 8,19E-10 por año. Este valor de FLR aún sería cribado en un APS de sucesos internos a Potencia de nivel 2 de una central nuclear. En relación al término fuente, se observa que el del caso predominante del APS de sucesos internos a Potencia de nivel 2 de central, cuyo valor es de 1,57E+19 Bq (caso R2), es cuatro órdenes de magnitud mayor que el término fuente calculado para los sucesos Caída5 y ACCAV (1,31E+15 Bq). Este término fuente ya es acoplable al peor caso del suceso Caída5 puesto que solo se puede transportar un contenedor a la vez, pero aún no es acoplable al peor caso de ACCAV en el que los 32 contenedores están sobre la losa sísmica. Multiplicando el término fuente de ACCAV por 32 se obtiene un valor de 4,19E+16 Bq, que aún sigue siendo menor que cualquiera de los términos fuente calculados en el APS de sucesos internos a Potencia de nivel 2 de la central. A la vista de la comparación realizada, y teniendo en cuenta el notable grado de conservadurismo inherente al APS de ATI, se concluye que los resultados orientativos obtenidos al respecto del riesgo del ATI son sustancialmente bajos, prácticamente despreciables, en comparación con el riesgo de la central en sí. En consecuencia, se concluye que la contribución del riesgo del ATI al riesgo total del emplazamiento es prácticamente nula.

7.10. Conclusiones

Los resultados orientativos al respecto del riesgo del ATI obtenidos en el desarrollo del modelo APS presentado señalan la existencia de dos sucesos iniciadores predominantes: el Suceso Iniciador Caída5, y

[17] La actividad total de liberación de radionúclidos del caso más favorable calculado en el APS nivel 2 de la central es de 5,85E+16 Bq.

[18] Serían necesarios cinco contenedores para extraer un núcleo de reactor de la piscina, por lo tanto, se considera que cinco es el número máximo de contenedores a cargar en un año.

el Suceso Iniciador ACCAV. El primero, que solo puede ocurrir durante la etapa de carga, representa la caída del contenedor MPC sobre la base del contenedor de almacenamiento, siendo la altura de caída de 5,8 m, en el momento en el que el primero es introducido en el segundo. La frecuencia de liberación de radionuclidos, ponderada para el primer año, del suceso Caída5 es de 1,47E-08 (año·contenedor)$^{-1}$, y su término fuente es de 1,31E+15 Bq. El suceso Caída5 es predominante en el primer año del período de almacenamiento de un contenedor, siendo su FLR tres órdenes de magnitud mayor que la siguiente más alta. El resultado obtenido pone de manifiesto que, en comparación con las otras maniobras de la etapa carga, y con el resto de operaciones del primer año de almacenamiento, la introducción vertical del MPC en el HI-STORM 100 es la mayor vulnerabilidad del procedimiento. De entre todos los elementos del modelo, el principal contribuyente a la FLR del suceso Caída5 es la probabilidad de fallo del contenedor MPC condicionada a la propia caída, que es de 0,282 veces por suceso. La caída estudiada, de 5,8 m, corresponde a la altura del contenedor HI-STORM. En consecuencia, la altura de caída no puede ser menor que 5,8 m en el procedimiento de inserción vertical del MPC en el interior del HI-STORM. De juzgarse el riesgo del suceso Caída5 como demasiado alto, se deberían plantear alternativas a la inserción vertical como, por ejemplo, la inserción horizontal, con la inversión en infraestructura que esto supondría, o bien el uso de medidas de protección y seguridad como elementos amortiguadores, sistemas de eslingas redundantes, u otros elementos que o bien redujesen la probabilidad de fallo del contenedor o la frecuencia de ocurrencia de una caída. No obstante, a la vista de los resultados obtenidos en comparación con los de la central nuclear, y teniendo en cuenta el notable grado de conservadurismo aplicado en el cálculo de la frecuencia del suceso iniciador, en el cálculo de la probabilidad de grieta en soldadura, y en el cálculo del término fuente del contenedor, se concluye que el riesgo inherente al suceso Caída5, y, por extensión, el riesgo inherente al primer año de almacenamiento de un contenedor en el ATI, no es significativo.

El Suceso Iniciador ACCAV representa el golpeo de un contenedor, estando éste en la zona de almacenamiento, por motivo del accidente de un avión. La frecuencia de liberación de radionúclidos, ponderada para el primer año, del suceso Caída5 es de 6,69E-11 (año·contenedor)$^{-1}$, y su término fuente es de 1,31E+15 Bq. El suceso ACCAV es predominante en la etapa de almacenamiento del proceso, y, por lo tanto, es el suceso predominante al respecto del riesgo del ATI en los años en los que el contenedor está a la intemperie en la zona de almacenamiento. El riesgo inducido por ACCAV podría reducirse con la construcción de un edificio de almacenamiento[19] en el que se introdujesen los contenedores, o con la inserción de los contenedores en cápsulas excavadas en la losa sísmica. No obstante, la FLR del suceso es tan baja, téngase en cuenta que sería cribada en el APS de sucesos internos a Potencia de nivel 2 de una central, que no se considera necesario llevar a cabo acción alguna para reducir su riesgo, que se valora como no significativo.

En la comparación de la FLR y el término fuente de los dos sucesos predominantes identificados con los resultados de un APS de sucesos internos a Potencia de nivel 2 de la central nuclear (véase la tabla 7.22) se observa que: la frecuencia de liberación del caso predominante del APS de sucesos internos a Potencia de nivel 2 de central, cuyo valor es de 1,72E-05 por año (caso R9), es tres órdenes de magnitud mayor que la FLR del caso más predominante identificado en el APS de ATI (suceso Caída5, FLR = 1,47E-08 por año y por contenedor), y aproximadamente seis órdenes de magnitud mayor que la FLR del suceso ACCAV (FLR = 6,69E-11 por año y por contenedor). Respecto al término fuente, se observa que el del caso predominante del APS de sucesos internos a Potencia de nivel 2 de central, cuyo valor es de 1,57E+19 Bq (caso R2), es cuatro órdenes de magnitud mayor que el término fuente calculado para los sucesos Caída5 y ACCAV (1,31E+15 Bq). Teniendo en cuenta estos resultados, se concluye que el riesgo orientativo asociado a un contenedor del ATI es sustancialmente inferior al inherente al reactor de la central nuclear.

Se han ajustado los valores de FLR y de término fuente de los sucesos del ATI multiplicándolos por el número máximo de contenedores esperados en cada caso para así poder comparar el riesgo del ATI con el riesgo de la central en los mismos términos. Los valores obtenidos son máximos puesto que representan los peores escenarios para cada caso. Se ha obtenido un valor máximo de FLR de 7,35E-08 por año

[19] De optar por una solución de este tipo, se debería garantizar que la frecuencia de ocurrencia del nivel mínimo de sismo que pudiese causar el fallo estructural del edificio es menor que la frecuencia de ocurrencia de ACCAV.

para el suceso Caída5, que sigue siendo sustancialmente menor, más de dos órdenes de magnitud, que el máximo del APS de sucesos internos a Potencia de nivel 2 de la central. Respecto al suceso ACCAV, conservadoramente, se ha obtenido el valor máximo de FLR considerando que la losa de almacenamiento del ATI soporta el mayor número de contenedores posibles. El valor máximo de FLR del suceso ACCAV obtenido en las condiciones descritas es de 8,19E-10 por año. Este valor de FLR aún sería cribado en un APS de sucesos internos a Potencia de nivel 2 de una central nuclear. Respecto al término fuente, el término calculado para los sucesos Caída5 y ACCAV (1,31E+15 Bq) ya es acoplable al peor caso del suceso Caída5 puesto que solo se transporta un contenedor a la vez, pero aún no es acoplable al peor caso de ACCAV en el que los 32 contenedores están sobre la losa sísmica. Se ha obtenido un término fuente de 4,19E+16 Bq para el peor caso de ACCAV, que aún sigue siendo menor que cualquiera de los términos fuente calculados en el APS de sucesos internos a Potencia de nivel 2 de la central. A la vista de los resultados obtenidos, y teniendo en cuenta el notable grado de conservadurismo inherente al APS de ATI, se concluye que los resultados, orientativos, obtenidos al respecto del riesgo del ATI son sustancialmente bajos, prácticamente despreciables, en comparación con el riesgo de la central en sí. En consecuencia, se concluye que la contribución del riesgo del ATI al riesgo total del emplazamiento es prácticamente nula.

Sin embargo, el modelo APS de ATI desarrollado mediante técnicas probabilistas presenta, en su cualidad de piloto, algunas carencias. Positivamente, en el desarrollo del modelo APS de ATI presentado en esta fase I se han llevado a cabo de forma detallada tareas como la familiarización con la instalación, la identificación de sucesos iniciadores, la delineación de las secuencias de accidente, o el análisis del sistema de ventilación del edificio de combustible. Contrariamente, los análisis estructural y termohidráulico se han llevado a cabo mediante la adaptación de resultados de estudios ajenos, la fracción de liberación estimada es un valor conservador derivado de un caso envolvente estudiado en un documento ajeno [5], y el análisis de fiabilidad humana y el análisis del sistema grúa han quedado fuera del alcance del modelo. Pese a que las tres carencias expuestas son significativas para el modelo, los análisis estructural y termohidráulico y la fracción de liberación, a diferencia del análisis de fiabilidad humana y el análisis de la grúa, tienen presencia en el modelo. Además, el tratamiento de ambas tareas es conservador, por lo que una mejora en su ejecución proporcionaría resultados más realistas, pero, también, aún más alejados de los valores de riesgo de la central. En cambio, debido a su ausencia en el modelo, el impacto del factor humano y del factor grúa en el riesgo es una incógnita, aunque se considera probable que un modelo que incluya ambos proporcione resultados de riesgo del ATI mayores debido a la gran cantidad de operaciones humanas a realizar en el proceso de almacenamiento. Consecuentemente, y pese a que en esta fase I se concluye que el riesgo del ATI es prácticamente despreciable en comparación con el de la central, se decide aplicar el análisis de fiabilidad humana y el análisis de la grúa en una segunda fase del proyecto puesto que es posible que la valoración del riesgo del ATI aumente al introducir ambos ítems. Asimismo, el análisis de fiabilidad humana es una técnica que forma parte de la metodología de aplicación del análisis probabilista de seguridad. Su aplicación en un contexto tan específico como el del ATI es una contribución novedosa al desarrollo de las técnicas de análisis del factor humano (véase el capítulo 8 para más detalle).

Capítulo 8

Aplicación piloto de la metodología APS (FASE II)

8.1. Introducción

El capítulo 7 presenta la segunda fase de la aplicación piloto de la metodología APS, descrita en el capítulo 6, en la estimación orientativa del riesgo del ATI. Si bien los resultados orientativos al respecto del riesgo del ATI obtenidos en la fase I desprenden que éste es muy bajo, prácticamente despreciable en comparación con el propio riesgo de la central, el modelo generado y cuantificado en la fase I tiene ciertas carencias, propias de un análisis piloto. Concretamente, dichas carencias son: la ausencia de análisis de fiabilidad humana y análisis del sistema grúa, la adaptación de resultados de estudios ajenos para completar los análisis estructural y termohidráulico, y la estimación de la fracción de liberación de radionúclidos mediante un valor conservador derivado de un caso envolvente estudiado en un documento ajeno. Tal y como se ha concluido en el capítulo dedicado a la primera fase, la carencia más importante de las tres identificadas es la ausencia del análisis de fiabilidad humana y el análisis del sistema grúa. En primer lugar, porque los análisis estructural y termohidráulico y la fracción de liberación ya tienen presencia en el modelo. El tratamiento de estas tareas es notablemente conservador así que, además, una mejora en su ejecución proporcionaría resultados más realistas que estarían aún más alejados de los valores de riesgo de la central. En segundo lugar, porque se considera hipotéticamente que un modelo que incluya el análisis de fiabilidad humana y el análisis del sistema grúa proporcionaría resultados de riesgo del ATI mayores debido a la gran cantidad de operaciones humanas a realizar con el sistema grúa durante el proceso de almacenamiento. Consecuentemente, en la segunda fase de la aplicación de la metodología APS se ha desarrollado el análisis de fiabilidad humana asociado a la instalación ATI, y se han incluido los resultados de dicho análisis en el modelo APS de ATI conjuntamente con el resultado del análisis del sistema grúa. Aunque la introducción de la fiabilidad humana y el análisis de la grúa suponen una mejora del modelo creado en la Fase I, éste no se considera como definitivo por las carencias expuestas anteriormente. El modelo continua siendo piloto, aunque en un estado más avanzado que el anterior. En consecuencia, los resultados obtenidos siguen considerándose más bien orientativos que no definitivos.

La realización de un análisis de fiabilidad humana comienza con la selección de la metodología más adecuada para su desarrollo. En el marco de esta tesis doctoral, tras un amplio periodo de búsqueda bibliográfica se decidió que ninguna de las metodologías publicadas hasta el momento se ajustaba a las particularidades del análisis y del ATI de estudio. En respuesta, se ha desarrollado un método novedoso de aplicación del análisis de fiabilidad humana en instalaciones ATI que combina diferentes técnicas existentes. Las conclusiones de la búsqueda bibliográifca, y la metodología finalmente utilizada se presentan en la sección 8.2. La aplicación de la metodología se resume en la sección 8.3, y los resultados obtenidos en

forma de probabilidades de fallo humano se presentan en la sección 8.4. La manera de incluir los resultados del análisis de fiabilidad humana en el modelo APS de ATI se discute en la sección 8.5. En dicha sección también se presenta el análisis del sistema grúa y la inclusión del mismo en el modelo APS. La sección 8.6 proporciona los resultados del nuevo modelo APS, que se comparan con los de la primera fase y con los del APS de sucesos internos a Potencia de nivel 2 de la central en la sección 8.7. Las conclusiones extraídas del desarrollo de la Fase II del modelo APS de ATI se presentan en la sección 8.8. La diversa terminología asociada al análisis de fiabilidad humana utilizada en el presente capítulo se define en un glosario contenido en el anexo I.

8.2. Metodología de análisis de fiabilidad humana

8.2.1. Elección de la metodología

La primera tarea de la Fase II del proyecto de aplicación piloto de la metodología APS a un ATI consistió en llevar a cabo un proceso de búsqueda bibliográfica con el fin de conocer diversos métodos de aplicación de análisis de fiabilidad humana. En primer lugar, se revisaron las metodologías publicadas en formato abierto más utilizadas[1] en la industria con el objetivo de encontrar aquella más adecuada para el APS de ATI . La conclusión extraída fue negativa: ninguno de los métodos de referencia más utilizados en la industria, publicados en formato abierto, es adecuado para el propósito del proyecto. El principal hecho que motiva dicha conclusión es que los métodos de análisis de fiabilidad humana más utilizados, desarrollados a la par que la metodología APS, están preparados para identificar y cuantificar eventos de fallo humano (comúnmente conocidos como *Human Failure Eevents* (HFE)) en la realización de acciones en el interior de la sala de control en situación de emergencia. Los métodos más utilizados están enfocados al contexto sala de control en situación de emergencia porque es dicho contexto el que se analiza en los modelos APS de sucesos internos a potencia[2], modelos que han sido el pilar del desarrollo de la metodología APS. En cambio, las acciones humanas relacionadas con la instalación ATI se ejecutan en condiciones normales, es decir, en caso de producirse el fallo humano, éste sería un iniciador y no una respuesta a una emergencia, en lugares ajenos a la sala de control de la central. En consecuencia, las metodologías de análisis de fiabilidad humana tradicionalmente más usadas no cubren el análisis del fallo humano en el contexto del ATI.

El modo de solventar la discrepancia entre el contexto de la actuación humana en el ATI y el contexto analizable mediante los métodos de análisis de fiabilidad humana más utilizados fue investigado por la propia NRC a principios de la decada de 2010 [86]. Como resultado de la investigación se publicaron dos documentos: «Human Reliability Analysis - Informed Insights on Cask Drops» [8], y «Preliminary, Qualitative, Human Reliability Analysis for Spent Fuel Handling» [9], ambos publicados en 2012. Ambos documentos representan el primer intento de la NRC para generar una metodología de análisis de fiabilidad humana adecuada para contextos de manejo de combustible gastado como es el del ATI. Ambos documentos recomiendan el uso de ATHEANA (*A Technique for Human Error ANAlysis*) como método para seguir desarrollando el análisis de fiabilidad humana en contextos de manejo de combustible. En el momento del desarrollo de esta parte de la tesis doctoral no se había publicado ningún análisis de fiabilidad de un ATI llevado a cabo mediante la metodología ATHEANA.

Una de las características definitorias de la metodología ATHEANA, véase la subsección 8.2.2 para más detalle, es que su método de cuantificación se basa exclusivamente en el juicio de expertos [74]. La obligación que supone basar la cuantificación únicamente en el juicio de expertos es una restricción para el uso de ATHEANA en aquellos contextos en los que expertos en la materia no estén disponibles. Concretamente,

[1] En el campo del análisis de fiabilidad humana, que una metodología sea ampliamente utilizada es sinónimo de que se considere válida.

[2] El APS de sucesos internos a potencia analiza la evolución de la planta tras un suceso iniciador interno. La evolución de la planta tras uno de estos sucesos viene marcada por el cumplimiento de los procedimientos de operación en emergencia, que se ejecutan desde sala de control.

esta situación se puede dar cuando el análisis de fiabilidad humana se quiera aplicar en una fase temprana del desarrollo del ATI, por ejemplo, en el marco de un APS de diseño, o cuando las operaciones del ATI sean llevadas a cabo por equipos externos a la central. En el marco del proyecto presentado en esta tesis doctoral, ATHEANA no puede ser aplicado en su totalidad porque no se ha gozado de la disponibilidad de expertos en la materia para llevar a cabo el proceso de cuantificación.

A raíz de las dificultades para aplicar una metodología ya existente, se ha decidido desarrollar una metodología novedosa de análisis de fiabilidad humana que pueda aplicarse al contexto del ATI. Se ha decidido, no obstante, que dicha metodología sea todo lo similar a ATHEANA que sea posible para respetar la recomendación de la NRC. En consecuencia, se ha desarrollado un método de cuantificación de la probabilidad de error humano que es adecuado para complementar a ATHEANA, y en el cual el uso del juicio de expertos no es obligatorio. A continuación se describe la metodología de referencia, ATHEANA, y se define el método de cuantificación desarrollado.

8.2.2. Metodología de referencia: ATHEANA

ATHEANA es una metodología de aplicación de HRA desarrollada por la NRC y publicada en el año 2007 [3]. Su principal objetivo es el cálculo de probabilidades de fallo humano (comúnmente conocidas como HEP (*Human Error Probability*)) válidas para el marco de los análisis probabilistas de seguridad. ATHEANA presenta un procedimiento secuencial para definir el alcance, identificar, describir y evaluar cualitativamente y cuantitativamente el error humano. Este método esta formado por nueve pasos entre los cuales destaca la definición y análisis de *Error-Forcing Contexts* (EFCs)[3], contextos en los que la tendencia a fallar del operador aumenta debido a las condiciones que impone el escenario. Los nueve pasos que forman el procedimiento de aplicación de ATHEANA se dividen en dos partes, la parte cualitativa y la parte cuantitativa, siendo en la última en la que se aplica el procedimiento de cuantificación. La figura 8.1 presenta los diferentes pasos a seguir para aplicar ATHEANA.

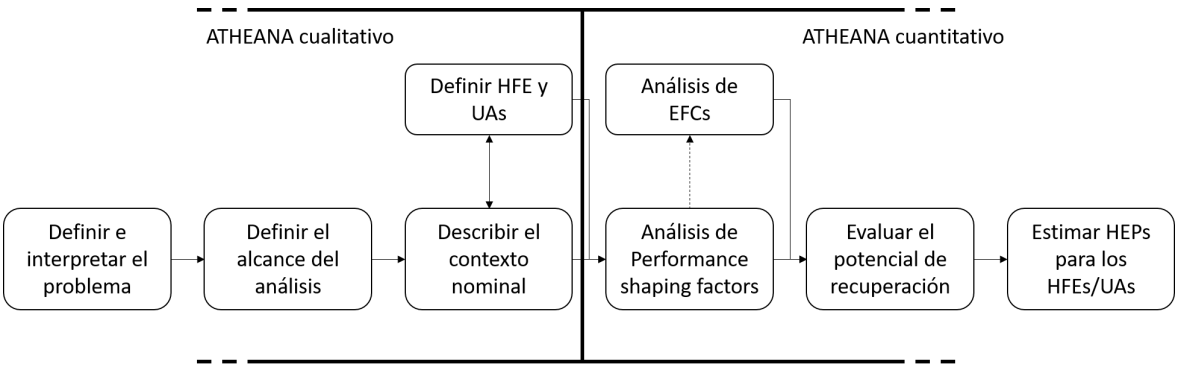


Figura 8.1: Procedimiento de aplicación de la metodología ATHEANA. Fuente: modificado de [3]

La mayoría de los pasos del procedimiento secuencial de ATHEANA se basan en las denominadas HRA *good practices*[57], lo que significa que no son particularmente únicos y no representan novedades en el uso del HRA. En particular, la parte cualitativa es muy similar al procedimiento SHARP (*Systematic Human Action Reliability Procedure*), uno de los métodos tradicionalmente más utilizados en el análisis de fiabilidad humana. A parte de la definición y análisis de EFCs[4], el otro rasgo que define a ATHEANA es

[3] La definición académica de EFC dada por la guía de usuario de ATHEANA [3] es: *The situation that arises when particular combinations of performance shaping factors and plant conditions create an environment in which unsafe actions are more likely to occur.*

[4] De forma única entre las metodologías HRA, ATHEANA requiere analizar en detalle el contexto nominal de fallo humano con el objetivo de identificar posibles desviaciones del mismo en las que el fallo humano pudiese ser más probable. Una vez identificados los EFCs, se ha de estimar su probabilidad de ocurrencia para añadir su contribución al cálculo de las probabilidades de error humano.

su procedimiento de cuantificación. El procedimiento de cuantificación, incluyendo la selección y definición de PSFs, evaluación del potencial de recuperación, y análisis de dependencias, se lleva a cabo mediante el juicio de expertos. Esto significa que no se utiliza ningún algoritmo de cuantificación ni valores provenientes de experiencia para cuantificar las HEPs, sino que expertos de primera mano en la temática de estudio se reúnen con analistas HRA y deciden los valores que han de tener los PSFs, el potencial de recuperación y, en definitiva, las HEPs.

Tal y como se ha comentado previamente, en el marco del proyecto presentado en esta tesis doctoral no se puede aplicar el procedimiento de cuantificación sugerido por ATHEANA porque no se ha gozado de la disponibilidad de expertos en la materia. Sin embargo, la parte cualitativa de ATHEANA, incluyendo la identificación y definición de EFCs, que es una de las bases de la posterior cuantificación, sí que es aplicable en el marco de este proyecto. Por lo tanto, el análisis de fiabilidad humana al ATI se ha aplicado mediante el seguimiento de la parte cualitativa de ATHEANA y el desarrollo de un nuevo procedimiento de cuantificación acoplable a dicha parte cualitativa.

8.2.3. Nuevo procedimiento de cuantificación

8.2.3.1. Fundamentos del nuevo método

El objetivo fundamental es desarrollar un método de cuantificación que sustituya al juicio de expertos en el marco ATHEANA con la condición *sine qua non* de que este nuevo procedimiento no necesite de la participación de expertos en la materia para su ejecución. El método de cuantificación desarrollado se apoya en dos características fundamentales (ver figura 8.2): la descomposición de los eventos de fallo humano, y el análisis detallado del contexto en el que se estudia el fallo humano.

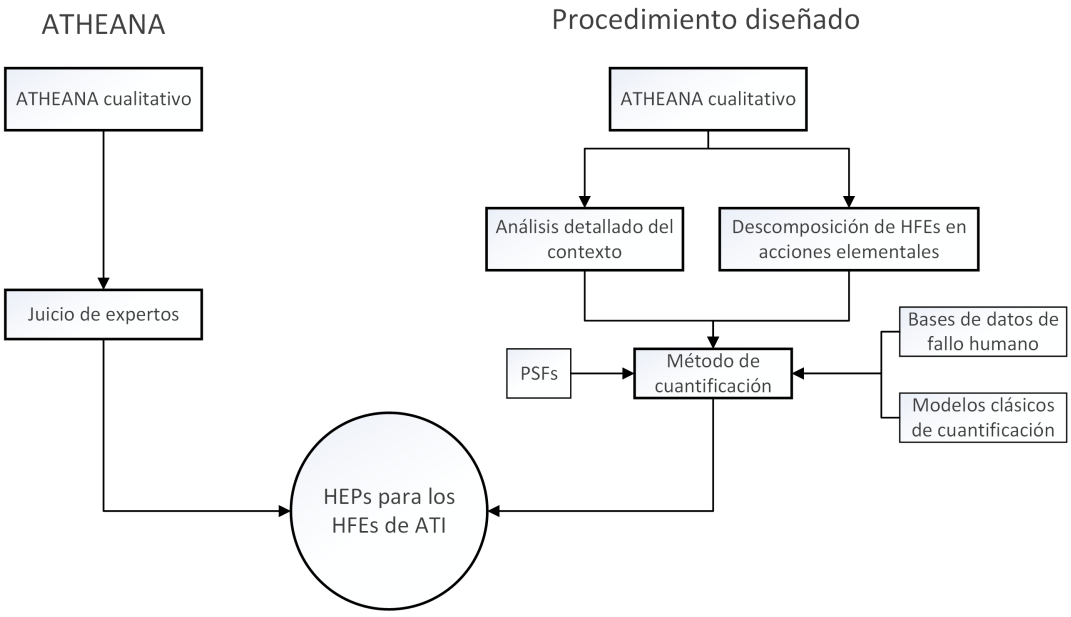


Figura 8.2: Los fundamentos del nuevo procedimiento de cuantificación

Los árboles de fallo utilizados en el APS son un buen ejemplo de que un alto nivel de descomposición de un sistema complejo permite describir y cuantificar la indisponibilidad o fallo del sistema utilizando elementos sencillos sin perder de vista la complejidad propia del sistema. Los eventos de fallo humano identificados

en un contexto ATI son únicos[5] y difícilmente comparables a aquellos identificados en situaciones de emergencia en sala de control o en otros contextos. Sin embargo, las acciones elementales llevadas a cabo en las operaciones humanas del contexto ATI, tales como apretar un botón, sí que son similares a las tareas elementales a realizar en otros contextos como el de operación en sala de control. Siguiendo el ejemplo de la teoría de los árboles de fallo, en el nuevo método de cuantificación, los eventos de fallo humano se descomponen en estructuras de acciones elementales para cuantificar la probabilidad de ocurrencia de los HFE a partir de unidades elementales de fallo humano[6]. La probabilidad genérica de ocurrencia de estas unidades elementales de fallo humano se puede cuantificar de forma independiente mediante modelos clásicos (véase la sección 8.2.3.3 para más detalle) y/o bases de datos que contengan valores genéricos de probabilidad de fallo humano (ejemplos en la sección 8.3.9).

En referencia al contexto en el que sea realizan las operaciones relacionadas con el ATI, éste es bien conocido, y, en condiciones normales, prácticamente invariante[7]. Por lo tanto, los métodos y modelos utilizados en la industria para aplicar PSFs (*Performance Shaping Factors*, véase los anexos I y J para más detalle) pueden ser utilizados para ajustar las probabilidades genéricas de las unidades elementales de fallo humano al contexto específico del ATI.

8.2.3.2. Descomposición de eventos de fallo humano: Árboles detallados de eventos de fallo humano

La característica más importante a implementar en el método de cuantificación es una herramienta que permita descomponer las descripciones de HFEs provenientes del ATHEANA cualitativo en combinaciones de unidades elementales de fallo humano. Los árboles de fallo utilizados en los APS no son una herramienta adecuada por dos motivos: primero, porque no pueden plasmar la secuencia de ejecución de las acciones elementales, y, segundo, porque no pueden incluir acciones de recuperación. Los árboles de sucesos utilizados en el APS permitirían tanto descomponer los HFE en una cadena secuencial de acciones elementales como incluir acciones ejecutadas correctamente, pero la estructura resultante podría llegar a tener un tamaño tan desproporcionado que entorpecería su análisis. Se considera que los árboles de eventos de fallo humano, comúnmente conocidos como *Human Failure Event Trees* (HFET) en el NUREG/CR-1278 [6], son el mejor método para descomponer los eventos de fallo humano en unidades de fallo humano. Los HFET describen y delinean eventos de fallo humano mediante una estructura lógica deductiva [6] (véase la figura 8.3) que puede incluir tanto acciones de recuperación como acciones correctamente ejecutadas. La estructura de los HFET está formada por sucesos, o unidades, básicos de fallo humano llamados acciones no seguras (comúnmente conocidas como *Unsafe Actions* (UA)). Además, los HFET también pueden ser utilizados para cuantificar la probabilidad de ocurrencia de los eventos de fallo humano. Sin embargo, el nivel de descomposición de los HFETs propuesto en el NUREG/CR-1278 es bajo, lo que hace que los HFETs, tal y como están descritos en este NUREG, sean insuficientes para el caso de estudio. Los HFETs han de incluir todas las acciones elementales llevadas a cabo en las operaciones de ATI para que sean adecuados para el nuevo método de cuantificación. Por lo tanto, a los HFET utilizados en el nuevo método de cuantificación se les llama árboles detallados de eventos de fallo humano (*Detailed Human Failure Event Trees* (DHFET)) porque tienen un grado de detalle superior y son más complejos que los propuestos en el NUREG/CR-1278.

En el contexto ATI, los eventos de fallo humano pueden descomponerse de forma precisa mediante DHFETs partiendo de una revisión exhaustiva de los procedimientos de operación que han de seguir los trabajadores. Los llamados procedimientos de operación describen todas las acciones elementales que han de llevar a cabo los trabajadores al realizar una actividad específica. Por lo tanto, dichos procedimientos son la mejor

[5] Entiéndase por únicos que difícilmente se identificaran eventos de fallo humano iguales en el estudio de otras operaciones en otros contextos.

[6] Se entiende como unidad elemental de fallo humano a la realización incorrecta (fallo al realizar) de una acción elemental.

[7] A parte de otros condicionantes específicos de cada evento de fallo humano, el contexto de las operaciones de ATI, en el interior del edificio de combustible, destaca por dificultades visuales, dificultades a la hora de comunicarse con otros trabajadores, y dificultades asociadas a la existencia de altas temperaturas.

referencia para identificar potenciales unidades elementales de fallo humano a introducir en los DHFETs mediante UAs.

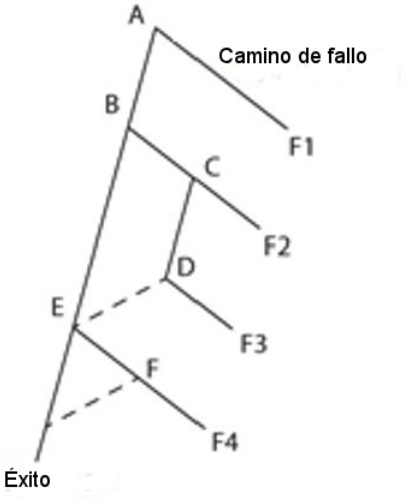


Figura 8.3: Ejemplo de DHFET simple. Las UAs se introducen mediante letras mayúsculas

8.2.3.3. Cuantificación de acciones no seguras

La probabilidad de ocurrencia de las acciones no seguras, o unidades elementales de fallo humano en este caso, ha de ser estimada para posteriormente poder cuantificar la probabilidad de fallo de los eventos de fallo humano mediante los DHFETs. Un modelo de cuantificación clásico, véase la figura 8.4 y la ecuación L.1, se incorpora al método de cuantificación para estimar la probabilidad genérica de ocurrencia de las UAs. A la probabilidad genérica de ocurrencia se le da el nombre *Nominal Human Error Probability* (NHEP) en el modelo de cuantificación. Dicho modelo clásico de cuantificación incluye tanto el fallo cognitivo[8] (FP_{cog}) como el fallo manual (FP_{man}) de los trabajadores.

$$NHEP = FP_{cog} + (1 - FP_{cog}) * FP_{man} \tag{8.1}$$

La probabilidad de fallo cognitivo se puede estimar con metodologías bien conocidas como, por ejemplo, la TRC (Time Reliability Correlation) y la HCR[9] (Human Cognitive Reliability, véase el anexo J para más detalle sobre esta metodología) [87]. Esta última, la HCR, es la metodología utilizada en la aplicación de la metodología al caso de estudio. La probabilidad de fallo manual puede obtenerse de bases de datos. Idealmente, los datos incluidos en la base de datos seleccionada deberían reflejar la experiencia del personal de planta, o personal externo si es el caso, en la ejecución de las acciones elementales llevadas a cabo en el contexto ATI. Estos datos pueden provenir de recabar la experiencia operativa y/o de ejercicios de entrenamiento in situ o en simuladores. Si una base de datos de estas características no está disponible, se ha de analizar si es posible utilizar bases de datos de acceso abierto[10]. Por ejemplo, la base de datos abierta adjunta al THERP (*Technique for Human Error Rate Prediction*) [6] proviene de datos de experiencia operativa dentro de sala de control. Pese a tratarse de un contexto diferente, se puede utilizar la base de datos adjunta al THERP para estimar la probabilidad de fallo manual de acciones no seguras en el

[8] Fallo en el proceso interno de toma de decisiones. Se considera fallo tanto tardar demasiado en tomar la decisión de ejecutar la acción correcta, como equivocarse a la hora de decidir cuál es la acción correcta a ejecutar.

[9] Mediante el método HCR, la probabilidad de fallo se calcula a partir del tiempo disponible para realizar una acción y el tiempo necesario para detectar y analizar la necesidad de realizar dicha acción.

[10] Bases de datos disponibles para el gran público.

contexto ATI debido a que las acciones descritas son elementales (girar, pulsar, leer, etc) y son nominales, es decir, no incluyen la influencia de PSFs.

El método SPAR-H [88] (*Standarized Plant Analysis Risk-Human Reliability*, véase el anexo J para más detalle sobre la metodología) se introduce en el nuevo método de cuantificación para analizar el contexto y aplicar PSFs a los valores genéricos de NHEP calculados mediante la ecuación L.1. El tratamiento de los PSFs es de importancia pues permite analizar y cuantificar de forma precisa las condiciones especiales en las que se realiza el manejo de contenedores y combustible para ajustar las probabilidades de fallo humano al escenario en el que se postulan. Se selecciona SPAR-H como método de introducción de los PSFs en el nuevo método de cuantificación porque el tratamiento de PSFs es de gran importancia en su metodología de estimación del fallo humano. SPAR-H presenta una lista de ocho PSFs a evaluar: *Available Time* (AT), *Stress/Stressors* (S), *Complexity* (C), *Experience/training* (ET), *Procedures* (P), *Ergonomics/HMI* (EH), *Fitness for duty* (F), y *Work Processes* (WP)[11]. El anexo J contiene una descripción detallada de cada uno de los PSFs. Cada uno de estos PSFs se asocia a más de tres multiplicadores. Dichos multiplicadores representan la influencia del PSF sobre la actuación humana en el contexto de estudio.

A diferencia de la mayoría de metodologías HRA, el análisis de PSFs del método SPAR-H permite definir contextos positivos para la actuación humana. Esta característica es particularmente útil para analizar la actuación humana asociada al contexto ATI puesto que el contexto nominal de ATI es la operación normal. La ecuación de cuantificación de SPAR-H, véase la ecuación L.2, estima una HEP ajustada al contexto de estudio a partir de una NHEP genérica y del producto de PSFs (PSF_{comp})[12]. En consecuencia, es una ecuación adecuada para ajustar la probabilidad de ocurrencia de las UAs al contexto del ATI.

$$HEP = \frac{NHEP * PSF_{comp}}{NHEP * (PSF_{comp} - 1) + 1} \tag{8.2}$$

La figura 8.4 plasma la metodología desarrollada para estimar la probabilidad de ocurrencia de las UAs presentes en los DHFET. La metodología se divide en dos pasos: en primer lugar, la estimación de la HEP nominal, NHEP, mediante un modelo clásico. En segundo lugar, el análisis de PSFs utilizando SPAR-H y la cuantificación de una HEP ajustada al contexto de análisis.

Cuanto más simples y elementales sean las UAs, más importancia cobra el análisis de contexto y menos importancia tiene la base de datos elegida para estimar la probabilidad de fallo manual genérica. Se recomienda firmemente postular UAs elementales y sencillas cuando no se disponga de bases de datos que reflejen específicamente la experiencia en operaciones de ATI para no depender de hipótesis ni de documentación externa.

8.2.3.4. Cuantificación de probabilidades de fallo humano

La cuantificación de la probabilidad de ocurrencia de eventos de fallo humano mediante DHFETs es simple. La estructura de un DHFET, véase la figura 8.3, se divide en caminos de éxito (UAs llevadas a cabo correctamente) y de fallo (UAs realizadas erróneamente). La probabilidad de ocurrencia de un camino de fallo es el producto de las probabilidades de fallo de las UAs presentes en el propio camino de fallo (véase la ecuación L.3) si se desprecian recuperaciones internas [13]. Las recuperaciones internas se desprecian si las probabilidades de ocurrencia de las UAs son menores que 0,01 [6]. La suma de las probabilidades de ocurrencia de los caminos de fallo presentes en el árbol es la probabilidad de ocurrencia del HFE descrito mediante el árbol [6] (véase la ecuación L.4).

[11] La traducción de los ocho PSFs es la siguiente: Tiempo disponible, estrés/elementos estresantes, complejidad, experiencia/entrenamiento, procedimientos, ergonomía/interfaz humano-máquina, aptitud para el trabajo, procesos de trabajo.

[12] Además, la ecuación esta diseñada para evitar valores de probabilidad imposibles, es decir, por encima de 1.

[13] Ejecución correcta de una acción no segura que retorna la progresión del fallo al estado o camino de fallo anterior. La ejecución correcta de está acción no significa que se evite la ocurrencia del evento de fallo humano. El fallo podría ocurrir en otro camino de fallo.

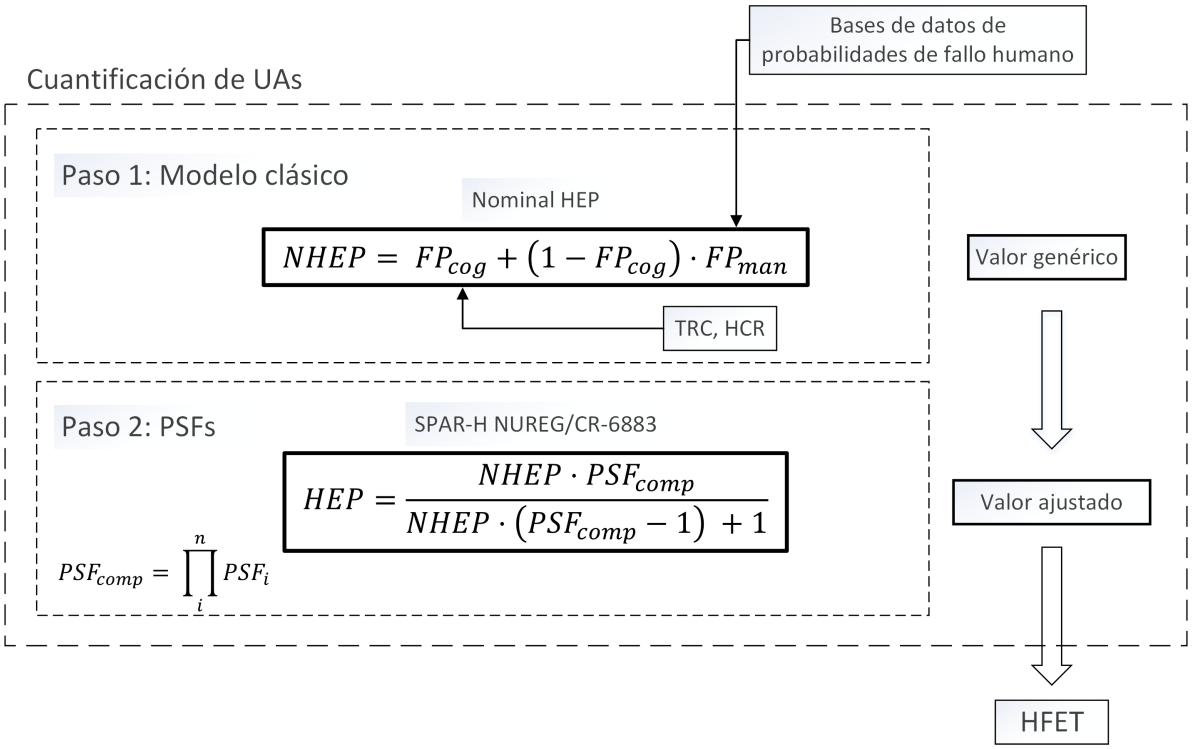


Figura 8.4: Metodología de cuantificación de las UAs presentes en los DHFET

$$F = \prod_{i}^{n} UA_i \tag{8.3}$$

$$HEP(HFE) = \sum_{i}^{n} F_i \tag{8.4}$$

8.2.4. Integración del nuevo procedimiento de cuantificación en el alcance de la metodología ATHEANA

El nuevo método de cuantificación es un procedimiento aislado de cuantificación de la probabilidad de fallo humano que no obliga a hacer uso del juicio de expertos. En consecuencia, se le han de proporcionar *inputs* para poder estimar las probabilidades de fallo humano asociadas a un caso de estudio. Aunque el origen de los *inputs* puede ser diverso, el procedimiento de cuantificación presentado ha sido especialmente diseñado para tener como entrada el resultado de aplicar la parte cualitativa de ATHEANA al contexto de un ATI. La parte cualitativa de ATHEANA incluye: la definición y descripción de los eventos de fallo humano, previa definición del problema y del alcance del análisis, la identificación de los EFC, y la definición de potenciales acciones de recuperación. La figura 8.5 muestra la metodología final a utilizar para aplicar el análisis de fiabilidad humana al contexto ATI de estudio.

En cuanto a ampliaciones y/o mejoras del método de cuantificación presentado en esta sección, cabe destacar que el desarrollo de procedimientos para realizar el análisis de dependencias entre UAs y el análisis de incertidumbre ha quedado fuera del alcance de esta tesis. Ambos análisis proporcionarían información sensible tanto para el análisis de resultados como para la introducción de las HEPs en un

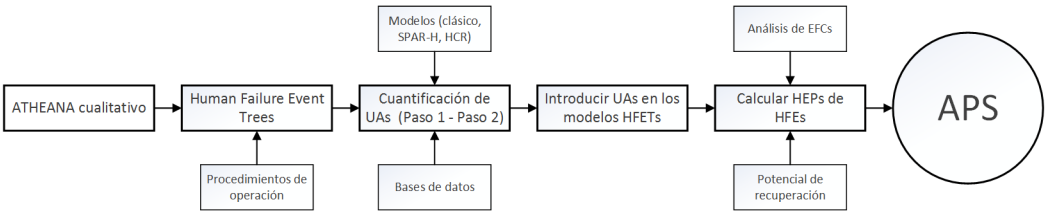


Figura 8.5: Metodología final de análisis de fiabilidad humana incluyendo ATHEANA y el nuevo método de cuantificación

APS. Teniendo en cuenta el uso de árboles de eventos de fallo humano, el análisis de incertidumbre se podría aplicar, de la misma manera que en la metodología APS, mediante técnicas Monte Carlo. Además, el uso del nuevo método de cuantificación genera una gran cantidad de datos cuantitativos a almacenar durante la realización del análisis (por ejemplo, los multiplicadores de los PSFs). Una aplicación que permitiese controlar la trazabilidad de los datos sería una herramienta interesante para poder revisar, modificar, o actualizar los datos utilizados. Una posible solución al problema de la trazabilidad sería utilizar el software *RiskSpectrum® HRA* para almacenar todos los datos cuantitativos generados en el desarrollo del análisis.

8.3. Aplicación de la metodología de análisis de fiabilidad humana

8.3.1. Introducción

La metodología de análisis de fiabilidad humana formada por el acoplamiento de la parte cualitativa de ATHEANA y el nuevo método de cuantificación se ha aplicado en el contexto del ATI de estudio. La aplicación de la metodología HRA al contexto del ATI de estudio tiene dos claros objetivos. Por un lado, el objetivo por el que se ha desarrollado dicha metodología: obtener resultados para completar el APS en su fase II de desarrollo. Por otro lado, esta aplicación sirve para comprobar el funcionamiento de la metodología, identificando todas las dificultades inherentes a su ejecución. Al tratarse del primer uso de esta metodología de análisis de fiabilidad humana se considera que los resultados obtenidos son orientativos. Para realizar una valoración de los mismos se han comparado con resultados obtenidos en análisis con los que guarda cierto grado de similitud.

La aplicación de la metodología de análisis de fiabilidad humana se divide en diversas tareas. Estrictamente, estas tareas son: definir e interpretar la cuestión a analizar, definir el alcance del análisis, describir el contexto nominal, identificar, definir, y describir los HFEs, descomponer los HFEs por medio de DHFETs, tratamiento de PSFs, definición de EFCs, análisis del potencial de recuperación, y cuantificación de la probabilidad de ocurrencia de los HFEs. La cuestión a analizar es bien conocida puesto que se trata del fallo humano en el contexto del ATI con el objetivo de obtener HEPs para introducirlas en el modelo APS de ATI. El resto de tareas se presentan entre la subsección 8.3.2 y la subsección 8.3.9. Por motivos de espacio, en varias de las tareas se hace uso de ejemplos para ilustrar el desarrollo llevado a cabo. La totalidad de datos y de información generados en la aplicación del análisis de fiabilidad humana se puede consultar en el anexo I.

8.3.2. Alcance del análisis

El alcance del análisis de fiabilidad humana se acota al estudio de todas las acciones humanas a llevar a cabo durante una campaña de carga[14] de contenedores (comúnmente conocidas como *Cask Loading*

[14] Una campaña de carga hace referencia a la carga y traslado a la zona de almacenamiento del ATI de uno o más contenedores durante un periodo de tiempo. Las campañas de carga se han de llevar a cabo en operación normal porque por

Campaign (CLC)) cuyo fallo pueda trasladarse posteriormente en forma de HEP al APS de ATI. En este caso, al haberse desarrollado con anterioridad el modelo APS, basta con analizar los árboles de eventos, y, concretamente, los sucesos iniciadores, para conocer qué elementos del modelo pueden verse afectados por acciones humanas. En el caso estudiado, el análisis de los árboles de eventos reduce las acciones humanas a analizar a todas aquellas que puedan causar la caída del contenedor en el interior del edificio de combustible[15]. Además, la NRC recomienda analizar los casos de carga errónea o, como se conocen comúnmente, *Misload* [9], en sus estudios preliminares de la actuación humana en un ATI. Un suceso de carga errónea hace referencia a la carga del contenedor con elementos de combustible gastado no seleccionados para su traslado o con los elementos seleccionados, pero en una configuración diferente. Siguiendo la recomendación de la NRC, se ha decidido estudiar las acciones humanas que pueden causar la carga errónea del contenedor pese a que no se trate de un Suceso Iniciador del APS. El análisis de estos dos tipos de sucesos implica estudiar las acciones humanas que se llevan a cabo desde la carga del MPC con elementos de combustible gastado hasta la introducción del MPC en el HI-STORM 100.

Las principales acciones humanas llevadas a cabo durante la etapa de carga de un campaña de carga de contenedores son elevar la carga, bajar la carga, ajustar, engranar, trasladar, revisar, apretar, observar, soldar, probar, y sellar, entre otras. Estas acciones cubren la mayoría del proceso y algunas no están relacionadas con casos de caída o carga errónea. En consecuencia, acciones tales como soldar, inspeccionar, y sellar quedan fuera del alcance de este análisis por no ser una posible causa de caídas o cargas erróneas.

El edificio de combustible de la central nuclear contiene la piscina de combustible, el canal de transferencia, la piscina seca de combustible en seco, y el pozo de transferencia o pozo del contenedor. El edificio también acoge otras estructuras necesarias para llevar a cabo las campañas de carga de contenedores como la zona de preparación, soldadura, y sellado de contenedores y la zona de transporte. La figura O.10 del anexo O presenta un plano de planta del edificio de combustible. En una campaña de carga de contenedores, las acciones humanas anteriormente mencionadas se llevan a cabo en la piscina de combustible, el pozo de cofres, la zona de preparación, soldadura, y sellado, y la zona de transporte. Consecuentemente, el análisis de fiabilidad humana se concentra en estas estructuras.

Se utilizan dos grúas del edificio de combustible, ambas diseñadas siguiendo el criterio de fallo simple, durante una campaña de carga de contenedores: la grúa pórtico y la grúa puente. La grúa pórtico se utiliza para trasladar elementos de combustible gastado desde la piscina de combustible hasta el contenedor MPC, que se encuentra en el pozo del contenedor. La grúa puente traslada el contenedor de transferencia a través del camino seguro carga[16] del edificio de combustible. Ambas máquinas tienen un papel importante en el análisis de fiabilidad humana ya que son los únicos sistemas que trabajan de forma activa durante la carga y traslado de contenedores y que, además, juegan un papel en la caída del contenedor o en la carga errónea del mismo. Por lo tanto, todas las acciones humanas a estudiar están relacionadas en mayor o menor medida con el uso de estas grúas.

En conclusión, el alcance del análisis de fiabilidad humana incluye todas las acciones humanas de una campaña de carga de contenedores que pueden causar la caída del contenedor o la carga errónea del contenedor. Estas acciones humanas se llevan a cabo en el interior del edificio de combustible y la mayoría de ellas están relacionadas con el uso de las grúas y el movimiento del contenedor.

8.3.3. Contexto nominal

En esta sección se describe y se acota el contexto nominal en el que se analiza la actuación humana.

motivos de espacio y de recursos humanos no pueden coincidir con periodos de recarga.

[15] Las acciones humanas que pudiesen derivar en la caída del contenedor en el traslado del mismo a la zona de almacenamiento también podrían ser motivo de estudio. No obstante, debido a que el suceso de caída fuera del edificio de combustible ha sido cribado en el APS por imposibilidad de rotura de las barreras de confinamiento, también quedan fuera del alcance del HRA las acciones humanas que pudiesen causar este tipo de caídas.

[16] Camino preconcebido para llevar la carga por encima de él. El criterio para decidir cuál es el camino seguro de carga es que las consecuencias sobre la planta de una caída de contenedor sean mínimas.

8.3.3.1. Descripción general de una campaña de carga de contenedores

Una campaña de carga de contenedores se divide en cuatro etapas: preparación, carga, transferencia, y almacenamiento. La etapa de preparación aglutina tres importantes tareas: la inspección de los contenedores y las grúas, el diseño del plan de movimiento del combustible gastado, y el posicionamiento de los contenedores en los lugares adecuados. El contenedor de almacenamiento se coloca en la zona de transporte, el MPC se introduce en el contenedor de transferencia, y el contenedor de transferencia se coloca en el interior del pozo del contenedor. El plan de movimiento del combustible gastado establece qué elementos de combustible tienen que colocarse en el interior del MPC y en qué posiciones se han de colocar. Todas estas acciones se realizan en el interior del edificio de combustible.

La etapa de carga cubre desde la carga del contenedor con elementos de combustible gastado hasta la transferencia del contenedor MPC al interior del contenedor de almacenamiento. Todas las tareas se llevan a cabo en el interior del edificio de combustible.

La etapa de transferencia hace referencia al traslado del contenedor de almacenamiento desde edificio de combustible hasta la zona de almacenamiento del ATI. Un vehículo oruga es utilizado para mover el contenedor. Finalmente, la etapa de almacenamiento corresponde al tiempo que el contenedor permanece en la zona de almacenamiento del ATI. Tal y como se ha mencionado en la sección anterior, el alcance del análisis cubre únicamente la etapa de carga.

A no ser que la central se encuentre en periodo de desmantelamiento, las campañas de carga de contenedores se realizan durante la operación normal de la central. Una CLC no se puede llevar a cabo a la vez que una parada de recarga porque comparten equipo y personal crítico [8]. En el caso de estudio, la central se encuentra en estado operacional, así que las CLCs se llevaran a cabo durante la operación normal del reactor. La realización de una campaña de carga no incrementa el riesgo de daño al núcleo de la central pues no interfiere con ninguno de los elementos que aseguran el cumplimiento de las funciones de seguridad de la central.

8.3.3.2. Características ambientales del edificio de combustible

El interior del edificio de combustible está a presión negativa y a una temperatura estable de entre 18 y 35 ºC gracias a la actuación del sistema de ventilación del edificio. La presión del interior del edificio es negativa para evitar que partículas radioactivas escapen a través de las penetraciones del edificio. La temperatura del edificio unida a los trajes de protección contra la radiación que han de llevar los trabajadores que se acercan al contenedor hacen que la sensación de calor de dichos trabajadores sea alta. El ruido en el interior del edificio es frecuente y de volumen alto cuando se llevan a cabo tareas con la maquinaria presente. Esta situación no es diferente para el contexto de las CLCs pues las grúas se utilizan durante prácticamente todo el proceso. El alto nivel de ruido es un inconveniente importante pues dificulta en gran medida la comunicación entre trabajadores. El grado de visibilidad de los elementos de combustible en piscina no es óptimo debido a la refracción del agua y a posibles partículas en suspensión en el agua. Esto dificulta la tarea de carga del contenedor MPC con los elementos de combustible gastado seleccionados.

8.3.3.3. Procedimientos y personal involucrado

La descripción de las maniobras llevadas a cabo en el contexto nominal de la etapa de carga, véase anexo A para más detalle, se basa en los procedimientos de manejo proporcionados por la central. El objetivo de estos procedimientos es guiar la realización de las acciones y maniobras que se han de ejecutar para llevar a cabo la etapa de carga de forma exitosa. Estos procedimientos son similares a los procedimientos generales de operación y a los procedimientos de operación de sistemas. Esto implica que su principal norma de uso es que se han de seguir los pasos en orden, a no ser que el procedimiento explícitamente

permita realizar tareas en paralelo, y que el próximo paso solo se puede realizar cuando la acción actual y sus consecuencias hayan finalizado. Los procedimientos se definen como de uso en mano, lo que significa que cada instrucción es leída en voz alta por el responsable técnico antes de ser ejecutada. Una vez se han realizado todas las tareas especificadas en el procedimiento, éste se vuelve a leer para comprobar que todas las tareas se hayan realizado de forma correcta y se hayan documentado.

Los procedimientos definen las responsabilidades de los diferentes departamentos involucrados en la etapa de carga. Estos departamentos son:

- Ingeniería de reactor y de salvaguardias nucleares: proporciona el responsable de la carga, el supervisor independiente del contenedor, el responsable técnico, y el técnico de garantía de calidad. Su responsabilidad es coordinar el proceso de carga del contenedor y traslado a la zona de almacenamiento. Los procedimientos requieren su atención en algunas situaciones.
- Protección radiológica (PR): el responsable de PR se encarga de determinar las medidas y contramedidas a adoptar desde un punto de vista radiológico. Es una tarea de soporte a las acciones descritas en los procedimientos.
- Química: la responsabilidad del departamento de química es cumplir con los requisitos de vigilancia que les afectan y determinar medidas que haya que adoptar desde su punto de vista.
- Operación: proporciona personal para ejecutar los requisitos de vigilancia y para realizar las maniobras descritas en los procedimientos. Los principales miembros del grupo de trabajo que se encargan de realizar las maniobras son el operador de grúa, los observadores, los revisores, y el personal encargado de anclar el equipo de elevación y el contenedor.
- Prevención del riesgo: este departamento tiene como responsabilidad determinar medidas a adoptar desde el punto de vista de la prevención del riesgo.

Los procedimientos de operación consultados en la realización de este análisis de fiabilidad humana no especifican algunas características del manejo de contenedores. Concretamente, algunas de las características no detalladas son: la cantidad de operadores que se necesitan para descontaminar los contenedores, la cantidad de operadores que realizan las tareas de anclaje, dónde se colocan los operadores a pie cuando el contenedor se traslada por el edificio, distancias entre zonas de descanso del contenedor, tiempos disponibles para realizar acciones[17], y otros. Algunas de estas características han tenido que ser supuestas en la realización del análisis de fiabilidad humana.

8.3.3.4. Hipótesis y situación inicial de la etapa de carga

Hipótesis En el contexto del análisis de fiabilidad humana, se asume que todas las tareas de la etapa de preparación se realizan correctamente. Esto significa que ningún error o fallo cometido en la etapa de preparación puede influir en el análisis de la etapa de carga. De forma análoga al APS, se asume también que en el contenedor no se colocan elementos de combustible dañados.

Los anclajes y las revisiones de dichos anclajes son realizados por individuos diferentes. Esto implica que hay tantos revisores como revisiones se han de realizar y tanto personal de anclaje como anclajes se han de realizar. La documentación proporcionada por la central no aclara si los anclajes y sus posteriores revisiones son llevados a cabo por el mismo operador o por operadores diferentes así que, que sean realizados por individuos diferentes, es una hipótesis perfectamente posible. Esta hipótesis es importante porque simplifica en gran medida el análisis de dependencias.

[17] Los procedimientos consultados especifican que los tiempos disponibles para realizar ciertas acciones han de ser calculados previamente a comenzar el movimiento del contenedor.

Se supone que el camino seguro de carga no presenta obstáculos laterales. Por lo tanto, se asume que el contenedor nunca se moverá en horizontal durante un sector recto del camino seguro de carga. Más allá, se supone que los operadores nunca trasladarán el contenedor fuera del camino seguro de carga.

Se supone que en una CLC se carga más de un contenedor. En consonancia con el peor caso analizado en el APS de ATI, se supone que en una CLC se cargan cinco contenedores. Los contenedores se cargan secuencialmente sin que ninguna otra operación interrumpa la CLC. En el contexto nominal, se supone que la CLC se ha planeado con antelación suficiente a la siguiente parada de recarga.

Se asume, en el contexto nominal, que la carga térmica del contenedor una vez cargado con elementos de combustible cargado es del 80 al 90 por ciento de la carga térmica de diseño.

En el contexto nominal, se supone que la experiencia de los trabajadores que realizan tareas de la CLC es media. Esto significa que no es su primer movimiento de carga pero tampoco el último de una CLC.

El sistema de ventilación del edificio de combustible funciona perfectamente al iniciarse la CLC. La temperatura del edificio se mantiene entre 18 y 35 ºC.

Las descripciones de los eventos de fallo humano, véase la sección 8.3.4, contienen otras hipótesis específicas de cada caso. Estas hipótesis se han tomado para contrarrestar la falta de información al respecto de alguna de las maniobras realizadas durante la carga y traslado de contenedores como las mencionadas en la sección anterior.

Situación inicial La situación inicial del contexto nominal de análisis es la siguiente:

- El contenedor de almacenamiento, HI-STORM 100, se haya colocado en la plataforma de traslado en la zona de transporte del edificio de combustible.
- El MPC está dentro del contenedor de transferencia HI-TRAC 125D. El HI-TRAC se ha trasladado a la zona del pozo de cofres y se ha colocado sobre el pozo. El pozo se ha inundado con agua de la piscina de combustible. La camisa de agua del HI-TRAC se ha llenado con agua mineral cuando se introducía el contenedor en el pozo de cofres. Finalmente, el contenedor HI-TRAC reposa en el interior del pozo del contenedor.
- El personal está preparado para comenzar el traslado de elementos de combustible gastado desde la piscina hasta el interior del MPC. Varios trabajadores rodean el pozo de cofres, preparados para descontaminar la superficie del contenedor HI-TRAC.

8.3.3.5. Fases de la etapa de carga

La etapa de carga se ha dividido en diversas fases en el contexto del análisis de fiabilidad humana. La división en fases permite especificar y distinguir las diferentes condiciones por las que pasa el contenedor al llevarse a cabo la etapa de carga. Además, la división del contexto nominal en diversas fases ha facilitado la identificación de eventos de fallo humano. Las seis fases en las que se ha dividido la etapa de carga se presentan en la tabla 8.1.

Fase	Descripción
1	Carga del contenedor MPC con 32 elementos de combustible gastado.
2	Extracción del contenedor del pozo de cofres y colocación, sin soldadura, de la tapa del MPC. Inspección y descontaminación del HI-TRAC mientras se extrae del pozo.
3	Traslado del contenedor a la zona de soldadura, pruebas y sellado. El traslado es recto y se ha de realizar con el contenedor tan cerca del suelo como sea posible.
4	Soldadura de la tapa del MPC, ejecución de pruebas hidrostáticas, sellado del contendor y rellenado con helio.
5	Traslado del contenedor desde la zona de soldadura hasta la plataforma de traslado. El contenedor HI-TRAC se coloca encima del HI-STORM, lo que implica que se ha de alzar 5,9 metros.
6	Introducción del MPC en el HI-STORM. Se quita la tapa inferior del HI-TRAC, se ancla el MPC a la grúa puente mediante el sistema de bloqueo de alzamiento, y se baja el MPC hasta que descansa en el interior del HI-STORM.

Tabla 8.1: Fases de la etapa de carga

Una descripción más detallada de las tareas a realizar en cada una de las fases de la etapa de carga se incluye en el anexo A. La información aquí expuesta y la del anexo A provienen de los procedimientos de operación proporcionados por la central.

8.3.4. Identificación y descripción de HFEs

8.3.4.1. Introducción

En esta tarea se identifican y describen las acciones humanas de interés y sus correspondientes eventos de fallo humano. En el contexto de estudio, las acciones humanas de interés son todas aquellas cuya omisión o ejecución errónea pueda causar la caída del contenedor. Además, también se analizan todas aquellas acciones que puedan causar que el contenedor se cargue erróneamente por recomendación de la NRC.

Identificar y definir HFEs para la etapa de carga de una CLC es una tarea complicada. La mayoría de acciones y procesos llevados a cabo son fáciles y monótonos, es decir, se basan en la habilidad del trabajador, lo que genera un ambiente de trabajo relajado. Por lo tanto, los operadores no son tan propensos a cometer errores como en situaciones de emergencia en las que se hayan de ejecutar acciones complicadas. Sin embargo, los estudios preliminares de HRA para ATI realizados por la NRC defienden que los operadores pueden presentar ciertas vulnerabilidades al realizar tareas sencillas, basadas en su propia habilidad, en contextos relajados y monótonos [9]. Además, el ambiente en el interior del edificio de combustible, descrito en la sección anterior (ruido, temperatura, problemas de visibilidad), puede entorpecer la actuación del personal de operación. La suma de vulnerabilidades y de las dificultades inherentes al ambiente del edificio de combustible se han utilizado como base para identificar, definir, y describir posibles eventos de fallo humano. Algunos ejemplos de estas dificultades y vulnerabilidades son: actividades que no suponen una motivación, dificultades visuales, dificultades comunicativas, y exceso de confianza entre otros. El anexo K describe las vulnerabilidades extraídas de las guías NUREG/CR-7016 y NUREG/CR-7017.

El procedimiento seguido para identificar y definir eventos de fallo humano consta de dos pasos. En primer lugar, se identifican, mediante un proceso lógico de deducción, posibles causas raíz, con componente humana, de los sucesos a estudiar, es decir, caídas y cargas erróneas. A dichas causas raíz se les llama

eventos de fallo humano genéricos. En segundo lugar, se analizan en profundidad, y por separado, las distintas fases de la etapa de carga con el objetivo de identificar qué causas raíz podrían ocurrir en cada fase y por qué y cómo podrían ocurrir. El por qué y el cómo podrían ocurrir dichas causas raíz forman la definición de los eventos de fallo humano. Por motivos de espacio, el segundo paso del proceso se ilustra con el análisis realizado para la quinta fase de la etapa de carga, una de las más completas. El resto del análisis se documenta en el anexo I.

8.3.4.2. Eventos de fallo humano genéricos

Los casos de carga errónea dependen totalmente de la transferencia de elementos de combustible gastado entre la piscina y el contenedor. El traslado de elementos de combustible es ejecutado por el operador de la grúa polar de la piscina de combustible y por un observador a nivel de piscina. Los elementos de combustible gastado se colocan primero en un espacio vacío de la piscina en la configuración planeada, si caben, para luego introducirse en el contenedor. Un supervisor comprueba que la configuración final es igual a la planeada. Las causas raíz, con componente humana, de un caso de carga errónea están relacionadas con la selección y con el traslado de elementos de combustible. Por un lado, una de las causas raíz sería la selección errónea de elementos de combustible, por parte del operador de grúa, que generaría que se cargase el MPC con elementos de combustible gastado no planificados. Por otra parte, otra de las causas raíz sería que se cargase el contenedor con los elementos seleccionados pero en una configuración errónea. En ambos casos el observador tiene parte de responsabilidad, pues su tarea es comprobar, en cada movimiento, que se ha seleccionado el elemento de combustible gastado objetivo, y que se coloca en el lugar adecuado. Cabe destacar que la ocurrencia de un suceso de carga errónea no implica que el contenedor acabe con una carga térmica mayor que la de diseño, esto dependerá de que elementos de combustible gastado se introduzcan en el contenedor.

El suceso de caída de carga se relaciona con toda aquella acción de operador que pueda causar la caída del contenedor. La acción humana puede ser la causa directa de la caída o puede ser una de sus causas indirectas, conjuntamente con fallos de la grúa. Teniendo en cuenta que las acciones malintencionadas quedan fuera del alcance del análisis de fiabilidad humana, mediante el proceso lógico de deducción se han identificado tres posibles causas raíz con componente humana:

- Evento de *two-blocking*: Es causado por un izado inadvertido del contenedor. El evento de *two-blocking* hace referencia a una caída del contenedor causada por el desgarro de los cables de izado del sistema grúa puente. El desgarro ocurriría al chocar el gancho de la grúa con el armazón de la grúa puente. El gancho chocaría con el armazón de la grúa puente como consecuencia de un izado inadvertido del mismo y, a la vez, un fallo de los dispositivos de seguridad de la grúa puente.
- Fallo de anclaje: Esta causa raíz hace referencia a la ocurrencia de un fallo humano en la tarea de anclar el dispositivo de izado con el contenedor. Un fallo en el proceso de anclaje causaría la caída del contenedor cuando este se izase.
- Obstaculización del movimiento del contenedor: hace referencia a una situación en la cual el movimiento de izado del contenedor se ve interrumpido cuando el contenedor choca con algún obstáculo. Si el operador de grúa falla a parar el movimiento de izado pese a que el contenedor queda bloqueado, tanto el dispositivo de anclaje como los cables de izado podrían romperse, lo que causaría la caída del contenedor.

El proceso de identificación y definición de los eventos de fallo humano del contexto de estudio se divide según las fases de la etapa de carga. La siguiente sección ilustra el análisis realizado proporcionando a modo de ejemplo el análisis de la quinta fase de la etapa de carga. No obstante, tal y como se puede observar en la tabla 8.2, antes de realizar el análisis detallado se relacionan las diferentes causas raíz con las fases en las que pueden ocurrir.

Causa raíz	Fase 1	Fase 2	Fase 3	Fase 4	Fase 5	Fase 6
Carga errónea	X					
Two-blocking			X		X	
Anclaje		X			X	X
Obstaculización		X				

Tabla 8.2: Causas raíz y fases en las que pueden ocurrir.

Las causas raíz del suceso de carga errónea solo pueden ocurrir durante la primera fase, que es cuando se trasladan los elementos de combustible gastado al contenedor. La fase 4 no contiene ni cargas ni movimientos del contenedor, así que no aplica ninguna causa raíz. La causa de *two-blocking* se aplica en aquellas fases en las que el contenedor se alza por encima del nivel del suelo. La causa de obstaculización solo se considera en las fases en las que el contenedor se saca del pozo de contenedor puesto que se asume que el camino seguro de carga está limpio. Sin embargo, se avanza que finalmente no se ha identificado ningún posible evento de fallo humano que cause la obstaculización y posterior caída del contenedor (véase el anexo L para más detalle). El fallo al anclar se considera en todas aquellas fases en las que se han de conectar el gancho de izado y el contenedor.

8.3.4.3. Definición detallada de los eventos de fallo humano identificados

Se ejemplifica la definición detallada de los eventos de fallo humano mediante el análisis de la fase 5. La definición detallada de los eventos de fallo humano se apoya en la descripción de las tareas y acciones a realizar en las diferentes fases de la etapa de carga según los procedimientos de operación proporcionados por la central nuclear. El resto de definiciones se encuentra en el anexo L.

Fase 5: Traslado del contenedor desde la zona de soldadura hasta la plataforma de traslado. El contenedor HI-TRAC se coloca encima del HI-STORM Se analizan dos posibles causas raíz, véase la tabla 8.2, en la fase 5: fallo de anclaje y *two-blocking*. El fallo de anclaje de la fase 5 es similar al analizado en la fase 2. La única diferencia es que en la fase 5 el contenedor está en el suelo en lugar de en el interior del pozo de cofres. El contenedor se ha de alzar unos 6 metros para que la base del HI-TRAC quede por encima de la tapa del HI-STORM. El fallo de anclaje se define con un único evento de fallo humano.

El suceso de *two-blocking* es causado por un izado inadvertido del contenedor que culmina, si fallan los dispositivos de seguridad de la grúa, en el desgarro de los cables de izado y la caída del contenedor. El *two-blocking* es más probable en la fase 5 que en la fase 3 porque, siguiendo el procedimiento, el contenedor se ha de alzar alrededor de seis metros. Cuando el contenedor HI-TRAC está por encima del HI-STORM, la distancia entre el gancho de izado y el armazón de la grúa puente es de 1,6 m. Se necesitan 62 segundos de izado inadvertido[18] para que el gancho golpee el armazón de la grúa. La causa *two-blocking* se define con un único evento de fallo humano. Algunas características del movimiento realizado en la fase 5 son:

- Comparando la situación con la fase 2, menos individuos rodean el contenedor porque ya no hay necesidad de descontaminar el contenedor. En consecuencia, hay menos observadores para advertir problemas.
- A juzgar por la configuración del puesto de mando de la grúa, es posible que el operador de la grúa deje la palanca de mando en la posición de movimiento continuo en lugar de en la posición de parada debido a la configuración de la propia palanca.

[18] La velocidad máxima de izado de la grúa es de 1,524 metros por minuto.

HFE5.1: El contenedor cae debido al anclaje defectuoso del sistema de izado

Descripción: el evento de fallo humano HFE5.1 define la caída del contenedor sobre la superficie del edificio de combustible debido al fallo del operador de grúa a anclar correctamente el dispositivo de izado[19]. La configuración exacta de los brazos del yugo de izado y de las articulaciones del contenedor de transferencia se puede consultar en el anexo O. Los trabajdores observadores han de omitir o ejecutar incorrectamente la tarea de revisar el anclaje para que la caída pueda ocurrir. Además, este HFE tiene en cuenta una posible acción de recuperación: los trabajadores observadores podrían darse cuenta del chirrido que produce el desenganche, así que podrían decirle al operador de grúa que pare el movimiento de izado. En la ocurrencia del evento HFE5.1 se tiene en cuenta la posibilidad de que los trabajadores omitan el uso de procedimientos.

HFE5.2: Suceso *two-blocking*

Descripción: el evento de fallo humano HFE5.2 define el fallo del operador de grúa a parar el izado del contenedor una vez éste ha superado la altura del HI-STORM. Cabe la posibilidad que el operador deje la palanca de mando en la posición de movimiento continuo en lugar de cambiarla a la posición de parada. Los trabajadores observadores podrían darse cuenta de que el contenedor se iza más de lo esperado, pero solo hay 62 segundos de tiempo disponible para que los observadores avisen al operador de grúa del izado incorrecto y éste pare el movimiento. Podría haber problemas de comunicación entre los observadores y el operador de grúa debido al ruido existente en el interior del edificio de combustible.

8.3.4.4. Eventos de fallo humano

Como resultado de esta tarea, La tabla 11.1 presenta la definición de todos los eventos de fallo humano identificados en el desarrollo del análisis de fiabilidad humana del ATI de estudio.

HFE	Definición
HFE1.1	Colocar un elemento de combustible gastado seleccionado en una posición errónea en el contenedor
HFE1.2	Seleccionar un elemento de combustible equivocado para su colocación en el contenedor
HFE2.1	El contenedor cae debido al anclaje defectuoso del sistema de izado (fase 2)
HFE3.1	Suceso *two-blocking* (fase 3)
HFE5.1	El contenedor cae debido al anclaje defectuoso del sistema de izado (fase 5)
HFE5.2	Suceso *two-blocking* (fase 5)
HFE6.1	Caída del MPC en el interior del HI-STORM 100 debido al anclaje defectuoso del primero

Tabla 8.3: Definición de los eventos de fallo humano identificados.

8.3.5. Delineación de DHFETs

Siguiendo el caso de la tarea anterior, se ejemplifica la realización de los DHFETs presentando el análisis realizado para los eventos de fallo humano de la fase 5. El primer paso de la tarea de delineación de DHFETs es identificar todas las acciones elementales a realizar por los trabajadores, ya sean individuales o cadenas de acciones, cuyo fallo u omisión desencadenaría en la ocurrencia de los HFE. A su vez, se

[19] El anclaje del dispositivo de izado con el contenedor se ejecuta introduciendo los brazos del yugo de izado en los muñones del contenedor de transferencia.

identifican posibles acciones de recuperación, es decir, acciones que, de realizarse, evitarían la ocurrencia del HFE. La identificación de ambos tipos de acciones, las que desencadenarían un HFE y las que lo evitarían, se realiza a partir del seguimiento de los procedimientos de operación. Estas acciones son las que en los DHFETs ocupan el lugar de las acciones no seguras.

En el análisis desarrollado, el contenido de los procedimientos de operación se ha volcado en la descripción de las tareas de cada fase de la etapa de carga, véase el anexo A, y en la definición de los HFE, en la sección anterior. No obstante, se han vuelto a consultar los procedimientos de operación en los casos que se ha creído necesario. En algunas operaciones como, por ejemplo, el anclaje del dispositivo de izado al HI-TRAC, el procedimiento no es lo suficientemente detallado como para conocer todas las acciones elementales que ha de realizar el personal para llevar a cabo la operación. En casos como este, se ha optado por el conservadurismo en la definición de las UAs.

A continuación se presenta el análisis y la delineación de DHFETs de los sucesos HFE5.1 y HFE5.2. El anexo L contiene el resto de UAs identificadas y de DHFETs delineados.

8.3.5.1. Árbol de eventos de fallo humano de HFE5.1

El evento HFE5.1 hace referencia a la caída del contenedor debida al anclaje defectuoso del sistema de izado con el HI-TRAC. Se ha identificado una cadena de cuatro acciones elementales que, en caso de no realizarse correctamente combinaciones de ellas, puede derivar en la ocurrencia del suceso. La primera de las acciones de la cadena es la omisión del uso de procedimientos (UA llamada A en el DHFET, veáse la figura J.1). La omisión del uso de procedimientos conlleva que los trabajadores sean más propensos a cometer errores en las acciones siguientes, pero no es una causa directa de la caída del contenedor. No obstante, se tiene en cuenta para valorar el peor caso, es decir, que los trabajadores decidan no utilizar procedimientos. La siguiente acción elemental de la cadena es el fallo a anclar correctamente el dispositivo de izado. En el árbol de la figura J.1 existen dos versiones de esta acción, una usando procedimientos (UA llamada N), y otra sin usar procedimientos (UA llamada O). Gracias a los procedimientos se conoce que el trabajador ha de bajar los brazos de anclaje y, una vez están a la altura adecuada, ha de moverlos en horizontal, hacia el contenedor, para introducir los muñones del contenedor en los agujeros del brazo. Posteriormente, ha de cerrar los agujeros de los brazos. No obstante, no se conoce qué botones ni que movimientos de la palanca de mando ha de realizar el operador de grúa para ejecutar la tarea descrita. En consecuencia, de forma conservadora, la unidad más elemental para describir dicha tarea es la ya mencionada «fallo a anclar correctamente el dispositivo de izado». Es totalmente necesario que se produzca el fallo al anclar para que ocurra el HFE5.1. Si el anclaje se realiza correctamente jamás podrá producirse la caída del contenedor. A continuación, el personal de revisión valoraría el anclaje. En caso de que esta revisión no se realice (UAs F (con procedimientos) y G (sin procedimientos)) o se realice de forma incorrecta (UAs H (con procedimientos) e I (sin procedimientos)), el contenedor podría caer. Se asume que, si la revisión se realiza de forma correcta, el anclaje también será el adecuado.

Se utiliza el condicional porque se han identificado acciones de recuperación que evitarían que cayese el contenedor. Concretamente, se ha identificado una cadena de acciones de recuperación, que son: en primer lugar, los trabajadores encargados de la revisión se dan cuenta de que el contenedor genera un sonido chirriante[20] producto del desenganche del anclaje defectuoso. Al darse cuenta, se lo comunican al operador de grúa. Éste último es capaz de parar el movimiento sin que haya consecuencias para el contenedor, es decir, sin que este caiga desde una altura comprometedora. En este caso, las tres acciones se han de realizar correctamente para evitar la caída del contenedor. Cada acción tiene asociada su propia UA: la UA llamada P hace refencia al fallo a darse cuenta del chirrido. La UA llamada L hace referencia a un fallo de comunicación entre los revisores y el operador de grúa. La UA llamada M hace referencia al fallo del operador de grúa a parar a tiempo el movimiento de izado. El árbol de eventos de fallo humano

[20] Este sonido chirriante puede producirse en uno u otro momento y a una u otra altura dependiendo de lo mal que se haya realizado el anclaje. Conservadoramente, en la introducción de los resultados del HRA en el APS se asume que el sonido se produce cuando el contenedor está a la máxima altura posible.

del suceso HFE5.1 se delinea teniendo en cuenta que la caída del contenedor ocurre sí y solo sí se produce la UA de fallo al anclaje y falla la revisión, ya sea por omisión o por ejecución errónea. Dado alguno de estos casos, se evita la caída del contenedor sí y solo sí se realizan correctamente todas las acciones de recuperación. La figura J.1 presenta el DHFET del evento HFE5.1.

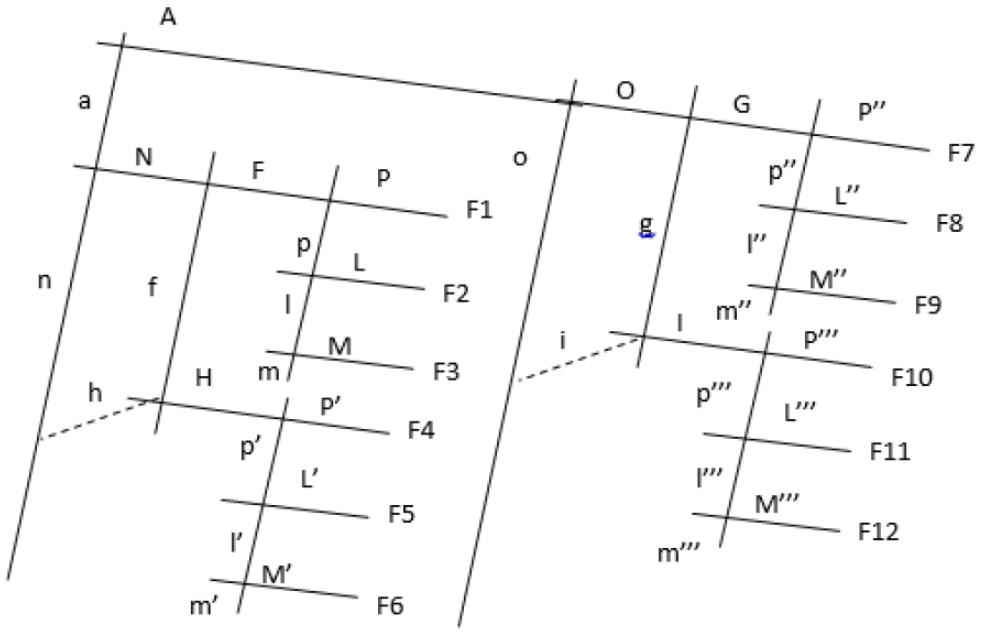


Figura 8.6: Árbol detallado de eventos de fallo humano del suceso HFE5.1

El árbol de eventos de fallo humano de la figura J.1 plasma las condiciones de ocurrencia del evento HFE5.1 estipuladas en el párrafo anterior. Las letras minúsculas hacen referencia a la correcta ejecución de las acciones no seguras postuladas. Las acciones no seguras P, L, y M tienen diferente cantidad de comillas según el contexto de ejecución para, precisamente, diferenciar entre dichos contextos. Las combinaciones de letra y número F1 a F12 hacen referencia a los doce caminos de fallo identificados mediante el DHFET. Es decir, el suceso HFE5.1 se puede producir de doce formas diferentes. Los caminos de fallo se traducen a ecuaciones para la posterior cuantificación de la probabilidad de ocurrencia del HFE. La figura 8.7 presenta dichas ecuaciones.

$$F1 = a \cdot N \cdot F \cdot P \quad F2 = a \cdot N \cdot F \cdot p \cdot L \quad F3 = a \cdot N \cdot F \cdot p \cdot l \cdot M \quad F4 = a \cdot N \cdot f \cdot H \cdot P'$$

$$F5 = a \cdot N \cdot f \cdot H \cdot p' \cdot L' \quad F6 = a \cdot N \cdot f \cdot H \cdot p' \cdot l' \cdot M' \quad F7 = A \cdot O \cdot G \cdot P''$$

$$F8 = A \cdot O \cdot G \cdot p'' \cdot L'' \quad F9 = A \cdot O \cdot G \cdot p'' \cdot l'' \cdot M'' \quad F10 = A \cdot O \cdot g \cdot I \cdot P'''$$

$$F11 = A \cdot O \cdot g \cdot I \cdot p''' \cdot L''' \quad F12 = A \cdot O \cdot g \cdot I \cdot p''' \cdot l''' \cdot M'''$$

Figura 8.7: Ecuaciones de los caminos de fallo del DHFET de HFE5.1

Cada una de estas ecuaciones se puede traducir a lenguaje escrito. Todas ellas deberían respetar las condiciones establecidas en párrafos anteriores. Para conocer que situación describe cada camino de fallo, se ha de seguir la línea continua desde la primera UA (A) hasta la F. Por ejemplo, la ecuación del camino

F12 describe la ocurrencia del evento HFE5.1 de la siguiente manera: Los operadores deciden omitir el uso de procedimientos (A) y el operador de grúa falla al anclar el dispositivo de izado con el HI-TRAC (O). No obstante, los revisores realizan su tarea (g) aunque de forma errónea, no detectando el fallo (I). Pese a que, posteriormente, los revisores se dan cuenta del sonido chirriante (p"') y se lo comunican correctamente al operador de grúa (l"'), éste no es capaz de parar el movimiento ascendente a tiempo, produciéndose la caída del contenedor (M"').

8.3.5.2. Árbol de eventos de fallo humano de HFE5.2

El evento HFE5.1 hace referencia a un suceso de *two-blocking*. En este caso se ha identificado una única acción elemental que, en caso de no realizarse correctamente, podría derivar en la ocurrencia del suceso. La acción elemental identificada es el fallo del operador de grúa a parar el movimiento ascendente de la grúa. En este caso no se tiene en cuenta si se utilizan procedimientos o no porque se considera que el operador es plenamente consciente de que ha de parar el izado del contenedor HI-TRAC cuando éste está por encima del contenedor HI-STORM. Además, la acción de parar es la única que ha de realizar una vez comienza el movimiento de izado. Por esta razón, tampoco se le da crédito a la omisión del operador a parar el movimiento ascendente de la grúa. Solo se considera la posibilidad de que el operador cometa un error de comisión[21] y falle a parar el movimiento. En este caso sí se conoce qué ha de hacer el operador para parar la grúa: mover la palanca de mando hasta la posición de parada. No obstante, para que la UA incluida en el DHFET sea lo más descriptiva posible se mantiene el nombre de fallo del operador de grúa a parar el movimiento ascendente de la misma (UA llamada Q en el árbol de la figura 8.8).

En este caso, se ha identificado una cadena de dos acciones elementales que, si se realizan ambas correctamente, evitarían el potencial suceso *two-blocking*[22]. Se considera que los revisores u observadores del movimiento se darán cuenta inmediatamente de que el contenedor ha superado la posición en la que debería parar e intentarán avisar al operador de grúa. El operador de grúa intentará parar el movimiento ascendente a tiempo, es decir, antes de que se produzca el choque, si entiende lo que le comunican los observadores. Cada acción tiene asociada su propia UA: la UA llamada L hace referencia al fallo de comunicación entre observadores y operador de grúa, y la UA llamada R hace referencia al fallo del operador de grúa a parar el movimiento ascendente a tiempo. Para que se produzca el suceso de *two-blocking*, a parte de fallar componentes de seguridad de la grúa, el operador de grúa ha de fallar a parar el movimiento ascendente y, o bien ha de fallar la comunicación entre los observadores y el operador, o bien ha de fallar el operador a parar el movimiento ascendiente a tiempo. La figura 8.8 presenta el árbol de eventos de fallo humano del suceso HFE5.2.

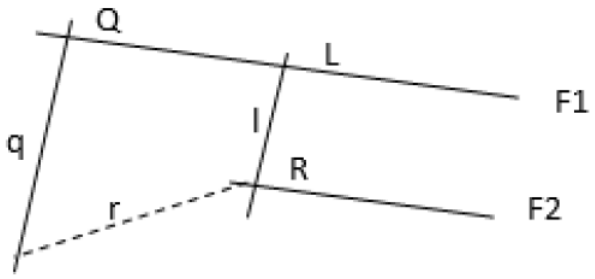


Figura 8.8: DHFET del suceso HFE5.2

Las ecuaciones asociadas a los caminos de fallo F1 y F2 se presentan en la figura 8.9

[21] Error no intencionado al realizar una acción. El resultado es la ejecución de una acción de forma errónea.

[22] Cabe recordar que para que se produzca un suceso de *two-blocking* también han de fallar elementos de seguridad de la grúa.

$$F1 = Q \cdot L \qquad F2 = Q \cdot l \cdot R$$

Figura 8.9: Ecuaciones de los caminos de fallo de HFE5.2

8.3.6. Análisis de PSFs

El propósito del análisis de PSF es incrementar el nivel de realismo de los análisis de fiabilidad humana mediante la evaluación de la influencia del contexto sobre la actuación humana. El análisis de PSF ha de ser lo suficientemente detallado como para identificar potenciales influencias del contexto sobre la actuación humana y valorarlas mediante los llamados multiplicadores. El método elegido para analizar los PSFs es SPAR-H, que presenta ocho PSF diferentes. La tabla 8.4 presenta los ocho PSFs de SPAR-H.

PSF	Descripción
Tiempo disponible	La cantidad de tiempo de la que dispone un operador para ejecutar una acción después de ocurrir un suceso anormal
Estrés / elementos estresantes	Fuerzas motivadoras, tanto positivas como negativas, que afectan a la actuación humana. El nivel de circunstancias y condiciones indeseables que dificultan que un operador complete fácilmente una tarea. Algunos elementos estresantes son: calor, ruido, ventilación, y otros. Una pequeña cantidad de estrés puede mejorar la actuación humana.
Complejidad	El grado de dificultad de una tarea en el contexto analizado. El PSF de complejidad tiene en cuenta tanto la tarea en sí como el ambiente en el que se realiza. El PSF también tiene en cuenta el esfuerzo mental requerido, como, por ejemplo, la necesidad de realizar cálculos o de utilizar la memoria.
Experiencia / entrenamiento	El grado de experiencia y/o entrenamiento de los operador que realizan una acción en relación con la acción en sí. Se ha de tener en cuenta el tiempo que ha pasado desde el último entrenamiento.
Procedimientos	Este PSF hace referencia a la existencia y uso de procedimientos formales para realizar la acción de estudio. Se ha de tener en cuenta si los procedimientos proporcionan información equivocada o inadecuada. Se hace especial hincapié en si los procedimientos presentan pasos ambiguos.
Ergonomía / HMI	Equipo, pantallas, controles, la cantidad y calidad de información que proporciona la instrumentación, y la interacción entre el operador y la máquina.
Aptitud para el trabajo	Hace referencia a si el individuo que realiza la tarea está preparado física y mentalmente para ella. Algunos de los elementos que pueden afectar a la preparación incluyen la fatiga, enfermedad, uso de drogas, exceso de confianza, problemas personales, y distracciones.
Procesos de trabajo	Incluye aspectos la organización interna, la cultura de seguridad, la planificación del trabajo, la comunicación, y la gestión.

Tabla 8.4: PSFs de SPAR-H

Cada PSF se descompone en varios niveles cualitativos que describen las posibles influencias de dicho

PSF sobre la actuación humana. Todos los niveles cualitativos están asociados a un multiplicador[23], que valora cuantitativamente la influencia sobre la actuación humana de cada nivel cualitativo. La tabla 8.5 presenta los niveles cualitativos y los multiplicadores de cada uno de los ocho PSFs. El anexo J contiene la descripción de cada uno de los niveles cualitativos presentes en la tabla 8.5.

PSF	Niveles cualitativos	Multiplicadores
Tiempo disponible (AT)	Tiempo inadecuado	Probabilidad de fallo = 1
	AT = tiempo requerido	10
	Tiempo nominal	1
	AT >= 5 veces el tiempo requerido	0,1
	AT >= 50 veces el tiempo requerido	0,01
Estrés (S)	Extremo	5
	Alto	2
	Nominal	1
Complejidad (C)	Muy complejo	5
	Moderadamente complejo	2
	Nominal	1
Experiencia / entrenamiento (ET)	Baja	3
	Nominal	1
	Alto	0,5
Procedimientos (P)	No disponible	50
	Incompletos	20
	Disponibles, pero pobres	5
	Nominal	1
Ergonomía/HMI (EH)	Faltan o confunden	50
	Pobre	10
	Nominal	1
	Bueno	0,5
Aptitud para el trabajo (F)	No apto	Probabilidad de fallo = 1
	Aptitud degradada	5
	Buena	1
Procesos de trabajo (WP)	Pobres	2
	Nominal	1
	Buenos	0,8

Tabla 8.5: Niveles cualitativos y multiplicadores de los PSFs

En consecuencia, el análisis de PSFs consiste en elegir, para cada UA identificada en la delineación de DHFETs, qué nivel cualitativo de cada PSF aplica según el contexto analizado. De manera similar a tareas anteriores, se ejemplifica el análisis de PSFs presentando el estudio llevado a cabo para los eventos de fallo humano de la quinta fase de la etapa de carga. El resto del análisis se puede consultar en el anexo L.

8.3.6.1. Análisis de PSFs para los eventos de fallo humano de la fase 5 de la etapa de carga

El análisis de PSFs consiste en seleccionar qué niveles cualitativos describen el contexto en el que se realizan cada una de las UAs. Los niveles cualitativos se han de ajustar lo máximo posible a las condiciones reales

[23] Los valores mayores que 1 son negativos para la acción a realizar, mientras que los valores menores que 1 son positivos para la acción a realizar.

en las que se realizan las acciones humanas. Las condiciones en las que se realizan las acciones de la fase 5 están descritas en la sección de descripción del contexto nominal, sección 8.3.3, y en el anexo A.

El nivel cualitativo Nominal se ha elegido por defecto en dos PSFs para toda UA en el contexto nominal: procesos de trabajo y experiencia / entrenamiento. La influencia de ambos sobre la ejecución de las UAs es nula en el contexto nominal por la propia definición del contexto. El resto de niveles cualitativos elegidos se presentan a continuación.

HFE5.1: El contenedor cae debido al anclaje defectuoso del sistema de izado

La tabla L.2 contiene los multiplicadores, y, por lo tanto, índica los niveles cualitativos, seleccionados para las UAs que forman el HFE5.1.

	PSFs					
UA ID	AT	Estrés	Complejidad	Procedimientos	Ergo/HMI	Aptitud
A	0,1	1	1	1	1	1
F	0,1	1	1	1	1	1
G	0,1	1	1	1	1	1
H	1	1	1	1	1	1
I	1	1	2	1	1	1
L	1	2	1	1	1	1
L’	1	2	1	1	1	1
L”	1	2	1	1	1	1
L”’	1	2	1	1	1	1
M	10	1	1	1	0,5	1
M’	10	1	1	1	0,5	1
M”	10	1	1	1	0,5	1
M”’	10	1	1	1	0,5	1
N	1	1	2	1	1	1
O	1	1	5	1	1	1
P	1	2	1	1	1	5
P’	1	2	1	1	1	5
P”	1	2	1	1	1	5
P”’	1	2	1	1	1	5

Tabla 8.6: Multiplicadores de PSF para el evento HFE5.1.

Se detallan a continuación las razones por las cuales se han elegido multiplicadores diferentes a Nominal para algunas de las UAs del suceso HFE5.1:

- Se ha elegido el nivel Aptitud degradada en la UA de fallo a darse cuenta del chirrido (P) para introducir la influencia del llamado concepto de pérdida. El concepto de pérdida hace referencia al hecho que las personas tienden a rechazar la existencia de un problema cuando escuchan o ven algo que no entienden [8, 9]. En el caso de la UA llamada P, los operadores oyen un ruido metálico y lo asocian al uso de maquinaria en otro lugar del edificio de combustible en lugar de pensar que se está desenganchando el contenedor.
- Se ha escogido el nivel Bueno para el PSF de ergonomía en la UA llamada M, fallo del operador de grúa a parar el movimiento. De esta manera se tiene en cuenta que la grúa puente del edificio de combustible ha sido mejorada recientemente, incluyendo el cambio del puesto de mando.
- El nivel de estrés para las UAs error de comunicación, UA llamada L, y para la UA de fallo a darse cuenta del chirrido, UA llamada P, se ha establecido en Alto para tener en cuenta que el volumen

del ruido en el interior del edificio de combustible es alto. El nivel de ruido afecta especialmente a la ejecución de estas dos acciones.

- Se considera que la tarea de anclar, UA llamada N usando procedimientos, es moderadamente compleja. Además, si no se utilizan procedimientos, UA llamada O, se considera que dicha tarea es muy compleja.
- Se escoge el nivel tiempo disponible = tiempo requerido para la UA de fallo del operador de grúa a parar la grúa (M) porque el tiempo disponible para parar la grúa en caso de notificarse el fallo es corto. Además, el PSF también tiene en cuenta posibles distracciones de los operadores y el hecho que es posible que el operador de grúa no vea el contenedor.
- Se considera que el tiempo disponible para tomar la decisión al respecto del uso de procedimientos y para realizar la tarea de revisión es suficientemente amplio como para considerarlo que es cinco veces más que el tiempo necesario para realizar dichas acciones.
- La complejidad de ejecutar la tarea de revisión sin utilizar procedimientos es moderada.

HFE5.2: Suceso *two-blocking*

La tabla L.3 contiene los multiplicadores, y, por lo tanto, índica los niveles cualitativos, seleccionados para las UAs que forman el HFE5.2.

	PSFs					
UA ID	AT	Estrés	Complejidad	Procedimientos	Ergo/HMI	Aptitud
L	1	2	1	1	1	5
Q	1	1	1	1	0,5	1
R	10	1	1	1	0,5	1

Tabla 8.7: Multiplicadores de PSF para el evento HFE5.2

Se detallan a continuación las razones por las cuales se han elegido multiplicadores diferentes a Nominal para algunas de las UAs del suceso HFE5.2:

- El nivel de estrés para las UA error de comunicación, UA llamada L, se ha establecido en Alto para tener en cuenta que el volumen del ruido en el interior del edificio de combustible es alto. El nivel de ruido afecta especialmente a la ejecución de esta acción.
- Se ha escogido el nivel Bueno para el PSF de ergonomía en las UAs llamada Q y R, fallo del operador de grúa a parar el izado, y fallo del operador de grúa a parar el movimiento a tiempo, respectivamente. De esta manera se tiene en cuenta que la grúa puente del edificio de combustible ha sido mejorada recientemente, incluyendo el cambio del puesto de mando.
- Se escoge el nivel tiempo disponible = tiempo requerido para la UA de fallo del operador de grúa a parar el izado a tiempo (R). El tiempo disponible para realizar esta acción es de 20 segundos, y el tiempo requerido para realizarla es de 2 segundos. No se ha escogido el nivel Nominal para tener en cuenta posibles distracciones y el hecho que es posible que el operador de grúa no vea el contenedor.
- Se ha escogido el nivel cualitativo de Aptitud degrada en la UA error de comunicación (L) para tener en cuenta que los trabajadores observadores confían en el operador de grúa. En este caso, es complicado diferenciar entre la altura correcta del contenedor y la altura de *two-blocking* debido a la poca distancia que las separa. Los observadores pueden darse cuenta de que el contenedor se ha alzado más de la cuenta pero pueden entonces pensar que el operador de grúa sabe lo que hace.

8.3.7. Definición de *error-forcing contexts*

El concepto de *error-forcing context* representa las posibles desviaciones respecto al contexto nominal en las que la probabilidad de error humano se incrementa debido a las nuevas condiciones establecidas. En el contexto de la metodología ATHEANA, se amplía el alcance del análisis HRA para estudiar y cuantificar los HFEs identificados anteriormente en todos aquellos EFCs plausibles. Gracias al nuevo método de cuantificación, el análisis de los HFE en los diferentes EFCs se traduce simplemente en el reanálisis de los PSFs[24]. Podrían haber infinitos EFCs, así que el análisis se acota a aquellos contextos que afecten de alguna manera al movimiento de combustible, a las condiciones de trabajo, o a las condiciones ambientales del edificio. Se excluyen en consecuencia aquellos EFCs relacionados con la ocurrencia de sucesos externos[25] en medio de una CLC. Los EFCs identificados en el caso de estudio son los siguientes:

- Parada de recarga programada pocos días después de la fecha de finalización de una CLC (EFC1).
- Alta temperatura en la parte superior del MPC (EFC2).
- Final de campaña de carga (EFC3).
- Primera campaña de carga (EFC4).

Estos EFCs han sido identificados valorando qué contextos podrían cambiar los niveles cualitativos de los PSFs utilizados en el contexto nominal. Además, los EFCs postulados aparecen en la lista de EFCs propuesta en el NUREG/CR-7017 [9]. En las secciones que siguen se describen los EFCs y se define que PSFs cambian. Los multiplicadores de los PSFs seleccionados para los diferentes EFCs se pueden consultar en el anexo J.

8.3.7.1. EFC1: Parada de recarga programa pocos días después de la finalización de una CLC

Las campañas de carga de contenedores requieren una gran cantidad de tiempo, espacio, y personal. Es por esta razón que, si la finalización de una CLC se retrasa, cualquier actividad programada después de la CLC se retrasa también. Esto no supone un problema para la mayoría de las actividades a realizar en el interior del edificio de combustible, pero sí lo es si esta actividad es una parada de recarga puesto que su planificación es muy poco flexible. En consecuencia, las CLC se planifican para terminar meses antes de cualquier parada de recarga. No obstante, retrasos o aplazamientos en la realización de una CLC pueden provocar que el final de ésta se aproxime a una parada de recarga. Una situación como la descrita en el EFC1 incrementaría la presión temporal y el estrés que sentirían los trabajadores, haciendo que el personal fuese más propenso a trabajar sin procedimientos. Los cambios en términos de PSF que provocaría el EFC1 son:

- **Presión temporal**: En una CLC los trabajadores necesitan tomarse su tiempo para realizar correctamente algunas de las acciones del proceso. Este hecho no acostumbra a ser un problema pues las CLCs se planifican para que los trabajadores tengan suficiente tiempo disponible. En el caso de EFC1, la lentitud de algunos procesos combinada con la necesidad de terminar lo antes posible puede afectar a la realización de las acciones mencionadas de forma negativa. Es por ello que se modifica el PSF de tiempo disponible. En todas aquellas acciones en las que se considera en el contexto nominal que el tiempo disponible es cinco veces mayor que el requerido (contexto positivo)

[24] Las UAs son válidas para cualquier contexto porque son elementales y genéricas. Se debería valorar, no obstante, si las condiciones de un EFC podrían implicar la realización de alguna acción más.

[25] Considerarlos sería incoherente teniendo en cuenta que en el APS no se han incluido como sucesos iniciadores de la etapa de carga.

pasa a considerarse el tiempo disponible como Nominal (contexto neutro). Esto afecta mayoritariamente a UAs de uso de procedimientos, revisiones y movimientos de combustible. Las acciones cuyo tiempo disponible se ciñe a criterios ALARA, por ejemplo, el anclaje de dispositivos de izado o la descontaminación de contenedores, no ven modificado su PSF.

- **Estrés**: Los trabajadores ven incrementado su nivel de estrés por la necesidad de acabar la CLC a tiempo. El PSF de Estrés se modifica seleccionado el siguiente nivel cualitativo más negativo para todas las acciones manuales.
- **Desviaciones en el uso de procedimientos**: El personal siente la necesitad de ejecutar las operaciones lo más rápido posible para acabar la campaña a tiempo. En consecuencia, los trabajadores son propensos a desviarse de, o omitir el uso de, los procedimientos en todas aquellas acciones monótonas basadas en su propia habilidad. El personal es propenso a utilizar atajos para evitar la lentitud que provoca utilizar procedimientos, que está principalmente causada por las revisiones, verificaciones y escritura de notas. La posible desviación en el uso de procedimientos se modela mediante el PSF de Aptitud para el trabajo. Se elige el siguiente nivel más negativo del PSF para todas aquellas acciones que describen la omisión del uso de procedimientos.
- **Procesos de trabajo**: Parte del personal involucrado en la CLC puede necesitarse en la preparación de la parada de recarga. Está interferencia se soluciona contratando personal externo para reemplazar al personal que se transfiere a la preparación de la campaña de recarga. A causa del nuevo personal, en la CLC pueden observarse diferencias en términos organizacionales, de planificación del trabajo, de cultura de seguridad, o de comunicación. En consecuencia, es probable que el desarrollo de los trabajos sea más confuso que en el contexto nominal. El PSF de procesos de trabajo se incluye en el análisis. Se supone que el personal externo se necesita únicamente en las tareas de anclaje de la fase 6. Se selecciona el nivel cualitativo Pobres (multiplicador = 2).

8.3.7.2. Alta temperatura en la parte superior del MPC (EFC2)

La carga térmica y la dosis de radiación del contenedor depende del enriquecimiento inicial y de los años de almacenamiento en mojado de los elementos de combustible gastado almacenados en el contenedor. Cuanto mayor sea el enriquecimiento inicial mayor es la carga térmica y la dosis. Al contrario, cuanto mayor sea el periodo de almacenamiento en mojado, menor es la carga térmica y la dosis. Un contenedor se carga con elementos de combustibles gastado de características diferentes. Por lo tanto, existe la posibilidad de que un contenedor se cargue con una combinación de elementos de combustible cuya carga térmica y dosis sean mayores que las del contexto nominal. Esta particular situación afecta a las acciones que se llevan a cabo encima del MPC ya que parte superior es la que esta peor blindada [78]. La alta temperatura resultado de la carga térmica se considera un elemento estresante. Por otra parte, la dosis se considera un factor que aumenta la presión temporal. Los cambios en términos de PSF que provocaría el EFC2 son:

- **Presión temporal**: El tiempo disponible para ejecutar acciones que se ven afectadas por la dosis de la parte superior del MPC se reduce para estar de acuerdo con criterios ALARA. Los trabajadores tienen que realizar las mismas acciones pero en menos tiempo. El PSF Tiempo disponible se modifica para tener en cuenta este cambio. Se elige el nivel cualitativo «El tiempo disponible es igual al tiempo requerido para realizar la acción» para todas aquellas acciones cuya área de trabajo es la parte superior del MPC.
- **Estrés**: Una temperatura más alta genera más sudor, problemas de visión, y más fatiga, empeorando así la actuación humana en la ejecución de acciones. La alta temperatura es considerada un elemento estresante. En consecuencia, el PSF de Estrés se modifica en todas las acciones cuya área de trabajo es la parte superior del MPC. Se selecciona un nivel de estrés Alto.

8.3.7.3. Final de campaña de carga (EFC3)

La mayoría de las acciones y procesos que se llevan a cabo durante una campaña de carga son monótonas y dependen de la habilidad del operador que las realiza. Además, algunas de ellas se han de ejecutar lentamente, a pesar de ser fáciles de realizar, debido a restricciones impuestas por los procedimientos. La experiencia ha demostrado que la percepción del riesgo que tienen los operadores disminuye cuando éstos se acostumbran a realizar acciones monótonas [9]. Además, la confianza en sí mismos y en los demás aumenta hasta el punto que son propensos a ejecutar acciones de forma no segura. Estas situaciones podrían darse en la última carga de contenedor de una campaña de carga dando lugar a comportamientos arriesgados. Algunos ejemplos de este tipo de comportamientos, específicos de una CLC, son:

- El operador responsable del traslado de elementos de combustible gastado decide no utilizar la planificación de movimientos para así poder completar la carga del contenedor en menos tiempo.
- Los operadores observadores y el supervisor confían en el criterio y la habilidad del operador responsable del traslado de elementos de combustible y no comprueban exhaustivamente que la configuración final sea la deseada.
- Los operadores a cargo de tareas de anclaje se desvían de, o no utilizan, las indicaciones de los procedimientos para poder completar la tarea en menos tiempo.
- Los revisores encargados de los anclajes confían en los operadores que se han encargado de la tarea y no comprueban exhaustivamente si los anclajes se han realizado correctamente.
- Los observadores confían en el operador de grúa y no siguen con la vista el movimiento del contenedor.

Todos estos comportamientos incrementan la probabilidad de ocurrencia de un HFE en el contexto EFC3. El PSF de Aptitud para el trabajo se modifica para tener en cuenta los posibles comportamientos arriesgados. El nivel cualitativo del PSF se sitúa en «Aptitud degradada» para todas las UAs relacionadas con la omisión o desviación de procedimientos, la implementación de procedimientos o revisiones, y las UAs de ejecución basada en la habilidad, como, por ejemplo, los anclajes. Por otra parte, la experiencia de los trabajadores ya es alta, fuese cual fuese la experiencia inicial, en la fase final de la campaña de carga. El PSF de Experiencia y entrenamiento se introduce en el análisis para tener en cuenta esta experiencia. El PSF se sitúa en nivel Alto para todas las acciones manuales.

8.3.7.4. Primera campaña de carga (EFC4)

La primera vez que se realiza una campaña de carga en una central nuclear el contexto general es diferente al contexto nominal descrito en el análisis de fiabilidad humana. Por una parte, la primera CLC se planeará con tiempo, dando espacio a reuniones para explicar a los operadores que han de hacer. Además, el periodo de tiempo planificado para la CLC será mayor que en el contexto nominal para darle a los operadores más tiempo para ejecutar las tareas de forma correcta. Por otra parte, la mayoría de las acciones se realizaran por primera vez en el contexto específico del edificio de combustible de la central nuclear. En consecuencia, la probabilidad de fallo humano al realizar dichas acciones será mayor. Los cambios en términos de PSF que provocaría el EFC4 son:

- **Tiempo disponible**: El PSF Tiempo disponible de todas las acciones no relacionadas con criterios ALARA se sitúa en «Cincuenta veces más que el tiempo requerido para realizar la acción». En contraste, el PSF se sitúa en «Tiempo disponible = tiempo requerido» para aquellas acciones a realizar en un contexto de temperatura y dosis exigentes.

- **Experiencia y entrenamiento**: El PSF de Experiencia y entrenamiento se incluye en el análisis y se sitúa en el nivel bajo para todas las acciones que no conllevan movimiento de combustible gastado[26].

8.3.8. Análisis del potencial de recuperación

En el contexto de la metodología ATHEANA, se entiende como potencial de recuperación a la probabilidad de enmendar un error humano mediante la realización de otra(s) acción(es) humana(s) antes de que la primera tenga consecuencias. Las acciones humanas realizadas a posteriori del error humano que enmiendan el error y evitan sus consecuencias son las llamadas acciones de recuperación. En el caso de estudio, los HFE identificados en la sección 8.3.4 son los errores humanos a enmendar mediante las acciones de recuperación. Se han identificado tres posibles acciones de recuperación poniendo especial atención en las UAs que causan cada HFE y la configuración final del contenedor de cada HFE.

- **Revisión de supervisor**: La revisión de supervisor representa una última revisión del estado del contenedor cuyo propósito es asegurar que la configuración final del contenedor es correcta. Esta revisión es llevada a cabo por un miembro especial del equipo que lleva a cabo la CLC. La aprobación de esta última supervisión permite al equipo continuar con el procedimiento. Esta acción de recuperación es aplicable a los eventos HFE1.1, HFE1.2, HFE2.1, HFE5.1, y HFE6.1. Los cinco HFE son resultado de la ejecución errónea de una serie de acciones llevadas a cabo para conseguir una configuración final del contenedor diferente a la inicial. Dicha configuración final es la que es revisada. Para estos casos, la probabilidad de ocurrencia del HFE se multiplica por la probabilidad de omitir o ejecutar de forma incorrecta la acción de recuperación para calcular la probabilidad final de ocurrencia del HFE.
- **Medida de la radiación**: La medida de la dosis de radiación en la superficie del contenedor es una acción de recuperación plausible para los eventos HFE1.1 y HFE1.2. En primer lugar, porque siguiendo los procedimientos se debería ejecutar tal acción. En segundo lugar, porque la dosis exterior del contenedor se calcula teóricamente una vez conocida la configuración final. Cualquier sustancial diferencia entre la dosis medida y la calculada sería producto de la ocurrencia del HFE1.1 o el HFE1.2. En este caso, la probabilidad de ocurrencia del HFE se multiplica por la probabilidad de omitir o ejecutar de forma incorrecta la acción de recuperación para calcular la probabilidad final de ocurrencia del HFE.
- **Advertir un error, comunicarlo, y realizar una parada de emergencia de la grúa**: En algunos HFE existe la posibilidad de que los operadores, especialmente los observadores, adviertan que alguna tarea se ha ejecutado incorrectamente. Una vez advertido el error, los operadores han de ser capaces de comunicarse con el operador de grúa para hacerle llegar la necesidad de interrumpir el movimiento. El operador de grúa ha de entender el mensaje de los observadores y ejecutar la acción de interrumpir el movimiento. Esta cadena de acciones de recuperación aplica a todos los eventos de *two-blocking* y a los fallos de anclaje. La cadena de acciones, a diferencia de las recuperaciones anteriormente explicadas, ha sido incluida en los árboles detallados de eventos de fallo humano de los HFE correspondientes.

8.3.9. Cuantificación de HFEs

La última tarea del análisis de fiabilidad humana es la cuantificación de la probabilidad de ocurrencia, o HEP, de los eventos de fallo humano identificados en la sección 8.3.4. En el caso de estudio, y a diferencia de ATHEANA, la tarea de cuantificación se ha llevado a cabo siguiendo el método de cuantificación

[26] Los operadores que realizan las acciones de movimiento de combustible tendrán la experiencia de las paradas de recarga que haya hecho la central.

presentado en la sección 8.2.3. Siguiendo el procedimiento mencionado, esta sección se divide en dos partes: la cuantificación de las acciones no seguras, y la propia cuantificación de los HFEs. Se ha ejemplificado la aplicación del procedimiento mediante el caso del HFE5.2 allá donde ha sido necesario.

8.3.9.1. Cuantificación de acciones no seguras

A su vez, siguiendo el procedimiento, la parte de cuantificación de acciones no seguras se divide en dos pasos: el uso de un modelo clásico de cuantificación que aglutina el fallo cognitivo y el fallo manual, y el ajuste de valores genéricos al contexto de estudio mediante *performance shaping factors*.

Modelo clásico de cuantificación La ecuación L.5, ya presentada en la sección 8.2.3.3 de descripción del procedimiento de cuantificación, representa el modelo clásico de cuantificación utilizado. En dicha ecuación, el fallo de un operador a ejecutar una acción de forma correcta tiene dos componentes: la cognitiva y la manual. Se considera que el operador falla completamente a realizar la acción si falla en cualquiera de sus dos componentes.

$$HEP_{UA} = FP_{cog} + (1 - FP_{cog}) * FP_{manual} \tag{8.5}$$

La componente cognitiva del fallo evalúa la capacidad de diagnóstico y decisión del operador en el tiempo disponible para realizar una acción. Tal y como se ha explicado a lo largo del análisis, el contexto de las acciones relacionadas con el ATI es de operación normal, lo que implica que, en la mayoría de casos, el tiempo disponible es mucho mayor que el requerido para realizar una acción. Se ha decidido despreciar la probabilidad de fallo cognitivo de estas acciones porque resultaría en valores infinitesimales. En consecuencia, en las únicas acciones en las que se da crédito a un posible fallo cognitivo es en las acciones de recuperación que implican la ejecución de una tarea bajo presión temporal. Concretamente, se aplica el análisis del fallo cognitivo sobre las acciones no seguras de «el operador de grúa falla a parar el movimiento» presentes en los DHFET de los eventos HFE2.1 y HFE5.1, y las acciones no seguras de «el operador de grúa falla a parar el movimiento a tiempo» de los HFE3.1 y HFE5.2, ambos sucesos *two-blocking*.

El análisis del fallo cognitivo se ha llevado a cabo mediante el método HCR. La tabla 8.8 presenta los resultados obtenidos. El desarrollo del análisis del fallo cognitivo se detalla en el anexo L.

HFE de la UAs analizadas	FP_{cog}
HFE2.1	1,47E-15
HFE3.1	ε
HFE5.1	1,47E-15
HFE5.2	2,56E-210 = ε

Tabla 8.8: Probabilidades de fallo cognitivo

Las probabilidades de fallo cognitivo calculadas son extremadamente bajas, especialmente si se comparan con las probabilidades de fallo manual (véase la tabla 8.9 a continuación) utilizadas en el caso de estudio. En consecuencia, se ha decidido negligir la parte cognitiva del fallo humano. El modelo utilizado finalmente solo tiene en cuenta la probabilidad de fallo manual para estimar la probabilidad genérica de ocurrencia de las acciones no seguras.

No se ha dispuesto de ninguna base de dados que refleje específicamente la experiencia en operaciones de ATI del personal de planta. Por lo tanto, la probabilidad de fallo manual se ha obtenido de bases de datos de acceso abierto. En el caso de estudio se han consultado tres bases de datos de fallo humano:

- Base de datos de fallo de THERP [6]: El manual NUREG/CR-1278 contiene un conjunto de tablas con valores de probabilidad de fallo humano que cubren la mayoría de acciones posibles en sala de control.
- *Savannah River Site Human Error Database Development for Nonreactor Nuclear Facilities (U)* (SHED) [89]: El documento contiene los resultados de un análisis realizado por Savannah River Site para estimar valores de probabilidad de ocurrencia de fallo humano en instalaciones nucleares no relacionadas con un reactor.
- EEG-74: *Probability of failure of the TRUDOCK crane system at the Waste Isolation Pilot Plant (WIPP)* [90]: Contiene los valores de la base de datos THERP utilizados en el análisis de fiabilidad humana de la grúa TRUDOCK de la WIPP.

Las tres bases de datos contienen probabilidades nominales, o genéricas, de fallo humano al realizar acciones específicas. Se ha consultado la base de datos THERP porque contiene una gran cantidad de valores de probabilidad de fallo humano. No obstante, se han de realizar las hipótesis oportunas para relacionar las acciones descritas en la base de datos THERP con las UAs elementales del contexto ATI. Por ejemplo, el fallo a apretar un perno en el contexto ATI se asocia con la siguiente acción de la tabla 20-12 de la base de datos de THERP: *Improperly mate a connector, including failure to test the locking feature for engagement*. Se ha utilizado el SHED porque contiene valores de probabilidad de fallo humano de contextos no relacionados con el reactor, como es el del ATI. El documento EEG-74 se tiene en consideración porque supone un ejemplo de aplicación de valores de la base de datos THERP en el análisis del uso de una grúa.

Se ha seleccionado, de una de estas tres bases de datos, el valor genérico de probabilidad de ocurrencia de fallo humano que mejor se ajusta a las acciones no seguras elementales identificadas en el caso de estudio. La tabla 8.9 relaciona las acciones no seguras identificadas con el valor medio de probabilidad de ocurrencia[27] seleccionado para cada una de ellas. Se explícita también la base de datos de la que se ha extraído el valor de probabilidad de ocurrencia.

[27] Al negligirse el fallo cognitivo, la probabilidad de fallo manual es directamente la probabilidad de ocurrencia de una UA.

Acción no segura	Probabilidad media de ocurrencia	Fuente
Omisión del uso de procedimientos	5,0E-03	SHED
Fallo al seleccionar la localización objetivo en el plan de movimientos	1,62E-02	SHED
Fallo al seleccionar la localización objetivo en el que colocar el elemento de combustible	3,75E-03	THERP tabla 20-9 ítem 4
Omisión de la revisión	1,25E-03	THERP tabla 20-7 ítem 1
Omisión de la revisión sin usar procedimientos	8,07E-02	THERP tabla 20-7 ítem 5
Ejecución incorrecta de la revisión	8,07E-02	THERP tabla 20-22 ítem 3
Fallo a posicionar la grúa polar sobre la localización objetivo de la piscina	3,75E-03	THERP tabla 20-9 ítem 4
Error de comunicación	1,25E-03	THERP tabla 20-8 ítem 1c
El operador de grúa falla a parar el movimiento a tiempo	6,25E-03	THERP tabla 20-12 ítem 11
Fallo a anclar	3,75E-03	THERP tabla 20-12 ítem 13 (utilizado en EEG-74)
Fallo a advertir un sonido chirriante	1,0E-02	SHED
El operador de grúa falla a para el movimiento	3,75E-03	THERP tabla 20-12 ítem 10
Revisión de supervisión (recuperación)	1,6E-01	SHED
Medida de radiación	1,0E-03	THERP tabla 20-3 ítem 4

Tabla 8.9: Valores de probabilidad de fallo manual seleccionados para las UAs identificadas

La selección de los valores de probabilidad presentados en la tabla 8.9 se justifica en el anexo L.

Ajuste de valores genéricos mediante PSFs El ajuste de los valores genéricos de probabilidad de ocurrencia de las UAs al contexto de estudio se realiza mediante la ecuación L.6, ya presentada en la sección 8.2.3.3, extraída del método SPAR-H. El PSF_{comp}presente en la ecuación es el producto de los multiplicadores de los PSFs, cuyo análisis se ha presentado ya en la sección 8.3.6.

$$HEP = \frac{NHEP * PSF_{comp}}{NHEP * (PSF_{comp} - 1) + 1} \tag{8.6}$$

A modo de ejemplo se presenta la cuantificación de las UAs del evento HFE5.2 en el contexto nominal. La tabla 8.10 presenta la NHEP de las UAs de HFE5.2, los multiplicadores de los PSFs, el PSF_{comp}, y el valor ajustado de probabilidad de ocurrencia de cada UA.

		PSFs							
UA	NHEP[28]	AT	S	C	P	EH	F	PSF_{comp}	HEP
L	1,25E-03	1	2	1	1	1	5	10	1,24E-02
Q	3,75E-03	1	1	1	1	0,5	1	0,5	1,88E-03
R	6,25E-03	10	1	1	1	0,5	1	5	3,05E-02

Tabla 8.10: Cuantificación de las UAs de HFE5.2 en el contexto nominal.

8.3.9.2. Cuantificación de la probabilidad de ocurrencia de HFE

Tal y como se ha visto en la sección 8.2.3.4, la probabilidad de ocurrencia de un HFE se estima a partir de la suma de las probabilidades de ocurrencia de los caminos de fallo presentes en los DHFET. A su vez, la probabilidad de ocurrencia de un camino de fallo es el producto de la probabilidad de ocurrencia de las acciones no seguras encadenadas en el camino de fallo (véase las ecuaciones L.3 y L.4, y las figuras 8.7 y 8.9). A modo de ejemplo, la tabla 8.11 presenta la probabilidad de ocurrencia de los dos caminos de fallo del evento HFE5.2 en todos los contextos estudiados, así como la probabilidad de ocurrencia del HFE en dichos contextos. El resto de los resultados generados en la cuantificación se presenta en el anexo L.

Camino de fallo	Nominal	EFC1	EFC2	EFC3	EFC4
F1	2,32E-05	4,63E-05	2,32E-05	2,91E-05	2,03E-04
F2	5,65E-05	1,13E-04	5,65E-05	3,39E-04	4,66E-04
HEP del HFE	7,98E-05	1,59E-04	7,98E-05	3,68E-04	6,69E-04

Tabla 8.11: Probabilidad de ocurrencia del evento de fallo humano HFE5.2

En ATHEANA, además, se cuantifica la llamada probabilidad global de fallo humano como la suma de las probabilidades de fallo humano de cada contexto ponderada por la probabilidad de ocurrencia de cada contexto (véase la ecuación 8.7). Sin embargo, se ha decido no cuantificar la probabilidad global de fallo humano de los HFE porque el modelo APS en el que se han de introducir los resultados del análisis, el modelo APS de la fase I, no contempla la existencia de otros contextos que no sean el nominal.

$$HEP(HFE)_{global} = \sum_{i}^{n} p(EFC_i) * HEP(HFE)_i \tag{8.7}$$

8.4. Resultados del análisis de fiabilidad humana

La tabla 8.12 presenta los resultados del análisis del fiabilidad humana, es decir, las probabilidades de ocurrencia de los eventos de fallo humano identificados en el contexto ATI. Las probabilidades de ocurrencia estimadas se han de entender como la probabilidad de que ocurra el HFE en un movimiento de elemento de combustible, en el caso de los eventos HFE1.1 y HFE1.2, o la probabilidad de que ocurra el HFE en el traslado de un contenedor. Solo los resultados del contexto nominal se introducen posteriormente en el modelo APS. En el contexto nominal, las probabilidades de ocurrencia de los eventos de fallo humano relacionados con la carga errónea del contenedor son sustancialmente bajas en comparación con el resto de resultados. Este hecho, unido a que en el modelo APS de la fase I no se ha creído necesario introducir ningún suceso iniciador relacionado con la carga errónea del contenedor porque sus consecuencias no serían relevantes, desaconseja su inclusión en el modelo APS porque los resultados obtenidos serían despreciables

en comparación. En consecuencia, los eventos de fallo humano HFE1.1 y HFE1.2 no se han trasladado al modelo APS.

Fase	HFE	Nominal	EFC1	EFC2	EFC3	EFC4
1	HFE1.1	6,81E-09	1,67E-05	6,81E-09	1,41E-06	2,15E-14
	HFE1.2	4,03E-09	1,14E-05	4,03E-09	8,41E-07	1,82E-14
2	HFE2.1	6,89E-05	3,36E-04	6,89E-05	3,58E-05	1,00E-08
3	HFE3.1	5,28E-06	1,05E-05	5,28E-06	9,53E-06	4,71E-05
5	HFE5.1	1,18E-05	8,95E-05	1,18E-05	2,72E-05	1,03E-09
	HFE5.2	7,98E-05	1,59E-04	7,98E-05	3,68E-04	6,69E-04
6	HFE6.1	4,55E-04	6,94E-03	1,39E-01	1,50E-03	6,20E-03

Tabla 8.12: Probabilidad de ocurrencia de los eventos de fallo humano del contexto ATI en el contexto nominal y en los EFC.

El evento de fallo humano más probable en el contexto nominal es el HFE6.1, «Caída del contenedor MPC en el interior del HI-STORM a causa de un anclaje defectuoso». La probabilidad de ocurrencia del HFE6.1, y la de los eventos HFE2.1 y HFE5.1, es decir, la probabilidad de los HFE cuya ocurrencia causaría la caída del contenedor, se compara con datos provenientes de la experiencia operativa de la industria americana. La comparación permite valorar con cierto grado de confianza si los resultados obtenidos son coherentes porque la principal causa de caída de cargas en la industria americana es el fallo humano [8]. Los datos de experiencia operativa utilizados se hallan en el NUREG-0612 [75] y en el NUREG-1774 [76]. Dichos datos hacen referencia al izado de cargas pesadas con grúas de diferentes diseños[29]. La figura 8.10 compara los datos presentes en los NUREGs con los resultados obtenidos. La probabilidad de caída de una carga pesada estimada en el NUREG-1774 es de 5,6E-05, mientras que la probabilidad de caída estimada en el NUREG-0612 se halla en el rango de valores entre 1,0E-05 y 1,5E-04.

Las HEPs de los eventos HFE2.1, HFE5.1, y HFE6.1 son del orden de magnitud de los valores estimados mediante la experiencia operativa de la industria americana. Por lo tanto, los resultados son coherentes con lo que ha ocurrido en el manejo de otro tipo de cargas pesadas con otros tipos de grúas. Esta conclusión permite valorar de forma positiva el nuevo procedimiento de cuantificación y su integración en ATHEANA, y proporciona razones para seguir desarrollando y aplicando la metodología utilizada. No obstante, dicha conclusión no es una validación definitiva del método por dos motivos: porque los resultados obtenidos son orientativos debido a la naturaleza piloto del análisis, y porque los datos de experiencia operativa provienen de contextos diferentes al analizado en el HRA.

8.5. Introducción de los resultados del análisis de fiabilidad humana en el APS. Modelización del sistema grúa

8.5.1. Introducción

Los resultados obtenidos en el análisis de fiabilidad humana del contexto ATI se introducen en el modelo fase I del APS de nivel 2 de ATI, presentado en el capítulo 7, para valorar el impacto de la actuación humana en el riesgo. El único de los tres modelos APS generados en la fase I que se ve afectado por la introducción de los eventos HFE es el de la etapa de carga pues el análisis HRA se ha limitado a las operaciones realizadas en dicha etapa.

[29] Mientras que la grúa de la central cumple con el criterio de fallo simple, las grúas presentes en los NUREGs no tienen porqué cumplir con dicho criterio. Una grúa que cumpla con el criterio de fallo simple es más fiable, es decir, su probabilidad de fallo será menor, que una que no cumpla con el criterio.

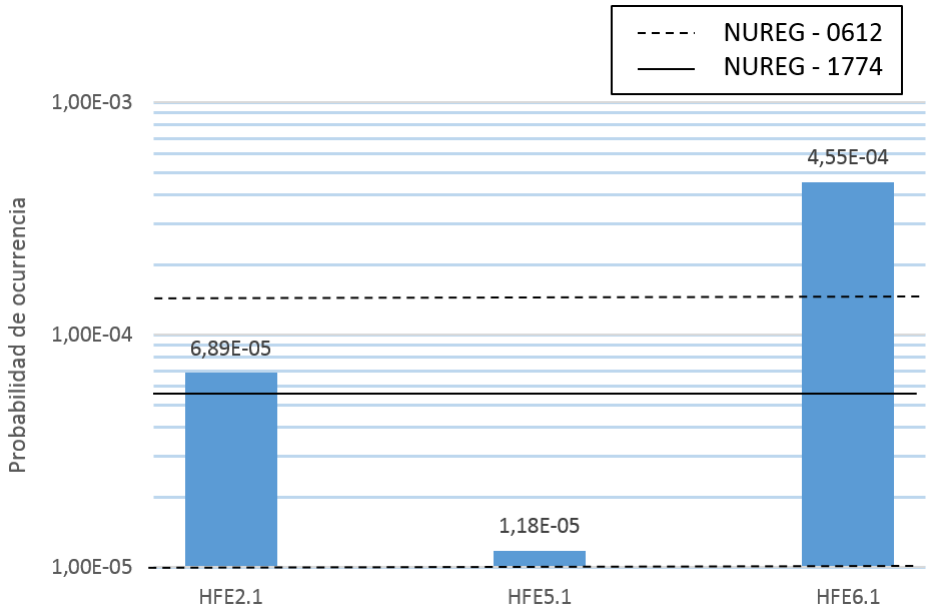


Figura 8.10: Comparación entre HEPs y valores de experiencia operativa.

A diferencia de los típicos HFE introducidos en un APS de reactor, los eventos de fallo humano identificados en el HRA del ATI son todos de tipo 2. Los eventos de fallo humano de tipo 2 son sucesos que causan, directa o indirectamente, la ocurrencia de un suceso iniciador. Los típicos HFE introducidos en un APS de sucesos internos a Potencia son tipo 3, tipo 4, o tipo 5, que hacen referencia a acciones de los procedimientos de emergencia, acciones de recuperación, y acciones de mitigación, respectivamente. Teniendo en cuenta su significado, los HFE típicos de un APS de reactor se introducen en los árboles de fallo de los cabeceros de los árboles de eventos del APS. En cambio, teniendo en cuenta su significado, los sucesos de fallo humano de tipo 2 se han de relacionar con la frecuencia de ocurrencia de los sucesos iniciadores introducidos en el modelo APS.

En el modelo APS de la fase I, los sucesos iniciadores se han modelado mediante un suceso básico asociado a una frecuencia de ocurrencia proveniente de datos de experiencia operativa de la industria. Dicha modelización no es compatible con la introducción de eventos HFE pues los datos de la industria ya cubren la componente humana. Si se introdujesen las probabilidades de fallo humano en paralelo[30] al modelo de frecuencia de los sucesos iniciadores, la componente humana se valoraría dos veces. En consecuencia, se han de cambiar los modelos de frecuencia de los sucesos iniciadores para poder introducir los sucesos de fallo humano en el modelo. Además de la componente humana, los nuevos modelos de frecuencia de los sucesos iniciadores también han de tener en cuenta la otra posible causa de caída del contenedor: el fallo, o la combinación de fallos, de algunos componentes de la grúa. Se hace necesario, por lo tanto, utilizar árboles de fallo para modelar la frecuencia de ocurrencia de los sucesos iniciadores. Las secciones a continuación presentan el desarrollo de los nuevos modelos de frecuencia de los sucesos iniciadores, así como los resultados obtenidos mediante dichos modelos.

8.5.2. Relación entre los sucesos iniciadores de la Fase I y los HFEs

Los HFE identificados son el resultado de la realización de un análisis de fiabilidad humana que ha generado, y se basa en, una gran cantidad de información al respecto de las operaciones de ATI que era

[30] Mediante un árbol de fallos con una puerta OR.

desconocida en el desarrollo del modelo APS de la fase I. Por lo tanto, los propios HFEs son una buena base de partida para la identificación, descripción, y cuantificación de los nuevos modelos de los sucesos iniciadores. Además, se introduce la división en fases de la etapa de carga presentada en el análisis del contexto del HRA, sección 8.3.3.5, en la descripción de los nuevos sucesos iniciadores para definir con precisión dónde y cuándo ocurren los sucesos postulados.

Pese a no contar con toda la información utilizada en la fase II, el modelo APS de fase I incluye ya diferentes situaciones en las que puede ocurrir la caída del contenedor y las posibles alturas de caída del contenedor, conjuntamente con las probabilidades de rotura[31] de las barreras de confinamiento asociadas. Por lo tanto, para no realizar cambios insustanciales en el modelo y ahorrar recursos, se hallan las relaciones entre los sucesos iniciadores anteriores y los HFE con el objetivo de sustituir en el modelo APS los antiguos sucesos iniciadores con los que se generen a partir de los HFE. Un Suceso Iniciador antiguo y un HFE están relacionados si describen una situación similar. La tabla 8.13 presenta la relación entre sucesos iniciadores antiguos y HFEs.

SI antiguo	Descripción del SI	HFEs relacionados	Descripción del HFE
Caída1	Caída de 0,5 metros del HI-TRAC (solo es posible en la fase 3)	Ninguno	No hay ningún HFE que describa la caída del contenedor desde la altura nominal de transporte en fase 3
Caída2	Caída de 8 metros por *two-blocking* (solo es posible en las fases 3 y 5)	HFE3.1 y HFE5.2	Eventos de fallo humano que podrían ser la causa de un suceso de *two-blocking* en las fases 3 y 5, respectivamente.
Caída3	Caída de 5,9 metros del HI-TRAC (solo es posible en la fase 5)	HFE5.1	Caída del contenedor en la fase 5 provocada por un anclaje defectuoso del sistema de izado y el contenedor.
Caída4	Caída de 13 metros del contenedor HI-TRAC en el interior del pozo de cofres (solo es posible en la fase 2)	HFE2.1	Caída del contenedor en el pozo de cofres por un anclaje defectuoso del sistema de izado y el contenedor.
Caída5	Caída de 5,8 metros del MPC en el interior del HI-STORM (solo es posible en la fase 6)	HFE6.1	Caída del contenedor MPC en el interior del HI-STORM por anclaje defectuoso del primero al sistema de izado.
Volcado	Volcado del contenedor al ser izado	Ninguno	

Tabla 8.13: Relación entre sucesos iniciadores antiguos y HFEs.

8.5.3. Nuevos sucesos iniciadores

La tabla 8.14 describe los nuevos sucesos iniciadores, basados en los eventos de fallo humano identificados en el análisis de fiabilidad humana. En la tabla 8.14 se muestra también la relación entre los nuevos sucesos iniciadores y los antiguos, es decir, se explicita qué suceso iniciador nuevo reemplaza a qué suceso

[31] Calculadas mediante un análisis estructural. Véase la sección

iniciador antiguo. Finalmente, la tabla también incluye los HFE que han de estar presentes en los modelos de frecuencia de cada nuevo suceso iniciador.

Nuevo SI[32]	Descripción	Suceso Iniciador antiguo relacionado	HFEs incluidos
LDP2	Caída de 13 m del contenedor cuando éste se alza desde el pozo de cofres (fase 2). La caída puede ser causada por el evento HFE2.1 o, independientemente, por el fallo de componentes de la grúa.	Caída4	HFE2.1
LDP3	Caída de 0,5 m, altura de traslado, del contenedor en la fase 3. El fallo de componentes de grúa es la única causa posible de este SI.	Caída1	Ninguno
TBP3	Caída del contenedor desde 8 m de altura debida a *two-blocking*. El *two-blocking* es causado por la combinación del suceso HFE3.1 y el fallo de los componentes de seguridad de la grúa.	Caída2	HFE3.1
LDP5	Caída del contenedor desde 5,9 m de altura. La caída puede ser causada por el evento HFE5.1 o, independientemente, por el fallo de componentes de la grúa.	Caída3	HFE5.1
TBP5	Caída del contenedor desde 8 m de altura debida a *two-blocking*. El *two-blocking* es causado por la combinación del suceso HFE5.2 y el fallo de los componentes de seguridad de la grúa.	Caída2	HFE5.2
LDP6	Caída del contenedor MPC en el interior del HI-STORM. El contenedor recorre 5,8 m antes de chocar con la base del HI-STORM. La caída puede ser causada por el evento HFE6.1 o, independientemente, por el fallo de componentes de la grúa.	Caída5	HFE6.1
Tip-over	El contenedor vuelca al ser alzado.	Volcado	Ninguno

Tabla 8.14: Nuevos sucesos iniciadores. Relación con los antiguos sucesos y con los HFE.

La relación directa entre los nuevos sucesos iniciadores identificados y los antiguos sucesos iniciadores de la fase I permite que los primeros sustituyan a los últimos en el modelo APS. El único cambio realizado es que el árbol de eventos del suceso Caída2 se ha duplicado para asignarlo a los nuevos sucesos iniciadores TBP3 y TBP5. Gracias a sustituir los antiguos sucesos iniciadores con los nuevos no es necesario rehacer los análisis estructural y termohidráulico.

8.5.4. Árboles de fallo humano de los nuevos sucesos iniciadores. Modelo de fallo de la grúa

Tal y como se muestra en la tabla 8.14, el factor humano no es el único contribuyente a la frecuencia de ocurrencia de los sucesos iniciadores. De hecho, el fallo de componentes de grúa, independientemente de la actuación humana, puede causar la caída de un contenedor. Además, la ocurrencia de los sucesos iniciadores TBP3 y TBP5 solo es posible si fallan componentes de seguridad de la grúa al mismo tiempo que se produce el fallo humano descrito en los eventos HFE3.1 y HFE5.2, respectivamente. Por lo tanto, los posibles modos de fallo de la grúa puente del edificio de combustible se incluyen en el modelo de cálculo de la frecuencia de los sucesos iniciadores para que ésta sea representativo de toda la casuística.

Las frecuencias de ocurrencia de los sucesos iniciadores se obtienen mediante árboles de fallo para poder incluir en una misma estructura el fallo humano y el fallo de la grúa. Las estructuras simples de los árboles de fallo de los sucesos iniciadores están formadas, por un lado, por un suceso básico que incluye la probabilidad de fallo humana asociada al suceso iniciador y, por otro lado, por un suceso triángulo[33] que representa la probabilidad de fallo de la grúa puente. Si el suceso iniciador modelizado es un caso de caída, el fallo humano y el fallo de la grúa se relacionan mediante una puerta OR. En cambio, si el suceso iniciador modelizado es un caso de *two-blocking*, el fallo humano y el fallo de la grúa se relacionan mediante una puerta AND, que implica que ambos han de ocurrir simultáneamente para que se produzca el suceso iniciador. La figura 8.11 muestra las estructuras simples de los árboles de fallo de los sucesos iniciadores.

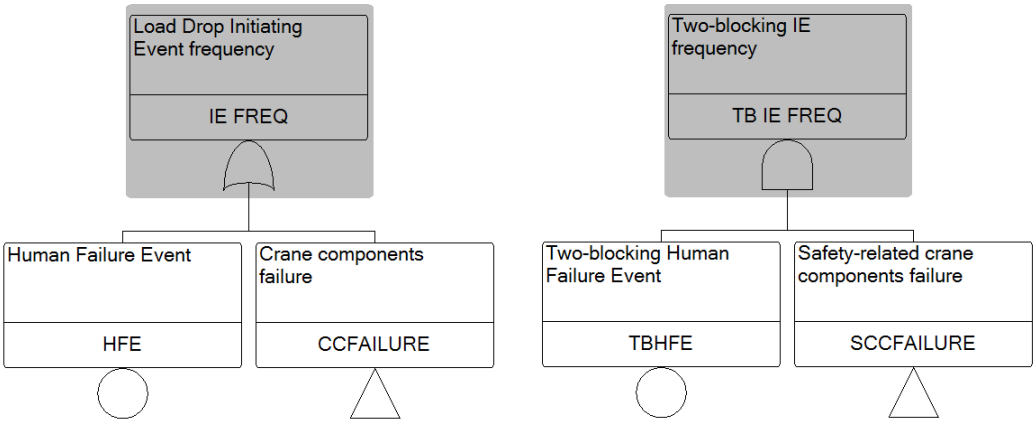


Figura 8.11: Estructuras simples de los árboles de fallo.

La documentación disponible al respecto del diseño de la grúa puente del edificio de combustible describe, principalmente, los dispositivos de seguridad incluidos en la grúa y los procedimientos de actuación de la misma. Sin embargo, la documentación no dispone de datos de todos los componentes y dispositivos que forman la grúa. En consecuencia, se utilizan datos externos para desarrollar y completar los árboles de fallo del puente grúa del edificio de combustible[34]. El documento *Probabilistic Risk Assessment (PRA) of Bolted Storage Casks: Updated Quantification and Analysis Report* [2] de EPRI contiene un árbol de fallos de una grúa puente que cumple con el criterio de fallo simple y con las guías de diseño estipuladas en el NUREG-0554 [77] y el NUREG-0612 [75]. Dicho árbol de fallos se ha utilizado como referencia para desarrollar los árboles de fallo del sistema grúa. Concretamente, al árbol de fallos de EPRI se le añaden, o se sustituyen sucesos básicos con, los diferentes dispositivos de seguridad de la grúa puente del caso de

[33] En Riskspectrum, un suceso triángulo, o de transferencia, conecta con el *top event* de un árbol de fallos desarrollado. Los sucesos triángulo se utilizan para minimizar el tamaño de los árboles de fallo.

[34] Estos árboles de fallo son con los que conectan los sucesos triángulo de las estructuras simples.

estudio. Los sucesos básicos que hacen referencia al fallo de componentes estructurales de la grúa quedan intactos. La estructura detallada de los árboles de fallo de los sucesos iniciadores se presenta en el anexo N.

El árbol de fallos de la grúa puente para sucesos *two-blocking* es diferente al del resto de caídas porque enfatiza, sobre todo, el fallo o indisponibilidad de componentes de seguridad de la grúa como, por ejemplo, los dispositivos de final de carrera. Estos dispositivos no se incluyen en el árbol de fallos del resto de caídas porque su indisponibilidad o fallo no puede causar ni directa ni indirectamente la caída del contenedor. En cambio, en conjunción con los eventos HFE3.1 y HFE5.2, el fallo de un dispositivo final de carrera podría causar que el contenedor se alzase hasta chocar con el dispositivo de izado.

Los datos de partida de la probabilidad de ocurrencia de los sucesos básicos incluidos en los árboles de fallo de la grúa puente se obtienen del documento [2]. Al no disponer de datos de indisponibilidad o fallo de la grúa puente del caso de estudio no se puede aplicar el ajuste bayesiano a los datos de partida. En consecuencia, la probabilidad de ocurrencia o la indisponibilidad de los sucesos básicos[35] incluidos en los árboles de fallo del caso de estudio proviene directamente de los datos de partida documentados. De manera similar a la probabilidad de ocurrencia de los HFEs, la referencia de las probabilidades de los sucesos básicos es el alzamiento del contenedor. Teniendo en cuenta que un contenedor MPC se carga y se traslada una única vez al año, cada uno de los alzamientos a los que se somete ocurren también una única vez al año. Como los sucesos iniciadores describen situaciones en las que el contenedor se alza una única vez, el resultado de cuantificar los árboles de fallo de los sucesos iniciadores es la frecuencia de ocurrencia[36] del suceso iniciador por año y por contenedor.

8.5.5. Frecuencia de ocurrencia de los nuevos sucesos iniciadores

La tabla 8.15 presenta la frecuencia de ocurrencia de los nuevos sucesos iniciadores. La cuantificación de estas frecuencias se ha realizado en *Riskspectrum® PSA* mediante *Fault Tree Analysis*. Se ha establecido un límite de truncamiento de 1,0E-20 para asegurar que todas las frecuencias de ocurrencia tengan resultado.

Suceso Iniciador	Frecuencia [(año·contenedor)$^{-1}$]
LDP2	7,42E-05
LDP3	5,28E-06
LDP5	1,71E-05
LDP6	4,60E-04
TBP3	5,39E-11
TBP5	8,14E-10
Tip-over	5,6E-05

Tabla 8.15: Frecuencia de ocurrencia de los nuevos sucesos iniciadores.

La frecuencia de ocurrencia de todos los sucesos iniciadores en el modelo APS de la fase I era de 5,6E-05 (año·contenedor)$^{-1}$. Se observa, a simple vista, que la introducción del análisis de fiabilidad humana y del sistema grúa en el modelo APS provoca sustanciales diferencias con respecto al valor de frecuencia de la fase I. La comparación detallada entre los resultados de la fase I y la fase II se presenta en la sección 8.7. Cabe destacar que los sucesos iniciadores TBP3 y TBP5 serían eliminados del análisis si se aplicasen los criterios de cribado de sucesos iniciadores de un APS de sucesos internos[37].

[35] Las probabilidades asociadas a los sucesos básicos de los árboles de fallo de grúa se puede consultar en el anexo M.

[36] Cabe recordar que, al tratarse de sucesos iniciadores de la etapa de carga, la frecuencia de estos sucesos iniciadores solo esta vigente durante el primer año de vida de un contenedor.

[37] En un APS de sucesos internos se criban los sucesos iniciadores cuya frecuencia de ocurrencia es inferior a 1,0E-06 año^{-1}.

8.6. Resultados del APS incluyendo el análisis de fiabilidad humana y la modelización del sistema grúa

Esta sección presenta la tarea de análisis e interpretación de los resultados obtenidos mediante el modelo APS fase II, es decir, la frecuencia de liberación de radionúclidos y el término fuente de los nuevos sucesos iniciadores. De los tres modelos que forman el APS de fase I, en la fase II se ha modificado únicamente el de la etapa de carga. Por lo tanto, se presentan solo los resultados asociados a dicha etapa. Se presenta también en esta sección el análisis de importancia (véase anexo Ñ) de la frecuencia de liberación de radionúclidos asociado al APS. La comparación de los resultados obtenidos con los del APS de sucesos internos a Potencia de nivel 2 de la central nuclear se reserva para la sección 8.7.

8.6.1. Interpretación de resultados

La tabla 8.16 presenta los resultados obtenidos en el modelo APS fase II para cada nuevo suceso iniciador. La tabla contiene la frecuencia de liberación de radionúclidos, la cantidad de CMFs, el estado final, y el término fuente. El estado final y el término fuente son iguales a los del modelo APS en fase I puesto que no se ha cambiado su parte del modelo. El límite de truncamiento utilizado en la cuantificación de la frecuencia de liberación de radionúclidos es de 1,0E-09 para el suceso LDP6[38], y de 1,0E-20 para el resto.

Suceso Iniciador	FLR [(año·contenedor)$^{-1}$]	# CMFs	Estado final	Término fuente [Bq]
LDP2	7,58E-11	439	Alto	1,31E+15
LDP3	4,75E-15	690	Muy bajo	5,31E+11
LDP5	8,73E-13	688	Muy bajo	5,31E+11
LDP6	2,90E-07	204	Alto	1,31E+15
TBP3	8,33E-18	65	Muy bajo	5,31E+11
TBP5	1,26E-16	97	Muy bajo	5,31E+11
Tip-over	5,05E-14	11	Muy bajo	5,31E+11

Tabla 8.16: Resultados obtenidos para la etapa de carga en la fase II del modelo APS.

Las FLRs de los sucesos iniciadores presentadas en la tabla 8.16 no son valores puntuales, al contrario, ya han sido calculadas en base anual al trasladar previamente las probabilidades en demanda de los sucesos iniciadores a frecuencias anuales de ocurrencia. Al igual que en el modelo APS de la fase I, los resultados remarcan la existencia de un sucesoiniciador predominante. El suceso predominante es LDP6, que representa la caída del contenedor MPC en el interior del HI-STORM con un recorrido de 5,8 m. Este suceso es homólogo a Caída5, el suceso iniciador predominante en la fase I. La FLR del resto de sucesos iniciadores es sustancialmente inferior a la del suceso LDP6. De hecho, si se aplicase el criterio de cribado utilizado en APS de sucesos internos de nivel 1 y 2[39], todos estos sucesos iniciadores serían eliminados del análisis. Tomando en consideración que los resultados de las etapas de transferencia y almacenamiento no han cambiado, la FLR del primer año, dominada por el suceso LDP6, es cuatro órdenes de magnitud superior que la de los años venideros[40]. En consecuencia, el suceso más importante en términos de riesgo del APS de fase II es el suceso iniciador LDP6.

[38] Se ha escogido un límite de truncamiento de 1,0E-09 porque con límites inferiores se obtenían una gran cantidad de CMFs que no aportaban ningún valor a la FLR.

[39] En un APS de sucesos internos de nivel 1 y/o 2 se utiliza un límite de truncamiento para la frecuencia de daño al núcleo de 1,0E-09. Cualquier suceso cuya FDN sea menor que el límite de truncamiento es cribado del análisis.

[40] La FLR de años venideros es de 6,88E-11 (año·contenedor)$^{-1}$.

8.6.2. Análisis de importancia

El análisis de importancia aplicado a los resultados del APS de ATI se puede consultar, en su totalidad, en el anexo Ñ. A la vista de la predominancia del suceso iniciador LDP6, en esta memoria de tesis se presenta únicamente el análisis de importancia que se ha aplicado a la FLR de dicho suceso. La principal motivación para volver a realizar los análisis de importancia es estudiar el impacto de la introducción del fallo humano y el fallo de la grúa en las ecuaciones booleanas del modelo. Se espera que el impacto del fallo humano y el fallo de grúa se significativo pues las FLRs de los sucesos iniciadores han sufrido cambios significativos. La tabla 8.17 muestra los sucesos básicos con mayor valor de la figura de importancia Fussell-Vesely para el caso estudiado.

Suceso básico	Indisponibilidad o probabilidad de fallo	Fussell-Vesely
HFE6.1	4,55E-04	9,89E-01
CMANT1A	1,16E-02	2,18E-01
CMANT3A	1,16E-02	2,18E-01
CMANT2A	1,16E-02	2,18E-01
CMANT2B	1,16E-02	2,18E-01
CMANT1B	1,16E-02	2,18E-01

Tabla 8.17: Sucesos básicos más importantes según la figura de Fussell-Vesely (Fase II).

Se observa que el suceso básico de HRA, HFE6.1, se coloca como el suceso más importante según la figura Fussell-Vesely. A continuación, los sucesos más importantes continúan siendo los relacionados con la indisponibilidad de las compuertas de los sistemas de extracción y suministro de aire. El suceso más importante relacionado con el fallo de grúa representa el fallo o indisponibilidad de todos los cables de la grúa por una causa común y tiene un Fussell-Vesely de 4,35E-03. Por lo tanto, en el caso del suceso iniciador LDP6, que es el predominante, el impacto de la inclusión del suceso HRA es significativo, mientras que la introducción del fallo de grúa no es especialmente relevante. No obstante, en el caso de los sucesos iniciadores de *two-blocking* está conclusión es diferente pues los sucesos de fallo de grúa también son importantes. En consecuencia, los resultados del análisis de importancia de LDP6 no son motivo para menospreciar la contribución del fallo del sistema grúa.

8.7. Comparación de resultados entre FASE I y FASE II del modelo APS

Los resultados del modelo APS de ATI de la fase I y de la fase II se comparan entre sí para evaluar el impacto de introducir el fallo humano y el fallo de la grúa en el APS. De los tres modelos que forman el APS de fase I, en la fase II se ha modificado únicamente el de la etapa de carga. Por lo tanto, solo se comparan los resultados asociados a dicha etapa.

La única tarea de la metodología APS de ATI que se ve afectada por la introducción del fallo humano y el fallo de la grúa puente en el modelo es el tratamiento de sucesos iniciadores. Consecuentemente, la comparación de resultados se centra en la frecuencia de sucesos iniciadores y en la frecuencia de liberación de radionúclidos asociada a cada suceso iniciador. Aspectos como el estado final de las secuencias de accidente y el término fuente permanecen intactos.

8.7.1. Frecuencias de sucesos iniciadores y FLR de sucesos iniciadores

La tabla 8.18 presenta la frecuencia de ocurrencia y la FLR de sucesos iniciadores de la fase I y la fase II. Cada fila contiene los resultados de un suceso de la fase I y de un suceso de la fase II que representan la misma situación. Consecuentemente, cada fila es una comparación entre fase I y fase II. La tabla no contiene el suceso iniciador de volcado porque es el único que no se ha tratado de manera diferente. Visualmente, la comparación entre los resultados de la fase I y los de la fase II se puede apreciar en la figura 8.12.

SI Fase I	Frecuencia [(año·c)$^{-1}$]	FLR [(año·c)$^{-1}$]	SI Fase II	Frecuencia [(año·c)$^{-1}$]	FLR [(año·c)$^{-1}$]
Caída1	5,60E-05	2,03E-14	LDP3	5,28E-06	4,75E-15
Caída3	5,60E-05	1,18E-12	LDP5	1,71E-05	8,73E-13
Caída4	5,60E-05	2,38E-11	LDP2	7,42E-05	7,58E-11
Caída5	5,60E-05	1,47E-08	LDP6	4,60E-04	2,90E-07
Caída2	5,60E-05	3,59E-12	TBP3	5,39E-11	8,33E-18
Caída2	5,60E-05	3,59E-12	TBP5	8,14E-10	1,26E-16

Tabla 8.18: Comparación entre los resultados de la fase I y la fase II del modelo APS.

La comparación entre el suceso Caída1 y el suceso LDP3, que no incluye ningún evento de fallo humano, pone de manifiesto la diferencia entre el valor de frecuencia de caída del contenedor proveniente de la experiencia operativa y el valor de frecuencia de caída por fallo de la grúa que proviene del árbol de fallos. Concretamente, la frecuencia de LDP3 es un orden de magnitud menor que la frecuencia proveniente de la experiencia operativa utilizada en la fase I del modelo. Este resultado es coherente con lo esperado puesto que las grúas que cumplen con el criterio de fallo simple son las más fiables [41], y el valor de experiencia operativa contiene cierta componente de fallo humano. Conocer la diferencia entre las frecuencias de Caída1 y LDP3 permite aislar y valorar la implicación de los eventos de fiabilidad humana en el resto de sucesos iniciadores no relacionados con *two-blocking*. Específicamente, la diferencia entre Caída 1 y LDP3 permite concluir que cualquier incremento de frecuencia de un suceso de la fase II respecto a su homólogo de la fase I, no relacionados con *two-blocking*, es causado por la introducción del fallo humano.

El incremento de la FLR LDP6 respecto a la de Caída5 es el que más destaca en la comparación entre sucesos iniciadores no relacionados con *two-blocking*. El incremento es de aproximadamente un orden de magnitud. El evento de fallo humano que provoca dicho incremento es el HFE6.1, es decir, la caída del MPC en el interior del HI-STORM 100. Las frecuencias de ocurrencia y las FLR de LDP2 y LDP5 son prácticamente iguales a las de sus sucesos homólogos de la fase I. En ambos casos, la introducción del fallo humano no tiene un impacto significativo en el riesgo.

Favorablemente, la FLR de ambos sucesos de *two-blocking*, TBP3 y TBP5, es entre cuatro y seis órdenes de magnitud más baja que la de su homólogo en la fase I, Caída2. La imposición, mediante el árbol de fallos, de que los dispositivos de seguridad de la grúa han de fallar a la vez que se produce el fallo humano es clave en la drástica reducción de la frecuencia de ambos sucesos. Aunque, en general, la introducción del fallo humano y el fallo de la grúa en el modelo APS incrementa el riesgo inherente al ATI a causa del suceso LDP6, en términos absolutos, el mayor impacto que recibe el modelo es la disminución del riesgo de los sucesos de *two-blocking*. Sin embargo, el riesgo del suceso *two-blocking* de la fase I ya era sustancialmente bajo, así que la obtención de valores aún más bajos en la fase II no tiene ninguna implicación en las conclusiones extraídas del APS.

En cuanto a la comparación con los resultados del APS de sucesos internos a Potencia de nivel 2 de la central nuclear, ésta se ciñe a valorar si el incremento de la FLR del suceso LDP6 en un orden de magnitud

[41] Los datos de experiencia operativa de los que proviene la frecuencia utilizada en la fase I aglutinan información de todo tipo de grúas.

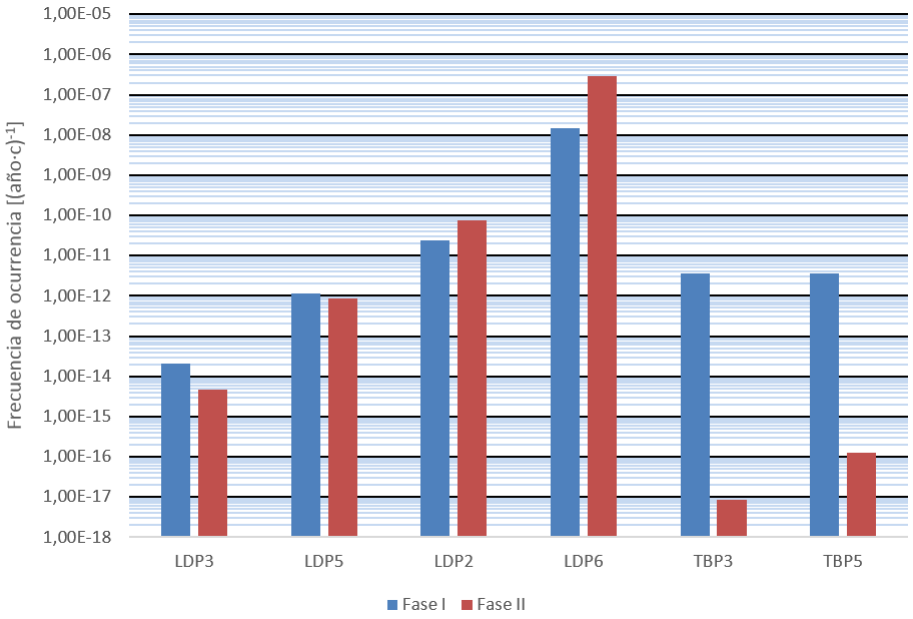


Figura 8.12: Comparación entre FLRs de la fase I y de la fase II.

es suficiente como para modificar las conclusiones extraídas en la fase I. A modo de recordatorio, la mayor frecuencia de liberación del APS de sucesos internos a Potencia de nivel 2 de la central, asociada a la categoría de liberación R9, es de 1,72E-05 año^{-1}. Siguiendo el ejemplo de la comparación realizada en la fase I[42], se obtiene un valor máximo de la FLR del suceso LDP6 es 1,45E-06 año^{-1}. Este valor sigue siendo un orden de magnitud menor que el máximo valor de frecuencia de liberación del APS nivel 2 de la central, pero no desentona entre el resto frecuencias de liberación estimadas en el APS de sucesos internos a Potencia de nivel 2. Concretamente, la FLR máxima de LDP6 es mayor que la de cinco de las doce categorías de liberación presentes en el APS de sucesos internos a Potencia de nivel 2 de la central. Si el riesgo inherente al ATI se valorase únicamente a partir de la FLR se concluiría que el riesgo se debería tener en cuenta pues sería hasta cierto punto comparable con el de la central en cada año que se almacenasen cinco nuevos contenedores. Sin embargo, al tratarse de un APS sucesos internos a Potencia de nivel 2, el riesgo también se valora a partir de la consecuencia, es decir, el término fuente. En la fase I se ha concluido que el término fuente del ATI, en global, es sustancialmente menor que el de la central. En definitiva, la nueva FLR máxima del APS de ATI de la fase II es más baja que la de central, aunque comparable, y el término fuente sigue siendo sustancialmente menor que el de la central.

A la vista de la comparación realizada, y teniendo en cuenta el notable grado de conservadurismo inherente a los análisis estructural y termohidráulico, y al análisis de la fracción de liberación, del APS de ATI en fase II, se concluye que los resultados orientativos siguen siendo sustancialmente bajos, prácticamente despreciables en relación al término fuente, en comparación con el riesgo de la central en sí. En consecuencia, se mantiene la conclusión de que la contribución del riesgo del ATI al riesgo total del emplazamiento es prácticamente nula.

8.8. Conclusiones

La aplicación de las técnicas de análisis de fiabilidad humana al contexto del ATI se ha llevado a cabo mediante la metodología ATHEANA. No obstante, la aplicación de HRA ha requerido del desarrollo de un

[42] Se multiplica el valor de FLR por cinco porque se considera que en un año se cargaran, como máximo, cinco contenedores.

nuevo método de cuantificación para la metodología ATHEANA, ya que en el caso de estudio no es posible aplicar el juicio de expertos en el que ATHEANA basa su análisis cuantitativo del fallo humano. El nuevo método de cuantificación está basado en el análisis del contexto de estudio y en la descomposición de los eventos de fallo humano en unidades elementales y genéricas de fallo humano. La aplicación del análisis de fiabilidad humana al contexto de estudio se acota a la etapa de carga, y resulta en la identificación de siete eventos de fallo humano, dos relacionados con casos de carga errónea y, el resto, relacionados con diferentes caídas del contenedor. Los dos eventos de fallo humano relacionados con la carga errónea del contenedor han sido cribados, es decir, no se introducen en el APS, porque su probabilidad de ocurrencia es sustancialmente más baja que la del resto de HFEs. El evento de fallo humano más probable es el HFE6.1, Caída del contenedor MPC en el interior del HI-STORM 100 por fallo al anclar el dispositivo de izado. Su probabilidad de ocurrencia por alzamiento del contenedor es de 4,55E-04, ligeramente superior a la probabilidad de caída de cargas pesadas proveniente de la experiencia operativa de la industria americana [75, 76] utilizada en la fase I del APS. Casualmente, el HFE6.1 y el suceso inicador predominante en la fase I, Caída5, describen la misma situación, hecho que refuerza que este tipo de caída es el evento más significativo que puede ocurrir en el interior del edificio de combustible. En conclusión, los resultados obtenidos en el HRA no son para nada despreciables en comparación con datos extraídos de otras fuentes. Al contrario, se consideran resultados que aportan información valiosa puesto que se han obtenido a partir de un análisis detallado del objeto de estudio. No obstante, los resultados son orientativos puesto que, debido a la falta de detalle en la descripción de algunas tareas en la documentación disponible, se han tenido que tomar hipótesis conservadoras en la modelización de algunos eventos de fallo humano. Por ejemplo, en el caso del suceso HFE6.1 se considera que si los operadores fallan a anclar un perno ya se puede producir la caída del contenedor. Ésta es una hipótesis conservadora porque el dispositivo de izado se ancla mediante varios pernos, pero, al desconocerse el número exacto de los mismos, no se puede modelar con exactitud esta acción humana. En caso de creerse conveniente, el procedimiento de cuantificación podría mejorarse incluyendo un proceso para analizar las dependencias entre acciones no seguras, y un método para valorar la incertidumbre de los resultados.

La introducción de los resultados del análisis de fiabilidad humana en el modelo APS de ATI, conjuntamente con el fallo de grúa, ha requerido modificar únicamente el tratamiento de los sucesos iniciadores del modelo de la etapa de carga. En la fase II del modelo APS, la frecuencia de ocurrencia de sucesos iniciadores se ha modelado mediante árboles de fallo que incluyen tanto el fallo humano como el fallo de la grúa puente del edificio de combustible. En comparación con la fase I, en la fase II se postula un suceso iniciador más. Este nuevo suceso representa un caso de *two-blocking*. En términos cuantitativos, la incorporación de los resultados del análisis de fiabilidad humana en el modelo APS solo afecta a la frecuencia de ocurrencia de los sucesos iniciadores. Debido a su relación, la frecuencia de liberación de radionúclidos de cada suceso iniciador se ve afectada en las mismas proporciones que la frecuencia de ocurrencia del suceso iniciador asociado.

El impacto en los resultados cuantitativos de la FLR de la introducción del fallo humano y del fallo de la grúa en el modelo APS es significativo. Concretamente, en términos generales, la frecuencia de liberación de radionúclidos total aumenta un orden de magnitud debido a que la FLR del caso predominante, LDP6 en la fase II y Caída5 en la fase I, aumenta dicho orden de magnitud. Específicamente, la FLR del suceso LDP6 es 2,90E-07 (año·contenedor)$^{-1}$, mientras que la del suceso Caída5 de la fase I es 1,47E-08 (año·contenedor)$^{-1}$. En términos absolutos, el mayor impacto de la introducción del fallo humano y el fallo de grúa es la drástica reducción, de entre cuatro y seis órdenes de magnitud, de la FLR asociada a los sucesos de *two-blocking*. La causa principal de dicha reducción es la introducción de fallo de la grúa en paralelo con el fallo humano en los casos de *two-blocking*. Sin embargo, a pesar de su sobreestimación por utilizar un modelo no detallado, el riesgo del suceso *two-blocking* de la fase I ya era sustancialmente bajo, así que la obtención de valores aún más bajos en la fase II no tiene ninguna implicación en las conclusiones extraídas del APS. Teniendo en cuenta que el término fuente del suceso LDP6, que es el mismo que el de Caída5 de la fase I, sigue siendo sustancialmente más bajo que los calculados en el APS de sucesos internos a Potencia de nivel 2 de la central, el aumento de un orden de magnitud de la FLR tampoco supone un cambio de las conclusiones extraídas en la fase I. Por lo tanto, teniendo en cuenta el notable grado de

conservadurismo inherente al APS de ATI en fase II, se concluye que los resultados orientativos respecto al riesgo del ATI siguen siendo sustancialmente bajos, prácticamente despreciables en relación al término fuente, en comparación con el riesgo de la central en sí. En consecuencia, se mantiene la conclusión de que la contribución del riesgo del ATI al riesgo total del emplazamiento es prácticamente nula.

El modelo APS de ATI desarrollado mediante técnicas probabilistas sigue presentando en su fase II, en su cualidad de piloto, algunas carencias. Una vez introducido el fallo humano y el fallo de la grúa, las carencias que sigue presentando el modelo son: el hecho que los análisis estructural y termohidráulico se han llevado a cabo mediante la adaptación de resultados de estudios ajenos, y que la fracción de liberación estimada es un valor conservador derivado de un caso envolvente estudiado en un documento ajeno [5]. Pese a que estas carencias son significativas, el tratamiento de ambas tareas es conservador, por lo que una mejora en su ejecución proporcionaría resultados más realistas, pero, también, aún más alejados de los valores de riesgo de la central. No obstante, una vez introducido el fallo de la grúa, el modelo sería más detallado si se realizase el análisis de fiabilidad humana de las acciones de revisión y prueba de los componentes de la grúa y el sistema de izado[43]. Estas acciones serían consideradas como pre-iniciadoras[44], y sus probabilidades de ocurrencia se incluirían en los árboles de fallo de los sucesos iniciadores como posibles causas del fallo de los componentes del sistema grúa. El impacto en el riesgo de este tipo de acciones es una incógnita. A diferencia del fallo humano ya incluido en el APS fase II, es difícilmente justificable tanto que aumenten como que disminuyan el riesgo inherente al ATI. En consecuencia, se recomienda realizar, al menos, el análisis de fiabilidad humana de estas acciones de revisión y comparar los resultados con las probabilidades de ocurrencia de los fallos de grúa ya incluidos en los árboles de fallo[45]. La realización de este análisis es una recomendación directa producto del desarrollo del APS fase II y no está incluido en esta tesis doctoral.

[43] Es decir, las acciones que se realizan durante la etapa de preparación.

[44] Una acción pre-iniciadora es aquella en que el fallo humano hace que la ocurrencia de un suceso iniciador se más probable pero no causa directamente el suceso iniciador.

[45] Las probabilidades de fallo humano se colocarían en una puerta OR junto con las probabilidades de fallo, o indisponibilidad, de los componentes de grúa. Por lo tanto, si las probabilidades de ocurrencia de los eventos de fallo humano son mucho menores que las probabilidades de fallo de los componentes de la grúa su inclusión en el modelo APS tendría impacto nulo.

Capítulo 9

Conclusiones

La investigación llevada a cabo en el marco de la aplicación de técnicas probabilistas para el análisis de seguridad de un ATI ha llevado al desarrollo de una metodología de análisis probabilista de seguridad para evaluar el riesgo inherente al ATI de la central nuclear similar a la de un APS estándar de sucesos internos a potencia. En general, las tareas a realizar para aplicar la metodología APS de ATI son las mismas que las de un APS estándar. La única diferencia sustancial entre ambas metodologías deriva de la cantidad y tipología de los sistemas frontales y sistemas soporte a analizar en el caso de un ATI. Concretamente, los únicos sistemas frontales a analizar en el contexto del APS de ATI son la grúa puente del edificio de combustible, el sistema de ventilación del edificio de combustible, y las barreras de confinamiento del combustible, que son las vainas de combustible y el propio contenedor. Dicha cantidad de sistemas es mínima en comparación con la cantidad a analizar en un APS de sucesos internos a potencia de una central. Además, los sistemas frontales de mayor importancia en el contexto del APS de ATI son las barreras de confinamiento del combustible, que son sistemas totalmente pasivos cuya función es mantener la integridad del combustible ante posibles accidentes. Por el hecho de tratarse de sistemas pasivos cuya función principal es estructural, el tratamiento probabilista del fallo de dichos sistemas es totalmente diferente al de los sistemas frontales de un APS estándar. En consecuencia, el análisis de sistemas se reduce al análisis del sistema de ventilación y de la grúa puente del edificio de combustible. El análisis de la probabilidad de fallo de las barreras de confinamiento se lleva cabo mediante dos nuevas actividades, los llamados análisis estructural y análisis termohidráulico, que se engloban dentro de la tarea de análisis de datos. La metodología aquí presentada se inspira en metodologías piloto desarrolladas por la NRC y por EPRI.

El APS de ATI se extiende hasta el nivel 2 para poder comparar el riesgo del ATI con el riesgo de la central nuclear. Una metodología APS de nivel 1 no permitiría comparar el riesgo inherente al ATI con el de la central nuclear porque las figuras de riesgo que se compararían, daño al combustible en el interior del contenedor y daño al núcleo, son sustancialmente diferentes[1]. En cambio, la metodología APS de nivel 2 proporciona las mismas figuras de riesgo para el caso del ATI y para la central nuclear: la frecuencia de liberación de radionúclidos y el término fuente. De esta manera, se ha valorado el riesgo inherente al ATI tanto individualmente como en proporción con el riesgo de la central nuclear.

El modelo APS de ATI desarrollado mediante técnicas probabilistas presenta, en su cualidad de piloto, algunas carencias. Positivamente, en el desarrollo del modelo APS de ATI de la fase I se han llevado a cabo de forma detallada tareas como la familiarización con la instalación, la identificación de sucesos iniciadores, la delineación de las secuencias de accidente, o el análisis del sistema de ventilación del edificio de combustible. Contrariamente, los análisis estructural y termohidráulico se han llevado a cabo mediante la adaptación de resultados de estudios ajenos, la fracción de liberación estimada es un valor conservador

[1] Ni la cantidad de elementos de combustible es la misma ni su estado es comparable.

derivado de un caso envolvente estudiado en un documento ajeno [5], y el análisis de fiabilidad humana y el análisis del sistema grúa han quedado fuera del alcance del modelo. Tanto los análisis estructural y termohidráulico como la estimación de la fracción de liberación son tareas totalmente ajenas al resto de metodologías de análisis probabilista de seguridad y, además, requieren del conocimiento de otras áreas de la técnica como ingeniería estructural y transferencia de calor. Por estos motivos, y con el objetivo de no entorpecer la obtención de resultados, se ha decidido no realizar estos análisis desde cero. Respecto al análisis de fiabilidad humana, siguiendo el ejemplo del NUREG-1864, se ha decidido no aplicar el análisis de fiabilidad humana en primera instancia, es decir, en la fase I, para aligerar la carga de análisis que conlleva el desarrollo desde cero del APS del ATI y para así poder, posteriormente, valorar de forma aislada la contribución de la actuación humana al riesgo del ATI. A raíz de la naturaleza piloto del análisis y de las carencias identificadas, los resultados obtenidos mediante esta aplicación no representan el riesgo asociado al ATI de forma minuciosa y, por lo tanto, no son definitivos. No obstante, los resultados obtenidos sí que son una estimación orientativa del riesgo de la instalación que permiten realizar, por una parte, una valoración cuantitativa del mismo en comparación con el riesgo de la central nuclear, y, por otra parte, una valoración cuantitativa de la contribución al riesgo de los diferentes elementos del modelo APS.

Los resultados orientativos al respecto del riesgo del ATI obtenidos en el desarrollo del modelo APS de la fase I señalan la existencia de dos sucesos iniciadores predominantes: el Suceso Iniciador Caída5, y el Suceso Iniciador ACCAV. El primero, que solo puede ocurrir durante la fase de carga, representa la caída del contenedor MPC sobre la base del contenedor de almacenamiento, siendo la altura de caída de 5,8 m, en el momento en el que el primero es introducido en el segundo. El suceso Caída5 es predominante en el primer año del período de almacenamiento de un contenedor, siendo su FLR tres órdenes de magnitud mayor que la siguiente más alta. El resultado obtenido pone de manifiesto que, en comparación con las otras maniobras de la fase carga, y con el resto de operaciones del primer año de almacenamiento, la introducción vertical del MPC en el HI-STORM 100 es la mayor vulnerabilidad del procedimiento. De entre todos los elementos del modelo, el principal contribuyente a la FLR del suceso Caída5 es la probabilidad de fallo del contenedor MPC condicionada a la propia caída. La caída estudiada, de 5,8 m, corresponde a la altura del contenedor HI-STORM. En consecuencia, la altura de caída no puede ser menor que 5,8 m en el procedimiento de inserción vertical del MPC en el interior del HI-STORM. De juzgarse el riesgo del suceso Caída5 como demasiado alto, se deberían plantear alternativas a la inserción vertical como, por ejemplo, la inserción horizontal, con la inversión en infraestructura que esto supondría, o bien el uso de medidas de protección y seguridad como elementos amortiguadores, sistemas de eslingas redundantes, u otros. No obstante, a la vista de los resultados obtenidos en comparación con los de la central nuclear, y teniendo en cuenta el notable grado de conservadurismo aplicado en el cálculo de la frecuencia del suceso iniciador, en el cálculo de la probabilidad de grieta en soldadura, y en el cálculo del término fuente del contenedor, se concluye que el riesgo inherente al suceso Caída5, y, por extensión, el riesgo inherente al primer año de almacenamiento de un contenedor en el ATI, no es significativo.

El Suceso Iniciador ACCAV representa el golpeo de un contenedor, estando éste en la zona de almacenamiento, a causa del accidente de un avión. El suceso ACCAV es predominante en la fase de almacenamiento del proceso, y, por lo tanto, es el suceso predominante al respecto del riesgo del ATI en los años en los que el contenedor está a la intemperie en la zona de almacenamiento. El riesgo inducido por ACCAV podría reducirse con la construcción de un edificio de almacenamiento [2] en el que se introdujesen los contenedores, o con la inserción de los contenedores en cápsulas excavadas en la losa sísmica. No obstante, la FLR del suceso es tan baja, téngase en cuenta que sería cribada en el APS a Potencia nivel 2 de una central, que no se considera necesario llevar a cabo acción alguna para reducir su riesgo, que se valora como no significativo.

Respecto a la comparación con el riesgo de la central, tanto a nivel de contenedor como a nivel de ATI, la frecuencia de liberación de radionúclidos y el término fuente de los sucesos iniciadores predominantes en el APS de ATI son varios órdenes de magnitud inferiores a sus homólogos del APS de nivel 2 de

[2] De optar por una solución de este tipo, se debería garantizar que la frecuencia de ocurrencia del nivel mínimo de sismo que pudiese causar el fallo estructural del edificio es menor que la frecuencia de ocurrencia de ACCAV.

la central. Por ejemplo, el valor máximo de FLR para el suceso Caída5, que es de 7,35E-08 (año^{-1}), es sustancialmente menor, más de dos órdenes de magnitud, que el máximo del APS de nivel 2 de la central, que es de 1,72E-05 (año^{-1}). A la vista de los resultados obtenidos, y teniendo en cuenta el notable grado de conservadurismo inherente al APS, se concluye que los resultados, orientativos, obtenidos al respecto del riesgo del ATI en el modelo APS de fase I son sustancialmente bajos, prácticamente despreciables, en comparación con el riesgo de la central en sí. En consecuencia, se concluye que, teniendo en cuenta los resultados obtenidos, la contribución del riesgo del ATI al riesgo total del emplazamiento es prácticamente nula.

Pese a que las tres carencias expuestas son significativas para el modelo APS de fase I, los análisis estructural y termohidráulico y la fracción de liberación, a diferencia del HRA y el análisis de la grúa, tienen presencia en el modelo. Además, el tratamiento de ambas tareas es conservador, por lo que una mejora en su ejecución proporcionaría resultados más realistas que, a su vez, estarían aún más alejados de los valores de riesgo de la central nuclear. En cambio, debido a su ausencia en el modelo, el impacto del factor humano y del factor grúa en el riesgo es una incógnita. No obstante, se considera probable que un modelo que incluya ambos factores proporcione resultados de riesgo del ATI mayores a los de la fase I debido a la gran cantidad de operaciones humanas a realizar en el proceso de almacenamiento identificadas en la fase de familiarización. Consecuentemente, y pese a que en la fase I se ha concluido que el riesgo del ATI es prácticamente despreciable en comparación con el de la central, se ha decidido aplicar el análisis de fiabilidad humana y el análisis de la grúa en una segunda fase del modelo APS puesto que es posible que la valoración del riesgo del ATI aumente al introducir ambos ítems.

La aplicación de las técnicas de análisis de fiabilidad humana al contexto del ATI se ha llevado a cabo mediante la metodología ATHEANA. No obstante, la aplicación del análisis de fiabilidad humana ha requerido del desarrollo de un nuevo procedimiento de cuantificación para la metodología ATHEANA, ya que en el caso de estudio no es posible aplicar el juicio de expertos en el que ATHEANA basa su análisis cuantitativo del fallo humano. El nuevo procedimiento de cuantificación presenta un algoritmo de estimación basado en el análisis del contexto de estudio y en la discretización de los eventos de fallo humano en unidades elementales y genéricas. El evento de fallo humano más probable es el HFE6.1: Caída del contenedor MPC en el interior del HI-STORM 100 por fallo al anclar el dispositivo de izado. Su probabilidad de ocurrencia por alzamiento del contenedor es de 4,55E-04, ligeramente superior a la probabilidad de caída de cargas pesadas proveniente de la experiencia operativa de la industria americana [75, 76] utilizada en la fase I del APS. Casualmente, el HFE6.1 y el suceso inicador predominante en la fase I, Caída5, describen la misma situación, hecho que refuerza la conclusión de que este tipo de caída es el evento más significativo que puede ocurrir en el interior del edificio de combustible. En conclusión, los resultados obtenidos en el análisis de fiabilidad humana no son para nada despreciables en comparación con datos extraídos de otras fuentes. Al contrario, se consideran resultados que aportan información valiosa puesto que se han obtenido a partir de un análisis detallado del objeto de estudio. No obstante, los resultados son orientativos puesto que, debido a la falta de detalle en la descripción de algunas tareas en la documentación disponible, se han tenido que tomar hipótesis conservadoras en la modelización de algunos eventos de fallo humano.

La introducción de los resultados del análisis de fiabilidad humana en el modelo APS de ATI, conjuntamente con el fallo de grúa, ha requerido modificar únicamente el tratamiento de los sucesos iniciadores del modelo de la etapa de carga. En la fase II del modelo APS, la frecuencia de ocurrencia de sucesos iniciadores se ha modelado mediante árboles de fallo que incluyen tanto el fallo humano como el fallo de la grúa puente del edificio de combustible. En términos cuantitativos, la incorporación de los resultados del análisis de fiabilidad humana en el modelo APS solo afecta a la frecuencia de ocurrencia de los sucesos iniciadores. Debido a su relación, la frecuencia de liberación de radionúclidos de cada suceso iniciador se ve afectada en las mismas proporciones que la frecuencia de ocurrencia del suceso.

El impacto en los resultados cuantitativos de la frecuencia de liberación de radionúclidos de la introducción del fallo humano y del fallo de la grúa en el modelo APS es significativo. Concretamente, en términos generales, la frecuencia de liberación de radionúclidos total aumenta un orden de magnitud debido a que

la frecuencia de liberación de radionúclidos del caso predominante, LDP6 en la fase II y Caída5 en la fase I, aumenta dicho orden de magnitud. Específicamente, la frecuencia de liberación de radionúclidos del suceso LDP6 es 2,90E-07 (año·contenedor)$^{-1}$, mientras que la del suceso Caída5 de la fase I es 1,47E-08 (año·contenedor)$^{-1}$. En términos absolutos, el mayor impacto de la introducción del fallo humano y el fallo de grúa es la drástica reducción, de entre cuatro y seis órdenes de magnitud, de la frecuencia de liberación de radionúclidos asociada a los sucesos de *two-blocking*. La causa principal de dicha reducción es la introducción de fallo de la grúa en serie con el fallo humano en los casos de *two-blocking*. Sin embargo, a pesar de su sobreestimación por utilizar un modelo no detallado, el riesgo asociado al suceso *two-blocking* de la fase I ya era sustancialmente bajo, así que la obtención de valores aún más bajos en la fase II no tiene ninguna implicación en las conclusiones extraídas del APS. Teniendo en cuenta que el término fuente del suceso LDP6, que es el mismo que el de Caída5 de la fase I, sigue siendo sustancialmente más bajo que los calculados en el APSde nivel 2 de la central nuclear, el aumento de un orden de magnitud de la frecuencia de liberación de radionúclidos no supone un cambio de las conclusiones extraídas en la fase I. Por lo tanto, considerando el notable grado de conservadurismo inherente al APS de ATI, se concluye que los resultados orientativos respecto al riesgo del ATI siguen siendo sustancialmente bajos, prácticamente despreciables en relación al término fuente, en comparación con el riesgo de la central en sí. En consecuencia, se mantiene la conclusión de que la contribución del riesgo del ATI al riesgo total del emplazamiento es prácticamente nula.

Parte III

Desarrollo de herramientas basadas en el APS para introducir la valoración del riesgo inducido por incendios en procesos de toma de decisiones en centrales nucleares

Capítulo 10

Introducción

10.1. Problemática

La tercera parte de la tesis contiene el desarrollo y aplicación de metodologías y herramientas, generadas mediante el APS de incendios, para incorporar el riesgo inducido por incendio en las prácticas habituales de evaluación informada por el riesgo de configuraciones de sistemas, componentes, y estructuras, en centrales nucleares. Tal y como se ha visto en la parte introductoria, la regulación e industria nuclear, especialmente la estadounidense, están inmiscuidas en un proceso de adaptación e instauración paulatina del uso y aplicación de procesos de decisión y gestión informados por el riesgo. Sirva como ejemplo de este tipo de procesos la regla de mantenimiento, objetivo de esta parte de la tesis, en la que se valora el riesgo de daño al núcleo, u otras figuras de riesgo, de las posibles configuraciones de ESCs de la central para dar soporte a la toma decisiones al respecto del mantenimiento on-line de componentes. En el marco de un proceso de decisión informado por el riesgo, la valoración del riesgo incluida ha de ser lo más completa posible para que las personas responsables de tomar la decisión final tengan la máxima cantidad de información posible en la que basar su decisión. Por lo tanto, el riesgo inducido por incendios debería formar parte de la valoración del riesgo en la mayoría de procesos de decisión. No obstante, a causa, principalmente, de la evolución tardía de la metodología APS de incendios, la valoración del riesgo inducido por incendios en procesos de decisión informados por el riesgo se ha llevado a cabo, históricamente, mediante metodologías alternativas al APS, con resultados cualitativos conservadores, o se ha menospreciado directamente. Valga como ejemplo que en el documento *Guideline for Addressing Fire Events in Maintenance Rule (a)(4) Risk Evaluations at Nuclear Power Plants* de EPRI, publicado en 2011, se presentan metodologías alternativas de evaluación del riesgo inducido por incendios para dar soporte a la regla de mantenimiento ajenas al uso del APS porque «...Sin embargo, debido a la limitada disponibilidad de APS de incendios en la industria, esta guía focaliza su atención en otros métodos disponibles para estimar el impacto en el riesgo inducido por incendios que no dependan de un APS». En consecuencia, las metodologías y herramientas de evaluación del riesgo inducido por incendios realizadas mediante APS de incendios aún no están desarrolladas en el marco de la regla de mantenimiento y otros procesos de decisión. Las herramientas y metodologías presentadas en esta parte de la tesis doctoral son una contribución novedosa en el campo de la toma de decisiones informada por el riesgo pues precisamente están basadas en el uso de un APS de incendios, y su objetivo es dar soporte a la regla de mantenimiento.

10.2. Antecedentes

10.2.1. APS de incendios

La evolución de la metodología APS de incendios ha ido siempre por detrás del desarrollo de la metodología de APS de internos. Los motivos son los siguientes: En primer lugar, porque en el desarrollo de las primeras aplicaciones de análisis de riesgo se consideró que los casos de incendio no serían un suceso predominante en el riesgo de una central nuclear, así que el estado del arte de las metodologías utilizadas no los incluía [91]. En segundo lugar, porque en el desarrollo, a posteriori, de metodologías de análisis de riesgo que cubriesen los casos de incendio se debían modelar procesos físicos complejos, dando lugar a altos niveles de conservadurismo en los APS de incendios. Finalmente, y especialmente en Estados Unidos, porque el beneficio que suponía tener un APS de incendios no quedó claro[1] hasta que comenzaron a implantar los procesos de decisión informados por el riesgo.

El primer borrador del *Reactor Safety Study (WASH-1400)* [24] no incluyó el análisis cuantitativo del riesgo inducido por incendios porque se creía, en aquel momento, que los incendios no serían un factor significativo en el riesgo de la central[91]. Sin embargo, el incendio de Browns Ferry en marzo de 1975 hizo cambiar la opinión general al respecto de la importancia de los casos de incendio. Concretamente, en el propio documento final del *Reactor Safety Study (WASH-1400)*, publicado en octubre de 1975, ya se incluyó una estimación de la probabilidad de daño al núcleo condicionada al estado en el que quedó la planta de Browns Ferry debido al incendio, y de la frecuencia de daño al núcleo inducida por un incendio como el de Browns Ferry. Esta última, que resultó ser del orden de magnitud de la frecuencia de daño al núcleo total [91], vino a confirmar que, al menos, el riesgo inducido por incendios no podía ser despreciado.

El análisis del riesgo inducido por incendios experimentó un gran empuje después de la publicación final del WASH-1400, tanto en la forma de nuevas aplicaciones como en la forma de desarrollo de metodologías específicas para su desarrollo. Concretamente, en 1977, el análisis de riesgo del reactor reproductor de Clinch River incluyó un modelo de análisis de riesgo inducido por incendios más detallado que el del WASH-1400 cuyo principal elemento era un estudio de modos de fallo y efectos de las posibles localizaciones de incendios. En 1980, el Renssenlaer Polytechnic Institute desarolló un APS de una planta BWR que incluía árboles de eventos para representar de forma probabilista la propagación de incendios, dividida en etapas de ignición, detección, extinción, y propagación. Entre finales de la década de los 70 y principios de los 80 la NRC esponsorizó un proyecto de investigación para desarrollar una metodología de APS de incendios en la universidad de UCLA. Este proyecto, liderado por Apostolakis, Kazarians y Siu, consiguió avanzar en el análisis de riesgo de grandes incendios. Específicamente, en el marco del proyecto se desarrollaron modelos físicos de propagación y extinción de incendios, métodos para propagar incertidumbres a través del modelo de riesgo, y se desarrolló el uso del teorema de Bayes para estimar la frecuencia de ocurrencia de incendios en lugares específicos en centrales nucleares concretas [91]. La metodología desarrollada en la UCLA fue aplicada, a petición de la NRC, en los APS de las centrales Zion, Indian Point, y Big Rock, a principios de los años 80, y fue la metodología que posteriormente se utilizó para analizar el riesgo de incendios en el marco del NUREG-1150 (*Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants*) [33], publicado en 1990.

Tras el desarrollo de los estudios que forman el NUREG-1150, la NRC dedicó su investigación en materia de incendios a la comprensión de diversos fenómenos y efectos relacionados como, por ejemplo, los efectos del humo sobre componentes eléctricos [91]. A raíz de las nuevas políticas adoptadas en materia del uso del APS y de la toma de decisiones informada por el riesgo, la NRC retomó la investigación en materia del análisis de riesgo de incendios en 1998. En un esfuerzo conjunto con EPRI y otras instituciones, la NRC lanzó un proyecto para analizar la capacidad de obtener APS de incendios realistas mediante las metodologías del momento. Como resultado, se desarrolló una nueva metodología mejorada de APS de

[1] El beneficio primordial de un APS es el de identificar debilidades y vulnerabilidades del diseño de planta. Aunque el APS de incendios permite identificar vulnerabilidades específicas que solo aparecerían durante un caso de incendio, este beneficio ya está cubierto, mayormente, por el APS de internos, que no incluye el análisis de procesos físicos complejos.

incendios, publicada en el NUREG/CR-6850 en 2005 [4], preparada para proporcionar APS de incendios en consonancia con los procesos de decisión basados en el riesgo[2]. A su vez, la *National Fire Protection Association* publicó en 2002 la NFPA 805, un nuevo estándar para la protección contra incendios en centrales nucleares de agua ligera. En el estándar de la NFPA 805 se promueve la evaluación de la idoneidad de la protección contra incendios de una central mediante figuras cuantitativas, como las figuras de riesgo proporcionadas por el APS. La principal ventaja del acercamiento de la NFPA 805 es que proporciona flexibilidad al licenciatario al respecto de cómo cumplir con los criterios de riesgo establecidos[3]. En 2004, la NRC adoptó la NFPA 805 como método voluntario para cumplir con la regulación de protección contra incendios [92].

El desarrollo de una nueva metodología de APS de incendios realista y la adopción de la NFPA 805 en la regulación supusieron un nuevo empuje para el desarrollo y aplicación del APS de incendios, aunque esta vez dirigido desde la propia industria. La cantidad de centrales que han adoptado la NFPA 805 ha ido creciendo paulatinamente, llegando a ser 26, 42 reactores, en agosto de 2014 [93]. Cada uno de estos reactores tiene su propio APS de incendios adaptado a los últimos estándares y guías técnicas,así que ya no se puede considerar que la disponibilidad de APS de incendios sea limitada. De forma similar, en el marco español las plantas también disponen en su mayoría de APS de incendios porque en la instrucción de seguridad IS-25 del Consejo de Seguridad Nuclear de España, publicada en 2010, se les requiere tenerlo [50]. En conclusión, el estado actual del APS de incendios permite utilizarlo para desarrollar herramientas y metodologías de valoración del riesgo inducido por incendios que puedan ser utilizadas en procesos de decisión.

10.2.2. La regla de mantenimiento

El NUMARC 93-01: *Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants*, en su revisión 4A de 2011 [66], incluyó, por primera vez, la consideración del impacto en el riesgo inducido por incendios en el análisis y gestión de configuraciones de planta en el marco de regla de mantenimiento[4]. La metodología propuesta en el NUMARC 93-01 está acotada, no obstante, a la identificación de ESCs cuya indisponibilidad podría tener un impacto en riesgo inducido por incendios, y no incluye ningún acercamiento para evaluar el propio impacto en el riesgo de la indisponibilidad de estos ESCs. Sin una valoración del impacto en el riesgo inducido por incendios, el listado de ESCs identificadas puede incluir algunas cuyo impacto en el riesgo sea ínfimo, y pueden quedar fuera de la lista algunas cuyo impacto en el riesgo sea significativo. Por lo tanto, el listado de ESCs significativas para el riesgo inducido por incendios producto de la aplicación del NUMARC puede ser poco preciso.

El documento *Guideline for Addressing Fire Events in Maintenance Rule (a)(4) Risk Evaluations at Nuclear Power Plants* de EPRI, publicado en 2011 en soporte al NUMARC, presenta metodologías para la evaluación del impacto en el riesgo inducido por incendios de la indisponibilidad de ESCs. No obstante, estas metodologías son ajenas al uso del APS de incendios, con lo que proporcionan valoraciones cualitativas. Pese a que se trata de una mejora, una valoración cualitativa es más difícil de interpretar que una cuantitativa y puede llevar a confusión si no es lo suficientemente clara. La valoración cuantitativa del impacto en el riesgo inducido por incendio de la indisponibilidad de ESCs facilitaría enormemente la selección de aquellas a incluir en la regla de mantenimiento. En este sentido, un APS de incendios desarrollado de acuerdo con las guías y estándares vigentes es la herramienta indicada para obtener dichas valoraciones cuantitativas. No obstante, en la creación de los documentos mencionados anteriormente no se desarrollaron metodologías y herramientas para obtener valoraciones cuantitativas del impacto en el

[2] Posteriormente, EPRI y NRC lanzaron un proyecto para el desarrollo de metodologías de análisis de fiabilidad humana aplicables en casos de incendio. Dicho proyecto culminó en la publicación del NUREG-1921: *EPRI/NRC-RES Fire Human Reliability Analysis Guidelines* en 2012.

[3] Es decir, todo diseño de sistema de protección contra incendios que cumpla con los criterios cuantitativos establecidos en la NFPA 805 es apto. Anteriores estándares se centraban en las propias características de diseño.

[4] Sección (a) (4) del 10CFR50.65 [67].

riesgo inducido por incendios por la falta de APS de incendios existentes en la industria hasta el momento. Sin embargo, el estado actual del APS de incendios permite utilizarlo para desarrollar herramientas y metodologías de valoración del riesgo inducido por incendios que puedan ser utilizadas en procesos de decisión.

10.3. Contenido

Esta parte de la tesis presenta metodologías y herramientas novedosas para evaluar cuantitativamente e incorporar el riesgo inducido por incendios en las prácticas habituales de evaluación de configuraciones de planta llevadas a cabo en el marco de la regla de mantenimiento y otros procesos de decisión informados por el riesgo. Específicamente, se proponen y describen dos herramientas novedosas, que se aplican al caso real de una central nuclear española. Estas herramientas han sido desarrolladas mediante el APS de incendios de la central nuclear. Las herramientas diseñadas proporcionan figuras cuantitativas para evaluar el impacto en el riesgo inducido por incendios de estructuras, sistemas, y componentes de la central nuclear.

Una de las herramientas desarrolladas es una matriz de compatibilidades de indisponibilidades de sistemas contra incendio y funciones clave de seguridad, llamada MCI a partir de este punto. La matriz MCI sirve para identificar ESCs importantes desde el punto de vista de su impacto en el riesgo inducido por incendios. Dicha matriz contiene la frecuencia de daño al núcleo, inducida por incendios, de la central obtenida mediante el APS de incendios al combinar la indisponibilidad de sistemas contra incendios y funciones clave de seguridad.

La otra herramienta diseñada es una matriz de riesgo de incendio de zonas de incendio y funciones clave de seguridad, llamada MRI a partir de este punto. La matriz MRI sirve para identificar en qué zonas de incendio de la planta se deberían aplicar acciones para gestionar y reducir el riesgo, las llamadas *risk management actions*. La matriz incluye la contribución de cada zona de incendio a la frecuencia de daño al núcleo de la central, es decir, la frecuencia de daño al núcleo debida únicamente a incendios que puedan ocurrir en la zona estudiada, condicionada a la indisponibilidad de ESCs representativos de funciones claves de seguridad.

Con el objetivo de presentar el desarrollo y aplicación de las herramientas mencionadas, la tercera parte de la tesis se divide en los siguientes capítulos: un primer capítulo de descripción del sistema contra incendios de la central, capítulo 11, un segundo capítulo de descripción de las particularidades del APS de incendios, tanto genéricas de la propia metodología como específicas del APS de la central, capítulo 12, un tercer capítulo en el que se explica el desarrollo del análisis matricial de las herramientas, capítulo 13, un cuarto capítulo de cuantificación de las herramientas matriciales, capítulo 14, un quinto capítulo en el que se desarrolla el análisis de incertidumbre de la matriz MCI y se analizan los resultados obtenidos mediante las herramientas matriciales, capítulo 15, y un último capítulo de conclusiones. Cabe destacar que parte del contenido presentado en esta parte de la tesis ha sido publicado por *Taylor & Francis* en la revista *Journal on Nuclear Science and Technology* el 17/06/2016. El artículo publicado, llamado *Development and assessment of fire-related risk unavailability matrices to support the application of the maintenance rule in a PWR nuclear power plant*, está disponible online en la siguiente dirección: http://www.tandfonline.com/10.1080/00223131.2016.1193066.

Capítulo 11

Sistema contra incendios

El presente capítulo presenta, define y describe de forma resumida el sistema contra incendios de la central nuclear. Los datos específicos aquí expuestos han sido extraídos del estudio final de seguridad de la central y de los documentos de soporte al APS de incendios de la central.

11.1. Definición

La *National Fire Protection Association* define a un sistema contra incendios, o sistema de protección contra incendios, como "cualquier dispositivo o sistema de alarma de incendios, o dispositivo o sistema de extinción de incendios, o combinación de ellos, que está diseñado e instalado para detectar, controlar, o extinguir un incendio o por otro lado alertar a los ocupantes, a los bomberos, o a ambos, de que hay un incendio" [94]. Las principales funciones de un sistema de protección contra incendios son:

- Asegurar que un incendio no impedirá el funcionamiento de los dispositivos necesarios para efectuar una parada segura de la central nuclear, ni producirá un incremento significativo del riesgo de fugas de radiactividad al exterior de la misma.
- Proporcionar medidas de protección para atenuar el riesgo de incendios con el ulterior objetivo de disminuir las pérdidas debidas a siniestros en la central, y las pérdidas debidas a la interrupción de sus disponibilidades operacionales.
- Asegurar que las consecuencias de un incendio serían mínimas en lo referente a la seguridad del personal de la central.

11.1.1. Criterios generales de diseño

El sistema de protección contra incendios de la central nuclear objeto de estudio está diseñado de acuerdo con los requerimientos del Criterio General de Diseño CGD-3 de la IS-27 [95] del Consejo de Seguridad Nuclear[1]. La figura 11.1 índica los principales requisitos de diseño impuestos en la CGD-3 de la IS-27, que siguen la filosofía de defensa en profundidad.

La tabla 11.1 contiene las definiciones oficiales, extraídas de la IS-27, de los principales requisitos impuestos por el CGD-3.

[1] La instrucción de seguridad 27 versa sobre los criterios generales de diseño de las centrales nucleares.

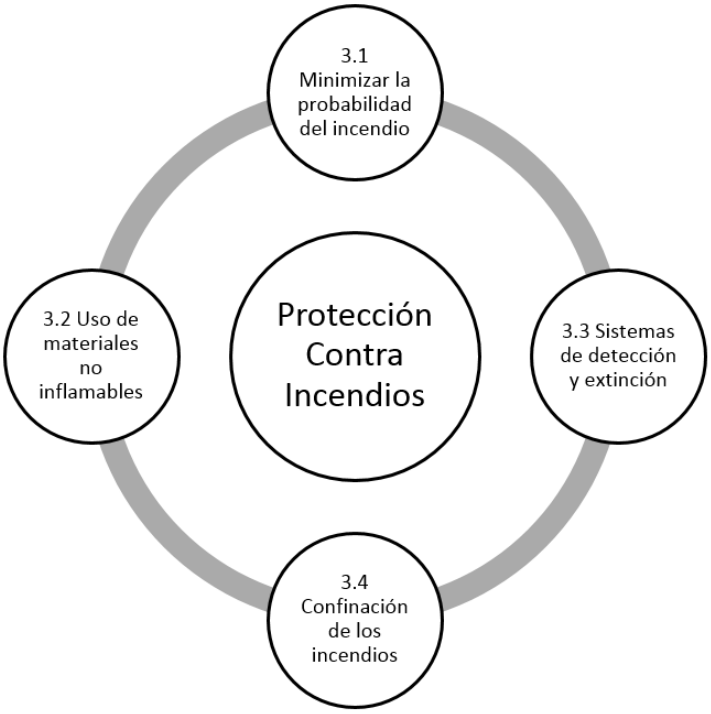


Figura 11.1: Criterios generales de diseño para un sistema de protección contra incendios según el CGD-3 de la IS-27.

Criterio	Definición
3.1. Minimizar la probabilidad del incendio	Las ESC importantes para la seguridad deberán estar diseñadas y ubicadas de manera que se minimice la probabilidad de fuegos o explosiones y sus efectos, siempre de una forma que sea coherente con otros requisitos de seguridad.
3.2. Uso de materiales no inflamables	Siempre que sea factible, y especialmente en zonas vitales de la central, tales como el recinto de contención y la sala de control, se deberán utilizar materiales no inflamables y resistentes al calor.
3.3. Sistemas de detección y extinción	Se deberán instalar sistemas de detección y de extinción del fuego de eficacia y capacidad adecuadas, que deberán estar diseñados para minimizar los efectos adversos del fuego en las ESC importantes para la seguridad. Los sistemas de extinción de incendios deberán diseñarse de forma que en caso de rotura o de operación indebida del sistema, la capacidad para realizar las funciones de seguridad de estas ESC no se vea afectada de forma significativa.
3.4. Confinación de los incendios	Se deberá disponer de las medidas de protección necesarias para limitar la propagación de incendios, garantizando que se mantienen confinados en áreas resistentes al fuego.

Tabla 11.1: Definición de los criterios de diseño CGD-3 de la IS-27.

El sistema de protección contra incendios de la central nuclear objeto de estudio está diseñado para detectar

y combatir incendios, así como para extinguir automáticamente los tipos de incendios que ocurren con más frecuencia en una central nuclear. El sistema se ha diseñado también para proteger la central de los daños que pueda producir el fuego, minimizar los riesgos del personal y disminuir las pérdidas en las propiedades. Las siguientes secciones describen las principales características del sistema contra incendios de la central.

11.2. Sistema contra incendios de la central

El sistema de protección contra incendios de la central nuclear consta de los siguientes subsistemas:

1. Un sistema de protección y extinción con agua formado por:
   a) Rociadores automáticos y manuales de tubería vacía.
   b) Cabinas de mangueras por toda la planta e hidrantes rodeando la misma.
2. Extintores portátiles, colocados por toda la central.
3. Sistemas de extinción de CO_2 de baja y alta presión.
4. Sistemas de extinción de FE-13.
5. Sistema de extinción mediante espuma.
6. Sistemas de detección:
   a) Iónica cruzada o doble.
   b) Iónica simple.
   c) Fotoeléctrica (óptico de humo).
   d) Termovelocimétrica.
   e) Radiación ultravioleta (óptico de llama).
   f) Radiación infrarroja (óptico de llama).
   g) Detección por aspiración.

Además, se han colocado compuertas cortafuego en aquellos conductos de ventilación y aire acondicionado que atraviesan los muros de separación de zonas de incendio, para evitar la transmisión del incendio de una zona a otra. En el edificio auxiliar se ha colocado un sistema de extracción de humos por medio de tres extractores situados en la parte alta de los huecos de escalera. También se ha colocado una compuerta cortafuego en la unidad de impulsión de aire del edificio auxiliar para evitar que entre aire al edificio en el caso de producirse un incendio.

11.2.1. Descripción general del sistema de agua para la protección contra incendios

El sistema de agua para protección contra incendios está formado de los siguientes componentes:

- Dos bombas, una eléctrica y otra diésel suministran el agua necesaria para el anillo del sistema de protección contra incendios. Estas bombas están separadas físicamente por una barrera metálica con imprimación ignífuga, y arrancan automáticamente al bajar la presión del anillo.

- Un anillo de 30,5 cm de diámetro rodea la planta con hidrantes y cabinas de mangueras a intervalos máximos de 85 m. El anillo se ha dividido en secciones separadas por válvulas de aislamiento para asegurar el suministro de agua en el caso de rotura de una sección del anillo.
- Los sistemas rociadores de tubería vacía están diseñados para liberar agua a través de un sistema de tuberías y boquillas hidráulicamente calculadas con el fin de lograr la densidad superficial de agua requerida en la zona. Estos sistemas están activados por detectores. La válvula de acceso a los sistemas rociadores puede ser manualmente operada presionando el correspondiente pulsador.

11.2.2. Descripción general del sistema de CO_2 para la protección contra incendios

El sistema de CO_2 para protección contra incendios está formado de los siguientes componentes:

- Un tanque de almacenamiento de CO_2 a baja presión, el cual suministra CO_2 para la extinción de incendios en algunas salas y para la purga del generador.
- Todo el sistema está diseñado de acuerdo con las normas NFPA Standard nº 12 [96]. Se usan válvulas "selector". Las válvulas "selector", al recibir una señal del equipo de detección de una zona a proteger, abren después de un tiempo predeterminado para permitir el paso de CO_2 hacia la zona en la que se ha producido la señal.
- Se han colocado caminos de alivio en las salas protegidas con CO_2 para evitar sobrepresiones en caso de descarga del gas.
- Se ha colocado un sistema de extracción de CO_2 de las salas del edificio auxiliar que tienen este sistema de protección contra incendios.

11.2.3. Vigilancia de incendios

La vigilancia de incendios se lleva a cabo mediante los sistemas de detección, que transmiten alarmas acústicas y visuales en la Sala de Control. Cada detector es ajustable individualmente dentro de un rango de sensibilidad que se considera apropiado para el área a proteger en cuestión.

Todos los sistemas fijos de detección y protección contra incendios se han previsto con alarmas locales, además del sistema anunciador en la Sala de Control. Las estaciones de mangueras (agua y/o CO_2) se han diseñado para dar indicación de uso. Cuando se extrae agua (mangueras en los edificios o aspersores en el exterior) con caudal superior a 3,2E-3 m^3/s, se producirá una caída de presión suficiente para ocasionar el arranque de una bomba contra incendios con aviso en la Sala de Control. Las mangueras de CO_2 están alimentadas desde tanques de baja presión, produciendo señalización cuando se retiran de sus soportes.

11.2.3.1. Indicación en la sala de control

Todos los paneles indicadores de alarma de incendio están alimentados de potencia a una tensión de 220 V.c.a. segura, siguiéndose el criterio de fallo simple. La energía puede también suministrarse desde sus propias baterías, cuando el suministro de corriente alterna no está disponible.

11.2.4. Prevención de condiciones de funcionamiento no seguras consecuencia de la operación del sistema

Los requisitos que aseguran que la operación del sistema de protección contra incendios no generará una condición de funcionamiento no segura son:

- Todas las zonas que contienen rociadores, dentro de la planta, contienen sistemas de drenaje adecuados para evitar el deterioro de cualquier sistema de seguridad citado.
- Los agentes extintores elegidos no dejan residuo.
- Los sistemas de lubricación de las bombas de refrigerante del reactor tienen un sistema de recogida y almacenamiento de las posibles fugas de aceite.

11.2.5. Criterios de diseño sísmico

El sistema de agua de protección contra incendios se ha diseñado de acuerdo con los criterios de Clase Sísmica II, excepto para aquellos elementos del sistema situados en el interior de edificios que contienen sistemas de Clase Sísmica I[2], que se han diseñado según Clase Sísmica I. En el edificio de Contención, la sujeción de las tuberías de agua se ha construido siguiendo los criterios de Clase Sísmica I.

[2] Un elemento de Clase Sísmica I ha de soportar el terremoto de parada segura (SSE), mientras que un elemento de Clase Sísmica II ha de soportar el terremoto de operación (OBE).

Capítulo 12

Metodología APS de incendios

12.1. Introducción

El capítulo 12 presenta la metodología APS de incendios utilizada para realizar el APS de incendios de la central. Con este objetivo, este capítulo se divide en dos partes, la sección 12.2 y la sección 12.3. En la primera parte, se presentan, de forma genérica, las características y tareas más relevantes de la metodología de desarrollo de un APS de incendios. En la segunda parte, se presentan en detalle las particularidades más significativas del APS de incendios de la central nuclear. Se hace especial hincapié en aquellas tareas que afectan al desarrollo matricial de las herramientas de valoración del riesgo inducido por incendios desarrolladas en esta parte de la tesis en los capítulos 13 y 14. En conjunto, el capítulo 12 da una visión global, y, a su vez, detallada, de las tareas a realizar en la metodología APS de incendios utilizada, así como de sus particularidades en comparación con la metodología APS de sucesos internos.

12.2. Metodología APS del NUREG/CR-6850

La metodología usada en la preparación del APS de incendios de la central nuclear es la contenida en el NUREG/CR-6850: *Fire PRA Methodology for Nuclear Power Facilities* [4]. Dicha metodología toma como referencia un APS de nivel 1 de sucesos internos y tiene como antecedentes el EPRI *Fire PRA Implementation Guide*, el NUREG-1150 *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants*, y el NUREG CR-4840 *Procedures for the External Event Core Damage Frequency Analyses for NUREG-1150* [97].

La metodología APS de Incendios del NUREG/CR-6850 evalúa la posibilidad de que un suceso iniciador de incendio, es decir, un caso singular de incendio, provoque daño al núcleo de forma directa o de forma indirecta a partir de ocasionar un suceso interno como los evaluados en el APS de sucesos internos[1]. De hecho, tal y como se explica en la sección 12.3 a continuación, el modelo APS de incendios de la central contiene el APS de sucesos internos de la central. Si la central no dispusiese de un APS de nivel 1 de sucesos internos, la realización del APS de incendios comportaría, también, la realización previa del APS de nivel 1 de sucesos internos.

[1] Es decir, pérdida de alimentación electrica, disparo del reactor y turbina, y pérdida de refrigerante del primario, entre otros.

12.2.1. Resumen de tareas del NUREG/CR-6850

La realización de un APS de Incendios es un proceso iterativo, ya que algunas tareas necesitan de un ajuste o mejora después de haber realizado tareas posteriores. Incluso, debido a su envergadura, el alcance inicial puede ser de detalle limitado para facilitar las tareas del análisis, siempre y cuando se añada detalle donde fuere necesario una vez obtenidos algunos resultados [4], como los del cribado cuantitativo. De esta forma los recursos disponibles para llevar a cabo el APS se centran en los puntos de mayor importancia, limitándose el esfuerzo dedicado a detalles que luego pudiesen valorarse como omisibles. Como ejemplo, las tareas 2 y 3, generación del listado de componentes y circuitos que entran en consideración en el APS, es probable que requieran de una revisión posterior después de realizar los cribados de las tareas 4 y 7. A continuación se listan todas las tareas descritas en la metodología del NUREG CR-6850 para la realización de un APS de incendios. No se incluyen tareas propias del APS de internos porque se considera que éste ha sido realizado con anterioridad.

- Tarea 1: Definición de límites y particionado de la planta.
- Tarea 2: Selección de componentes a tener en consideración para el APS de incendios[2].
- Tarea 3: Selección de cables.
- Tarea 4: Cribado cualitativo.
- Tarea 5: Desarrollo del modelo selectivo APS del riesgo inducido de incendio.
- Tarea 6: Estimación de la frecuencia de ignición de incendios.
- Tarea 7: Cribado cuantitativo.
- Tarea 8: Definición de y cribado de fuentes de incendio.
- Tarea 9: Análisis detallado del fallo de circuitería.
- Tarea 10: Análisis de la probabilidad de los modos de fallo de la circuitería.
- Tarea 11: Desarrollo del modelo detallado APS del riesgo de incendio inducido por la planta.
- Tarea 12: Análisis de fiabilidad humana después de un incendio.
- Tarea 13: Interacciones entre terremotos e incendios.
- Tarea 14: Cuantificación del riesgo inducido por incendio. Recomendaciones para la presentación de resultados.
- Tarea 15: Análisis de sensibilidad e incertidumbre.
- Tarea 16: Documentación del APS de incendios.

En sucesivos apartados se describen, de forma genérica, aquellas tareas consideradas como más relevantes para la creación del modelo APS de incendios.

12.2.2. Tarea 1: Definición de límites y particionado de planta

La primera tarea del desarrollo de un APS de incendios es definir y acotar los límites físicos de la central nuclear en el análisis, y dividir la superficie interior de dichos límites físicos en compartimentos de análisis. La superficie interior se divide, comúnmente, en áreas, zonas, y recintos de incendio. La sección 12.3 a continuación contiene la descripción de los diferentes compartimentos de análisis definidos en el APS de incendios de la central nuclear.

[2] La tarea 2 no está acotada a los componentes incluidos en el APS de internos. Cualquier componente de la central puede ser seleccionado.

12.2.3. Tareas 4 y 7: Cribados de compartimentos

En el marco del APS de incendios, el cribado consiste, en primer lugar, en la identificación de aquellos compartimentos cuya contribución al riesgo inducido por incendios de la central es despreciable, y, en segundo lugar, en la eliminación de estos compartimentos del análisis. En la tarea 4, el cribado se realiza sin haber elaborado una cuantificación previa. En el marco de esta tarea, se identifican aquellos compartimentos que no contienen ni componentes ni cables identificados en las tareas 2 y 3. También son cribados en la tarea 4 aquellos compartimentos que no pueden generar un disparo del reactor ya sea por procedimientos de planta, señales de disparo automáticas o requerimientos específicos técnicos.

La tarea 7, el cribado cuantitativo, se ejecuta a partir de la cuantificación del modelo APS de incendios provisional[3] desarrollado en la quinta tarea. Con el cribado cuantitativo no se retiran del APS de incendios los compartimentos identificados, simplemente no se tienen en cuenta en el análisis detallado de incendios posterior. Se tienen en consideración dos criterios, véanse las ecuaciones L.1 y L.2, respectivamente, para la realización del cribado cuantitativo. El primer criterio de cribado impone que todos aquellos compartimentos cuya FDN es inferior a 1,0E-07 año^{-1} se omiten en el análisis detallado. El segundo criterio se aplica para asegurar que el riesgo acumulado de los compartimentos cribados no es significativo. En caso de que no se cumpla el segundo criterio, el límite de cribado utilizado en el primero, es decir, 1,0E-07 año^{-1}, ha de reducirse tanto como sea necesario para que se cumpla el segundo criterio.

$$FDN^{crib} < 1,0E-07\, año^{-1} \tag{12.1}$$

$$\sum_i FDN_i^{crib} < 0,1 \cdot FDN^{internos} \tag{12.2}$$

12.2.4. Tareas 5 y 11: Modelos APS de incendios

La tarea 5 abarca el desarrollo de un primer modelo lógico que refleje las diferentes respuestas de la central nuclear ante un incendio. Este primer modelo parte de modificar el APS de sucesos internos para cuantificar la frecuencia de daño al núcleo inducida por incendios. Este modelo es altamente conservador pues en su desarrollo se considera que el incendio afecta a todos los componentes y bandejas de cables existentes en el compartimento en el que se postula el incendio y, además, no incluye la posibilidad de extinguir el incendio. El propósito del modelo generado en la tarea 5 es el de utilizarse en el cribado cuantitativo. Se considera que, si la FDN de un compartimento es lo suficientemente baja como para ser cribada en este modelo, la influencia de este compartimento sobre la FDN real inducida por incendios es despreciable debido al alto grado de conservadurismo del propio modelo. Se omiten de este análisis los incendios en la Sala de Control y en los compartimentos de turbinas, que pasan directamente al análisis detallado posterior.

La tarea 11 hace referencia a la creación del modelo APS de incendios final, también llamado detallado. Su origen es el APS de sucesos internos y el modelo de APS de incendios generado en la tarea 5. En el modelo APS generado en la tarea 11 se analizan detalladamente aquellos compartimentos que son potencialmente significativos para el riesgo, es decir, aquellos que no han sido cribados. A diferencia del de la tarea 5, el modelo APS de incendios detallado contempla el crecimiento del fuego, su propagación, y la posibilidad de su extinción antes de que dañe un componente concreto. También se da especial consideración en este modelo detallado a los incendios del generador de la turbina, incendios por hidrógeno, por arcos eléctricos de alta energía, por cableado, y a los incendios en el panel de control principal, en la Sala de Control. El diagrama de flujo de la figura 12.1, extraído del NUREG/CR-6850, presenta los once pasos que componen la tarea 11 del desarrollo de un APS de incendios.

[3] Se trata de un modelo conservador que no incluye la posibilidad de detectar y extinguir un incendio.

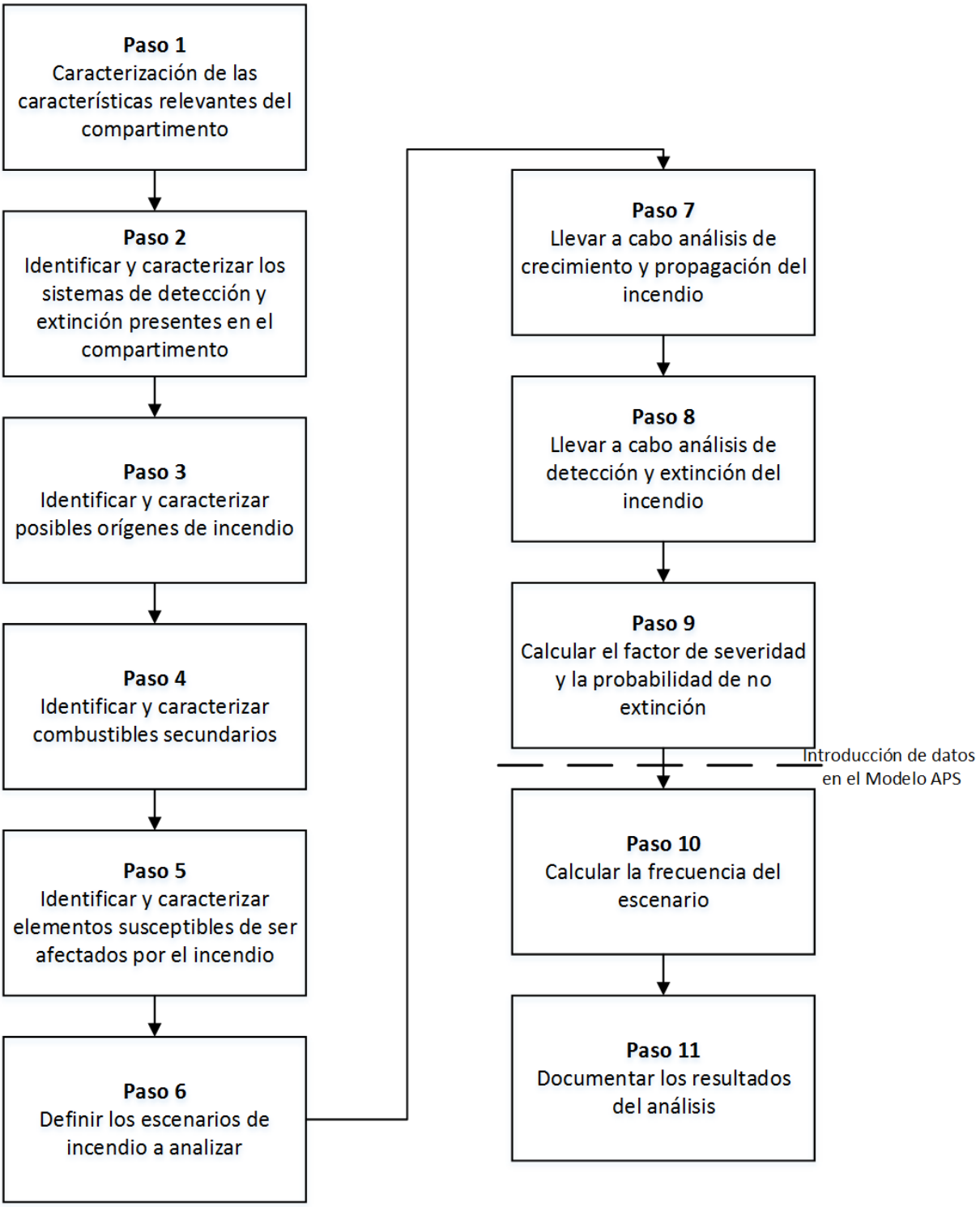


Figura 12.1: Metodología para llevar a cabo la tarea 11 del NUREG/CR-6850. Fuente: [4]

12.3. APS de incendios de la central nuclear

En esta sección se describen las principales características del APS de incendios de la central nuclear. Tal y como se ha comentado, para la realización de este APS se ha seguido la metodología descrita en el NUREG/CR-6850. El APS de incendios de la central nuclear es de nivel 1, y abarca la operación a Potencia. La información aquí expuesta ha sido extraída de los documentos de soporte del análisis probabilista de seguridad de incendios de la central. El software utilizado para revisar el modelo, que es el mismo que se ha utilizado para crearlo, es el *RiskSpectrum® PSA*.

12.3.1. Definición de límites y particionado de la planta

Siguiendo la metodología del NUREG/CR-6850, las zonas de análisis, o compartimentos, se definen de acuerdo con los siguientes criterios:

- Cada localización de la planta se corresponde con una única zona de análisis. El conjunto de todas las zonas de análisis cubre todos los edificios objetos de estudio.
- Una zona de análisis es un espacio cerrado bien definido de la central. Está delimitada por elementos físicos que pueden constituir o no barreras de fuego. Así, se consideran elementos de separación de las zonas de fuego las puertas normalmente cerradas, muros permanentes o muros desmontables. Los elementos de separación deben proporcionar una separación completa; las puertas deben encontrarse normalmente cerradas y los muros deben proporcionar un cerramiento completo, desde el suelo hasta el techo.
- Las barreras o muros parciales, los que se extienden desde el techo hacia abajo sin tocar el suelo o desde el suelo sin alcanzar el techo, así como las aberturas en el techo o estrechamientos, no se consideran posibles fronteras de zona de análisis a la hora de realizar las divisiones.
- Las rejillas que separan diferentes elevaciones no se consideran frontera entre zonas de análisis.

La división en zonas de análisis de los edificios incluidos en los límites físicos de la central se corresponde, principalmente, con la división en zonas de fuego definida en el documento de Análisis de Riesgo de Incendios (ARI)[4] de la central nuclear. La nomenclatura utilizada para la identificación de las zonas de análisis también se importa del análisis de riesgo de incendios de la central. No obstante, hay casos en los que ha sido necesario realizar una redefinición de zonas para cumplir con los criterios definidos en el NUREG/CR-6850, o por criterios de simplificación del análisis. Para cada edificio, la división en zonas se realiza por elevaciones, es decir, se definen diferentes zonas de análisis para cada elevación de los edificios incluidos en el análisis. A modo de ejemplo, se presenta un diagrama parcial de plano de la planta en la figura 12.2. En el diagrama se aprecia la distinción entre área, zona y recinto, y se pueden observar los distintos sistemas contra incendios. Entiéndase por área de incendio la mínima superficie de una elevación de un edificio que está delimitada por elementos físicos que constituyen barreras de fuego. Las zonas se corresponden con las zonas de análisis del APS de incendios.

[4] Este documento contiene un análisis determinista del riesgo de incendios de la central, incluyendo la definición de un camino de parada segura en caso de incendio en cualquiera de las zonas de fuego definidas.

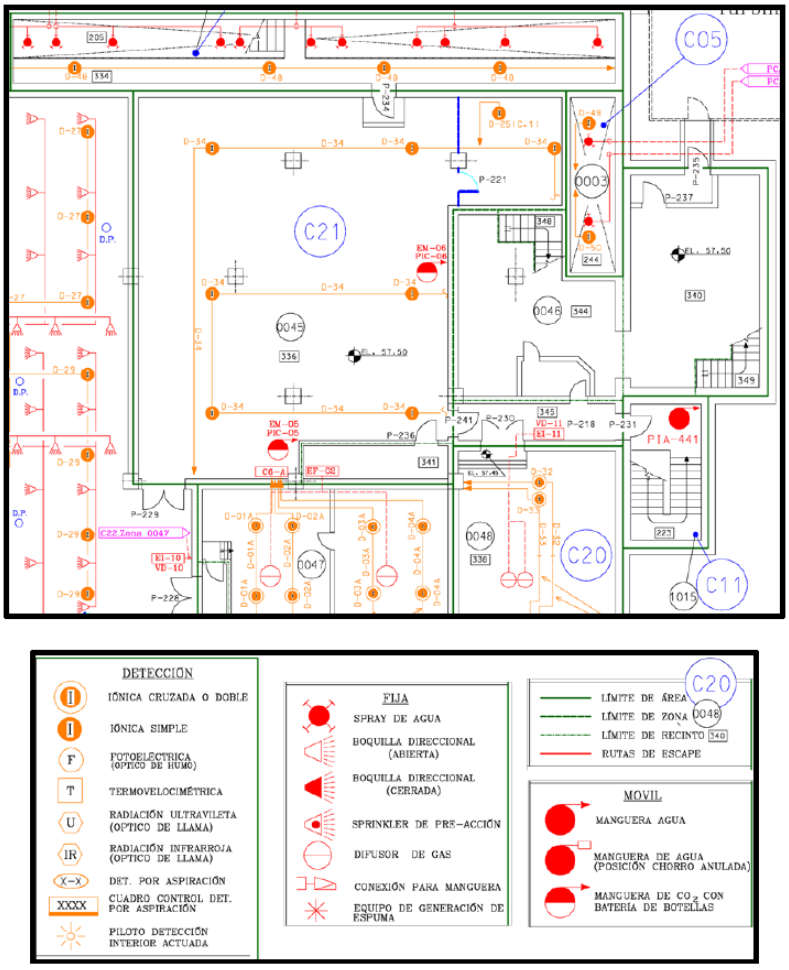


Figura 12.2: Diagrama parcial de plano de planta que contiene sistemas contra incendios.

12.3.2. Determinación de las frecuencias de incendio

El proceso de determinación de las frecuencias de incendio a utilizar en el APS de incendios se desarrolla a partir de la identificación de los diferentes grupos de orígenes[5] de incendio presentes en la central. La identificación de los diferentes grupos de orígenes de incendio a considerar en el desarrollo del APS se realiza siguiendo la guía contenida en el capítulo 6 del NUREG/CR-6850 y más concretamente en la tabla 6-1 de dicho capítulo. Se ha incluido la tabla 6-1 del NUREG/CR-6850 en el anexo S.

Dicha Tabla 6-1 contiene una estimación de las frecuencias genéricas de incendio para diferentes combinaciones de orígenes de incendio y localizaciones genéricas de la planta[6]. En el caso de las localizaciones genéricas de la planta, éstas se definen a nivel de edificio. Siguiendo la metodología del NUREG/CR-6850, se tienen que distribuir estas frecuencias genéricas entre las diferentes localizaciones o zonas de análisis de la central en las que se pueden localizar los diferentes tipos de orígenes de incendio. Se distribuyen las frecuencias de incendio genéricas entre las distintas zonas según factores de pesado proporcionados

[5] Entiéndase por origen de incendio el tipo de componente en el que se origina el fuego (transformador, cable, bomba, etc.).

[6] Entiéndase por localización genérica de planta los edificios que comúnmente se encuentran en una central nuclear como la Contención, el Edificio Auxiliar, o el Edificio de Generadores Diésel.

en el NUREG/CR-6850. Cabe destacar que las frecuencias genéricas presentes en el NUREG/CR-6850 son el resultado de un exhaustivo análisis de la experiencia operativa respecto a casos de incendio de la industria nuclear. Para determinar las frecuencias de incendio también se tiene en cuenta la experiencia operativa de la planta. Si existe algún suceso de incendio aplicable, el NUREG/CR-6850 propone realizar un ajuste bayesiano a la correspondiente frecuencia genérica de incendio con el objetivo de incluir la propia experiencia de la central.

12.3.3. Análisis de sucesos internos

Una de las principales tareas del APS de incendios es identificar qué sucesos internos pueden ser ocasionados por cada origen y tipo de incendios incluidos en el alcance del APS[7]. La selección de sucesos iniciadores del APS de sucesos internos a Potencia de nivel 1 se toma como base para el desarrollo de este análisis, estudiándose la aplicabilidad de estos sucesos al propio análisis de incendios. Adicionalmente se identifican algunos sucesos iniciadores de causa común que pueden ser originados por un incendio y que pueden considerarse específicos de este análisis. La realización de este análisis consiste en estudiar las consecuencias de cada combinación de origen de incendio y zona de incendio con el objetivo de determinar el, o los, suceso iniciador interno que provocaría, y, además, los equipos e instrumentación que son necesarios para su mitigación y que puedan verse afectados por el incendio. En consecuencia, el análisis de sucesos internos es la principal fuente de información para el cribado cualitativo a realizar en la tarea 4 del desarrollo del APS de incendios. La tabla 13.1 lista los sucesos iniciadores internos aplicables al análisis de incendios[8].

[7] Cabe recordar que, en el marco del APS de incendios, el riesgo de daño al núcleo inducido por incendios se divide en dos vertientes: el riesgo de que un incendio cause directamente daño al núcleo, y el riesgo de que un incendio cause una anomalía que derive en daño al núcleo.

[8] Se desestiman los sucesos internos que únicamente podrían ocurrir por causa de un fallo mecánico como, por ejemplo, un LOCA grande.

Sucesos internos aplicables al APS de incendios	Descripción
S2	LOCA pequeño
S3	LOCA muy pequeño
T2	Disparo de reactor y turbina
T3	Pérdida de vacío en el condensador
T4	Pérdida de Agua de Alimentación Principal
T7	Rotura de vapor principal aguas abajo de las válvulas de aislamiento[9]
TV	Rotura de vapor principal aguas arriba de las válvulas de aislamiento fuera de contención
T8	Actuaciones espurias de inyección de seguridad
T9A	Pérdida de la barra G1A de 125V de c.c.
T9B	Pérdida de la barra G1B de 125V de c.c.
T10	Pérdida de Agua de Refrigeración de Componentes
TS	Pérdida total del Agua de Servicios de Componentes
T11	Pérdida del sistema de Refrigeración de Salvaguardias
T12	Pérdida del sistema de Aire Comprimido de Instrumentos
T13	Pérdida total de Ventilación de Salas de Equipo Eléctrico del Edificio de Control
T14	Pérdidas de la barra 5A de 6,9KV de c.a.
T15	Pérdidas de la barra 6A de 6,9KVde c.a.
TB	Pérdida de la barra 9A de Alimentación de Salvaguardias
SI nº 28	Pérdida total de corriente alterna de salvaguardias
SI nº 29	Pérdida de dos o más barras vitales
SI nº 31	Pérdida total de barras vitales
SI nº 32	Pérdida de HVAC de Sala de Control

Tabla 12.1: Listado de sucesos iniciadores internos aplicables al APS de incendios.

12.3.4. Análisis selectivo

El análisis selectivo consiste en la aplicación de los cribados cualitativos y cuantitativos, respectivamente, para acotar el alcance del análisis de incendios. De acuerdo con el NUREG/CR-6850, las zonas de análisis que no contienen equipos cuya indisponibilidad pueda causar sucesos iniciadores, ni contienen equipos requeridos en la mitigación de transitorios o accidentes que puedan conducir a una situación de daño al núcleo, pueden ser eliminadas del alcance del APS de incendios. Por lo tanto, en el cribado cualitativo se identifican y eliminan aquellas zonas que no contienen cables, o directamente equipos, relacionados con los sucesos iniciadores internos aplicables al análisis ni con la mitigación de sus posibles consecuencias.

12.3.4.1. Cribado cuantitativo

El cribado cuantitativo se lleva a cabo mediante el modelo selectivo APS del riesgo inducido por incendios de la central. El modelo selectivo APS tiene las siguientes características principales:

- Se considera que todos los cables de una zona en la que se produzca un incendio se ven afectados por el mismo. En consecuencia, se considera que los incendios tienen las peores consecuencias posibles.
- A cada equipo se le asignan los modos de fallo que pueden ser causados por los fallos de sus cables, de acuerdo con la metodología del NUREG/CR-6850.
- No se da crédito a la extinción de un incendio.
- No se da crédito a la propagación de incendios entre zonas de análisis delimitadas y cerradas.
- En el análisis de los efectos del incendio en cada zona, con los criterios de daño adoptados, es posible que, dependiendo de los componentes que resultan afectados, se identifiquen como posibles más de un suceso iniciador. En ese caso, se asigna el suceso iniciador con consecuencias más severas. Si no es posible determinar el grado de severidad de los sucesos mediante criterios cualitativos, se aplican criterios cuantitativos. Para ello se cuantifica la zona con todos los sucesos iniciadores que se han considerado posibles en ella. Se selecciona el que tenga peores consecuencias para la central, a la vista de los resultados obtenidos.
- Para las zonas de análisis en las que no se ha identificado ningún suceso iniciador más severo, se considera que se produce un disparo de Reactor y Turbina (T2) cuando el suceso se produzca en cualquier edificio distinto del Edificio de Turbina. Cuando la localización sea en el Edificio de Turbina y tampoco se haya identificado ningún suceso iniciador más severo se considerará que se produce una Pérdida de Agua de Alimentación (T4).
- En las cuantificaciones de frecuencias de daño al núcleo inducidas por incendio se utiliza el modelo de *RiskSpectrum® PSA* desarrollado para el APS de sucesos internos. Los daños en cada zona de incendio se representan mediante la puesta a *True*[10] de los sucesos básicos recogidos en los árboles de fallo del APS que representan los modos de fallo de componentes que pueden ser causados por el fallo de los cables situados en la zona de análisis. En los casos en que el equipo afectado no ha sido modelado en el APS y, por tanto, no tenga un suceso básico asociado, se asigna un suceso básico con consecuencias semejantes sobre el modelo. Para la cuantificación de los daños causados por incendios se parte de la configuración de planta y de las condiciones de contorno propias de cada suceso iniciador utilizadas en el APS de sucesos internos a Potencia de nivel 1.

La aplicación de los criterios de cribado cuantitativo sobre los resultados obtenidos en el modelo selectivo APS da como resultado que se han de realizar análisis detallados para 41 zonas repartidas entre el Edificio Auxiliar, el Edificio de Control, el Edificio de Penetraciones Eléctricas, el Edificio de Turbina y el Edificio de Agua de Alimentación Auxiliar. Respecto al Edificio de Control, existen zonas que no han sido cuantificadas y que pasan directamente al análisis detallado. Dichas zonas son la Sala de Control, las salas que contienen cableado de la Sala de Control y las que contienen equipos de acondicionamiento del aire. De acuerdo con los resultados obtenidos, las zonas de análisis de los edificios de penetraciones mecánicas, la casa de bombas y la casa de bombas de agua de refrigeración de componentes, no requieren análisis detallado.

12.3.5. Análisis detallado. Modelo APS

El desarrollo del análisis detallado, y de su modelo APS de incendios asociado, responde a la necesidad de estudiar con precisión la contribución al riesgo inducido por incendios de aquellas zonas de análisis que han superado el cribado cuantitativo. De forma similar, la estructura del modelo APS detallado está basada en el APS de sucesos internos a Potencia considerando que son los incendios quienes generan un suceso interno. En contraste con el modelo selectivo, en el modelo de análisis detallado se tienen en cuenta aspectos relacionados con las características de ignición y crecimiento del incendio, las tasas de liberación

[10] Poner a *True* es equivalente a imponer la ocurrencia de un suceso.

de calor del mismo, y su propagación en términos de tiempo disponible para la extinción del mismo. En consecuencia, en el análisis detallado, los conjuntos de cables y equipos afectados por una fuente de incendio se definen de la forma más realista posible. Además, en el modelo APS detallado se añade la probabilidad de extinguir el incendio antes de que genere daños.

El método usado para modelizar la probabilidad de extinción está descrito en el Apéndice P del NUREG/CR-6850. La metodología se basa en la creación de un árbol de sucesos previo al desencadenamiento de un suceso interno. Este árbol de eventos, que se inicia con la ocurrencia de un incendio, debe contener los distintos sistemas contra incendios presentes en cada zona de análisis, que, a su vez, deben estar organizados según su lógica de actuación (antes de extinguir es necesario detectar) para modelar la probabilidad de la extinción del incendio.

12.3.5.1. Sistemas de detección y extinción

Teniendo en cuenta la gran cantidad, y las diferentes posibles combinaciones, de sistemas contra incendios descritos en el capítulo 11, y la gran cantidad de zonas de análisis, cabría esperar la necesidad de crear un modelo APS extenso y complejo para poder plasmar estos hechos. No obstante, siguiendo las directrices del NUREG/CR-6850 se pueden reducir los sistemas, o medios, contra incendios de la central a los cuatro sistemas generalistas detallados en los párrafos a continuación. Se acompaña a los sistemas con el código identificativo usado en el modelo y a lo largo de la memoria de tesis por razones de trazabilidad.

Extinción inicial (PS) Se considera que los incendios originados por actividades humanas como, por ejemplo, actividades de corte y soldadura son detectados siempre por la propia presencia humana en la zona. En consecuencia, existe la probabilidad de que el incendio sea extinguido en el inicio de su desarrollo, evitando que el mismo afecte a equipos y sistemas directa o indirectamente. El cálculo de la probabilidad de fallo en la extinción inicial depende del caso tratado.

Detección automática (PDA) En la planta hay instalados sistemas de detección automáticos como, por ejemplo, detectores térmicos, detectores ópticos de humos, detectores iónicos de humos, y otros. De acuerdo con el NUREG/CR-6850 se considera una probabilidad de fallo de 5,0E-02 para la detección automática.

Extinción automática (PEA) En la planta hay instalados sistemas de extinción automáticos como, por ejemplo, sistemas de CO_2, *sprinkler*s de preacción, sistemas de FE-13, y otros. Se considera una probabilidad de fallo para los *sprinklers* de preacción, los sistemas de agua pulverizada, espuma o nebulizada y los sistemas FE-13 de 5,0E-02. Para los sistemas de CO_2 de 4,0E-02.

Extinción por brigada contra incendios (PFB) La probabilidad de fallo de la brigada contra incendios depende directamente del caso considerado. Se calcula mediante las curvas de extinción aplicables al tipo de incendio de que se trate. En este caso se han utilizado las curvas de extinción manual contenidas en el suplemento 1 del NUREG/CR-6850 *Fire Probabilistic Risk Assessment Methods Enhancements* dentro del apartado 14 *Manual Non-Suppression Probability FAQ 08-0050* [98]. Las curvas proporcionadas en este documento recogen las probabilidades de fallo en la extinción del incendio en función del tiempo hasta daño del equipo y/o componente estudiado bajo las condiciones del incendio estudiado.

12.3.5.2. Árboles de sucesos de extinción

En el desarrollo del modelo APS de incendios detallado se utilizan dos modelos de árbol de sucesos de extinción genéricos. La principal diferencia entre los dos tipos de árboles de sucesos genéricos es el origen,

es decir, el tipo incendio. En el modelo APS detallado se consideran dos posibles tipos de incendio según su origen: incendios originados por actividades humanas de corte y soldadura, y incendios cuyo origen es distinto a actividades de corte y soldadura. Las figuras 14.2 y 14.3 muestran dos ejemplos árboles de sucesos de extinción genéricos. La diferencia entre ambos reside en la detección: en el caso de incendios originados por actividades humanas de corte y soldadura se considera que el incendio es detectado por el personal a cargo de dichas actividades.

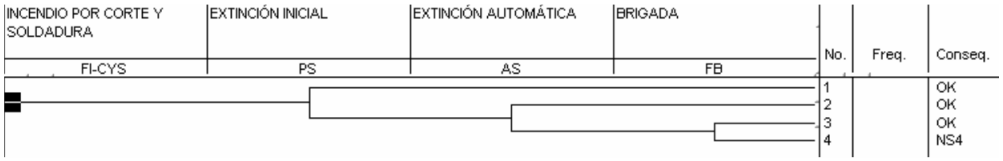


Figura 12.3: Árbol de sucesos de extinción genérico para un incendio por corte y soldadura. Fuente: Modelo APS detallado.

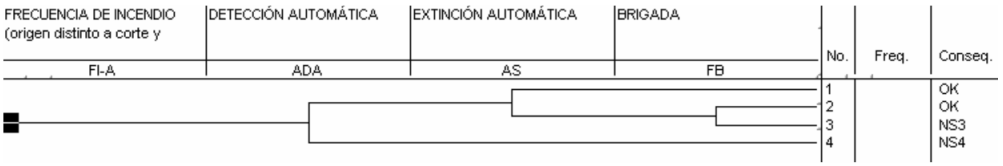


Figura 12.4: Árbol de sucesos de extinción genérico para un incendio cuyo origen es distinto a corte y soldadura. Fuente: Modelo APS detallado.

Las posibles consecuencias de los árboles de sucesos de extinción son la extinción del incendio antes de que se produzcan daños, o el fallo en la extinción, que conlleva un suceso interno y el daño de equipos que participan en la mitigación de dicho suceso interno. El éxito se representa en el ejemplo anterior con la consecuencia "OK". El fallo se representa con "NS3" y "NS4" según la evolución en el árbol. En el modelo APS final, la consecuencia del fallo en la extinción enlaza con el árbol de eventos de internos pertinente. Obsérvese que los cabeceros de los árboles se llaman PS, ADA, AS, y FB para la detección inicial (PS), detección automática (PDA), extinción automática (PEA) y extinción por brigada contra incendios (PFB) respectivamente.

12.3.5.3. Enlace entre árboles de sucesos extinción y árboles de sucesos de sucesos internos

La figura 12.5 presenta un ejemplo de enlace entre un árbol de sucesos extinción genéricos y un árbol de suceso interno.

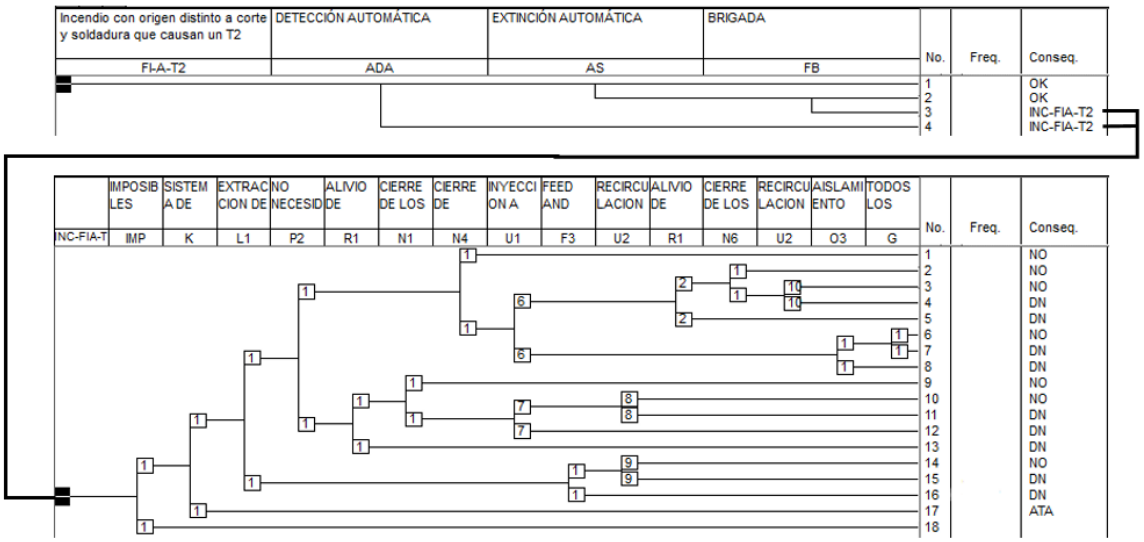


Figura 12.5: Enlace entre árboles de sucesos del modelo APS detallado.

En este ejemplo se modela la situación en la que un incendio con origen distinto a actividades de corte y soldadura provoca, de no ser extinguido, un disparo de reactor y turbina (T2). Por lo tanto, la consecuencia del fallo de la extinción, ya sea por fallo de la detección automática, o por fallo de la extinción automática y la brigada, es un disparo de reactor y turbina y se enlaza al árbol de eventos de dicho suceso interno. Las consecuencias negativas del árbol de extinción, INC-FIA-T2 en la figura 12.5, se introducen como *input* del suceso iniciador del árbol del suceso interno T2 de la figura 12.5 para ejecutar el enlace en el software *RiskSpectrum® PSA*. De esta manera, la frecuencia del suceso iniciador interno es la frecuencia de no extinción del incendio.

Los árboles contra incendios genéricos, llamados CI, que parten de incendios con origen distinto a actividades de corte y soldadura tienen en su nomenclatura el término "A". Se llaman "árboles CI-A" en la memoria de tesis para facilitar su referencia. Los árboles contra incendios genéricos que parten incendios con origen por actividades de corte y soldadura tienen en su nomenclatura el término "CYS". Se hace referencia a estos con el nombre de "árboles CI-CYS" en la memoria de tesis. Del mismo modo se usa la nomenclatura "origen A" y "origen CYS" para indicar cuando un incendio tiene como origen actividades distintas al corte y soldadura, o actividades de corte y soldadura, respectivamente.

El modelo APS detallado contiene un árbol genérico CI-A y un árbol genérico CY-CYS para cada suceso interno aplicable. Todos los árboles CI-A y CI-CYS son idénticos a los mostrados en los ejemplos de las figuras 14.2 y 14.3, respectivamente, con la diferencia de que la consecuencia del fallo de la extinción de cada árbol de extinción los enlaza con su árbol de sucesos internos correspondiente. Por lo tanto, cada árbol de sucesos de cada suceso interno se encuentra por duplicado en el modelo APS, siendo uno para orígenes "A" y otro para orígenes "CYS". Los árboles duplicados de los sucesos internos son prácticamente idénticos, la única diferencia radica en el suceso iniciador del árbol. Siguiendo la nomenclatura de los árboles contra incendios, se utilizan las siglas SI-A y SI-CYS para referenciar a los árboles de sucesos internos. La tabla 12.2 ejemplifica la duplicidad de árboles de sucesos internos.

Origen A		Origen CYS	
Suceso T2	Suceso S2	Suceso T2	Suceso S2
CI-A-T2 → SI-A-T2	CI-A-S2 → SI-A-S2	CI-CYS-T2 → SI-CYS-T2	CI-CYS-S2 → SI-CYS-S2

Tabla 12.2: Ejemplos de árboles de extinción y árboles de sucesos internos. Enlaces.

12.3.5.4. Implementación de frecuencias de incendios

El modelo APS de incendios detallado contiene dos árboles de eventos contra incendios genéricos (árbol CI-A- y árbol CI-CYS-) por cada suceso interno aplicable. Lo mismo ocurre con los árboles de eventos de sucesos internos (SI-), que se encuentran duplicados dependiendo de si el origen es A o CYS. Si en dos zonas distintas, por ejemplo, zona Z1 y zona Z2, se pueden producir incendios con origen CYS que generen, por ejemplo, un T2, los árboles CI-CYS-T2 y SI-CYS-T2 son compartidos por las zonas Z1 y Z2. No obstante, las frecuencias de incendio en la zona Z1 y la Z2 pueden ser distintas.

El primer cabecero de un árbol de eventos, que corresponde al suceso iniciador, o *input* del árbol, es una entrada a la cual se le asocia una frecuencia de ocurrencia. Esta entrada puede ser, directamente, la frecuencia de ocurrencia de un suceso interno, o bien una *top gate* de un árbol de fallos, o una consecuencia de otro árbol de eventos. Cada caso de incendio postulado en el modelo APS de incendios detallado contempla un suceso de incendio específico con una frecuencia de ocurrencia específica. Por lo tanto, si varios casos específicos comparten los mismos árboles de eventos, es decir, mismo árbol CI y SI[11], pero no las frecuencias de incendio, se deberían duplicar los árboles de eventos tantas veces como frecuencias distintas hubiese para poder analizar de forma independiente todos estos casos. Sin embargo, en el modelo APS de incendios detallado se ha optado por una solución diferente que no implica la duplicación de los árboles de sucesos genéricos asociados a un suceso interno.

Concretamente, en el modelo APS de incendios detallado se utiliza un árbol de fallos de frecuencias de incendios. La puerta superior de este árbol de fallos es el *input* o entrada de todos los árboles de sucesos contra incendios genéricos. La estructura del árbol de frecuencias de incendios se presenta de forma simplificada en la figura 12.6.

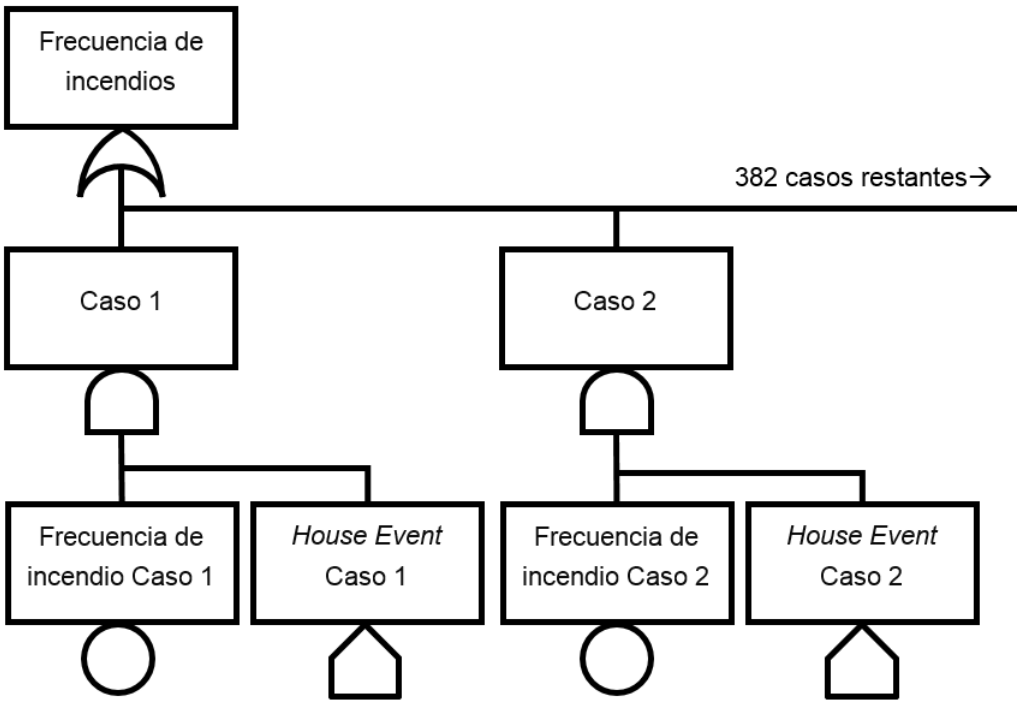


Figura 12.6: Extracto simplificado del árbol de fallos de frecuencias de incendio.

El árbol de la figura 12.6 se presenta de forma simplificada porque en el modelo real los casos se distribuyen

[11] Póngase, por ejemplo, que el suceso interno T2 puede ser causado por un incendio con origen en corte y soldadura en varias zonas de análisis. Todas estas zonas de análisis compartirían los árboles de sucesos CI-CYS-T2 y SI-CYS-T2.

en zonas, que, a su vez, se distribuyen en elevaciones de edificios, que, finalmente se agrupan por edificios. Este hecho causa que el tamaño del árbol sea considerable. A efectos prácticos, el funcionamiento del árbol simplificado es idéntico.

El árbol de fallos consta de un sumatorio (puerta OR) de todos los casos. Cada caso contiene dos tipos de eventos, un suceso básico y un *House Event* (evento casa). El suceso básico de cada caso contiene la frecuencia de ocurrencia de incendio calculada para ese caso. Un *House Event*, cualquiera que sea, tiene por defecto valor 0 o *FALSE*. Estos dos eventos son unidos mediante una puerta AND (o puerta Y, multiplicadora), que es la que representa al caso. Se obtiene por consecuencia que la puerta AND de cada caso vale 0 pues una multiplicación entre una frecuencia determinada y 0 da como resultado 0. Igualmente, sumando todos los casos (múltiples puertas AND) el resultado final sería 0. Sin embargo, los *House Event* cambian de valor de 0 a 1 (o *TRUE*) cuando se activa una condición de contorno (comúnmente llamadas *Boundary Condition Set* o *BC Set* en *RiskSpectrum® PSA*) con la que están relacionados. Las condiciones de contorno se describen en la sección 12.3.5.6 a continuación. Solo el *House Event* de uno de los caso a analizar ha de pasar al estado *TRUE* cuando se active una condición de contorno para que el árbol de fallos resulte efectivo y su puerta superior represente únicamente la frecuencia de uno de los caso de estudio. Por lo tanto, cada caso de incendio postulado en el APS está asociado a una condición de contorno única para que el árbol de fallos resulte útil. De esta manera, el árbol de fallo de frecuencias de incendio es un árbol seleccionador que toma el valor de la frecuencia del caso a analizar cuando se activa la *BC Set* de ese mismo caso.

La figura 12.7 esquematiza la relación de dependencia entre el árbol de fallos de frecuencias de incendio y los árboles de sucesos del modelo APS de incendios detallado. Un árbol de frecuencias de incendios común sirve de entrada para los árboles de sucesos contra incendios genéricos. Cada árbol de sucesos contra incendios genérico tiene asociado su árbol de sucesos internos. Diseñar el modelo APS mediante la estructura de la figura 12.7 permite evaluar todos los casos de análisis presentes en el APS mediante un número reducido de árboles de sucesos.

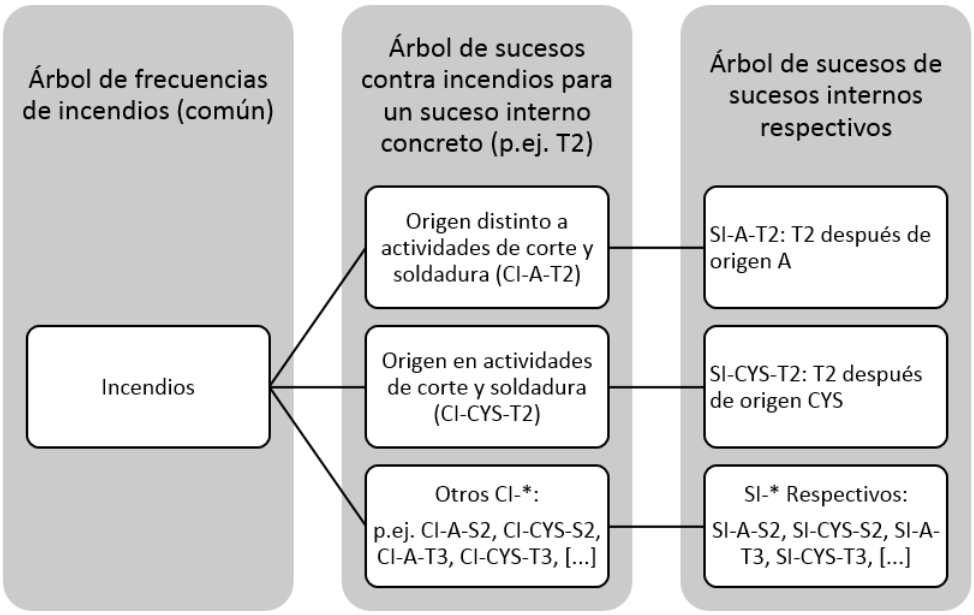


Figura 12.7: Esquema de funcionamiento enlazado del modelo APS detallado.

12.3.5.5. Cuantificación por casos de estudio. Los *consequence analysis cases*

El modelo APS de incendios detallado se crea con el software *RiskSpectrum® PSA* y en él se analizan los llamados casos de incendio. Cada caso de incendio es definido por un origen de incendio, un suceso interno generado por el incendio[12], el conjunto de equipos y componentes afectados por el incendio, y la respuesta de la central ante la situación impuesta por el caso. La frecuencia de daño al núcleo inducida por un caso de incendio se estima mediante la herramienta *Consequence Analysis Case* de *RiskSpectrum® PSA*. El modelo APS contiene tantos *Consequence Analysis Case* como casos detallados de incendio contiene. Concretamente, el modelo APS detallado de incendios contiene un total de 384 casos de incendio. En la creación de un *Consequence Analysis Case*, se han de especificar las siguientes entradas:

- Los árboles de eventos a incluir en la cuantificación. Cada incendio es de origen A o CYS, y puede provocar un suceso interno que ha sido estudiado con anterioridad[13]. Si el incendio tiene su origen en actividades de corte y soldadura y podría provocar, por ejemplo, un T2 se añaden en el *Consequence Analysis Case* los árboles de eventos CYS-T2, tanto contra incendios como de sucesos internos (CI-CYS-T2 y SI-CYS-T2).
- La consecuencia a estudiar. A cada secuencia de un árbol de sucesos se le asigna una consecuencia. En el *Consequence Analysis Case*, detallar la consecuencia a estudiar es sinónimo de indicar que se desea analizar conjuntamente todas las secuencias de accidente que llevan a la consecuencia seleccionada. En el caso de estudio, la consecuencia indiciada es DN, en referencia daño al núcleo.
- La condición de contorno del caso. Se indica la condición de contorno del caso estudiado. La condición de contorno se impone una vez obtenida la ecuación booleana del análisis.

El resultado de ejecutar un *Consequence Analysis Case* es la ecuación booleana de la frecuencia de ocurrencia de la consecuencia seleccionada así como la propia estimación cuantitativa de dicha frecuencia de ocurrencia. En el caso de seleccionarse una condición de contorno, los estados indicados en la misma sustituyen a los estados normales sobre la ecuación booleana. El límite de truncamiento impuesto en los *Consequence Analysis Case* es de 1,0E-09 año^{-1}.

12.3.5.6. Condiciones de contorno

Una condición de contorno es un conjunto de sucesos básicos con estado predefinido [14] y *House Events* que se agrupan bajo un único elemento del modelo, la propia *BC Set*. Los sucesos básicos y *House Events* del modelo APS cambian al estado predefinido en la condición de contorno cuando ésta se activa. Por lo tanto, las *BC Sets* se utilizan en el marco del APS para imponer en el modelo una situación específica de la planta o sistema analizado. En el software *RiskSpectrum® PSA*, la activación de una condición de contorno se puede asociar a la evaluación de uno o más de uno de los diferentes cabeceros de un árbol de sucesos o a la realización de un análisis de las secuencias, o las consecuencias, de un árbol de sucesos[15]. En el caso del modelo APS de incendios detallado, la activación de las condiciones de contorno de los casos de incendio se asocia al análisis de las consecuencias, *Consequence Anaylsis Case*, del caso.

Un incendio asociado a un caso de análisis, del mismo modo que puede generar un suceso interno, también puede dañar componentes o equipos necesarios en la mitigación del propio suceso interno, ya sea por

[12] Si un origen de incendio pudiese tener como consecuencia más de un suceso interno, en el modelo se generarían tantos casos como sucesos internos pudiese generar dicho origen.

[13] En una minoría de casos el incendio provoca directamente daño al núcleo.

[14] Los sucesos básicos de un APS pueden estar en uno de tres estados: *False*, Normal, o *True*. El estado normal corresponde a la probabilidad de ocurrencia del suceso.

[15] El análisis de secuencias consiste en la estimación de la frecuencia de ocurrencia de una de las secuencias de un árbol de sucesos. El análisis de consecuencias consiste en la estimación de la frecuencia de ocurrencia de una de las consecuencias de un árbol de sucesos. En el marco de un APS nivel 1, una misma consecuencia (Daño al núcleo) se asocia a diversas secuencias de un árbol de sucesos.

exposición directa del equipo o por la afectación de un cable relacionado. En las condiciones de contorno asociadas a un caso de incendio se impone que todos estos equipos afectados por el incendio estudiado se encuentran indisponibles cuando éste ocurre (en el programa se cambia el estado de los sucesos básicos que los representan de Normal a *True*). La condición de contorno asociada a un caso de incendio también incluye el *House Event* del caso de estudio. Recuérdese que el *House Event* de un caso, en estado *True*, es el que permite trasladar la frecuencia de incendio del caso concreto al cabecero del árbol de incendios (véase la figura 12.6). *RiskSpectrum® PSA* activa una condición de contorno asociada a un caso únicamente cuando se le indica que ha de cuantificar el análisis de consecuencias del caso. De esta manera, *RiskSpectrum® PSA* obtiene primero la ecuación booleana del caso objetivo y, a continuación, modifica la ecuación aplicando las condiciones indicadas en la *BC Set*.

12.3.5.7. Cuantificación por zonas. Los *MCS Analysis Cases*

Un *MCS Analysis Case* obtiene una única ecuación booleana, y, por lo tanto, un único valor de frecuencia, a partir de sumar, utilizando el álgebra booleana, las ecuaciones booleanas obtenidas en varios *Consequence Analysis Case*. Además, los *MCS Analysis Cases* permiten aplicar un post-proceso a la ecuación booleana obtenida, que corresponde a substituir unos sucesos básicos por otros siguiendo unas reglas establecidas en el propio post-proceso[16].

El análisis detallado contiene 384 casos de incendio que se reparten en 41 zonas de análisis. El APS de incendios detallado usa la funcionalidad de los *MCS Analysis Cases* para aglutinar todos los casos en sus respectivas zonas, y así estimar una única frecuencia de daño al núcleo inducida por incendios para cada zona. Existen consecuentemente tantos *MCS Analysis Cases* como zonas, 41 en total. Este dato resulta más útil que la frecuencia de un caso porque permite visualizar la distribución espacial del riesgo inducido por incendios en la planta y realizar análisis comparativos entre zonas y edificios. El límite de truncamiento impuesto en los *MCS Analysis Case* es de 1,0E-09 año^{-1}.

12.3.5.8. *Exchange events*

De forma general, todas las zonas de análisis pueden llegar a contener tantos sistemas contra incendios distintos como los definidos en la sección 12.3.5.1 anterior. Además, cada categoría de las definidas en la sección 12.3.5.1 abarca diversos sistemas contra incendios específicos, véase el capítulo 11 anterior para más detalle, que son los que realmente están instalados en las diferentes zonas de incendio de la planta. A pesar de su cantidad y su diversidad, la representación de la probabilidad de fallo de sistemas contra incendios en el modelo APS de incendios detallado se reduce a dos cabeceros genéricos, PDA y PEA, en los árboles CI-A y a un cabecero genérico, PEA, en los árboles CI-CYS (véase la sección 12.3.5.2 anterior). También sería necesario contemplar distintas opciones, dependiendo del origen de incendio y de otros factores[17], para representar la probabilidad de fallo de la extinción inicial (PS) y la probabilidad de fallo de la extinción por brigada contra incendios (PFB), que también reciben un tratamiento genérico en el modelo. Por lo tanto, el modelo APS de incendios detallado, tal y como ha sido descrito hasta el momento, es conservador pues no incluye ni la variedad de sistemas contra incendios, ni las distintas opciones a contemplar para representar la extinción inicial y la brigada en sus árboles de sucesos de extinción genéricos.

[16] El post-proceso se acostumbra a utilizar para introducir los resultados del análisis de dependencias entre sucesos de fallo humano, que se realiza a posteriori de la primera cuantificación. En el análisis de dependencias se identifica, en primer lugar, qué MCS contienen más de un suceso básico de fallo humano. Se analiza si existe, y en qué grado, dependencia entre los sucesos básicos de fallo humano que comparten MCS, y se propone un nuevo valor de probabilidad de ocurrencia para el último de ellos. Este valor de probabilidad de ocurrencia, que tiene en cuenta el grado de dependencia entre los sucesos, sería el que substituyese al suceso básico en el post-proceso.

[17] El tiempo disponible para realizar la extinción inicial o la extinción por brigada depende, entre otros, de la severidad del incendio, la localización, el tipo de incendio, y el tipo de componente quemado.

Se utilizan los denominados *Exchange Events* para introducir la diversidad de sistemas contra incendios y la diversidad de opciones para representar la extinción inicial y la brigada en el modelo APS de incendios detallado. Un *Exchange Event* es un suceso básico que sustituye a otro en el modelo APS cuando un *House Event,* relacionado con el *Exchange Event,* cambia a valor *TRUE* al activarse una *BC Set*. Un suceso básico puede estar relacionado con diferentes *Exchange Events*, que sustituirán al suceso básico original cuando su *House Event* relacionado pase a ser *TRUE* (véase la figura 12.8). El APS de incendios detallado presenta *Exchange Events* para cada caso de incendio estudiado. Los sucesos básicos genéricos de los cabeceros de los árboles de sucesos de extinción se sustituyen por los sucesos básicos que mejor representen los sistemas contra incendios de un caso de incendio al pasar a *TRUE* el *House Event* del caso de incendio estudiado debido a la activación de la *BC Set* impuesta en su *Consequence Analysis Case*. El paso a *TRUE* de un *House Event* puede implicar la sustitución de varios sucesos básicos por *Exchange Events*. Por lo tanto, se necesita tan solo un único *House Event* por cada caso de estudio para introducir todos los sucesos básicos específicos de los sistemas contra incendios del caso. El *House Event* de aplicación de *Exchange Events* es el mismo que se utiliza para seleccionar la frecuencia de incendio del caso estudiado. De esta manera, cada caso de estudio tiene un único *House Event* asociado. El uso de *Exchange Events* permite obtener resultados específicos de frecuencia de daño al núcleo inducida por incendios mediante el modelo APS de incendios detallado descrito en las secciones anteriores.

Se presenta, a modo de ejemplo, un extracto del programa *RiskSpectrum® PSA* en la figura 12.8. La figura 12.8 presenta los *Exchange Events* del suceso básico genérico INC-PFB, que hace referencia a la probabilidad de fallo por extinción de brigada. El suceso INC-PFB se sustituye por el correspondiente suceso básico de la columna *Exch. Event* al pasar a *TRUE* los *House Events* presentes en la primera columna de la figura.

Figura 12.8: Ejemplo de Exchange Events extraídos del modelo creado en RiskSpectrum® PSA.

12.3.5.9. Cuantificación de la frecuencia total de daño al núcleo

La cuantificación de la frecuencia total de daño al núcleo inducida por incendios de la central ($FDN^{incendios}$), véase la ecuación (L.3), se obtiene del sumatorio de las frecuencias de daño al núcleo de todas las zonas analizadas en el modelo APS detallado.

$$FDN^{incendios} = \sum_{i=1}^{41} MCS\ Analysis\ Case\ zona\ i \tag{12.3}$$

La frecuencia total de daño al núcleo inducida por incendios de la central es de 9,836E-06 año^{-1} para la central caso de estudio. Cada zona de análisis contribuye con su frecuencia de daño al núcleo inducida por incendios al valor total de la FDN de incendios de la central. Por este motivo, en distintas secciones de esta memoria de tesis se utiliza el término «contribución a la FDN de incendios» para hacer referencia a la frecuencia de daño al núcleo que aporta una zona de análisis o un conjunto de ellas. Al tener la cuantificación por zonas de análisis en el modelo APS de incendios detallado en *RiskSpectrum® PSA*, también es posible obtener la cuantificación de la FDN inducida por incendios de cada uno de los edificios de la central.

Capítulo 13

Desarrollo de las herramientas. Análisis matricial

13.1. Introducción

El capítulo 13 de la tercera parte de la memoria de tesis presenta las herramientas desarrolladas para evaluar cuantitativamente el riesgo inducido por incendios e incorporarlo en las prácticas habituales de evaluación de configuraciones de planta llevadas a cabo en el marco de la regla de mantenimiento en una central nuclear. Concretamente, el presente capítulo contiene la definición y justificación de las herramientas diseñadas, sección 13.2, y la descripción de las metodologías seguidas para diseñar dichas herramientas, secciones 13.3 y 13.4. Queda fuera de alcance de este capítulo la descripción de la metodología de cuantificación de las herramientas, que se expone íntegramente en el capítulo 14.

13.2. Definición y justificación de las herramientas diseñadas

El proyecto llevado a cabo en el marco de la tercera parte de esta tesis doctoral tiene por objetivo diseñar y desarrollar herramientas novedosas para la evaluación cuantitativa del riesgo de daño al núcleo inducido por incendios y su posterior incorporación en procesos de decisión informados por el riesgo. Específicamente, las herramientas aquí descritas se han diseñado con el objetivo de dar soporte a procesos de decisión relacionados con la evaluación de configuraciones de planta[1], y a procesos de decisión relacionados con el mantenimiento de componentes como lo es, concretamente, la regla de mantenimiento. Tal y como se ha visto en el capítulo de introducción, capítulo 10, que las herramientas proporcionen una valoración cuantitativa del riesgo de daño al núcleo inducido por incendios es un hecho diferencial, y novedoso, con respecto a las metodologías actualmente utilizadas. El análisis probabilista de seguridad es la aplicación ideal para obtener una valoración cuantitativa el riesgo de daño al núcleo puesto que cuantificar este riesgo es su principal objetivo. En consecuencia, el uso de un modelo APS de incendios para la valoración cuantitativa del riesgo inducido por incendios es condición *sine qua non* en el diseño y en el desarrollo de las herramientas definidas en este capítulo. Como en el resto de procesos de decisión, el APS de incendios utilizado para valorar riesgo ha de cumplir con los estándares de calidad del organismo regulador competente o, en su defecto, con los estándares de calidad descritos en la *Regulatory Guide* 1.200 de la NRC. Cabe recordar que, si no se han desarrollado hasta el momento este tipo de herramientas, ha sido por la

[1] En los procesos de decisión al respecto de configuraciones de planta se decide si una configuración, es decir, un conjunto de estados predefinidos de varias estructuras, sistemas, y componentes, es admisible desde el punto de vista de la seguridad. Una configuración es admisible si no está asociada a un riesgo inaceptable.

falta de APS de incendios en la industria. Dicha carencia esta siendo subsanada, en Estados Unidos, por la aplicación voluntaria de la NFPA-805. y, en otros países, por la implantación de reglas que imponen el desarrollo del análisis probabilista de seguridad [50].

Las herramientas desarrolladas en esta parte de la tesis se diseñan mediante análisis matricial, siendo su forma final la de una matriz bidimensional. El principal motivo por el que se ha decidido utilizar el análisis matricial bidimensional de riesgos o de variaciones de riesgo es que permite estudiar, con una sola matriz, tanto casos individuales (la indisponibilidad de un componente), como combinaciones de dos casos individuales (la indisponibilidad de dos componentes a la vez). Además, el producto del análisis matricial, la matriz, es una herramienta que facilita tanto la localización rápida de resultados como el posterior tratamiento de los resultados obtenidos. La utilización del análisis matricial en el desarrollo de herramientas de valoración, tanto cualitativa como cuantitativa, de riesgos es recurrente en el ámbito de los procesos de decisión informados por el riesgo.

La primera de las herramientas desarrolladas es la llamada matriz MCI: matriz de compatibilidades de indisponibilidades de sistemas contra incendio y funciones clave de seguridad. Dicha matriz contiene, como resultado, la frecuencia de daño al núcleo inducida por incendios de la central obtenida al combinar la indisponibilidad de sistemas contra incendios y funciones clave de seguridad[2]. La matriz MCI sirve para identificar aquellas ESCs cuya indisponibilidad tiene un impacto significativo en el riesgo inducido por incendios. En consecuencia, la inclusión de dichas ESCs en la regla de mantenimiento y en la evaluación de configuraciones de planta debería tomarse en consideración. De la misma manera, la matriz MCI sirve para identificar aquellos sistemas contra incendios que podrían incluirse en la regla de mantenimiento porque su indisponibilidad tiene un impacto significativo en el riesgo. Además, la matriz MCI también es útil para evaluar las combinaciones de indisponibilidad de sistemas contra incendio y funciones clave de seguridad, lo que también supone información valiosa para la aplicación de la regla de mantenimiento y las tareas de gestión del riesgo. Concretamente, la matriz permite conocer qué sistemas contra incendios habría que tener bajo vigilancia durante el mantenimiento de un equipo debido a que la indisponibilidad combinada de ambos, el sistema contra incendios y el equipo, pondría la central en un nivel de riesgo inaceptable. El diseño de esta matriz y la metodología seguida para obtenerla se detallan en la sección 13.3.

La segunda herramienta diseñada es la matriz MRI: matriz de riesgo de incendio de zonas de incendio y funciones clave de seguridad. Esta matriz incluye la contribución de cada zona de incendio a la frecuencia de daño al núcleo de la central, es decir, la frecuencia de daño al núcleo debida únicamente a incendios que puedan ocurrir en la zona estudiada, condicionada a la indisponibilidad de ESCs representativos de funciones claves de seguridad. La matriz MRI proporciona también información valiosa para la aplicación del mantenimiento y las tareas de gestión del riesgo. La matriz MRI permite identificar qué zonas de incendio son las más significativas para el riesgo inducido por incendios de la central o, de forma más precisa, en qué zonas de incendio de la planta se deberían aplicar acciones para gestionar y reducir el riesgo inducido por incendios en caso de indisponibilidad de un equipo representativo de funciones claves de seguridad de la central. El diseño de esta matriz y la metodología seguida para obtenerla se detallan en la sección 13.4.

13.3. Diseño de la matriz MCI

La matriz MCI contiene la frecuencia de daño al núcleo inducida por incendios para diversas combinaciones de indisponibilidad de sistemas contra incendios y funciones clave de seguridad. Por lo tanto, la filas y columnas de la matriz han de estar relacionadas con los sistemas contra incendios y con las funciones clave de seguridad de la central, respectivamente. A raíz de que existen más sistemas contra incendios que funciones clave de seguridad, se ha decidido que las filas de la matriz estén relacionadas con los sistemas

[2]También incluye los casos de indisponibilidad individual. Es decir, la matriz también valora de forma individual e independiente la indisponibilidad de sistemas contra incendios, y la indisponibilidad de funciones clave de seguridad

contra incendios y las columnas con las funciones clave de seguridad para facilitar la visualización de resultados.

13.3.1. Filas: sistemas contra incendio

El modelo APS de incendios detallado abarca el análisis de 41 zonas de incendio, cada una con sus respectivos sistemas contra incendios. Se considera que los sistemas contra incendios de las zonas de incendio de la central son independientes entre sí, por lo que la indisponibilidad de uno de ellos no implica la indisponibilidad de otros. Por lo tanto, la matriz MCI ha de contener una fila por cada uno de los sistemas contra incendios incluidos en el modelo APS de incendios detallado. Cada uno de estos sistemas contra incendios se incluye en uno de los cuatro tipos genéricos de sistema contra incendios definidos en el capítulo 6: extinción inicial, detección automática, extinción automática, y brigada contra incendios. Cada fila de la matriz se relaciona con uno de estos tipos genéricos de sistema contra incendios y con una zona de análisis de la planta. De esta manera, se facilita la comprensión, a simple vista, de los resultados de la matriz. Se aprecia en la figura 13.1 de la sección 13.1, que presenta el diseño final de la matriz MCI, la forma de introducir los sistemas contra incendio en dicha matriz. La matriz MCI cuenta con 167 filas relacionadas con sistemas contra incendios y con una para representar el estado de la central en el que todos los sistemas contra incendios están disponibles.

13.3.2. Columnas: funciones clave de seguridad

La funciones de seguridad fundamentales para la implantación del concepto de defensa en profundidad en una central nuclear son: el control de la reactividad, la extracción del calor del núcleo del reactor, y el confinamiento de los materiales radiactivos [1]. El cumplimiento de estas funciones de seguridad en todos los modos de operación evita la iniciación y/o progresión de secuencias accidentales. En el marco del diseño de la matriz MCI, las funciones de seguridad fundamentales se representan mediante seis funciones clave de seguridad para describir y analizar con más detalle la seguridad de la central. Estas seis funciones clave de seguridad son:

- Subcriticidad (control de reactividad).
- Refrigeración del reactor.
- Disponibilidad del sumidero de calor.
- Integridad del sistema de refrigeración del reactor.
- Inventario del sistema de refrigeración del reactor.
- Suministro eléctrico.

La función clave de seguridad de subcriticidad es equivalente a la función de seguridad fundamental de control de la reactividad. Las funciones de refrigeración del reactor, disponibilidad del sumidero de calor, y de inventario del sistema de refrigeración del reactor se han de mantener para garantizar que se cumple la función fundamental de extracción del calor del núcleo. La función clave de seguridad de integridad del sistema de refrigeración del reactor hace referencia al confinamiento de los materiales radiactivos. La integridad del Edificio de Contención no se incluye como función clave de seguridad a analizar porque el APS de incendios es de nivel 1 y, por lo tanto, no la analiza. Pese a tratarse de un sistema soporte, se incluye el suministro eléctrico como función clave de seguridad porque un fallo o indisponibilidad de dicha función podría poner en peligro el cumplimiento de las tres funciones fundamentales, tanto a la vez como de forma separada.

13.3.2.1. Representación de las funciones clave de seguridad

Las seis funciones clave de seguridad a analizar no se pueden asociar directamente con las columnas de la matriz MCI por dos principales razones. En primer lugar, porque su indisponibilidad podría darse de maneras diferentes. Habría que identificar, para cada caso, cuál es la configuración de planta más probable en la que una de las funciones clave de seguridad está totalmente indisponible. Dado el nivel de detalle de un APS, en el que la planta está descrita a nivel de componentes en árboles de fallo de sistemas y funciones de seguridad, realizar estudios a nivel de funciones clave de seguridad no sería una tarea trivial. Además, la introducción directa de las funciones clave de seguridad en las columnas de la MCI complicaría la extracción de conclusiones válidas para procesos de decisión orientados al mantenimiento, puesto que se debería profundizar en el análisis para saber qué componentes están, de hecho, indisponibles. En segundo lugar, porque la indisponibilidad total de una función clave de seguridad puede suponer la merma de otras funciones, especialmente en aquellas que aseguran el cumplimiento de la misma función fundamental de seguridad. Por lo tanto, en estos casos, la importancia en el riesgo inducido por incendios de la indisponibilidad total de una función clave de seguridad estaría sesgado por la merma de otras funciones. En consecuencia, se ha de realizar un análisis previo de las funciones clave de seguridad para poder introducirlas en la matriz MCI.

Las funciones fundamentales de seguridad, y, por lo tanto, las funciones claves de seguridad, se descomponen en diversas funciones de seguridad en el marco de los análisis probabilista de seguridad. Estas funciones de seguridad son más numerosas y versátiles[3], pues se definen en función de los procedimientos y acciones que se han de llevar a cabo para asegurar el cumplimiento de las funciones clave de seguridad. Incluso, las funciones de seguridad pueden tener diferentes variantes dependiendo de si existen diferentes configuraciones o formas para cumplirlas. Por ejemplo, una de las funciones de seguridad es la extracción del calor del secundario, que tiene como variantes, entre otras, la extracción de calor mediante la turbobomba del sistema de agua de alimentación auxiliar o, en su defecto, con una de sus motobombas.

En el marco de un modelo APS, las funciones de seguridad se introducen normalmente como cabeceros de los árboles de sucesos y se modelizan mediante árboles de fallo. Tal y como se ha descrito con anterioridad en el capítulo 2, los árboles de fallo son estructuras lógico-deductivas formadas por una sucesión de puertas lógicas y sucesos básicos, que permiten estimar la probabilidad de fallo o indisponibilidad del sistema o función representados. Los sucesos básicos, que, siendo independientes entre sí, representan la indisponibilidad o el fallo de componentes, son la unidad elemental de los árboles de fallo. En consecuencia, los sucesos básicos son también la unidad representativa más elemental de la indisponibilidad de las funciones de seguridad, las funciones clave de seguridad, y las funciones fundamentales de seguridad. Teniendo en cuenta que los sucesos básicos son representativos de la indisponibilidad de las funciones clave de seguridad y de la indisponibilidad de componentes, se ha decidido relacionar las columnas de la matriz con los sucesos básicos más representativos de las funciones clave de seguridad. Se ha de tener en cuenta que no todos los sucesos básicos tienen la misma importancia o impacto en la indisponibilidad de una función clave de seguridad, y que algunos están asociados a la indisponibilidad de varias funciones clave de seguridad a la vez. Por lo tanto, se ha de realizar un análisis para seleccionar los sucesos básicos más representativos de cada función clave de seguridad.

13.3.2.2. Análisis selectivo de sucesos básicos representativos de las funciones clave de seguridad

El análisis selectivo de sucesos básicos representativos de las funciones clave de seguridad se basa en la herramienta de análisis de importancia del APS. El análisis de importancia clasifica los sucesos básicos participantes en una ecuación booleana según el valor de unas figuras, llamadas medidas de importancia, que representan la influencia del propio suceso en la frecuencia o indisponibilidad estimada mediante la

[3] Una misma función clave de seguridad se podría descomponer en diversos paquetes de funciones de seguridad. Además, su alcance es reducido.

ecuación booleana. Los sucesos básicos que encabezan el análisis de importancia son los que más influyen en la frecuencia o indisponibilidad objetivo y, por lo tanto, son los más representativos de la misma. En consecuencia, realizando este tipo de análisis se podrían obtener los sucesos básicos más representativos de las funciones clave de seguridad a analizar.

En el caso del diseño de la matriz MCI, se han realizado análisis de importancia para la indisponibilidad de cada cabecero, es decir, cada función de seguridad, presente en el APS de incendios. Normalmente, los análisis de importancia cuyo objetivo es identificar los sucesos básicos más influyentes se aplican a la ecuación booleana de la frecuencia de daño al núcleo total. No obstante, mediante el procedimiento seguido es más sencillo, por una parte, relacionar sucesos básicos con la función a la que representan[4] y, por otra parte, obtener sucesos básicos únicamente relacionados con la indisponibilidad de una función de seguridad. Sin embargo, como contrapartida, el análisis es más extenso. Los análisis de importancia contienen todos los sucesos básicos incluidos en una ecuación booleana, así que para escoger los más representativos se ha de establecer algún tipo de criterio cuantitativo sobre las medidas de importancia. En este caso, se ha decidido que los sucesos básicos representativos son aquellos cuya medida de importancia RAW[5] (*Risk Achivement Worth*, veáse el anexo Ñ para más detalle) es mayor o igual a diez (10). El límite de cribado es mayor que el utilizado en análisis en los que se estudia la ecuación booleana total, donde acostumbra a utilizarse un límite de dos (2), porque las ecuaciones booleanas de los árboles de fallo de los cabeceros son de menor alcance. Al incluir menos sucesos básicos, las medidas de importancia toman valores más altos. Se considera que con un límite de cribado para el RAW igual a diez (10) se obtienen únicamente sucesos básicos representativos de las funciones de seguridad. Cada lista de sucesos básicos representativos de un cabecero se completa con sucesos básicos representativos de componentes significativos para el cumplimiento[6] de la función de seguridad analizada, siempre y cuando no haya ninguno ya entre los elegidos, para asegurar que la MCI no obvia componentes importantes para el cumplimiento de las funciones.

En el diseño de la matriz MCI se obtiene un listado de sucesos básicos representativos de cada cabecero del APS. Los listados de aquellos cabeceros que son variantes de la misma función de seguridad se unen en único listado. Con el objetivo de reducir el alcance del análisis, se eliminan de estas listas, dejando un único representante, aquellos sucesos básicos cuya influencia sobre una función de seguridad es la misma por razones funcionales. Las principales razones funcionales por las que dos o más sucesos básicos deberían tener la misma importancia son: porque hagan referencia al mismo componente[7], porque hagan referencia a componentes que están en serie en un tren, o porque hagan referencia a componentes redundantes entre trenes o entre sistemas[8].

Los listados de sucesos básicos representativos de las funciones de seguridad del APS se unen en un último listado conjunto. De este último conjunto se elimina todo suceso básico repetido puesto que la repetición implica que es representativo de más de una función de seguridad. De esta manera, se obtiene un conjunto de sucesos básicos que son lo más significativos posible, lo más exclusivos posible, y que no omiten ninguna función clave de seguridad. El listado final contiene 27 sucesos básicos representativos de funciones clave de seguridad. Las tablas 13.1 y 13.2 contienen dicho listado[9].

[4] Si se realizase un único análisis de importancia, habría que, a posteriori, identificar qué funciones de seguridad representan los sucesos básicos. Este análisis implicaría el estudio del diseño del modelo APS.

[5] La medida de importancia RAW índica cuanto aumentaría la frecuencia o indisponiiblidad de la ecuación booleana del caso de estudio en caso de que el suceso básico analizado hubiese sucedido.

[6] Por ejemplo, en el caso de una de las variantes de la función de seguridad de extracción de calor del secundario en las que se requiera la actuación de una bomba, se incluye uno de los sucesos básicos de la bomba o bombas si no hay ninguno entre los más representativos.

[7] Por ejemplo, sucesos básicos de fallo al cierre y fallo a la apertura de una misma válvula.

[8] Solo si las configuraciones son equiprobables. En el caso que no lo sean, uno de los sucesos básicos predominará sobre el resto. Por lo tanto, es mejor incluir todos los sucesos básicos para evitar descartar el de mayor influencia.

[9] Por motivos de confidencialidad, se omite parte del código de identificación de los sucesos básicos.

Suceso básico	Identificador	Componente / función / Sistema	Función clave de seguridad
1VMXXXXXO	SB1	Válvula en el camino de inyección de los acumuladores.	Refrigeración del reactor
1VRXXXXXA	SB2	Válvula en el camino de inyección de los acumuladores.	Refrigeración del reactor
1BMXXXXXS	SB3	Bomba motorizada A del sistema AAA (Agua de Alimentación Auxiliar).	Disponibilidad del sumidero de calor
1BMXXXXXS	SB4	Bomba motorizada B del sistema AAA.	Disponibilidad del sumidero de calor
1TBXXXXXS	SB5	Turbobomba del sistema AAA.	Disponibilidad del sumidero de calor
1BHXXXXXF	SB6	Una de las principales barras de suministro eléctrico.	Suministro eléctrico
1BHXXXXXF	SB7	Una de las principales barras de suministro eléctrico.	Suministro eléctrico
1BLXXXXXF	SB8	Barra de distribución de suministro eléctrico.	Suministro eléctrico
1BLXXXXXF	SB9	Barra de distribución de suministro eléctrico.	Suministro eléctrico
1GDXXXXS	SB10	Generador diésel. Suministro eléctrico de emergencia.	Suministro eléctrico
1BMXXXXR	SB11	Bomba A del sistema de inyección de seguridad de alta presión	Inventario del sistema de refrigeración del reactor
1BMXXXXR	SB12	Bomba B del sistema de inyección de seguridad de alta presión	Inventario del sistema de refrigeración del reactor
1VRXXXXA	SB13	Válvula en el sistema de inyección de seguridad de alta presión (tercer lazo)	Inventario del sistema de refrigeración del reactor

Tabla 13.1: Listado de sucesos básicos representativos de funciones clave de seguridad (1).

Suceso básico	Identificador	Componente / función / Sistema	Función clave de seguridad
1VRXXXXXA	SB14	Válvula en el sistema de inyección de seguridad de alta presión (segundo lazo)	Inventario del sistema de refrigeración del reactor
1VCXXXXXA	SB15	Válvula de alivio de la línea principal de vapor	Integridad del sistema de refrigeración del reactor
1VCXXXXXC	SB16	Válvula de alivio de la línea principal de vapor	Integridad del sistema de refrigeración del reactor
1BDXXXXXR	SB17	Bomba de prueba hidrostática del sistema de inyección de emergencia al núcleo	Inventario del sistema de refrigeración del reactor
1VMXXXXXO	SB18	Válvula en la inyección a sellos del sistema de inyección de emergencia al núcleo	Inventario del sistema de refrigeración del reactor
1VAXXXXXA	SB19	Válvula de seguridad del presionador	Integridad del sistema de refrigeración del reactor
1VPXXXXXA	SB20	Válvula de alivio del presionador	Integridad del sistema de refrigeración del reactor
1VPXXXXXC	SB21	Válvula de alivio del presionador	Integridad del sistema de refrigeración del reactor
1VPXXXXXA	SB22	Válvula de alivio del presionador	Integridad del sistema de refrigeración del reactor
1BMXXXXXR	SB23	Bomba A del sistema de evacuación del calor residual	Refrigeración del reactor
1BMXXXXXR	SB24	Bomba B del sistema de evacuación del calor residual	Refrigeración del reactor
1BMXXXXXS	SB25	Bomba A del sistema de agua de servicio de salvaguardias	Disponibilidad del sumidero de calor
1BMXXXXXR	SB26	Bomba B del sistema de agua de servicio de salvaguardias	Disponibilidad del sumidero de calor
1VNXXXXXA	SB27	Válvula del sistema de agua de servicio de salvaguardias	Disponibilidad del sumidero de calor

Tabla 13.2: Listado de sucesos básicos representativos de funciones clave de seguridad (2).

13.3.3. Diseño final de la matriz MCI

La figura 13.1 presenta el diseño definitivo de la matriz MCI. El acrónimo SB utilizado hace referencia a suceso básico. La matriz incluye una fila para representar la situación en que ninguno de los sistemas contra incendios está indisponible. A su vez, la matriz incluye una columna para representar la situación en la que ninguno de los componentes representativos de funciones clave de seguridad está indisponible. Por lo tanto, el elemento (1,1) de la matriz es la frecuencia de daño al núcleo inducida por incendios de la central en condiciones normales de funcionamiento. La matriz MCI contiene 4704 elementos en 168 filas y 28 columnas.

		OK	SB1	SB2	SB3	...	SBn
OK		$FDN_{(OK, OK)}$	$FDN_{(OK, SB1)}$	...	...	...	...
Zona A	PDA	$FDN_{(A\text{-}PDA, OK)}$	$FDN_{(A\text{-}PDA, SB1)}$	...	...	...	...
	PS	$FDN_{(A\text{-}PS, OK)}$	$FDN_{(A\text{-}PS, SB1)}$	...	...	...	...
	PEA	$FDN_{(A\text{-}PEA, OK)}$	$FDN_{(A\text{-}PEA, SB1)}$	...	...	...	...
	PFB	$FDN_{(A\text{-}PFB, OK)}$	$FDN_{(A\text{-}PFB, SB1)}$	...	...	...	...
Zona B	PDA	$FDN_{(B\text{-}PDA, OK)}$	$FDN_{(B\text{-}PDA, SB1)}$	...	...	...	...
	PS	$FDN_{(B\text{-}PS, OK)}$	$FDN_{(B\text{-}PS, SB1)}$	...	...	...	...
	PEA	$FDN_{(B\text{-}PEA, OK)}$	$FDN_{(B\text{-}PEA, SB1)}$	...	...	...	...
	PFB	$FDN_{(B\text{-}PFB, OK)}$	$FDN_{(B\text{-}PFB, SB1)}$	...	...	...	...

Figura 13.1: Diseño final de la matriz MCI.

13.4. Diseño de la matriz MRI

La matriz MRI contiene la contribución de cada zona de incendio a la frecuencia de daño al núcleo de la central, es decir, la frecuencia de daño al núcleo debida únicamente a incendios que puedan ocurrir en la zona estudiada, condicionada a la indisponibilidad de ESCs representativos de funciones claves de seguridad. Por lo tanto, la filas y columnas de la matriz han de estar relacionadas con las zonas de incendio de la central y con ESCs representativos de las funciones clave de seguridad de la central, respectivamente. En este caso, se ha decidido que las zonas de incendio ocupen las filas de la matriz y que, por lo tanto, las ESCs representativos de las funciones clave de seguridad se relacionen con las columnas de la matriz MRI.

13.4.1. Filas: zonas de incendio

La matriz MRI tiene una fila por cada una de las 41 zonas de incendio analizadas en el APS detallado de incendios. Además, la matriz también incluye dos filas auxiliares: una para introducir la frecuencia total de daño al núcleo inducida por incendios de la central, y otra para incluir el tiempo de exposición de la central. El tiempo de exposición se define como la cantidad de tiempo que ha de pasar para que el incremento de probabilidad de daño al núcleo de la central asociado a un estado anormal o anómalo de la misma supere el umbral de 1,0E-06[10]. Un estado anormal de planta es más o menos significativo desde el punto de vista del riesgo dependiendo del tiempo de exposición asociado, llegándose a poder declarar que un estado anormal de planta es inaceptable si el tiempo de exposición es menor que el tiempo necesario para restablecer la operación normal [64] de la central. Cada columna de la matriz MRI describe un estado de planta diferente en el que una ESCs representativa de una función clave de seguridad está indisponible. Por lo tanto, ambas filas auxiliares proporcionan información adicional que permite valorar la importancia, desde el punto de vista del riesgo, de los estados y configuraciones de planta descritos por las columnas. De esta manera, la matriz MRI permite identificar qué zonas de incendio son realmente significativas para el riesgo inducido por incendios de la central. La introducción de las filas auxiliares evita que se declaren como significativas para el riesgo zonas cuya contribución significativa a la FDN se

[10] Valor umbral normalmente utilizado para identificar estados anormales de planta significativos para el riesgo [46].

da en estados o configuraciones de planta no significativos desde el punto de vista del riesgo inducido por incendios.

13.4.2. Columnas: ESCs representativas de funciones clave de seguridad de la central

Puesto que las estructuras, sistemas, y componentes de la central se introducen en el APS mediante sucesos básicos[11], las columnas de la matriz MRI se relacionan con sucesos básicos del modelo APS. Los sucesos básicos a introducir en el diseño de la matriz MRI han de ser representativos de ESCs que, a su vez, han de ser representativas de funciones clave de seguridad. El análisis necesario para seleccionar sucesos básicos que cumplan dichas condiciones ya ha sido realizado en el marco del diseño de la matriz MCI. Por lo tanto, las columnas de la matriz MRI se relacionan con los 27 sucesos básicos representativos de funciones clave de seguridad seleccionados en el diseño de la matriz MCI.

13.4.3. Diseño final de la matriz MRI

La figura 13.2 presenta el diseño definitivo de la matriz MRI. El acrónimo dFDN hace referencia a la contribución de una zona de incendio a la frecuencia de daño al núcleo inducida por incendios de la central. El elemento (1,1) de la matriz es la frecuencia de daño al núcleo inducida por incendios de la central en condiciones normales de funcionamiento.

	OK	SB1	SB2	SB3	...	SBn
FDN total	$FDN_{(TOT,OK)}$	$FDN_{(TOT,SB1)}$	...	...	...	...
Tiempo de exposición	$TE_{(TOT,OK)}$	$TE_{(TOT,SB1)}$	...	...	...	...
Zona A	$dFDN_{(A,OK)}$	$dFDN_{(A,B1)}$	...	...	...	...
Zona B	$dFDN_{(B,OK)}$	$dFDN_{(B,B1)}$	...	...	...	...
Zona C	$dFDN_{(C,OK)}$	$dFDN_{(C,B1)}$	...	...	...	...
Zona D	$dFDN_{(D,OK)}$	$dFDN_{(D,B1)}$	...	...	...	...

Figura 13.2: Diseño final de la matriz MRI. Matriz ejemplo.

[11] Los sistemas se modelan con árboles de fallos que están formados por sucesos básicos.

Capítulo 14

Cuantificación de las matrices MCI y MRI

14.1. Introducción

El presente capítulo detalla las metodologías de cuantificación seguidas para calcular los elementos de las matrices MCI y MRI en las secciones 14.2 y 14.3, respectivamente. La cuantificación de los elementos de estas matrices se basa en el uso del software *RiskSpectrum® PSA* y en la ejecución de scripts en Python™. Por una parte, el software *RiskSpectrum® PSA* permite obtener las contribuciones a la frecuencia de daño al núcleo inducida por incendios de la central, es decir, las dFDN, de las zonas de incendio condicionadas a los diferentes estados de planta definidos por las filas y las columnas de las matrices. Por otra parte, los scripts en Python™ ejecutan la base matemática de cálculo, presentada en la sección 14.2.1, de tal manera que los elementos de las matrices se calculan de forma rápida, véase la sección 14.2.3, a partir de las dFDN obtenidas mediante *RiskSpectrum® PSA*. No es objetivo de este capítulo presentar los resultados obtenidos en el proceso de cuantificación. Los resultados de la cuantificación, y, por extensión, del análisis matricial, se presentan en el capítulo 15.

14.2. Cuantificación de la matriz MCI

14.2.1. Base matemática

El APS de incendios detallado estudia 384 casos de incendio que se reparten en 41 zonas de análisis. El modelo APS de incendios detallado usa la funcionalidad de los *MCS Analysis Cases* para aglutinar todos los casos en sus respectivas zonas, y así estimar una única frecuencia de daño al núcleo inducida por incendios para cada zona de análisis. La frecuencia total de daño al núcleo de la planta inducida por incendios se obtiene del sumatorio de las frecuencias de daño al núcleo de todas las zonas analizadas en el modelo APS detallado (véase la ecuación L.1).

$$FDN^{incendios} = \sum_{i=1}^{41} MCS\,Analysis\,Case\,zona\,i = \sum_{i}^{41} dFDN_i \tag{14.1}$$

Los elementos de la matriz MCI representan estados o configuraciones particulares de planta en los que un sistema contra incendios y/o un componente representativo de una función clave de seguridad están indisponibles. Las particularidades de estos estados o configuraciones de planta se han de tener en

consideración al cuantificar las dFDN de las zonas de incendio mediante el modelo APS desarrollado en *RiskSpectrum® PSA*. La sección 14.2.2 a continuación detalla el procedimiento a seguir para obtener las dFDNs asociadas a uno de los elementos de la matriz. Una vez obtenidas las dFDN asociadas a un elemento de la matriz, la FDN inducida por incendios asociada a este elemento se calcula utilizando la ecuación L.2, que es un desarrollo de la ecuación L.1 general.

$$FDN_{zona_i,sist,SB} = \sum_{zona} (dFDN_{zona,OK,SB}) - dFDN_{zona_i,OK,SB} + dFDN_{zona_i,sist,SB} \tag{14.2}$$

Los tres grados de libertad de la ecuación L.2, zona, sist, y SB, se corresponden con los tres índices que definen cada uno de los elementos de la matriz: la zona en la que se encuentra el sistema contra incendios indisponible (zona) y el sistema contra incendios indisponible (sist) que, juntos, indican la fila del elemento estudiado, y el suceso básico representativo de una función clave de seguridad (SB), que indica la columna del elemento estudiado. Los grados de libertad sist y SB tienen dos estados: el propio estado sist o SB, que indica la indisponibilidad del suceso básico objetivo, y el estado OK, que implica que el sistema o componente objetivo está en estado normal. El primer término de la ecuación L.2 es equivalente a la ecuación L.1, aunque con la particularidad de que las dFDN se calculan con un suceso básico representativo de función clave de seguridad (SB) en estado *TRUE*, es decir, componente indisponible, si así lo indica el estado de planta asociado al elemento de la matriz estudiado. El segundo termino es la resta de la contribución de la zona de incendio afectada por la indisponibilidad de un sistema contra incendios (sist), si la hubiese. Los dos primeros términos de la ecuación L.2 se podrían substituir por el sumatorio de las 40 zonas de análisis no afectadas por la indisponibilidad de un sistema contra incendios. No obstante, se ha decidido presentar la ecuación L.2 con estos dos términos en lugar de un sumatorio para facilitar la explicación de la misma. Finalmente, el tercer término de la ecuación L.2 es la adición de la dFDN de la zona de incendios afectada por la indisponibilidad de un sistema contra incendios calculada con el sistema contra incendios indisponible (sist), suceso básico asociado en estado *TRUE*, y con el suceso básico representativo de función clave de seguridad también en estado *TRU*E si así lo indica el estado de planta asociado al elemento de la matriz estudiado. Este último término añade, en condiciones especiales, la contribución de la zona de incendios eliminada en el segundo término de la ecuación. El resultado de la ecuación L.2 es la suma de 41 dFDN, una por cada zona de incendio, teniendo una de ellas un sistema contra incendios indisponible y habiendo un representante de función clave de seguridad indisponible para toda zona de análisis, si así lo indica el estado de planta asociado al elemento de la matriz estudiado.

La indisponibilidad de un componente representativo de una función clave de seguridad (SB) afecta a toda la planta, por lo tanto, se aplica en todos los términos de la ecuación L.2 y en todas las dFDN que los forman. Sin embargo, la indisponibilidad de un sistema contra incendios (sist), que se consideran independientes entre sí, afecta únicamente a la zona de análisis en la que está ubicado. Debido a la distribución de la cuantificación del modelo APS de incendios detallado en casos de incendio y en zonas de incendio, los sucesos básicos representativos de los sistemas contra incendios se comparten, por simplicidad[1], entre casos y zonas[2][3]. Esto implica, por lo tanto, que el cambio a *TRUE* del estado un suceso básico de sistema contra incendios puede afectar a la dFDN de varias zonas de incendio, al estar este suceso básico presente en el análisis de estas varias zonas. En consecuencia, si se pusiese a *TRUE* el estado de un suceso básico de sistemas contra incendios, se cuantificasen las dFDN de las zonas de incendio, y se cuantificase la FDN de la central mediante la ecuación L.1, esta última no sería representativa de un estado de planta en el que únicamente está indisponible un sistema contra incendios de una zona puesto que incluiría la afectación de varias zonas. Es por este motivo que se ha desarrollado la ecuación L.2, que sí que permite obtener una FDN representativa de estas situaciones al separar la zona afectada por la indisponibilidad de un sistema

[1] De esta manera se reduce la cantidad de sucesos básicos en el modelo.

[2] Al no volcar las ecuaciones booleanas de las zonas en una única ecuación booleana para toda la planta, no es necesario que los sucesos básicos de los sistemas contra incendios sean independientes entre sí como sí lo son los sistemas representados.

[3] Por ejemplo, todos los sistemas automáticos de rociado con *sprinklers* comparten el mismo suceso básico para representar su indisponibilidad a pesar de ser sistemas independientes. Si se pone a *TRUE* este suceso básico, se consideran indisponibles todos los sistemas de rociado de la central.

contra incendios del resto del análisis. En la sección 14.2.2 a continuación, se detalla como se cuantifica un elemento de la matriz mediante la ecuación L.2 y el modelo APS de incendios detallado desarrollado en *RiskSpectrum® PSA*.

14.2.2. Cálculo de un elemento de la matriz

Siguiendo la ecuación L.2 presentada en la sección anterior, el procedimiento a seguir para cuantificar la FDN asociada al estado de planta indicado por uno de los elementos de la matriz mediante *RiskSpectrum® PSA* sería el siguiente:

1. Primer término de la ecuación:
   a) Si no lo estuviesen, poner todos los sucesos básicos de sistemas contra incendio en estado Normal.
   b) Poner el suceso básico representativo de la función clave de seguridad (SB) asociado al elemento de la matriz objetivo en estado *TRUE*.
   c) Ordenar al programa la ejecución de 384 *Consequence Analysis Cases*, uno por caso, y 41 *MCS Analysis Cases*, uno por zona de análisis. En total, 425 simulaciones.
   d) Sumar los 41 valores resultantes de los *MCS Analysis Cases*.
2. Segundo término de la ecuación:
   a) Restar al primer término el valor de la dFDN de la zona afectada por la indisponibilidad de un sistema contra incendios. Tanto la zona como el sistema contra incendios objetivo vienen indicados por la fila de la matriz a la que pertenece el elemento objetivo. Se conseguiría el mismo valor si solo se sumasen 40 dFDNs en el punto uno, es decir, todas menos la de la zona afectada.
3. Tercer término de la ecuación:
   a) Poner el suceso básico del sistema contra incendios objetivo (sist) en estado *TRUE*.
   b) Ejecutar todos los *Consequence Analysis Cases* de la zona afectada, así como el *MCS Analysis Case* de esa misma zona.
   c) Sumar el valor del punto 3.b al obtenido en el 2.a para tener la FDN inducida por incendios de la central condicionada a la indisponibilidad de un sistema contra incendios y a la indisponibilidad de un componente representativo de una función clave de seguridad.

Aplicado sucesivamente a los diferentes elementos de la matriz, el procedimiento presentado podría utilizarse para cuantificar todos los elementos que conforman la matriz MCI. Se estima, en base a la experiencia con el software *RiskSpectrum® PSA* y el hardware disponible, que el tiempo necesario para calcular la FDN de un elemento la matriz siguiendo el procedimiento especificado es de 10 minutos. Al contar con 4704 elementos, la cuantificación de la matriz MCI llevaría 47040 minutos o, lo que es lo mismo, 784 horas. Considerando que esta cantidad de tiempo es excesiva, se ha diseñado una metodología optimizada de cuantificación de la matriz.

14.2.3. Metodología optimizada de cálculo de la matriz MCI

La optimización del proceso cálculo de todos los elementos de la matriz MCI utilizando la ecuación de cuantificación de la FDN de los elementos de la matriz, ecuación L.2 en la sección 14.2.1, implica la mejora del proceso de obtención de valores dFDN y la mejora del pos-procesado de los mismos. Los valores de dFDN utilizados en la ecuación L.2 se obtienen mediante la cuantificación de 384 *Consequence Analysis Cases* y 41 *MCS Analysis Cases*, uno por zona, en el modelo APS de incendios detallado desarrollado en *RiskSpectrum® PSA*. El post-procesado consiste en el tratamiento de los valores de dFDN proporcionados por *RiskSpectrum® PSA* para obtener los valores de FDN inducida por incendios de cada elemento de la matriz. Aunque el pos-procesado puede realizarse de múltiples maneras, todas ellas deberían incluir la automatización de la obtención de valores FDN mediante la ecuación L.2 para una correcta optimización del tiempo de análisis.

14.2.3.1. Optimización de la cuantificación en *RiskSpectrum® PSA*

La optimización de la cuantificación de valores dFDN mediante *RiskSpectrum® PSA* implica reducir tanto como sea posible la cantidad de cuantificaciones a ejecutar para obtener todos los valores dFDN utilizados en el cálculo de los elementos de la matriz. Por lo tanto, los objetivos de este proceso de optimización son: que toda cuantificación ejecutada mediante *RiskSpectrum® PSA* proporcione valores dFDN que se vayan a utilizar[4] en el posterior cálculo de elementos de la matriz MCI, y que, cumpliéndose el primer objetivo, toda cuantificación ejecutada mediante *RiskSpectrum® PSA* proporcione tantos valores de dFDN como sea posible de forma simultánea. La cantidad máxima de valores dFDN simultáneos que puede proporcionar el modelo APS en *RiskSpectrum® PSA* es fija y corresponde a los 41 *MCS Analysis Cases*, uno por zona de análisis, que contiene. En consecuencia, toda cuantificación de valores dFDN ha de hacer uso de los 41 *MCS Analysis Cases*[5].

El procedimiento de cuantificación optimizado se basa en que el primer término de la ecuación L.2 se utiliza de forma indistinta en todos los elementos de la matriz pertenecientes a una misma columna. De hecho, la FDN de los elementos la primera fila de la matriz, que corresponde al estado normal de todos los sistemas contra incendios, se obtiene directamente del primer término de la ecuación. Los valores de dFDN incluidos en el sumatorio del primer término de la ecuación se pueden obtener de una única cuantificación en el modelo APS en *RiskSpectrum® PSA* imponiendo en el modelo el estado de las funciones clave de seguridad indicado por la columna de la matriz objeto de estudio. Consecuentemente, con una única cuantificación se obtiene un elemento de la matriz y la gran mayoría de valores dFDN necesarios para calcular todos los elementos de una columna de la matriz. Si a continuación, por ejemplo, se impone en el modelo la indisponibilidad de todos los sistemas de detección automática (PDA) de la central, manteniendo el estado de las funciones claves de seguridad descrito por la columna objetivo, y se cuantifica la dFDN de todas las zonas de análisis, los 41 valores obtenidos sirven para calcular 41 elementos de la matriz FDN utilizando la ecuación L.2. Si, seguidamente, los sistemas PDA se retornan al estado normal, y se impone la indisponibilidad de todos los sistemas de extinción automática, PEA, los 41 valores de dFDN obtenidos en la cuantificación sirven para calcular otros 41 elementos de la matriz FDN. Teniendo en cuenta que en la matriz se incluyen cuatro[6] sistemas contra incendios generales por zona, PS, PDA, PEA, y PFB, se pueden obtener los 167 elementos que forman una columna ejecutando tan solo cinco cuantificaciones en *RiskSpectrum® PSA*. Por lo tanto, todos los elementos de la matriz MCI se obtendrían ejecutando 140 cuantificaciones en el modelo APS de incendios detallado.

El procedimiento de cuantificación finalmente utilizado, véase la figura 14.1, pivota entorno a los sistemas contra incendios, es decir, las filas de la matriz, en lugar de entorno al estado de las funciones clave de

[4] Un valor repetido se considera como no utilizable.

[5] En el caso del cálculo del tercer término de la ecuación utilizando la metodología básica presentada en la sección 14.2.2 solo se utiliza un *MCS Analysis Case*.

[6] Algunas zonas concretas presentan sistemas contra incendios especiales. Véase la sección 14.2.3.3 a continuación.

seguridad, es decir, las columnas. Se impone la indisponibilidad de todos los sistemas contra incendios de un tipo general, por ejemplo, PEA, y se cuantifican, secuencialmente, los valores de dFDN correspondientes a los 28 estados de planta diferentes representados por las columnas de la matriz. Una vez completado este proceso se impone la indisponibilidad de otro tipo de sistema contra incendios general y se repite la cuantificación de valores dFDN en los 28 estados de planta descritos en la matriz. Se utiliza este procedimiento porque imponer la indisponibilidad de todos los sistemas contra incendios asociados a uno de los tipos genéricos de sistemas contra incendio requiere más tiempo que imponer la indisponibilidad de un único suceso básico representativo de una función clave de seguridad. Los sistemas contra incendios están representados en el modelo APS mediante diversos *Exchange Events*, véase la sección 12.3.5.8 del capítulo 12, por lo tanto, imponer la indisponibilidad de todos los sistemas contra incendios asociados un tipo genérico requiere poner, simultáneamente, varios sucesos básicos en estado *TRUE*. El anexo P presenta los sucesos básicos que se han de poner en estado *TRUE* para considerar que todos los sistemas contra incendios asociados a un tipo general están indisponibles.

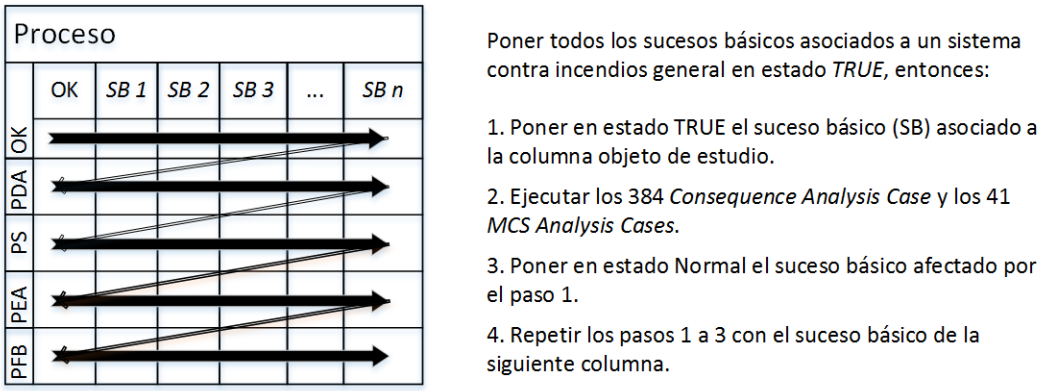


Figura 14.1: Procedimiento de cuantificación de valores dFDN en RiskSpectrum® PSA.

14.2.3.2. Optimización del pos-procesado

Cada uno de los procesos de cuantificación de 41 *MCS Analysis Cases* ejecutados siguiendo la metodología presentada en la sección anterior proporciona un único[7] archivo de texto que contiene, entre otros datos, los 41 valores de dFDN, uno por zona, del caso estudiado y cuantificado. Son estos archivos de texto los que se han de pos-procesar para obtener la matriz MCI. En este caso, se ha decidido llevar a cabo el pos-proceso de los archivos de texto mediante dos scripts[8] de Python™. El anexo Q detalla el contenido y el funcionamiento de ambos scripts.

El primer script, llamado *AGR.py*, se ejecuta a continuación de cada cuantificación y tiene por objetivo organizar los datos obtenidos en la cuantificación. La función del script *AGR.py* es seleccionar los valores dFDN del archivo de texto objetivo[9] y copiarlos en un nuevo archivo de texto al que le da un nombre siguiendo un formato preestablecido: sist+_ (barra baja) +número del suceso básico + - (guión) + nombre del suceso básico. Por ejemplo, un nombre de archivo podría ser PDA_01-1VMXXXXXBO.TXT.

El segundo script, llamado *results.py*, se ejecuta una vez se hayan llevado a cabo todas las cuantificaciones. En primer lugar, el script *results.py* agrupa, de forma ordenada, todas las dFDN contenidas en los archivos de texto generados por *AGR.py* en una estructura matricial auxiliar llamada matriz dFDN. Las filas de la

[7] Se utiliza la herramienta *Analysis Case Group* de *RiskSpectrum® PSA* para obtener un único archivo de texto. Dicha herramienta permite agrupar la cuantificación de casos de análisis y proporciona un único archivo de texto como resultado.

[8] Un script es un programa simple, almacenado en un archivo de texto plano e interpretado en su ejecución, es decir, no está compilado. También son llamados archivos de órdenes, archivo de procesamiento por lotes o guiones.

[9] Es decir, los archivos de texto que contiene los resultados de cuantificar 41 *MCS Analysis Cases*.

matriz dFDN hacen referencia a combinaciones de zona de incendio y sistema contra incendios indisponible, incluyendo una fila para el estado normal de todos los sistemas contra incendio, y las columnas, al igual que las de la matriz MCI, se asocian a los sucesos básicos representativos de funciones clave de seguridad. En segundo lugar, *results.py* calcula los elementos de la matriz MCI mediante la ecuación L.2 a partir de los valores dFDN almacenados en la matriz auxiliar dFDN. El script genera dos archivos de texto, uno que contiene la matriz auxiliar y otro que contiene la matriz MCI. La matriz auxiliar, a parte de facilitar el cálculo de los elementos de la matriz MCI al estar todas las dFDN agrupadas en una misma estructura, es una herramienta útil para detectar la causa de posibles resultados anómalos pues contiene todas las componentes utilizadas en el cálculo de cada uno de los elementos de la matriz MCI.

14.2.3.3. Casos especiales

Los análisis de las zonas de incendio CXXX6 y CXXX1[10] presentan ciertas particularidades en cuanto a las consecuencias derivadas de los incendios estudiados, y en cuanto a los sistemas contra incendio presentes en dichas zonas. En el caso de la zona CXXX6, que es una sala de reparto de cables, sus árboles de sucesos de extinción de incendios, véase las figuras 14.2 y 14.3 , llevan a daño al núcleo de forma directa. Por lo tanto, no se postula ningún suceso interno intermedio. Además, las figuras 14.2 y 14.3 muestran que en el análisis de incendios de la zona CXXX6 se han postulado ocho tipos distintos de sistemas contra de incendios susceptibles de fallo.

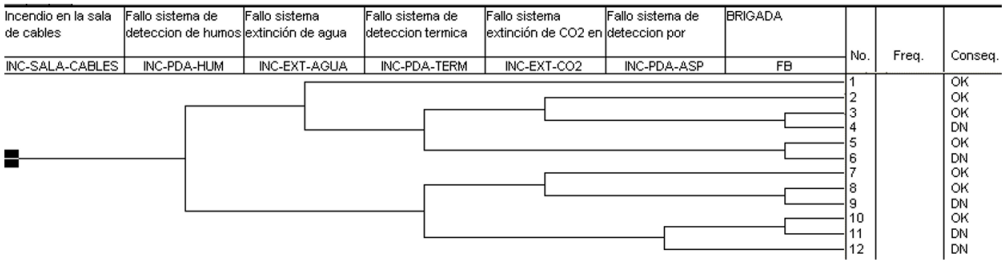


Figura 14.2: Árbol de sucesos CI-A de la zona C0016.

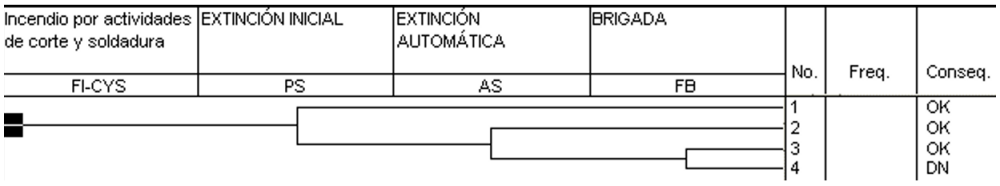


Figura 14.3: Árbol de sucesos CI-CYS de la zona C0016.

Solamente dos de estos sistemas se repiten como en el caso general: PFB y PS. Los otros seis, considerados en exclusiva para la zona CXXX6, son HUM, AGUA, TERM, CO2, ASP y PEA2. Se ha cambiado el código de PEA, el cabecero AS en la figura 14.3, a PEA2 porque si se pusiera PEA a *TRUE* como en las demás zonas también se asumirían indisponibles AGUA y CO2, simultáneamente[11]. Así el "Fallo sistema extinción de CO2 en sala de cables" tiene por código CO2; el "Fallo sistema extinción de agua en sala de cables" tiene por código AGUA, y, por lo tanto, PEA2 se refiere a la "EXTINCIÓN AUTOMÁTICA".

[10] Por motivos de confidencialidad, no se indican ni los nombres completos ni los códigos utilizados para hacer referencia a estas zonas.

[11] Los sucesos básicos AGUA y CO2 son *Exchange Events* de PEA. Véase el anexo P para más detalle.

La contribución dFDN de la zona CXXX6 es independiente a las funciones clave de seguridad de la central al tener como consecuencia directa el daño al núcleo. En consecuencia, no ha sido necesario ejecutar las cuantificaciones de los casos que analizan la indisponibilidad combinada de sistemas contra incendios y equipos representantes de funciones clave de seguridad. Por lo tanto, sólo son necesarias seis cuantificaciones de la dFDN de la zona CXXX6 para poder completar la matriz MCI.

El análisis de la zona CXXX1 contempla trece casos de incendio independientes. En sólo tres de ellos se da crédito a sistemas de detección y extinción. Estos sistemas se asocian a los códigos ASP, EXT, y HUM. ASP representa la fiabilidad del sistema de detección por aspiración (INC-SCONT-SIST-ASP). EXT simboliza la probabilidad de fallo en la extinción (INC-SCONT-EXT-ASP). Finalmente, HUM responde a la probabilidad de fallo humano al alinear correctamente la ventilación en modo extracción de humos (INC-SCONT-HUM). Los sistemas ASP, EXT, y HUM de la zona CXXX1 se incluyen en los sistemas generales PDA, PS, Y PEA, respectivamente, para evitar tener que realizar cuantificaciones específicas para ellos.

La consecuencia es directamente daño al núcleo en siete de los trece casos de análisis incluidos en la zona CXXX1. En los seis restantes la consecuencia lleva a otro árbol de sucesos donde se da crédito a las funciones de seguridad. Es por lo tanto necesario tener en cuenta las interacciones provocadas por indisponibilidades simultáneas de sistemas contra incendios y equipos representantes de funciones clave de seguridad.

14.2.3.4. Metodología optimizada

La figura 14.4 muestra la metodología optimizada de cuantificación de la matriz MCI. Es necesario ejecutar 146 cuantificaciones en *RiskSpectrum® PSA* para obtener la matriz completa. Seis de las 146 cuantificaciones corresponden al caso de la zona especial CXXX6. Asumiendo una media de 10 minutos por cuantificación[12], el tiempo de ejecución de la metodología optimizada para obtener la matriz MCI es de 1460 minutos, o, lo que es lo mismo, 24,33 horas[13]. Por lo tanto, la metodología optimizada consigue reducir el tiempo de cálculo de la matriz MCI en 760 horas con respecto a la metodología presentada en la sección 14.2.2.

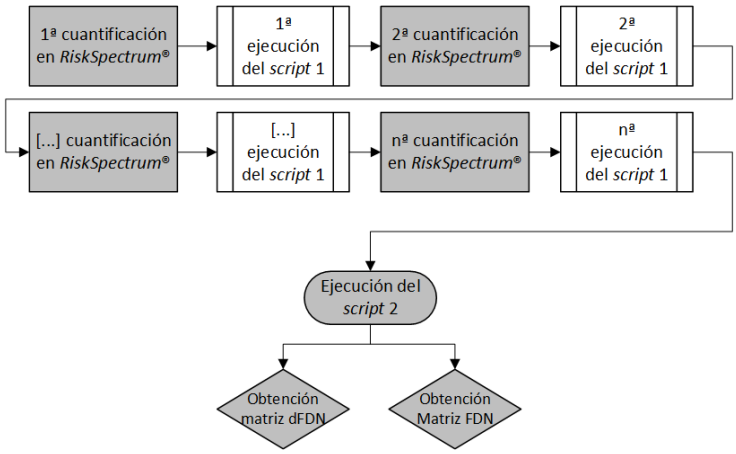


Figura 14.4: Metodología optimizada de cuantificación de la matriz MCI.

[12] Se tiene en cuenta la preparación de la cuantificación. La preparación difiere entre casos. Toma más tiempo cuando hay que cambiar el sistema contra incendios general indisponible.

[13] Este tiempo no incluye el diseño de los scripts en Python™. La duración de la ejecución de los scripts se considera despreciable.

14.3. Cuantificación de la matriz MRI

La matriz MRI contiene tres figuras distintas: en la primera fila, la FDN inducida por incendios de la central condicionada a la indisponibilidad de representantes de funciones clave de seguridad, es decir, condicionada al estado de planta asociado a cada columna de la matriz. En la segunda fila, el tiempo de exposición permitido para los estados de planta asociados a las columnas. En el resto de filas, las dFDN de las zonas de incendio que, sumadas, conforman la FDN inducida por incendios de la planta presentada en la primera fila. Las FDN inducidas por incendios presentes en la primera fila de la matriz y las dFDN de cada zona de incendio se obtienen en el proceso de cuantificación de la matriz MCI. De hecho, la primera fila de la matriz MRI es también la primera fila de la matriz MCI. Por otra parte, las dFDN incluidas en la matriz MRI se encuentran almacenadas en la matriz auxiliar dFDN creada en el proceso de cuantificación de la MCI. Por lo tanto, la única figura a cuantificar es el tiempo de exposición permitido para los estados asociados a las columnas de la matriz. El tiempo de exposición se obtiene, para cada columna, mediante la ecuación 15.1. En el denominador de la ecuación se restan la frecuencia inducida por incendios de la planta condicionada al estado definido por la columna objetivo y la frecuencia inducida por incendios de la planta de referencia, es decir, la frecuencia en operación normal.

$$T_E(días) = \frac{1,0E-06}{\left(FDN_{fila_1}^{incendios} - FDN_{referencia}^{incendios}\right) \cdot 365} \tag{14.3}$$

La matriz MRI se ha construido en una hoja de cálculo de Microsoft Excel® a partir de los archivos de texto que contienen la matriz dFDN auxiliar y la matriz MCI utilizando las herramientas de selección del software. Se ha utilizado la herramienta de formulación del software Excel® para calcular el tiempo de exposición de cada columna y así completar la matriz.

Capítulo 15

Presentación y análisis de resultados

15.1. Introducción

El capitulo 15 de la tercera parte de la tesis se divide en tres bloques: la presentación de los resultados obtenidos en la cuantificación de las matrices MCI y MRI, el análisis de incertidumbre de la matriz MCI, y el análisis detallado de los resultados de las matrices MCI y MRI. La sección 15.2 presenta los resultados obtenidos en la cuantificación de las matrices MCI y MRI. Con el objetivo de obtener conclusiones concretas, la interpretación y análisis de los resultados obtenidos está sujeta a la aplicación de los llamados criterios de valoración del riesgo. Se incluye en la sección 15.2 la descripción de los criterios de valoración del riesgo utilizados en el análisis de los resultados, cuya aplicación ha sido consensuada con expertos de la central nuclear.

La sección 15.3 presenta el desarrollo y resultados del análisis de incertidumbre de la matriz MCI. En el marco del análisis de incertidumbre se calcula una nueva matriz MCI que contiene el percentil 95 de todos los elementos de la matriz original. La matriz MCI de percentiles 95 se evalúa con los mismos criterios de valoración del riesgo que los utilizados en la matriz MCI, véase la sección 15.2.1.1, y se compara con la matriz original. Como resultado del análisis comparativo de ambas matrices se extrae cuántos elementos de la matriz ascienden de categoría de riesgo y en qué magnitud. Dicho análisis permite evaluar la robustez del análisis matricial y de la herramienta resultado, la propia matriz MCI original, y permite valorar la confianza a depositar en las conclusiones extraídas del análisis de resultados. Las conclusiones extraídas en el análisis de incertidumbre de la matriz MCI son extrapolables a los resultados de la matriz MRI puesto que estos últimos se utilizan para obtener los resultados de la primera.

Finalmente, el análisis detallado de los resultados de cada matriz se presenta en la sección 15.4. El análisis detallado de los resultados de ambas matrices permite extraer conclusiones al respecto de qué combinaciones de indisponibilidad de equipos no deberían permitirse, qué equipos podrían incluirse en la regla de mantenimiento, y en qué zonas de incendio podrían aplicarse acciones de gestión del riesgo para reducir la frecuencia de daño al núcleo inducida por incendios de la central.

15.2. Presentación de resultados

15.2.1. Matriz MCI

15.2.1.1. Criterios de valoración del riesgo

Los resultados cuantitativos al respecto de una figura de riesgo de una central nuclear como, por ejemplo, la frecuencia de daño al núcleo, son difícilmente evaluables por sí solos[1].Sin embargo, en la mayoría de casos existe un valor de referencia con el que poder comparar la figura de riesgo a evaluar, y así decidir si el riesgo de la situación evaluada es mayor o menor que el de esta referencia. En el caso de una central nuclear, el valor de referencia de una figura de riesgo es el asociado a una configuración preestablecida de la planta que se considera representativa de la operación normal de la misma. En el caso que el resultado obtenido sea menor o igual que el de referencia, se concluye que la situación analizada no es significativa desde el punto de vista del riesgo[2] [22]. Si el resultado obtenido es mayor que el de referencia, la situación estudiada se ha de evaluar mediante criterios de valoración del riesgo para poder decidir si es significativa desde el punto de vista del riesgo. Los criterios de valoración del riesgo utilizados normalmente en aplicaciones de toma de decisiones informadas por el riesgo, véanse, por ejemplo, los incluidos en el capítulo 3 de la primera parte de la memoria de tesis, difieren entre sí con respecto a si se analizan situaciones permanentes[3], o situaciones temporales[4]. Se utilizan criterios de valoración del riesgo basados en el incremento de la figura de riesgo cuantificada, ΔFDN para la frecuencia de daño al núcleo, en el análisis de situaciones permanentes. Las situaciones temporales se analizan mediante criterios de valoración del riesgo basados en el concepto de incremento de probabilidad de riesgo asociado al tiempo de exposición a la situación analizada. La ecuación 15.1 es la utilizada para cuantificar el incremento de probabilidad de riesgo[5] asociado a una situación específica a la que la central ha estado expuesta durante un tiempo de exposición llamado T_E.

$$\Delta PDN = \frac{\Delta FDN}{365} T_E(días) \tag{15.1}$$

Las combinaciones de indisponibilidad analizadas mediante la matriz MCI son situaciones de cariz temporal de las cuales se desconoce el tiempo de exposición. En consecuencia, los elementos de la matriz MCI se evalúan mediante criterios de valoración del riesgo basados en el concepto de incremento de probabilidad de riesgo asociado al tiempo de exposición a la situación analizada. No obstante, al desconocerse el tiempo de exposición a la situación analizada por tratarse de un análisis prospectivo, los criterios utilizados no analizan el incremento de probabilidad de riesgo sino el tiempo de exposición necesario para alcanzar un valor de incremento de probabilidad de riesgo significativo. De acuerdo con otras aplicaciones [4, 64, 46], se fija en 1,0E-06 el valor umbral de incremento de probabilidad de riesgo que discierne entre situaciones significativas y no significativas desde el punto de vista del riesgo. La tabla 15.1 presenta los criterios de valoración de riesgo aplicados, en consenso con expertos de la central nuclear, a los resultados de la matriz MCI. Se le ha asignado un color a cada nivel de riesgo para facilitar el análisis visual de la matriz. Los criterios cuantitativos presentados en la tercera columna de la tabla 15.1 son el resultado de aislar la FDN de la situación analizada (FDN_a) de los criterios presentes en la segunda columna. El valor de la FDN de incendios de referencia de la central es de 9,61E-06 año^{-1}.

[1] A no ser que sean cercanos al valor de cribado, 1,0E-09 año^{-1} para la frecuencia de daño al núcleo, o sean un valor extremadamente alto (entre 1,0E-04 y 1,0E-03 por año según la RG 1.174 [22]).

[2] Aquellos análisis cuyo objetivo es demostrar que una configuración tiene asociado un riesgo menor que el de referencia son una excepción a este criterio.

[3] Por ejemplo, modificaciones de diseño o nuevas configuraciones.

[4] Mantenimientos, hallazgos, o indisponibilidades no previstas, entre otros.

[5] Incremento de probabilidad de daño al núcleo si el riesgo es cuantificado mediante la figura de frecuencia de daño al núcleo.

Color	Criterios cualitativos	Criterios cuantitativos	Criterios al respecto de FDN_a[año^{-1}]
Verde	Muy bajo	$\Delta FDN \cdot (7/365) < 1,0E-06$	$FDN_a < 6,20E-05$
Amarillo	Bajo	$\Delta FDN \cdot (7/365) > 1,0E-06$	$6,20E-05 < FDN_a < 1,31E-04$
Naranja	Moderado	$\Delta FDN \cdot (3/365) > 1,0E-06$	$1,31E-04 < FDN_a < 1,0E-03$
Rojo	Alto	$FDN_a > 1,0E-03$	$FDN_a > 1,0E-03$

Tabla 15.1: Criterios de riesgo utilizados para evaluar la matriz MCI.

Los criterios de riesgo utilizados en la evaluación de la matriz MCI se dividen en cuatro niveles cualitativos: muy bajo (verde), bajo (amarillo), moderado (naranja), y alto (rojo). El riesgo inherente a incendios es significativo a partir del nivel de riesgo amarillo inclusive. Para el nivel de riesgo muy bajo (verde), no se alcanza el umbral de ΔPDN de 1,0E-06 en, al menos, los primeros siete días de operación bajo las condiciones impuestas por la situación analizada. En estos casos no es necesario realizar acciones correctivas[6] de la situación de planta. Si la situación analizada es producto de un mantenimiento, las operaciones de mantenimiento pueden durar cuanto sea necesario, siempre y cuando la situación no se vuelva permanente. Para el nivel de riesgo bajo (amarillo), el umbral de ΔPDN de 1,0E-06 se alcanza pasados tres días, y en no más de siete, de operación bajo las condiciones impuestas por la situación analizada. Se deberían realizar acciones correctivas para corregir la situación analizada antes de que pasen siete días de operación bajo las condiciones impuestas por la misma. Si la situación analizada es producto de un mantenimiento, las operaciones de mantenimiento pueden durar como máximo siete días. Respecto al nivel de riesgo moderado, el umbral de ΔPDN de 1,0E-06 se alcanza antes de que pasen tres días de operación bajo las condiciones impuestas por la situación analizada. Se deberían realizar acciones correctivas para corregir la situación analizada, como muy tarde, antes de que pasen tres días de operación bajo las condiciones impuestas por la misma. Si la situación analizada es producto de un mantenimiento, las operaciones de mantenimiento pueden durar como máximo tres días. Para entrar en el nivel de riesgo alto (rojo), la FDN de la situación analizada ha de ser mayor o igual a 1,0E-03. De darse una situación así, se deberían llevar a cabo acciones correctivas de forma inmediata y es posible que fuese necesario llevar la planta a parada segura[7] para garantizar que la situación analizada no afecte a la correcta operación y a la seguridad de la central. Una situación de riesgo alto no puede ser producto de un mantenimiento online[8]. Un mantenimiento online asociado a una FDN tan elevada no puede, y no debe, permitirse. Estos criterios de valoración del riesgo ya han sido aplicados a los resultados presentados en la sección 15.2.1.2 a continuación.

15.2.1.2. Resultados de la matriz MCI

La matriz MCI se presenta en el anexo S debido a que sus dimensiones, 4704 elementos en 168 filas y 28 columnas, harían impracticable su inclusión y análisis en la memoria tesis. La tabla 15.2 resume los resultados obtenidos de acuerdo con los criterios de valoración del riesgo descritos en la sección anterior. De las 4704 situaciones analizadas, tan solo un 3,57 % se incluyen en la categoría de riesgo alto. La gran mayoría de la situaciones analizadas, un 77,47_ %, se asocian a un riesgo muy bajo, y, por lo tanto, pueden darse durante la operación normal de la central sin que tengan una afectación significativa sobre la seguridad de la planta. El análisis de los resultados de la matriz MCI se expone más adelante.

[6] Se entienden por acciones correctivas todas aquellas acciones que permitan continuar operando en situación segura o que trasladen la planta a un estado seguro. Por ejemplo, el cambio de tren en servicio para el sistema afectado por la situación de planta o el traslado a otros modos de operación son acciones correctivas. Se prioriza, si es posible, mantener la operación a potencia mediante cambios de la configuración de planta.

[7] Modo de operación en el que se considera que la planta está estiable y es segura durante el tiempo necesario como para que se puedan subsanar los motivos que han llevado a esta situación. Normalmente la parada segura se asocia al modo 3, espera en caliente, o al modo 4, parada caliente.

[8] Tareas de mantenimiento realizadas durante la operación a potencia de la central.

Riesgo	# elementos	% total
Verde	3644	77,47
Amarillo	522	11,10
Naranja	370	7,87
Rojo	168	3,57
Total	4704	100

Tabla 15.2: Resumen de los resultados obtenidos mediante la matriz MCI.

15.2.2. Matriz MRI

15.2.2.1. Criterios de valoración del riesgo

Los criterios de valoración del riesgo utilizados en la evaluación de los resultados de la matriz MRI son diferentes según las fila analizada. Las dos primeras filas, que contienen, respectivamente, la FDN inducida por incendios y el tiempo de exposición necesario para llegar a un ΔPDN de 1,0E-06 en la situaciones estipuladas por las columnas de la matriz, se evalúan mediante los mismos criterios que los utilizados para la matriz MCI. El resto de filas, que contienen las contribuciones a la frecuencia de daño al núcleo de cada zona de incendio incluidas en el análisis, las llamadas dFDN, se analizan mediante un degradado de color por columnas con el cuál se destaca la dFDN más alta de cada columna en color rojo. Las sucesivas dFDN se marcan con tonos de rojo más tenues a medida que el valor de FDN disminuye. Se identifica, de esta manera, para cada columna, cuál es la zona de incendio que más contribuye a la FDN inducida por incendios y, a su vez, , mediante las filas asociadas a la FDN inducida por incendios y al tiempo de exposición, si esa columna corresponde a una situación significativa desde el punto de vista del riesgo según los criterios aplicados a la matriz MCI. Se conocen, juntando ambos criterios, las zonas de incendio más significativas desde el punto de vista del riesgo inducido por incendios.

15.2.2.2. Resultados de la matriz MRI

La matriz MRI se presenta en el anexo S debido a que sus dimensiones, 1290 elementos en 43 filas y 28 columnas, harían impracticable su inclusión y análisis en la memoria tesis. No se presenta un resumen similar al de la sección 15.2.1.2 porque los resultados de la matriz MRI no se evalúan con los mismos criterios de riesgo que los utilizados para la matriz MCI. No obstante, los criterios utilizados destacan que la indisponibilidad de una de las barras de distribución de suministro eléctrico generaría una situación de riesgo muy elevado. La zona de incendio cuya dFDN es mayor en la situación descrita por la indisponibilidad de la barra de distribución de suministro eléctrico es la CXXX5, una zona de equipo eléctrico. El análisis detallado de los resultados de la matriz MRI se expone más adelante.

15.3. Análisis de incertidumbre de la matriz MCI

15.3.1. Introducción

En procesos de decisión, la información que proporcionan los análisis de incertidumbre de los resultados cuantitativos es relevante para decidir sobre cuáles de ellos depositar una mayor confianza. Aunque sea de forma indirecta y/o cualitativa, toda figura cuantitativa considerada en un proceso de toma de decisiones ha de ir acompañada de una valoración de su incertidumbre asociada. Las matrices MCI y MRI han sido desarrolladas para evaluar cuantitativamente el riesgo inducido por incendios en una central nuclear e incorporarlo en las prácticas habituales de evaluación y toma de decisiones al respecto de configuraciones

de planta. Por lo tanto, la incertidumbre asociada a los resultados de estas herramientas ha de ser analizada para que puedan incorporarse en las prácticas de toma de decisiones.

En el marco del análisis de incertidumbre se ha decidido calcular nuevas matrices MCI que contengan el percentil 95, la media, la mediana, y el percentil 5 % de todos los elementos de la matriz original. La metodología base utilizada para obtener estas matrices se detalla en la sección 15.3.3. El cálculo de estos parámetros estadísticos responde a la propagación de la incertidumbre epistémica[9] de los parámetros de fiabilidad[10] utilizados en el modelo APS de incendios detallado. En ningún caso el análisis de incertidumbre realiza una valoración de la incertidumbre epistémica asociada al propio modelo APS. No obstante, se considera que el modelo es conservador respecto a la realidad, así que el impacto del análisis de la incertidumbre asociada al modelo debería traducirse en valores de FDN menores a los obtenidos.

La matriz MCI de percentiles 95 se evalúa con los mismos criterios de valoración del riesgo que los utilizados en la matriz MCI y se compara con la matriz original. Como resultado del análisis comparativo de ambas matrices se extrae cuántos elementos de la matriz ascienden de categoría de riesgo y en qué magnitud. De esta manera se valora la robustez de los resultados y la confianza a depositar en los mismos en función de la cantidad de elementos de la matriz que hayan ascendido de categoría. La incertidumbre asociada a los resultados de la matriz MRI se valora de manera indirecta a partir de la incertidumbre de la matriz MCI. Los elementos de la matriz MCI son el resultado de sumar valores de dFDN contenidos en la matriz MRI. En consecuencia, los elementos de la matriz MRI son precisamente la fuente de incertidumbre de los elementos de la matriz MCI. Por lo tanto, si se determina que la incertidumbre de los resultados de la matriz MCI es baja, aún más lo será la incertidumbre de la matriz MCI. En caso contrario, la incertidumbre de los resultados de la matriz MRI también se juzgaría como alta.

15.3.2. Metodología de análisis de incertidumbre de *RiskSpectrum® PSA*

El software *RiskSpectrum® PSA* viene provisto de un módulo de análisis de incertidumbre basado en el método Monte Carlo. El módulo de análisis de incertidumbre permite al usuario escoger cuántas simulaciones se han de realizar y qué raíz utilizar. En cada simulación se generan, o bien valores aleatorios de los parámetros de fiabilidad e indisponibilidad del modelo, o valores aleatorios de la probabilidad de fallo de los sucesos básicos del modelo, y se calcula la probabilidad o frecuencia de la secuencia o secuencias de accidente objetivo mediante su ecuación booleana de conjuntos mínimos de fallo. El valor aleatorio, para cada simulación, de los parámetros de indisponibilidad o de la probabilidad de fallo de sucesos básicos se obtiene de sus distribuciones estadísticas asociadas, que deben ser introducidas previamente por el usuario en el modelo APS. Concretamente, se utiliza la *cummulative distribution function* (CDF) para obtener estos valores a partir de semillas aleatorias. El resultado proporcionado por *RiskSpectrum® PSA* en el marco del análisis de incertidumbre es la media de la frecuencia o probabilidad objetivo, los percentiles 5, 50, y 95 de esta frecuencia o probabilidad, y tanto la *Probability density function* (PDF) como la CDF, ambas en formato discontinuo, de la probabilidad o frecuencia objetivo. *RiskSpectrum® PSA* proporciona los resultados de su modulo de análisis de incertidumbre en archivos de texto de extensión .UNC.

No obstante, tal y como se ha explicado en el capítulo 14, los elementos de la matriz MCI no provienen directamente de la ejecución de procesos de cuantificación en *RiskSpectrum® PSA*, sino que son el producto de pos-procesar resultados provenientes del modelo APS de incendios detallado desarrollado en *RiskSpectrum® PSA*. Consecuentemente, el módulo de análisis de incertidumbre del software *RiskSpectrum® PSA* no se puede utilizar para cuantificar la incertidumbre de los elementos de la matriz MCI. A pesar de ello, el módulo de análisis de incertidumbre de *RiskSpectrum® PSA* se ha utilizado como herramienta de validación de la metodología base desarrollada, véase la sección 15.3.3.4 a continuación.

[9] La incertidumbre que responde a una falta de conocimiento respecto valor puntual de un parámetro o variable.
[10] Probabilidades de fallo y tasas de fallo.

15.3.3. Metodología base

La matriz MCI contiene 4704 elementos que representan la frecuencia de daño al núcleo de la central inducida por incendios en contextos en los que un sistema contra incendios y/o un componente representativo de una función de seguridad están indisponibles. Cada elemento de la matriz MCI se cuantifica de la misma manera: a partir de la suma de frecuencias de daño al núcleo inherentes a las diferentes zonas de análisis de incendio en las que se divide la central. Por lo tanto, una metodología desarrollada para analizar la incertidumbre de un elemento de la matriz puede ser posteriormente aplicada de manera secuencial a todos los elementos de la matriz MCI para completar el análisis de incertidumbre de la matriz. Se ha optado por esta opción y se ha llamado metodología base a la metodología desarrollada para analizar la incertidumbre de un único elemento de la matriz.

15.3.3.1. Datos de partida

Los datos de partida utilizados para cuantificar los elementos de la matriz MCI son las diferentes dFDN almacenadas en la matriz MRI. A diferencia de los resultados finales, estas dFDN sí que provienen directamente del modelo APS de incendios detallado de la central construido en *RiskSpectrum® PSA*. Como resultado, se puede cuantificar la incertidumbre asociada a estas dFDN mediante el módulo de análisis de incertidumbre que contiene *RiskSpectrum® PSA* y, de este modo, convertirlas en variables aleatorias. En consecuencia, los datos de partida del análisis de incertidumbre de la matriz MCI son las variables aleatorias dFDN, cuyos datos de incertidumbre son calculados mediante el módulo de *RiskSpectrum® PSA*. Los resultados que proporciona el módulo de análisis de incertidumbre de *RiskSpectrum® PSA* son:

- El valor promedio de la dFDN objetivo.
- Los percentiles 5, 50, y 95 de la dFDN objetivo.
- La *probability density function* de la dFDN objetivo. Se proporcionan valores discretos de la PDF.
- La *cummulative distribution function* de la frecuencia objetivo. Se proporcionan valores discretos de la CDF.

El valor promedio y los percentiles 5, 50, y 95 son parámetros informativos que no permiten propagar la incertidumbre que representan. Debido a que el tipo de la distribución de probabilidad resultado es desconocido, no es posible analizar analíticamente la incertidumbre de los resultados. En consecuencia, se desconocen parámetros de incertidumbre básicos como la desviación estándar y la variancia, lo que impide aplicar ciertas técnicas de propagación de incertidumbre para cuantificar la dispersión de los elementos de la matriz MCI. Se ha utilizado el software Matlab® en un caso de ejemplo para obtener el ajuste de la PDF discreta a la distribución de probabilidad Gamma, que a priori es la más adecuada para frecuencias. Mediante un ajuste correcto se obtendría la distribución de probabilidad asociada a la dFDN objetivo y, a su vez, los parámetros de incertidumbre básicos que permitirían calcular la incertidumbre de los elementos de la matriz MCI a partir de métodos de propagación. No obstante, no ha sido posible ajustar las PDFs resultado a distribuciones Gamma de probabilidad. Por lo tanto, las PDFs y las CDFs de las dFDN contenidas en la matriz MRI son los únicos datos de partida a utilizar en el análisis de incertidumbre de los elementos de la matriz MCI. La figura 15.1 presenta un ejemplo de *cummulative distribution function* discreta.

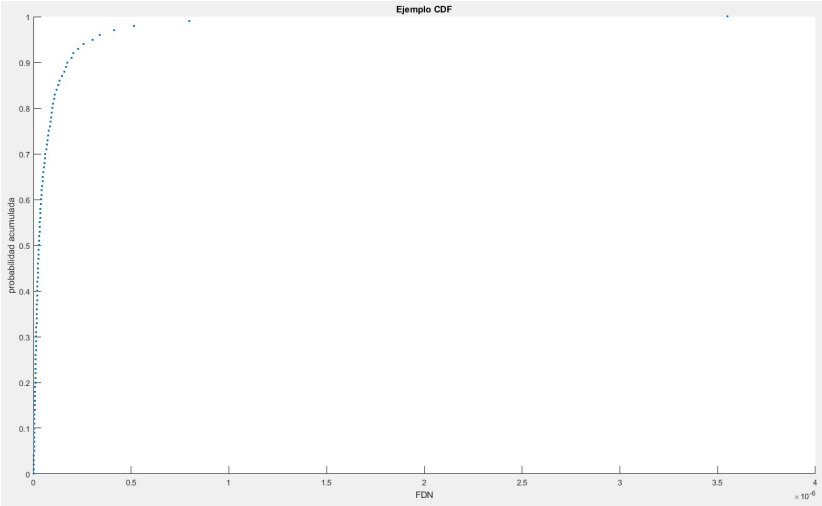


Figura 15.1: Ejemplo de *cummulative distribution function* discreta.

RiskSpectrum® PSA proporciona las *cummulative distribution function* de las dFDN de manera discreta mediante parejas de valores de probabilidad acumulada (F(x) o y) y FDN (x) en archivos de texto. El rango de la probabilidad acumulada es de 0 a 100, y se dan valores cada 1 %. La figura 15.2 presenta un ejemplo de CDF de una dFDN de zona de incendio proporcionada por *RiskSpectrum® PSA*.

x	F(x)
1.362E-010	0.0
9.730E-010	1.0
1.465E-009	2.0
1.765E-009	3.0
2.127E-009	4.0
2.413E-009	5.0
2.919E-009	6.0

Figura 15.2: Ejemplo de CDF en formato texto proporcionada por RiskSpectrum® PSA.

15.3.3.2. Metodología seleccionada

El procedimiento llevado a cabo por el módulo de análisis de incertidumbre de *RiskSpectrum® PSA* se toma como referencia para construir la metodología base de análisis de incertidumbre de la matriz de

compatibilidades de indisponibilidades. El principal motivo para tomar como referencia este módulo es que utiliza las *cummulative distribution functions* de las variables aleatorias input [11] para obtener los valores puntuales de estas mismas en cada simulación. Tal y como se ha explicado anteriormente, las *cummulative distribution functions* de las dFDN contenidas en la matriz MRI son uno de los datos de partida disponibles para realizar el análisis de incertidumbre de los elementos de la matriz MCI. Por lo tanto, la simulación Monte Carlo a partir de valores aleatorios generados mediante *cummulative distribution functions* es la metodología seleccionada para llevar a cabo el análisis de incertidumbre de los elementos de la matriz MCI. La figura 15.3 presenta el diagrama de flujo de la metodología seleccionada.

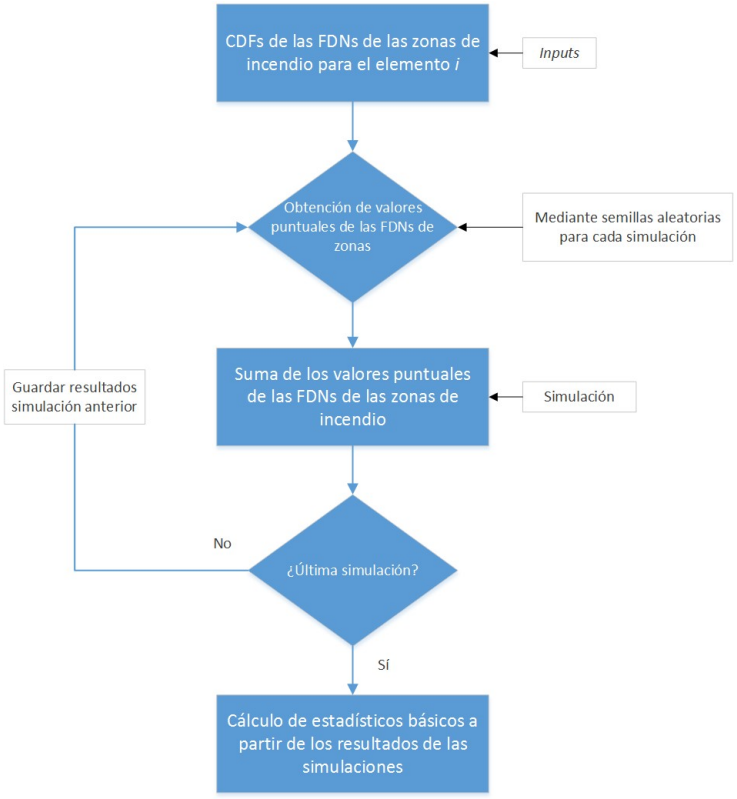


Figura 15.3: Diagrama de flujo de la metodología de análisis de incertidumbre seleccionada.

Las variables aleatorias input consideradas en cada simulación son las dFDN de las zonas de incendio contenidas en la matriz MRI asociadas al cálculo de la FDN un elemento objetivo de la Matriz MCI. Cada dFDN tiene una CDF discreta asociada que ha sido calculada [12] previamente en *RiskSpectrum® PSA*. A partir de valores aleatorios generados por una semilla se obtienen valores puntuales de las variables aleatorias utilizando la CDF discreta de cada una. La generación de valores aleatorios a partir de semillas puede proporcionar cualquier valor continuo entre 0 y 1 (o 0 y 100 si se desea). En el estado en el que *RiskSpectrum® PSA* proporciona las CDFs, forma discreta de la figuras 15.1 y 15.2, no sería posible consultar el valor de la dFDN para cualquier valor aleatorio continuo generado por la semilla. Se considera que se debería obtener una FDN específica para cualquier valor aleatorio generado por la semilla en pos de que el análisis de incertidumbre sea lo más preciso posible. Se han intentado ajustar las CDFs a expresiones analíticas mediante Matlab®, pero el resultado no ha sido satisfactorio. En su lugar, se ha optado por

[11] Es decir, los parámetros de indisponibilidad o las probabilidades de fallo de los sucesos básicos introducidos en un modelo.

[12] La explicación de cómo se consiguen estas CDF queda fuera del alcance de este documento.

representar cada intervalo de las CDFs mediante una expresión analítica, entendiéndose por intervalo el rango entre dos parejas de valores consecutivas. Se ha decidido ajustar cada intervalo de las CDFs a una recta que pasa por la pareja de valores inicial del intervalo (x_i, y_i) y por la pareja de valores final del intervalo (x_{i+1}, y_{i+1}). De esta manera, para un valor aleatorio y_n de la simulación n entre y_i e y_{i+1}, se utilizaría la ecuación de la recta ajustada mediante(x_i, y_i) y (x_{i+1}, y_{i+1}) para obtener x_n, que sería la dFDN puntual de la zona de incendios analizada para la simulación n. En el caso de las porciones extremo, entre $y = 0 - 0{,}1$, e $y = 0{,}99 - 1$, se ha optado por asociar cualquier valor de estas porciones al de x(y= 0,1) o x(y = 0,99), respectivamente. De esta manera se evita introducir en el análisis la incertidumbre residual asociada a los extremos de la CDF, que incluyen, en ínfimos rangos de probabilidad acumulada, amplios rangos de valores de dFDN. Cabe recordar que los límites de una CDF teórica son 0 y $+\infty$. El script generado para obtener valores puntuales de dFDN a partir de sus *cummulative distribution functions* y valores aleatorios ha sido escrito en el código del software Matlab® y se engloba en el script diseñado para aplicar la metodología base. El anexo R contiene una descripción detallada tanto del script generado para aplicar la metodología base como del script generado para aplicar la metodología base a todos los elementos de la matriz.

La simulación se ejecuta una vez obtenidos los valores puntuales de dFDN. En el caso de los elementos de la matriz MCI, la simulación consiste en obtener el resultado de la ecuación 15.2. El script de la metodología base presenta una ejecución simplificada de la ecuación 15.2, véase el anexo R, en la que ésta cuenta con solo cuatro zonas de incendio para facilitar la posterior validación de la metodología.

$$FDN_{zona_i,sist,SB} = \sum_{zona} (dFDN_{zona,OK,SB}) - dFDN_{zona_i,OK,SB} + dFDN_{zona_i,sist,SB} \tag{15.2}$$

Una vez obtenido el resultado de la ecuación 15.2, éste se almacena en un vector de resultados de las simulaciones, véase el anexo R. Si la simulación realizada es la última requerida, se calculan los estadísticos básicos del elemento de la matriz MCI objetivo a partir de los resultados de las simulaciones. Aparte de la media y del percentil 95, también se proporcionan la mediana y el percentil 5.

15.3.3.3. Análisis de estabilidad. Número de simulaciones

El número de simulaciones a realizar en la aplicación de la metodología base se ha decidido en base a un análisis de estabilidad de los estadísticos básicos. En el análisis de estabilidad se representa la progresión de los estadísticos básicos en relación a la progresión de la simulaciones. Es decir, cada punto de la gráfica, por ejemplo, la gráfica de la figura 15.4 a continuación, representa el estadístico básico objetivo calculado mediante el resultado de todas las simulaciones realizadas hasta dicho punto. De esta manera, mediante estas representaciones se identifica el número de simulaciones (ns) a partir del cual los parámetros estadísticos básicos no varían de forma significativa, considerándose estables.

Se ha obtenido la progresión de los parámetros estadísticos para ns = 1000 y ns = 10000 en un caso de ejemplo de cuatro zonas de incendio elegidas de forma aleatoria. Las figuras 15.4 y 15.5 presentan la progresión de los parámetros estadísticos para ns 1000.

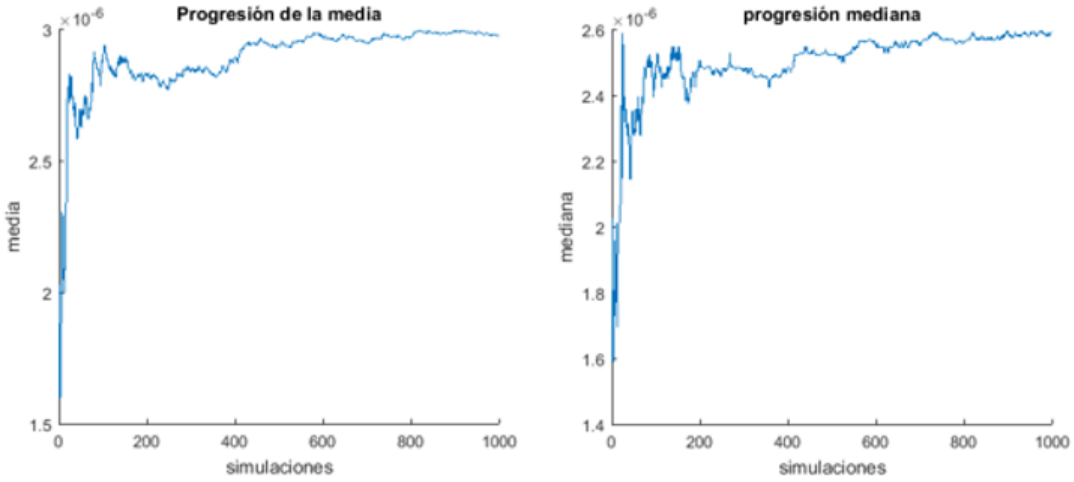


Figura 15.4: Progresión de la media y la mediana para un caso ejemplo con 1000 simulaciones.

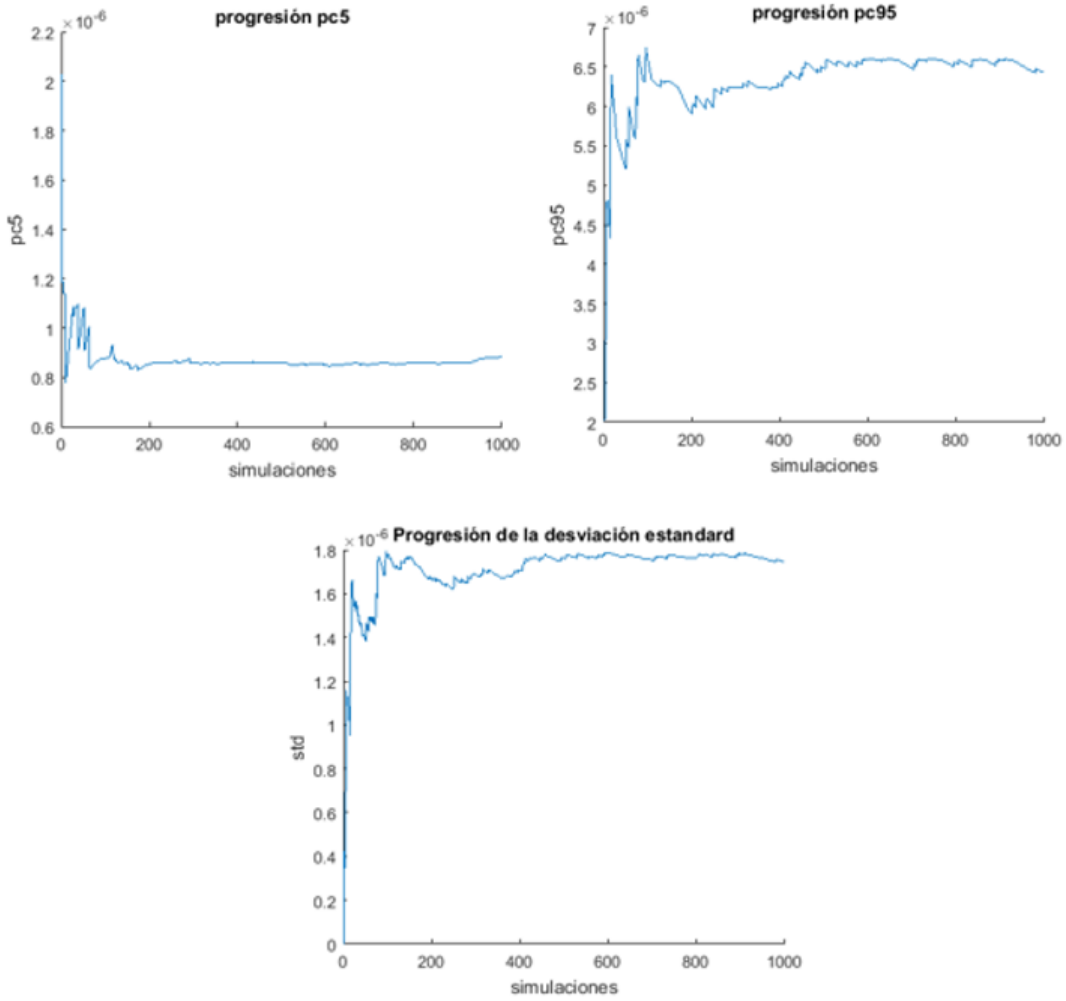


Figura 15.5: Progresión de los percentiles 5 y 95, y de la desviación estándar para un caso ejemplo con 1000 simulaciones.

La estabilidad de la media, del percentil 95, de la mediana y de la desviación estándar es discutible para el caso ns = 1000. Las figuras 15.6 y 15.7 presenta la progresión de los parámetros estadísticos para ns = 10000.

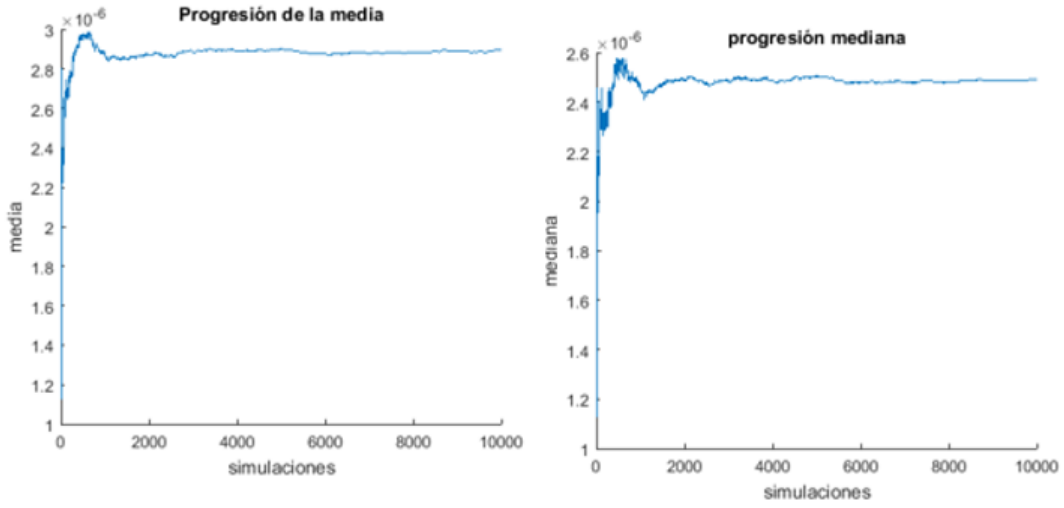


Figura 15.6: Progresión de la media y la mediana para un caso ejemplo con 10000 simulaciones.

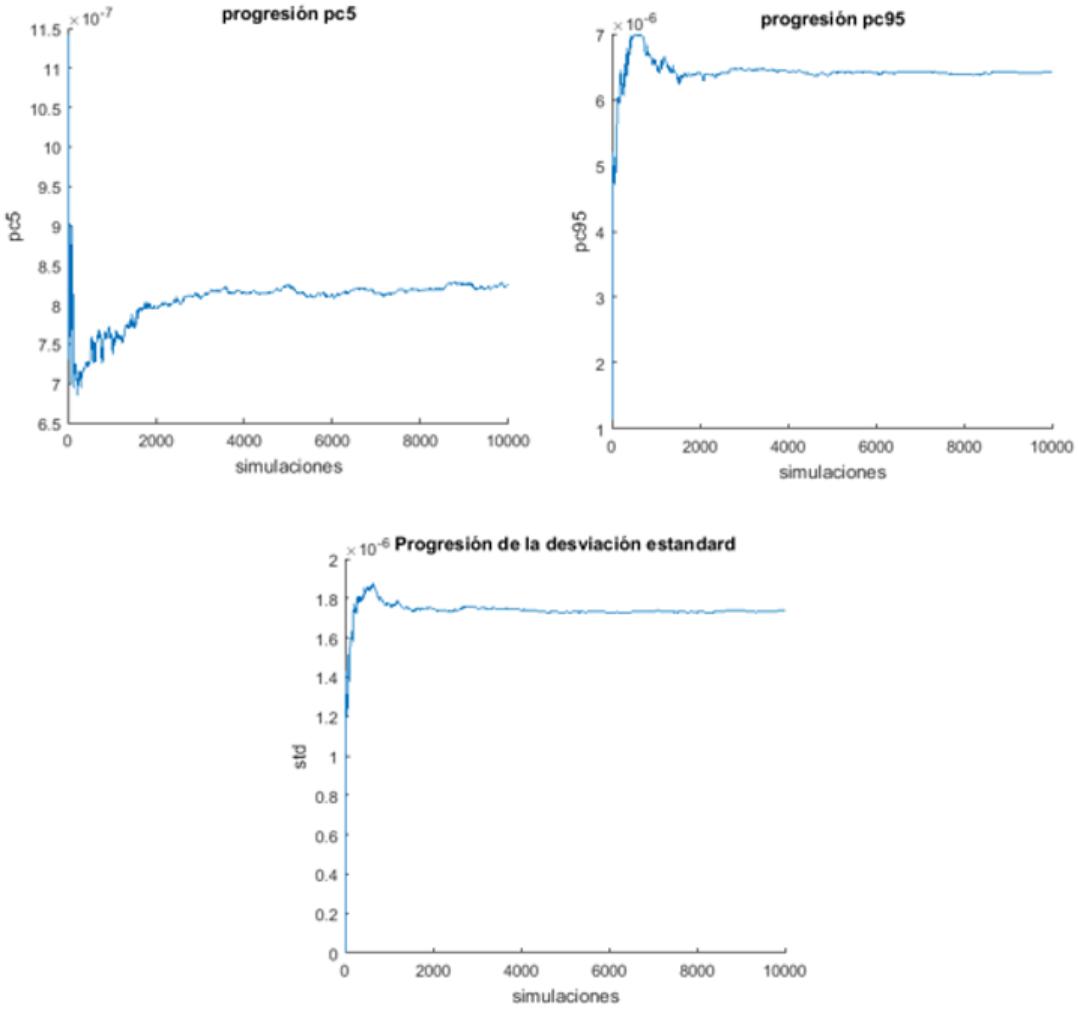


Figura 15.7: Progresión de los percentiles 5 y 95, y de la desviación estándar para un caso ejemplo con 10000 simulaciones.

La media, la mediana, el percentil 95 y la desviación estándar se estabilizan alrededor de las 6000 simulaciones. No obstante, el percentil 5 se estabiliza cerca de las 10000 simulaciones. 10000 simulaciones es una cantidad adecuada para considerar los resultados de los parámetros estadísticos básicos como estables. En consecuencia, se elige 10000 como el número de simulaciones a llevar a cabo mediante el script de la metodología base desarrollado en Matlab®.

15.3.3.4. Validación de la metodología base

La metodología base desarrollada para la estimación de la incertidumbre se valida comparando resultados obtenidos mediante la misma con resultados del módulo de análisis de incertidumbre de *RiskSpectrum® PSA*, que cabe recordar que ha servido de referencia para el desarrollo de dicha metodología base. Concretamente, se comparan los resultados obtenidos para un caso en el que los inputs los forman cuatro tasas de fallo presentes en el modelo APS de incendios detallado.

Modelo de *RiskSpectrum® PSA* para obtener resultados de referencia El modelo de comparación lo forman cuatro tasas de fallo cuya distribución de probabilidad es la distribución Gamma. Las cuatro tasas de fallo han sido elegidas de forma aleatoria de entre todas las tasas de fallo presentes en el modelo APS de incendios detallado de la central nuclear. Las cuatro tasas de fallo son independientes entre sí, tal y como lo son las dFDN. La tabla 15.3 contiene las cuatro tasas de fallo seleccionadas:

ID	Descripción	Media	P1	P2[13]
BL00F	Fallo local barra de CC	8,31E-08	8,67E-01	1,04E+07
BMRS0R	Bomba motorizada falla en operación	2,53E-06	2	7,90E+05
REP2KE	Fallo a energización de relé	1,35E-07	3,01	2,23E+07
VMAA1O	Válvula motorizada falla a permanecer abierta	1,79E-07	2,08	1,15E+07

Tabla 15.3: Tasas de fallo utilizadas en el modelo de validación.

Se ha creado un árbol de fallos cuya *top gate* es una puerta OR que abarca las cuatro tasas de fallo en forma de elementos *Frequency*, es decir, sucesos básicos que representan a una frecuencia. El árbol de fallos con puerta OR representa la suma que se realiza en la metodología base para calcular la FDN de incendios de uno de los elementos de la matriz MCI. La figura 15.8 muestra el árbol de fallos.

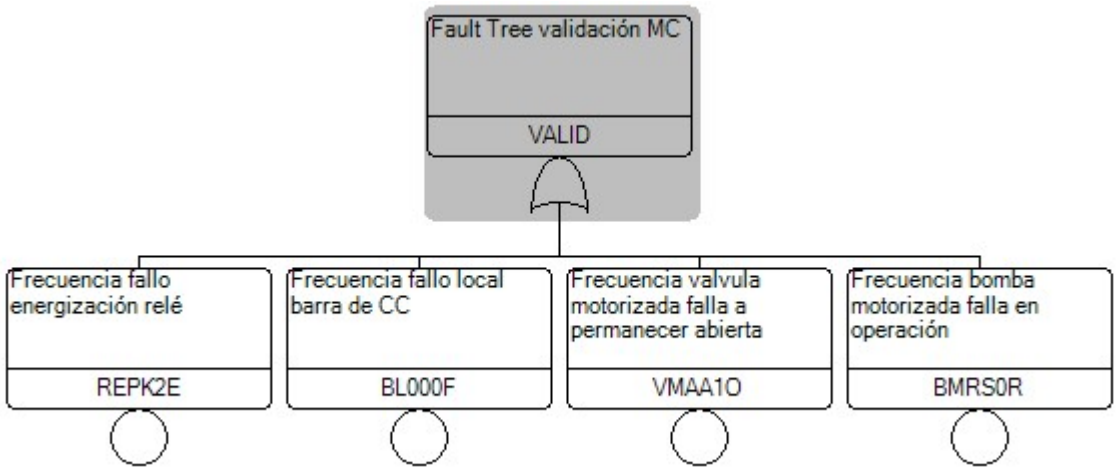


Figura 15.8: Árbol de fallos con puerta OR que suma las cuatro tasas de fallo.

El módulo de análisis de incertidumbre de *RiskSpectrum® PSA* se aplica a un *Fault Tree Analysis Case* asociado al árbol de fallos de la figura 15.8 . Se obtienen de esta manera resultados de referencia de los parámetros básicos de incertidumbre calculados mediante la metodología base. El módulo de análisis de incertidumbre de *RiskSpectrum® PSA* permite obtener parámetros de incertidumbre para diferentes cantidades de simulaciones. Se han obtenido resultados de incertidumbre de referencia para 10000 simulaciones, en consonancia con la cantidad de simulaciones a realizar en la metodología base.

Ajuste del script de la metodología base En el caso de la validación, las distribuciones de probabilidad de los inputs, las tasas de fallo, son conocidas. Matlab® permite obtener parejas de valores de *cummulative distribution functions* cuya distribución de probabilidad es conocida. En consecuencia, se modifica la adquisición del input del *script* de aplicación de la metodología base para que proporcione parejas de valores de la CDF de distribuciones de probabilidad conocidas, las asociadas a las tasas de fallo. Estas parejas de valores cubren el total del rango de probabilidad acumulada (de 0 a 1) en intervalos

de 0,1, tal y como lo hacen las CDF introducidas en el script de la metodología base presentado en la sección 15.3.3.2. El anexo R contiene una explicación más detallada del ajuste realizado sobre el script de la metodología base para que adquiera valores de CDFs de distribuciones de probabilidad conocidas.

Comparación de resultados. Validación La tabla presenta los resultados obtenidos mediante el módulo de incertidumbres de *RiskSpectrum® PSA* y mediante el script de aplicación de la metodología base.

ns = 10000	media	mediana	pc5	pc95
RiskSpectrum® PSA	2,91E-06	2,50E-06	8,17E-07	6,38E-06
Script de validación	2,89E-06	2,49E-06	8,24E-07	6,42E-06

Tabla 15.4: Comparación de resultados para la validación de la metodología base.

Los resultados obtenidos mediante el *script* de validación de la metodología base son prácticamente idénticos a los resultados de referencia obtenidos mediante RiskSpectrum® PSA. En consecuencia, el *script* de aplicación de la metodología base escrito en software Matlab® es válido para su utilización en la aplicación del análisis de incertidumbre a la matriz de compatibilidades de indisponibilidades.

15.3.4. Aplicación de la metodología base al conjunto de la matriz MCI

El script presentado en el apartado anterior está preparado para llevar a cabo 10000 simulaciones a partir de archivos de texto input del tipo .UNC, véase el anexo R, presentes en el directorio de ejecución del script. El resultado de la aplicación del script son los parámetros estadísticos asociados a las 10000 simulaciones. Tal y como se ha comentado anteriormente, el script de la metodología base solo sirve para calcular los parámetros estadísticos de un elemento de la matriz. Con el objetivo de aplicar el script de la metodología base a todos y cada uno de los elementos de la matriz MCI, se ha generado una estructura de carpetas, véase la figura 15.9, que organiza los inputs, es decir los archivos .UNC de las dFDN, de las simulaciones de cada elemento de la matriz.

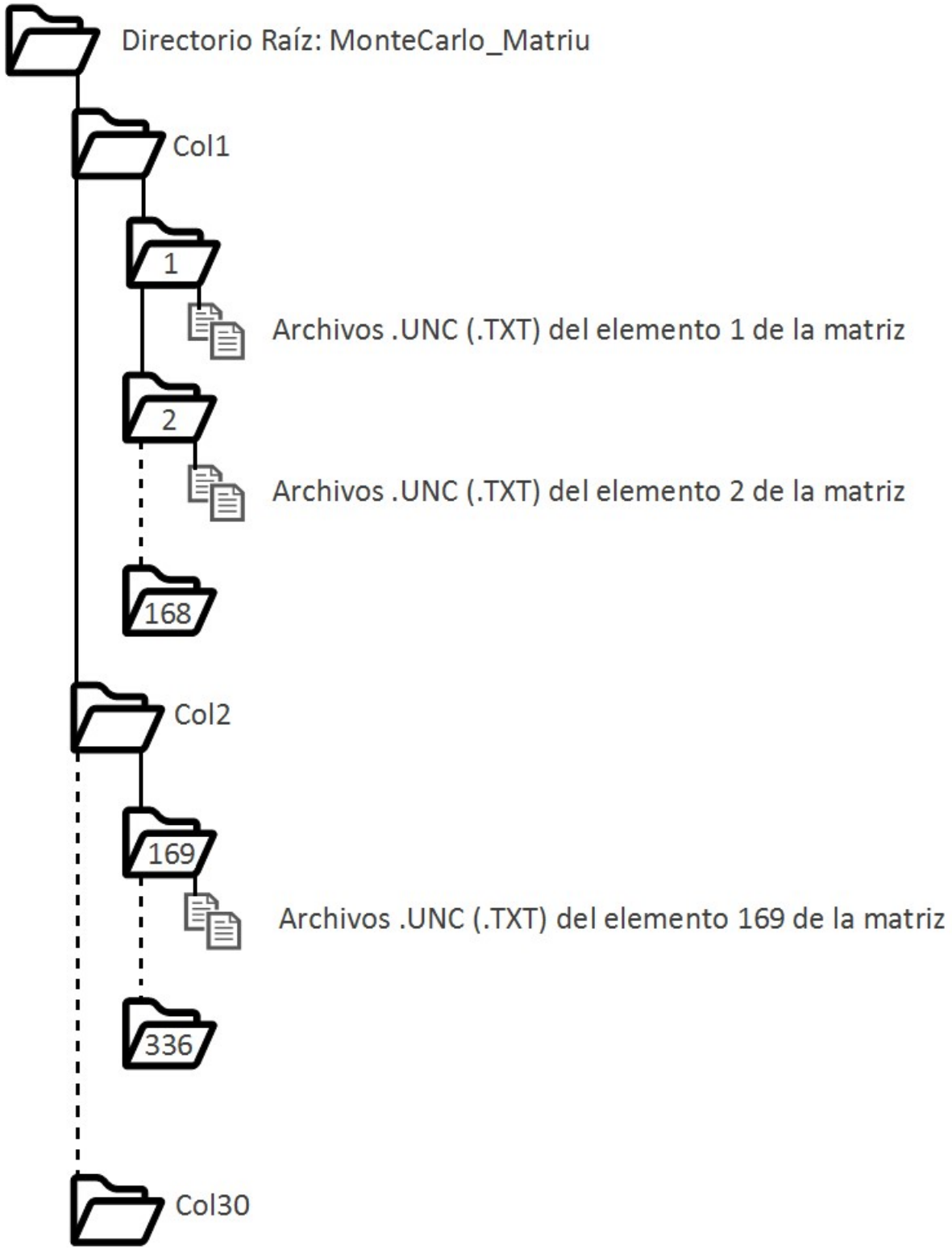


Figura 15.9: Estructura de carpetas que permite aplicar el análisis de incertidumbre a la matriz MCI.

Una carpeta principal llamada *MonteCarlo_ Matriu* incluye 30[14] carpetas llamadas colXX donde XX es el número de columna de la matriz MCI que representan dichas carpetas. Carpetas que representan a los elementos de la matriz asociados a las columnas de la matriz se encuentran en el interior las carpetas colXX. Cada columna contiene 168 elementos de la matriz. La nomenclatura de las carpetas elemento de la matriz es un identificador numérico que se corresponde con el índice del elemento de la matriz en la propia matriz. Se ordenan los elementos de la matriz a partir del elemento (1,1), al que se le asigna el identificador 1, y se barren primero columnas y luego filas. Así, el elemento de la matriz (1,2) es el elemento 169 según la ordenación estipulada. A modo de ejemplo, la carpeta col1 contiene 168 carpetas con identificadores 1 a 168 y la carpeta col2 contiene 168 carpetas con identificadores 169 a 336. Dentro de cada carpeta elemento de la matriz se colocan los archivos .UNC input de las simulaciones de cada elemento de la matriz. Se ha cambiado la extensión de los archivos .UNC a .TXT para evitar problemas de reconocimiento. La descripción del procedimiento seguido para incluir los archivos de incertidumbre .UNC en la estructura de carpetas queda fuera de alcance de este documento.

El script de la metodología base se ha ampliado para que sea capaz de aplicar la parte de la simulación,véase el anexo R, en cada una de las carpetas elemento de la matriz. Se han añadido órdenes del tipo *for* que cambian el directorio de trabajo al del siguiente elemento de la matriz cada vez que se ha llevado a cabo el proceso de simulación para el elemento de la matriz previo. Se han añadido variables para colocar los parámetros estadísticos resultado de cada elemento de la matriz MCI en un grupo de matrices resultado, una por parámetro estadístico, en la misma posición que la que ocupa el elemento en la matriz MCI. Las figuras del anexo R muestran el script utilizado para aplicar el análisis de incertidumbre a todos los elementos de la matriz.

15.3.5. Resultados del análisis de incertidumbre

El anexo S contiene la matriz de compatibilidades de indisponibilidades que incluye los valores promedio de la FDN de incendios de planta calculados mediante el análisis de incertidumbre, y la matriz de compatibilidades de indisponibilidades que incluye los valores percentil 95 de la FDN de incendios total de planta. Los valores promedio obtenidos mediante el análisis de incertidumbre son siempre mayores que los valores puntuales obtenidos mediante la cuantificación detallada en el capítulo 14. No obstante, el incremento es mínimo; por ejemplo, para el caso del primer elemento de la matriz el incremento es de 2,06E-07, que corresponde a un 2 % del propio valor del primer elemento de la matriz. 161 elementos de la matriz, un 3,4 % del total de 4704, cambian a la categoría de valoración del riesgo inmediatamente superior en la comparación entre valores promedio y valores puntuales. 146 de los 161 elementos pertenecen a la columna 8 de la matriz (suceso básico 1BHXXXXXAF) y tienen valores puntuales en torno al 1,30E-4, muy próximo al valor de FDN límite entre los rangos amarillo y naranja, que es de 1,31E-04. El incremento medio de los elementos de la columna 8 es de 6,06E-06, dos órdenes de magnitud por debajo de los propios valores de FDN asociados a los elementos de la columna. En la comparación entre valores percentil 95 y valores promedio, 266 elementos de la matriz, un 5,65 % del total, cambian a la categoría de valoración del riesgo inmediatamente superior. 152 de los 266 pertenecen a la columna 28 de la matriz (suceso básico 1VNXXXXX1A) y tienen valores promedio en torno a 1,19E-04, muy próximo al valor de FDN límite entre los rangos amarillo y naranja.

427 elementos de la matriz, un 9 % del total de 4704, cambian a la categoría de valoración del riesgo inmediatamente superior en la comparación entre valores percentil 95 y valores puntuales. Ningún elemento de la matriz ha cambiado su categoría de riesgo a una dos veces superior a pesar de las dos fuentes de incremento. La mayoría de los elementos que cambian de categoría de valoración del riesgo pertenecen a las columnas 8 y 28, cuyos valores puntuales son muy próximos al valor de FDN límite entre los rangos amarillo y naranja, que es de 1,31E-04. El resto de elementos pertenecen a diferentes columnas, pero, en

[14] En un primer análisis, la matriz MCI contenía 2 sucesos básicos de componentes representativos de funciones clave de seguridad más. El análisis de incertidumbre se realizó cuando estos sucesos aún no habían sido eliminados del alcance de la matriz.

todo caso, el motivo más plausible para su aumento de categoría de riesgo es la proximidad al umbral entre dos categorías.

Las figuras 15.10, 15.11, y 15.12 presentan, a modo de ejemplo, el análisis de incertidumbre de las columnas 7, 8, y 28, respectivamente. Las figuras 15.11 y 15.12 plasman la influencia que tienen las columnas 8 y 28 sobre la cantidad de elementos que ven aumentada su categoría de riesgo. Los valores puntuales de las columnas 8 y 28 son tan próximos al valor límite entre la categoría de riesgo amarilla y la naranja que todos aquellos que no lo estaban ya pasan a ser considerados de riesgo alto (naranja) pese a que la incertidumbre asociada dichos valores es similar a la de otros casos como el de la columna 7. En el caso de la columna 7, prácticamente ningún valor percentil 95 pasa a la categoría de riesgo inmediatamente superior debido a que la incertidumbre asociada a los valores de FDN no es lo suficientemente importante.

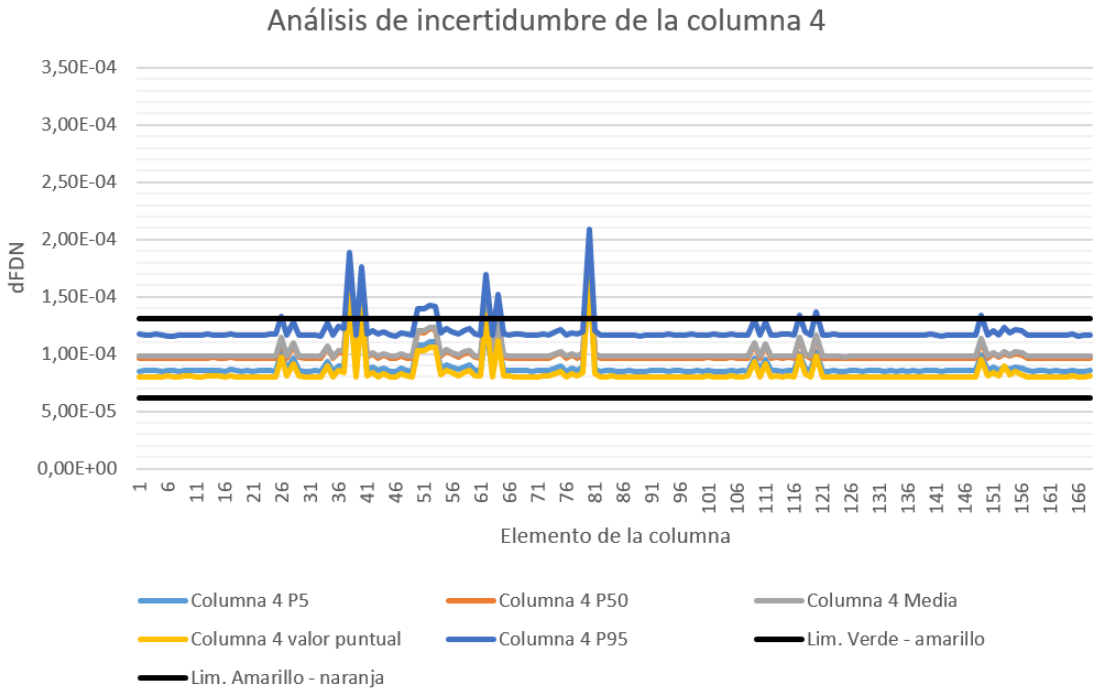


Figura 15.10: Análisis de incertidumbre de la columna 7.

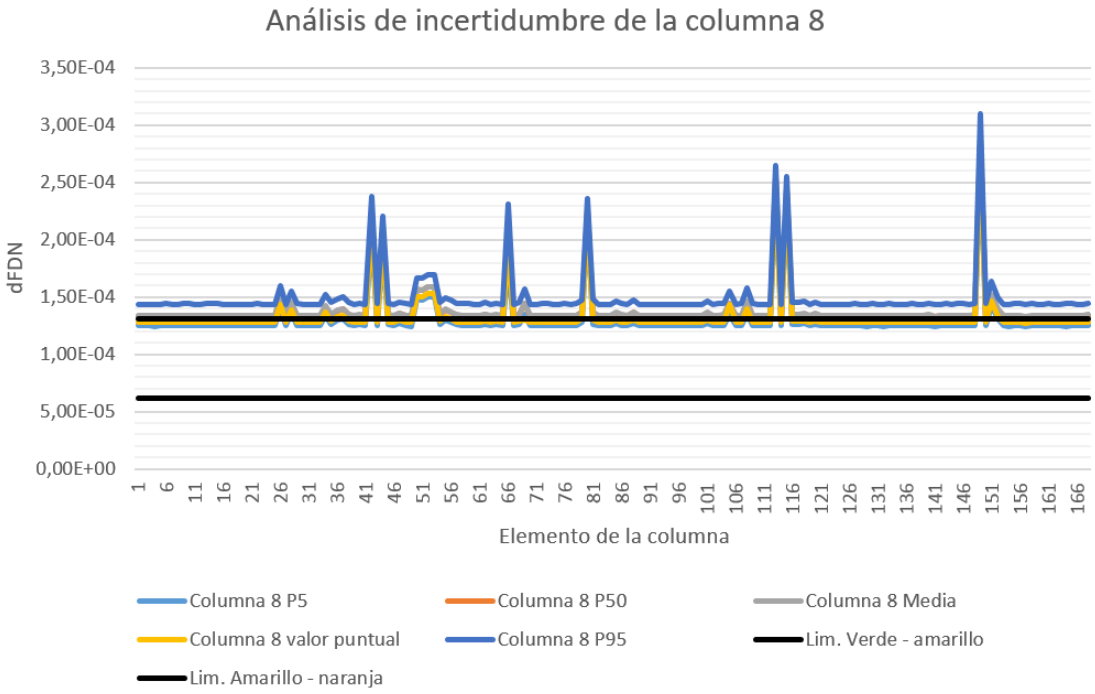


Figura 15.11: Análisis de incertidumbre de la columna 8.

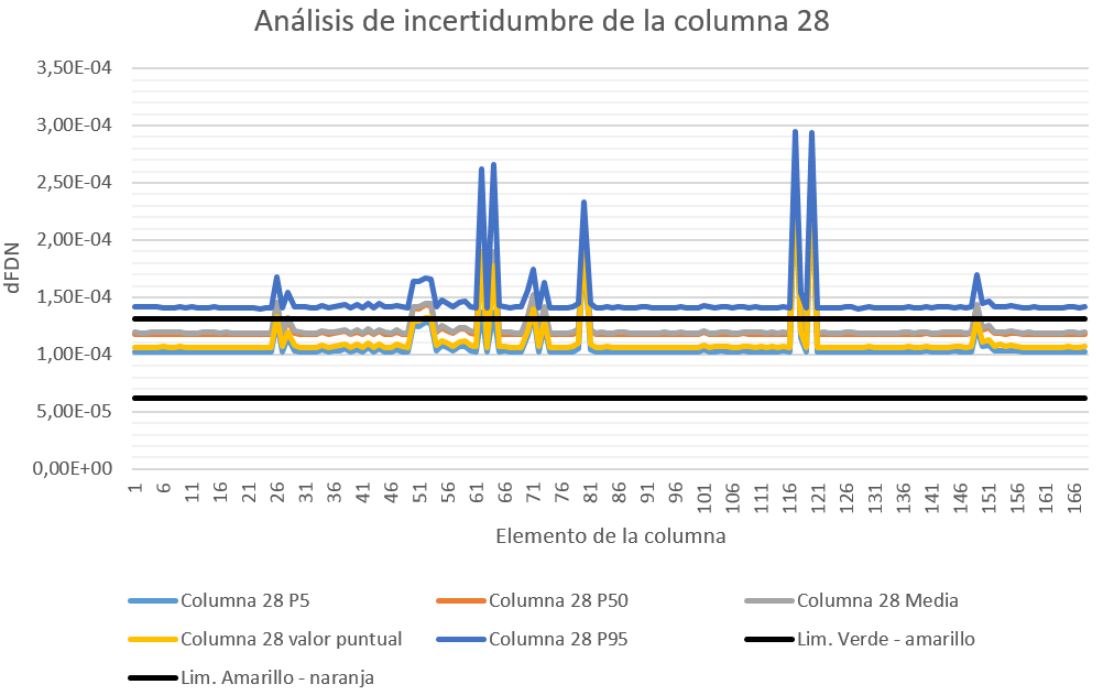


Figura 15.12: Análisis de incertidumbre de la columna 28.

15.3.6. Conclusiones

Se considera el percentil 95 de la FDN de incendios total de planta como la figura representativa de la incertidumbre asociada al análisis matricial y a los inputs del propio análisis. La comparación entre valores percentil 95 y valores puntuales muestra que 427 elementos de la matriz del total de 4704, es decir, un 9 % del total, cambian a la categoría de valoración del riesgo inmediatamente superior. La comparación de los valores extremo, percentil 95 y valor puntual, señala que las dos columnas más afectadas por el análisis y cuantificación de la incertidumbre son la columna 8 y la columna 28. En ambas, la mayoría de elementos pasa de categoría de riesgo amarillo a riesgo naranja. Sin embargo, el cambio de categoría de riesgo se explica por la proximidad de los valores de estas columnas al umbral numérico que separa las categorías mencionadas, no por una elevada incertidumbre asociada a los elementos de estas columnas. Cabe destacar que ningún elemento de la matriz pasa a la categoría de riesgo alto (rojo), ni se acerca, por motivo de añadir a los valores puntuales su incertidumbre asociada.

En conclusión, la incertidumbre asociada al análisis matricial y a los inputs del propio análisis es baja y poco significativa debido a que:

- Solo un 9 % de los elementos de la matriz pasan a una categoría de riesgo superior en la comparación entre valores percentil 95 y valores puntuales. La mayoría de estos elementos ya estaban asociados a categorías de riesgo significativo, es decir, amarillo o superior.
- Tal y como plasman las figuras 15.11 y 15.12, la gran mayoría de este 9 % de elementos que ven aumentada su categoría de riesgo lo hacen por motivo de que sus valores puntales son muy próximos al umbral que separa dos categorías de riesgo y no a raíz de una incertidumbre elevada.
- Ningún elemento de la matriz pasa a la categoría de riesgo alto (rojo), ni se acerca, por motivo de añadir la incertidumbre asociada a los valores puntuales.
- En ningún caso un elemento de la matriz pasa a una categoría de riesgo dos veces superior (p.ej: de verde a naranja) por motivo del análisis de incertidumbre. Teniendo en cuenta la proximidad entre el umbral de las categorías verde y amarillo y el umbral de las categorías amarillo y naranja, 5E-05 aproximadamente[15], este resultado también es un indicativo de la baja incertidumbre asociada a los elementos de la matriz MCI.

Se concluye en consecuencia que los resultados de la matriz de compatibilidades de indisponibilidades de sistemas contra incendio y funciones clave de seguridad son robustos y fiables desde el punto de vista de la incertidumbre. Las columnas 8 y 28 se señalan como casos especiales en los que la proximidad de sus valores al umbral entre las categorías de riesgo amarillo y naranja no permite discernir a cual de ella pertenecen. No obstante, por conservadurismo, se asignan a la categoría de riesgo naranja en la sección 15.4.

15.4. Análisis de resultados

15.4.1. Introducción

La sección anterior demuestra que la incertidumbre asociada a los resultados de las matrices MCI y MRI es lo suficientemente baja como para interpretar estos resultados con la confianza de que las conclusiones extraídas no serán de poco valor. La interpretación de los resultados de la matriz MCI se dirige a:

[15] Mientras que la categoría de riesgo amarillo barre un 5E-05 del rango de FDN, la categoría de riesgo naranja barre un 9E-04 del rango de FDN.

- Identificar aquellas ESCs cuya indisponibilidad tiene un impacto en el riesgo significativo. La inclusión de dichas ESCs en la regla de mantenimiento debería tomarse en consideración.
- Identificar aquellos sistemas contra incendios que podrían incluirse en la regla de mantenimiento porque su indisponibilidad tiene un impacto significativo en el riesgo.
- Evaluar las combinaciones de indisponibilidad de sistemas contra incendio y funciones clave de seguridad. Analizar qué sistemas contra incendios habría que tener bajo vigilancia durante el mantenimiento de un equipo debido a que la indisponibilidad combinada de ambos, el sistema contra incendios y el equipo, pondría a la planta en un nivel de riesgo inaceptable. A la inversa, analizar qué equipos habría que tener bajo vigilancia durante el mantenimiento de un sistema contra incendios.

Por su parte, la interpretación de los resultados de la matriz MRI se dirige a identificar qué zonas de incendio son las más significativas para el riesgo inducido por incendios de la central nuclear. De forma más precisa, la matriz MRI permite analizar en qué zonas de incendio de la planta se deberían aplicar acciones para gestionar y reducir el riesgo inducido por incendios en caso de indisponibilidad de un equipo representativo de funciones claves de seguridad de la central. A continuación se presenta, por separado para cada matriz, el proceso de interpretación de resultados y las conclusiones extraídas.

15.4.2. Interpretación de resultados de la matriz MCI

La tabla 15.5 presenta la cantidad de elementos de la matriz MCI que pertenecen a cada uno de los niveles de riesgo definidos en los criterios de valoración del riesgo. La matriz MCI se puede consultar en el anexo S. A raíz del análisis de incertidumbre, se considera que los elementos de las columnas 8 y 28 pertenecen todos a la franja de riesgo alto (Naranja).

Color	Nivel de riesgo	Cantidad absoluta	% del Total
Verde	Muy bajo	3644	77,4
Amarillo	Bajo	211	4,5
Naranja	Moderado	681	14,5
Rojo	Alto	168	3,6
	Total	4704	

Tabla 15.5: Elementos de la matriz asociados a cada nivel de riesgo

La primera conclusión que se extrae en la interpretación de los resultados de la matriz MCI es positiva: la gran mayoría de combinaciones de indisponibilidad de sistemas contra incendios y funciones clave de seguridad analizadas en el marco de la matriz MCI tienen un nivel de riesgo inducido por incendios Muy bajo (región verde). Las situaciones descritas por los elementos de la matriz pertenecientes a la región verde no resultan una preocupación desde el punto de vista de la seguridad, y no requieren de la aplicación de medidas correctivas siempre y cuando se recupere la situación normal en un tiempo prudencial. Concretamente, tres de cada cuatro combinaciones estudiadas pertenecen al nivel de riesgo Muy Bajo y no son significativas desde el punto de vista del riesgo. Cabe destacar que la cantidad de elementos de riesgo moderado es superior a los de riesgo bajo debido a que se han incluido la totalidad de elementos de las columnas 8 y 28 en dicha categoría a raíz de las conclusiones extraídas en el análisis de incertidumbre.

Respecto a los elementos asociados a un nivel de riesgo bajo o superior, es decir, las regiones amarillo, naranja, y rojo, se destaca que la gran mayoría de estos elementos se concentra en seis columnas (representantes de funciones clave de seguridad) y una fila (representantes de sistemas contra incendios). Los

equipos representantes de función clave de seguridad y el sistema contra incendios asociados a estas seis columnas y una fila son[16]:

- Una de las bomba motorizadas del sistema de Agua de Alimentación Auxiliar. El sistema de agua de alimentación auxiliar es el que proporciona condensado a los generadores de vapor en caso de parada del reactor.
- Las dos barras de salvaguardias de media tensión (cada una está asociada a una columna). Estas barras proporcionan alimentación eléctrica a través de la red exterior o de los generadores diésel de emergencia a todos los equipos que se necesitan para llevar a la central a parada segura.
- Una válvula neumática del sistema de agua de servicios de salvaguardias. Este sistema es el que disipa el calor producido en el sistema primario al último sumidero de calor.
- Una de las válvulas de retención del sistema de inyección de seguridad.
- Una de las barras de corriente continua de la central. Estas barras son especialmente importantes para la seguridad en caso de *Station Black-out* (SBO).
- El sistema contra incendios de extinción de la zona CXXX1.

La tabla 15.6 indica el nivel de riesgo, el sistema, y la función clave de seguridad asociada de cada uno de los siete equipos indicados. Se destaca que la barra de corriente continua es el único de estos siete equipos cuyos elementos de la matriz pertenecen al nivel de riesgo Alto.

Descripción	Riesgo	Sistema	Función Clave de Seguridad
Bomba motorizada	Bajo	Agua de alimentación auxiliar	Sumidero de calor
Extinción de Sala de Control	Bajo	Contra incendios	
Barra de salvaguardias A	Moderado	Suministro eléctrico	Suministro eléctrico
Válvula neumática	Moderado	Agua de servicios de salvaguardias	Sumidero de calor
Válvula de retención	Moderado	Inyección de alta presión	Inventario del RCS
Barra de salvaguardias B	Moderado	Suministro eléctrico	Suministro eléctrico
Barra de corriente continua	Alto	Suministro eléctrico	Suministro eléctrico

Tabla 15.6: Sistemas contra incendios y equipos representantes de función de seguridad significativos para el riesgo.

En conclusión, se han de incluir nuevas restricciones y/o declaraciones en la regla de mantenimiento de la central que hagan referencia a estos seis equipos y a este sistema en caso que no los hubiese ya. Aparte de los elementos de la matriz que pertenecen a las columnas y fila de los equipos indicados, existe una pequeña cantidad de combinaciones de indisponibilidad aisladas cuyo nivel de riesgo asociado es Bajo o mayor. Concretamente, son 30 los elementos de la matriz cuyo riesgo asociado es Bajo o mayor y que no pertenecen a las columnas y filas de los equipos indicados. Estas 30 combinaciones de indisponibilidad son la única evidencia del impacto en el riesgo inducido por incendios de la central de la indisponibilidad

[16] Por motivos de confidencialidad no se proporciona una descripción más detallada de estos componentes.

de sistemas contra incendios más allá de la fila perteneciente al sistema de extinción de la zona CXXX1. En consecuencia, se concluye que, aparte de la indisponibilidad del sistema de extinción de CXXX1, la indisponibilidad de sistemas contra incendios no tiene un impacto en el riesgo suficiente como para que se vea reflejado en los resultados de la matriz MCI. Los sistemas contra incendios asociados a estos 30 elementos aislados cuyo de nivel de riesgo es Bajo o mayor pertenecen a los edificios Auxiliar, Control, y el edificio de las bombas de agua de alimentación auxiliar. Los resultados de la matriz MCI indican que las combinaciones de indisponibilidad cuyo riesgo inducido por incendios es significativo están en su mayoría influenciadas por la indisponibilidad de seis equipos representativos de funciones clave de seguridad.

15.4.2.1. Análisis de importancia de sistemas contra incendio

Debido a la concentración de combinaciones de indisponibilidad significativas para el riesgo en seis filas y una columna de la matriz MCI, no es posible obtener conclusiones al respecto de la diferente influencia en el riesgo de incendios de los sistemas contra incendio mediante un análisis visual de la matriz. No obstante, se conoce que existen 30 combinaciones de indisponibilidad aisladas cuyo riesgo es significativo y que, aunque no se plasme en diferentes niveles de riesgo, existen diferencias respecto a las FDN promedio asociadas a la indisponibilidad de los sistemas contra incendio. Por lo tanto, la indisponibilidad de cada sistema contra incendio tiene una influencia diferente sobre el riesgo inducido de incendios de la central. Se ha llevado a cabo un análisis de importancia para obtener una valoración cuantitativa de la influencia en el riesgo de la indisponibilidad de cada sistema contra incendio.

La metodología de análisis de importancia de sistemas contra incendios se fundamenta en la comparación entre dos estados de planta. Específicamente, se compara el estado planta en el que un sistema contra incendios está indisponible, con el estado de planta en el que ningún sistema contra incendios indisponible. La indisponibilidad de un sistema contra incendios está representada por una fila de la matriz, en la que hay 28 columnas, cada una representando un estado diferente de las funciones clave de seguridad. Se le llama fila nominal a la primera fila de la matriz, que representa el estado de planta en el que no hay ningún sistema contra incendios indisponible. La fila nominal comparte con cualquier otra fila las mismas condiciones que imponen las 28 columnas. Es por lo tanto posible hacer la comparación $FDN_{i,j}$ con $FDN_{0,j}$ para todo valor de j $(0-27)$. Se aprovecha la circunstancia de que las columnas imponen las mismas condiciones a todas las filas para obtener un valor representativo de cada fila usando el promedio establecido en la ecuación 15.3.

$$promedio_i = \left(\sum_{j}^{n} FDN_{i,,j} \right) / n \tag{15.3}$$

El promedio de cada fila se compara con el de la fila con la fila nominal, la fila i=0. Al no tener ningún sistema contra incendios indisponible, el promedio de la fila nominal es el límite inferior de los promedios de todas las filas. Cuánto más grande es el valor promedio de una fila en comparación con el de la fila nominal, más alto es el impacto que tiene la indisponibilidad de un sistema contra incendios en el riesgo inducido por incendios de la central. Se utiliza la figura "error relativo respecto al promedio base", descrita en la ecuación 15.4 , para poder comparar la importancia en el riesgo de la indisponibilidad de un sistema contra incendios frente a la indisponibilidad de otros.

$$error\,relativo_i = \frac{promedio_i - promedio_0}{promedio_0} \tag{15.4}$$

Los sistemas contra incendio cuya indisponibilidad tiene un mayor impacto en el riesgo inducido por incendios se muestran en la Tabla 15.7, junto al error relativo asociado a cada uno de ellos.

Zona y tipo de sistema contra incendios	Error relativo
CXXX1-EXT	1,57
SXXX7 - PDA	0,85
CXXX9 - PDA	0,53
CXXX8 - PDA	0,47
CXXX6 - TERM	0,43
CXXX6 - CO2	0,43

Tabla 15.7: Sistemas contra incendio con mayor error relativo.

Tal y como se ha indicado anteriormente, el sistema contra incendios cuya indisponibilidad tiene una mayor influencia sobre el riesgo inducido de incendios de la central es el sistema de extinción de CXXX1. Los sistemas contra incendios cuya indisponibilidad tiene una mayor influencia sobre el riesgo inducido por incendios de la central son: el sistema de detección de la zona donde se encuentra un panel de accionamiento remoto en el edificio de las bombas de agua de alimentación auxiliar (SXXX7 - PDA), el sistema de detección de una sala de cabinas de media tensión del tren A (CXXX9 - PDA), el sistema de detección de una de las salas de instrumentación y equipo eléctrico del tren A (CXXX8 - PDA), el sistema de detección termovelocimétrico de la sala de cables (CXXX6 - TERM), y el sistema de extinción por inundación de CO_2 de la misma sala de cables (CXXX6 - CO2). Todas las zonas cuyo identificador tiene por primera letra una C pertenecen al edificio de Control. En conclusión, se ha de valorar incluir nuevas restricciones y/o declaraciones en la regla de mantenimiento de la central que hagan referencia a estos sistemas contra incendio en caso que no los hubiese ya.

15.4.3. Interpretación de resultados de la matriz MRI

A la vista de las conclusiones extraídas en la interpretación de los resultados de la matriz MCI, dedicadas particularmente a los equipos representativos de funciones clave de seguridad, los resultados de la matriz MRI permiten ampliar las conclusiones relacionadas con las zonas y sistemas contra incendio. La matriz MRI, que se presenta en el anexo S, permite conocer qué zonas de incendio son las que tienen una mayor contribución respecto a la FDN inducida por incendios de la central cuando uno de los equipos representativos de función clave de seguridad del listado obtenido en el capítulo 13 se encuentra indisponible. Sin embargo, tal y como se ha visto en la interpretación de resultados de la matriz MCI, únicamente 6 de los 27 equipos represenativos de FCS son importantes desde el punto de vista del riesgo. Consecuentemente, la interpretación de resultados de la matriz MRI se dirige a extraer qué zonas son las que tienen una mayor contribución respecto a la FDN inducida por incendios de la central cuando uno de estos seis equipos se encuentra indisponible. A continuación se listan las zonas identificadas[17] para cada equipo:

- Bomba motorizada del sistema AAA (columna 4):
  - Zona CXXX3.
  - Zona SXXX0.
  - Zona CXXX8.
- Barra de salvaguardias A (columna 7):
  - Zona SXXX0.
  - Zona CXXX3.
- Válvula neumática de agua de servicios de salvaguardias (columna 27):

[17] Por motivos de confidencialidad, en esta memoria, no se pueden indicar los códigos ni las descripciones de estas zonas.

    - Zona PEXXX3.
    - Zona CXXX8.

- Válvula de retención de inyección de seguridad a alta presión (columna 26):
    - Zona RXXX4.
    - Zona RXXX9.
    - Zona RXXX3.

- Barra de salvaguardias B (columna 8):
    - Zona PEXXX2.
    - Zona CXXX5.
    - Zona CXXX9.

- Barra de corriente continua (columna 9):
    - Zona CXXX5.
    - Zona CXXX9.
    - Zona PEXXX0.

Por lo tanto, de las 41 zonas analizadas en el modelo APS de incendios detallado[18] de la central, se identifican 11 zonas de incendio significativas para el riesgo. Las zonas identificadas contienen equipos, o cables asociados a equipos, que quedarían indisponibles en caso de incendio en la zona provocando, en combinación con la indisponibilidad del equipo representativo de función clave de seguridad indicado, un aumento de la FDN inducida por incendios de la central. Todas estas zonas son candidatas a ser el objetivo de acciones de gestión del riesgo (*Risk Management Actions*, RMA) como, por ejemplo: incremento de la frecuencia de rondas que pasan por la zona, o la retirada de combustibles transitorios. El hecho de que la zona CXXX1 no aparezca entre las de mayor riesgo pone de manifiesto que la aparición de su sistema de extinción entre los elementos de riesgo significativo, ver tabla 15.6 anterior, se debe principalmente a la importancia del propio sistema contra incendios de esa zona y no a la importancia de la zona.

[18] La cantidad total de zonas es mucho mayor a 41 pues se ha llevado a cabo un proceso de cribado de zonas no contribuyentes al riesgo durante el desarrollo del modelo APS.

Capítulo 16

Conclusiones

La investigación llevada a cabo para analizar la manera de introducir el riesgo inducido por incendios en los procesos de toma de decisión informada por el riesgo ha concluido con el desarrollo de dos herramientas de valoración del riesgo que utilizan los resultados de un APS de incendios. Las dos herramientas desarrolladas tienen una estructura matricial y permiten evaluar el impacto de las estructuras, sistemas, y componentes incluidos en el APS de incendios en el riesgo inducido por incendios de la central nuclear analizada. Por consiguiente, la información resultante de aplicar estas herramientas tiene por objetivo el ser utilizada en procesos de decisión informados por el riesgo como, por ejemplo, la regla de mantenimiento. La primera de las herramientas desarrolladas es la matriz MCI: matriz de compatibilidades de indisponibilidades de sistemas contra incendio y funciones clave de seguridad. Dicha matriz contiene, en cada uno de sus elementos. la frecuencia de daño al núcleo inducida por incendios de una central condicionada a la indisponibilidad combinada de sistemas contra incendios y funciones clave de seguridad. La matriz MCI permite identificar aquellas ESCs, incluyendo sistemas contra incendios, cuya indisponibilidad tiene un impacto en el riesgo inducido por incendios significativo. La inclusión de dichas ESCs en la regla de mantenimiento debería tomarse en consideración. La segunda herramienta diseñada es la matriz MRI: matriz de riesgo de incendio de zonas de incendio y funciones clave de seguridad. Esta matriz incluye la contribución de cada zona de incendio a la frecuencia de daño al núcleo de la central, es decir, la frecuencia de daño al núcleo debida únicamente a incendios que puedan ocurrir en la zona objetivo, condicionada a la indisponibilidad de ESCs representativos de funciones claves de seguridad. La matriz MRI permite identificar qué zonas de incendio son las más significativas para el riesgo inducido por incendios de la central o, de forma más precisa, en qué zonas de incendio de la planta se deberían aplicar acciones para gestionar y reducir el riesgo inducido por incendios en caso de indisponibilidad de un equipo representativo de funciones claves de seguridad. Las herramientas matriciales descritas se han desarrollado y aplicado para un caso real de una central nuclear española. La central nuclear española ha prestado su apoyo en cuestiones técnicas y ha cedido la última versión de APS de incendios disponible en el formato del software *RiskSpectrum® PSA*.

El proceso de cuantificación de las matrices ha requerido del apoyo de scripts de programación ajenos al software *RiskSpectrum® PSA* para obtener los resultados de las matrices en un tiempo razonable. Pese a que la base matemática de cálculo de los elementos de la matriz es sencilla, el gran tamaño de las matrices, (168,28) para la matriz MCI y (43,28) para la MRI, y la complejidad interna del modelo APS de incendios detallado, han hecho imposible obtener los resultados de la matriz en un tiempo manejable utilizando únicamente *RiskSpectrum® PSA*. Se ha diseñado un proceso de cuantificación que, aparte de optimizar la obtención de datos de frecuencia de daño al núcleo mediante el modelo APS, utiliza dos scripts escritos en lenguaje *Python*$^{\text{TM}}$que organizan los datos obtenidos de *RiskSpectrum® PSA* y realizan los cálculos necesarios para obtener las matrices MCI y MRI. El proceso de cuantificación diseñado ha permitido obtener, en un ordenador de sobremesa al uso, ambas matrices en un tiempo de cálculo de 24,33

horas. Se ha estimado que, de no utilizar estos scripts, la obtención de ambas matrices mediante métodos convencionales podría tardar unas 780 horas aproximadamente.

Los resultados cuantitativos al respecto de una figura de riesgo como, por ejemplo, la frecuencia de daño al núcleo, son difícilmente valorables por sí solos. Es decir, un análisis a simple vista de los resultados no permite discernir si la configuración representada por la figura de riesgo objetivo es significativa o no, a no ser que el valor de ésta sea extremadamente alto o bajo. Se hace necesario, en consecuencia, establecer unos criterios cuantitativos de valoración del riesgo para poder interpretar los resultados y extraer las conclusiones oportunas. Dichos criterios varían según si se analiza una situación permanente, como, por ejemplo, una modificación de diseño, o una situación temporal. En el caso de las matrices MCI y MRI se evalúan configuraciones temporales de planta tales como la indisponibilidad de uno o más ESCs. Las situaciones temporales se analizan mediante criterios de valoración del riesgo basados en el concepto de incremento de probabilidad de riesgo asociado al tiempo de exposición a la situación analizada. Entiéndase el concepto de incremento de probabilidad de riesgo como el producto entre el incremento de la figura de riesgo analizada, en este caso la FDN de incendios, y el tiempo de exposición a la situación analizada, es decir, el tiempo que dura la situación analizada. Tradicionalmente, en los procesos de decisión informados por el riesgo se utiliza un valor límite de 1,0E-06 para el incremento de probabilidad de riesgo para diferenciar entre situaciones significativas y situaciones no significativas. No obstante, las matrices diseñadas son un análisis prospectivo en el que se desconoce el tiempo de exposición a las situaciones planteadas. En consecuencia, los criterios de valoración del riesgo para las matrices MCI y MRI se han diseñado desde el punto de vista del tiempo de exposición necesario para que una situación alcance el umbral de incremento de probabilidad de 1,0E-06. Estos criterios, que han sido consensuados con personal técnico de la central nuclear, dividen el dominio de la frecuencia de daño al núcleo inducida por incendios de la central en cuatro intervalos. A cada intervalo se le asigna un nivel cualitativo de riesgo: Alto, moderado, bajo, y muy bajo.

En procesos de decisión, la información que proporcionan los análisis de incertidumbre de los resultados cuantitativos sobre los que se basa la toma de decisiones es relevante para decidir sobre cuáles de ellos depositar una mayor confianza. Aunque sea de forma indirecta y/o cualitativa, toda figura cuantitativa considerada en un proceso de toma de decisiones ha de ir acompañada de una valoración de su incertidumbre asociada. Por lo tanto, la incertidumbre asociada a los resultados de las matrices ha sido analizada para que puedan incorporarse en las prácticas de toma de decisiones. La incertidumbre de los resultados de las matrices MCI y MRI se ha valorado mediante una metodología de análisis Monte Carlo utilizando el software Matlab®. De la aplicación del análisis de incertidumbre se concluye que los resultados de las matrices MCI y MRI son robustos y fiables.

La gran mayoría de combinaciones de indisponibilidad de sistemas contra incendios y funciones clave de seguridad analizadas en el marco de la matriz MCI tienen un nivel de riesgo inducido por incendios muy bajo. Respecto a los elementos asociados a un nivel de riesgo bajo o superior, los resultados de la matriz son concluyentes y muestran que las combinaciones de indisponibilidad cuyo riesgo inducido por incendios es significativo están en su mayoría influenciadas por la indisponibilidad de seis equipos representativos de funciones clave de seguridad y la indisponibilidad de un sistema contra incendios. Las funciones clave de seguridad representadas por estos seis equipos son: sumidero de calor, suministro eléctrico, e inventario del RCS. El sistema contra incendios señalado es el sistema de extinción de la sala CXXX1. Se han de incluir nuevas restricciones y/o declaraciones en la regla de mantenimiento de la central que hagan referencia a estos seis equipos y a este sistema en caso que no los hubiese ya. Aparte de la indisponibilidad del sistema de extinción de la zona CXXX1, la indisponibilidad de sistemas contra incendios no tiene un impacto en el riesgo suficiente como para que se vea reflejado en los resultados de la matriz MCI. Por este motivo, se ha llevado a cabo un análisis de importancia de los sistemas contra incendio. De este análisis se concluye que los sistemas contra incendios cuya importancia respecto al riesgo es mayor se encuentran en el edificio de control y en el edificio de bombas del sistema de agua de alimentación auxiliar. De forma análoga al caso anterior, se ha de valorar incluir nuevas restricciones y/o declaraciones en la regla de mantenimiento de la central que hagan referencia a estos sistemas contra incendio.

A partir de los resultados de la matriz MRI se concluye que 11 de las 41 zonas analizadas en el modelo APS de incendios detallado de la central son significativas para el riesgo. Estas zonas contienen equipos, o cables asociados a equipos, que quedarían indisponibles en caso de incendio en la zona provocando, en combinación con la indisponibilidad del equipo representativo de función clave de seguridad, un aumento de la FDN inducida por incendios de la planta. Todas estas zonas son candidatas a ser el objetivo de acciones de gestión del riesgo.

Se concluye del resultado de ambas matrices que todo elemento con impacto en el riesgo inducido por incendios de la central está localizado en un grupo reducido de equipos, sistemas contra incendio, y zonas de incendio. Cabe destacar que solo se han identificado seis equipos con impacto significativo en el riesgo de entre los miles de equipos presentes en la central[1], cinco sistemas contra incendios con impacto significativo de entre los 167 existentes en la central, y 11 zonas de entre las cientos de zonas en las que se divide[2] la central. Esta es una conclusión positiva para la central puesto que les permitirá centrar los recursos disponibles únicamente en los elementos señalados. Pese a que un incendio puede ocurrir en prácticamente cualquier zona de la central y afectar prácticamente a cualquier equipo, las acciones a tomar para reducir el riesgo inducidos por incendios de la central se podrán focalizar en los elementos señalados por las matrices MCI y MRI.

[1] Utilizando como medida el modelo APS, se trata de seis sucesos básicos de un total de aproximadamente 3000.

[2] El modelo APS detallado solo contiene 41 zonas. No obstante, estas 41 zonas son producto de un proceso de cribado cualitativo y un cribado cuantitativo. Cada elevación de un edificio se divide en varias zonas, por lo que se estima que la cantidad total de zonas presentes en una central nuclear debe ser de entre 100 y 300.

Capítulo 17

Producción científica

Los trabajos y proyectos desarrollados en el marco de esta tesis doctoral han dado como resultado la producción del material divulgativo listado a continuación. El material relacionado con los proyectos y trabajos presentados en esta memoria se recoge en la sección 17.1, mientras que el material vinculado con otros proyectos y trabajos, también desarrollados durante la tesis doctoral pero que han quedado fuera del alcance de esta memoria, se presentan en la sección 17.2. Queda fuera del alcance de este capítulo citar el material interno generado durante el desarrollo de la tesis.

17.1. Ponencias y artículos relacionados con el contenido de la Tesis Doctoral

Artículo en revista

Development and assessment of fire-related risk unavailability matrices to support the application of the maintenance rule in a PWR nuclear power plant. P.Díaz, E. Estruch, J. Dies, C. Tapia, A. De Blas, M. Asamoah. Journal of Nuclear Science and Technology. DOI: 10.1080/00223131.2016.1193066. Publicado online en julio de 2016.

Ponencia en congreso internacional

P. Díaz, E. Estruch, J. Dies, C. Tapia, A. De Blas. *Fire-related systems and key safety functions unavailability matrix development and assessment.* PSA 2015: International Topical Meeting on Probabilistic Safety Assessment and analysis from American Nuclear Society. Abril 2015.

P. Díaz, D. Lomeña, J. Dies, C. Tapia, A. De Blas. *Development and application of a methodology to apply human reliability analysis to an independent spent fuel storage installation.* PSA 2015: International Topical Meeting on Probabilistic Safety Assessment and analysis from American Nuclear Society. Abril 2015.

Ponencia en congreso nacional

P. Díaz, M.M. Cid, J. Dies, C. Tapia. Comparación de técnicas para realizar un estudio probabilista de seguridad de un Almacén Temporal Individualizado. XXXVIII Reunión Anual de la Sociedad Nuclear Española. Octubre 2012.

P. Díaz, J. Dies, C. Tapia, A De Blas. Desarrollo de una metodología de aplicación del Análisis de Fiabilidad Humana a una instalación de Almacén Temporal Individualizado. XL Reunión Anual de la Sociedad Nuclear Española. Octubre 2014.

P. Díaz, E. Estruch, J. Dies, C. Tapia, A. De Blas, M. Asamoah. Desarrollo y evaluación de una matriz de compatibilidades de indisponibilidades de sistemas contra incendios y funciones clave de seguridad de una central PWR. XLI Reunión Anual de la Sociedad Nuclear Española. Octubre 2015.

17.2. Otras ponencias y artículos desarrollado en el marco de la Tesis Doctoral

Artículo en revista

M.M. Cid, J. Dies, C. Tapia, P. Díaz. *Outage Key Safety Functions Configuration risk assessment for a three loops Westinghouse PWR.* Nuclear Engineering and Design volume 291. Pages 271-276. Setiembre de 2015.

Ponencia en congreso nacional

P. Díaz, M. Gonzalez, J. Dies, C. Tapia, A. De Blas. Metodología de análisis de fallos de componentes en período de infancia de una Central Nuclear. XL Reunión Anual de la Sociedad Nuclear Española. Octubre 2014.

P. Díaz, B. Cirera, J. Dies, C. Tapia, A. De Blas. Introducción de un árbol de eventos de PPE en modo Recarga en el APS de una Piscina de Combustible. XL Reunión Anual de la Sociedad Nuclear Española. Octubre 2014.

Bibliografía

[1] IAEA. Assessment of Defence in Depth for Nuclear Power Plants. *Safety Reports Series No. 46*, 2005.

[2] EPRI. Probabilistic Risk Assessement (PRA) of Bolted Storage Casks. Updated quantification and Analysis report. *1009691*, 2004.

[3] NRC. ATHEANA User ' s Guide Final Report. *NUREG-1880*, 2006.

[4] NRC-RES EPRI. Fire PRA Methodology for Nuclear Power Facilities. *NUREG/CR-6850*, 2005.

[5] NRC. A Pilot Probabilistic Risk Assessment Of a Dry Cask Storage System At a Nuclear Power Plant. *NUREG-1864*, 2007.

[6] Swain and Guttman. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. *NUREG/CR-1278*, 1983.

[7] Licao Dai, Zhang Li, and Pengcheng Li. HRA in China: Model and data. *Safety Science*, 49(3):468–472, mar 2011.

[8] NRC. Human Reliability Analysis- Informed Insights on Cask Drops. *NUREG/CR-7016*, 2012.

[9] NRC. Preliminary , Qualitative Human Reliability Analysis for Spent Fuel Handling. *NUREG/CR-7017*, 2012.

[10] IAEA. Defence in Depth in Nuclear Safety. *INSAG-10*, 1996.

[11] IAEA. Basic Safety Principles for Nuclear Power Plants. *INSAG-12*, 1999.

[12] CSN. Instrucción IS-26, sobre requisitos básicos de seguridad nuclear aplicables a las instalaciones nucleares. *Instrucción de Seguridad*, 2010.

[13] IAEA. Fundamental Safety Principles. *Safety Fundamentals*, SF-1, 2006.

[14] Fernando Pelayo. International Organizations in the nuclear field. In *Master in Nuclear Engineering. Regulations and safety slides.*

[15] IAEA. Governmental , Legal and Regulatory Framework for Safety. *Safety Standards*, 2010.

[16] IAEA. Safety of Nuclear Power Plants : Commissioning and Operation. *SSR-2/2*, 2011.

[17] IAEA. Safety culture. *INSAG-4*, 1991.

[18] IAEA. Safety of nuclear power plants : Design. *Specific Safety Requirements*, No. SSR-2, 2012.

[19] IAEA. The safety of nuclear power. *INSAG-5*, 1992.

[20] CSN. Actualización y Mantenimiento de los Análisis Probabilistas de Seguridad. *Guía de Seguridad 1.15*, 2004.

[21] IAEA. Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants. *Specific Safety Guide SSG-3*, pages 1–215, 2010.

[22] NRC. An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis. *Regulatory Guide 1.174*, 2011.

[23] IAEA. A Common Basis for Judging the Safety of Nuclear Power Plants Built to Earlier Standards. *INSAG-8*, 1995.

[24] NRC. Reactor Safety Study. An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants. *WASH-1400. NUREG-75/014.*

[25] Francesc Reventos. The Three Mile Island 2 accident. In *Master in Nuclear Engineering. Regulations and safety slides.*

[26] Luis E Herranz. The Chernobyl-4 Accident: Facts & Hypo's. In *Master in Nuclear Engineering. Regulations and safety slides.*

[27] IAEA. Summary Report on the Post-accident review meeting on the Chernobyl accident. *INSAG-1*, 1986.

[28] UK-EPR. Level 1 Probabilistic Safety Assessment. *Fundamental safety overview*, 2: Design:Subchapter R.1 p. 1–38.

[29] Health & Safety executive nuclear directorate. Westinghouse AP 1000 Step 2 PSA Assessment. *Assessment Report.*

[30] Luis E Herranz. The Fukushima accident: Current insights into initiation and development. In *Master in Nuclear Engineering. Regulations and safety slides.*

[31] CSN. Pruebas de resistencia realizadas a las Centrales Nucleares Españolas. *Informe Final.*

[32] NASA. Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners. 2002.

[33] NRC. Severe Accident Risks: An Assessment for Five U.S Nuclear Power Plants. *NUREG-1150*, 1, 1990.

[34] H.W et al Lewis. Risk Assessment Review Group Report to the U.S. Nuclear Regulatory Commission. *NUREG/CR-0400.*

[35] IAEA. Probabilistic Safety Assessment. *INSAG-6*, 1992.

[36] Mitchel Rogovin Frampton and George T. Three Mile Island; A Report to the Commissioners and to the Public. *NUREG/CR-1250*, I-II, 1980.

[37] NRC. The Status of Recommendations of the President's Commission on the Accident at Three Mile Island. *NUREG-1355*, 1989.

[38] NRC. PRA Procedures Guide. *NUREG/CR-2300*, 1983.

[39] NRC. History of the NRC's Risk-Informed Regulatory Programs.

[40] NRC. Use of Probabilistic Risk Assessment Methods in Nuclear Activities: Final Policy Statement. *60 FR 42622*, 1995.

[41] NRC. Plan for the implementation of the commission's phased approach to PRA quality. *SECY-04-0118*, 2004.

[42] NRC. Status of the plan for implementation of the commission's phased apporach to probabilistic risk assessment quality. *SECY-07-0042*, 2010, 2008.

[43] NRC. Annual Update on PRA Quality Expectations To support risk-informed regulatory activities, the expectations for PRA quality need to be provided. 2013.

[44] NRC. U.S. Code of Federal Regulations, Title 10, Part 50, Section 10CFR50.71. Maintenance of records, making of reports.

[45] CSN. Programa Integrado de realización y utilización de los análisis probabilista de seguridad en España, 1986.

[46] CSN. Sistema integrado de supervisión de centrales (SISC). *Manual de procedimientos de gestión*, 2014.

[47] CSN. Caracterización de los hallazgos de inspección y proceso de determinación de la significación para situaciones a potencia. *Manual de Procedimientos Técnicos IV 301*, 2013.

[48] CSN. Proceso de determinación de la significación para el mantenimiento de los APS. *Manual de procedimientos técnicos*, 2006.

[49] CSN. Proceso de determinación de la significación para operaciones en parada. *Manual de procedimientos técnicos*, 2010.

[50] CSN. Instrucción IS-25, sobre criterios y requisitos sobre la realización de los análisis probabilistas de seguridad y sus aplicaciones a las centrales nuclares. *BOE nº 153*, Junio, 2010.

[51] NRC. Probabilistic Risk Assessment (PRA).

[52] NRC. Industry-Average Performance for Components and Initiating Events at U . S . Commercial Nuclear Power Plants. *NUREG/CR-6928*, 2007.

[53] Asociación española de la Industria Eléctrica (UNESA). Documento Base de Datos Genérica de las Centrales Nucleares Españolas. *UNESA CEN - 35*, Abril, 2013.

[54] NRC. Reliability and availability Data Sytem (RADS).

[55] NRC. Handbook of Parameter Estimation for Probabilistic Risk Assessment. *NUREG/CR-6823*, 2003.

[56] IAEA. Applications of probabilistic safety assessment for nuclear power plants. *TECDOC-1200*, 2001.

[57] NRC. Good Practices for Implementing Human Reliability Analysis. *NUREG - 1792*, 2005.

[58] M van der Borst and H Schoonakker. An overview of PSA importance measures. *Reliability Engineering & System Safety*, 72(3):241–245, jun 2001.

[59] IAEA. A Framework for an Integrated Risk Informed Decision Making Process. *INSAG-25*, 2011.

[60] IAEA. Safety Assessment for Facilities and Activities: General Safety Requirements. *GSR Part 4*, 2009.

[61] CSN. Criterios básicos para la realización de aplicaciones de los Análisis Probabilistas de Seguridad. *Guía de Seguridad 1.14*, 2007.

[62] NRC. Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed decision Making. *NUREG-1855*, 2009.

[63] NRC. An approach for determining the technical adequacy of probabilistic risk assessment results for risk-informed activities. *Regulatory Guide 1.200*, 2009.

[64] M M Cid, J Dies, C Tapia, and P Diaz. Outage Key Safety Functions Configuration Risk Assessment for a three loops Westinghouse PWR. *Nuclear Engineering and Design*, 291:271–276, 2015.

[65] IAEA. Advances in safety related maintenance. *TECDOC-1138*, 2000.

[66] NEI. Industry Guideline for Monitoring the Effectiveness of Maintenance At Nuclear Power Plants. *NUMARC 93-01*, 2011.

[67] NRC. U.S. Code of Federal Regulations, Title 10, Part 50, Section 10CFR50.65. Requirements for monitoring the effectiveness of maintenance at nuclear power plants.

[68] NRC. Guidelines for categorizing structures, systems, and components in nuclear power plants according to their safety significance. *Regulatory Guide 1.201*, 2006.

[69] NRC. An approach for plant-specific, risk-informed decisionmaking: inservice testing. *Regulatory Guide 1.175*, 1998.

[70] NRC. Final general regulatory guide and standard review plan for risk-informed regulation of power reactors. *SECY-98-015*.

[71] George Apostolakis, Christiana Lui, Mark Cunnigham, George Pangburn, William Reckley, John Adams, Michel Call, Dennis Damon, Don Dube, Earl Easton, Timothy McCartin, Geary Mizuno, and Joel Piper. A Proposed Risk Management Regulatory Framework. 2012.

[72] IAEA. Nuclear Fuel Cycle Information System - Facilities.

[73] Pedro Díaz-Bayona, Javier Dies, Carlos Tapia, Manel Martínez Cid, and Alfredo De Blas. Comparación de Técnicas para realizar un estudio probabilista de seguridad de un almacén temporal individualizado. *XXXVIII Reunión Anual de la Sociedad Nuclear Española*, 2012.

[74] NRC. Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA). *NUREG-1624*, 2000.

[75] NRC. Control of heavy loads at Nuclear Power Plants. *NUREG-0612*, 1980.

[76] NRC. A Survey of Crane Operating Experience at U.S. Nuclear Power Plants from 1968 through 2002. *NUREG-1774*, 2002.

[77] NRC. Single-failure proof cranes for nuclear power plants. *NUREG-0554*, 1979.

[78] Holtec International. *Final Safety Analysis Report for the HI-STORM 100 Cask System.* 2010.

[79] EPRI. Dry Cask Storage Probabilistic Risk Assessment Scoping Study. 2002.

[80] NRC. Final Report: Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities. *NUREG-1407*, 1991.

[81] NRC. Evaluation of explosions postulated to occur on transportation routes near nuclear power plant sites. *Regulatory Guide 1.91*, 1975.

[82] IAEA. Component reliabiliy data for use in probabilistic safety assessment. *TECDOC-478*, 1988.

[83] B.N. Roy. Savannah River Site Generic Data Base development (U). *WSRC-TR-93-262*, 1998.

[84] NRC. Cladding Considerations for the Transportation and Storage of Spent Fuel. *Spent Fuel Project Office Interim Staff Guidance - 11 , Revision 3*, 2003.

[85] AKSteel. 304/304l stainless steel. *Product Data Bulletin*, 2013.

[86] NRC. Review and Evaluation of the Nuclear Regulatory Commission Safety Research Program. *NUREG-1635*, 2012.

[87] G.W. Hannaman and A.J. Spurgin. *Human Cognitive Reliability Model for PRA Analysis, NUS-4531.* 1984.

[88] NRC. The SPAR-H Human Reliability Analysis Method. *NUREG/CR-6883*, 2005.

[89] H.C. Benhardt, S.A. Eide, J.E. Held, L.M. Olsen, and R.E. Vail. Savannah river site human error data base development for nonreactor nuclear facilities. *WSRC-TR-93-581*, 1994.

[90] Moses A. Greenfield and Thomas J. Sargent. Probability of Failure of the TRUDOCK Crane System at the Waste Isolation Pilot Plant (WIPP). *EEG-74*, 2000.

[91] NRC. A short history of fire safety research sponsored by the u.s. nuclear regulatory commission, 1975-2008. *NUREG/BR-0364*, 2009.

[92] NRC. U.s. code of federal regulations, title 10, part 50 section 10cfr50.48. fire protecion.

[93] Garill Coles Steve Short. Implementing the nfpa 805 process: Observations of a technical reviewer. *PSA 2015, Sun Valley, Idaho*, 2015.

[94] NFPA. Fire code. *NFPA 1*, 2015.

[95] CSN. Instrucción IS-27, sobre criterios generales de diseño de centrales nucleares. *Instrucción de Seguridad*, 2010.

[96] NFPA. Standard on carbon dioxide extinguishing systems. *NFPA 12*, 2011.

[97] NRC. Procedures for the external event core damage frequency analyses for nureg-1150. *NUREG/CR-4840*, 1990.

[98] NRC. Fire probabilistic risk assessment methods enhancements. *NUREG/CR-6850 Supplement 1*, 2010.

[99] American Society of Structural Engineers. Structural Design for Physical Security. 1999.

[100] NRC. Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition. Section 3.5.1.6 Aircraft Hazards. *NUREG-0800.*

Parte IV

Anexos asociados a la parte II

Apéndice A

Descripción de las tareas de las diferentes fases de la etapa de carga

El presente anexo contiene la descripción de las tareas más importantes que conforman las diferentes fases de la etapa de carga de una campaña de carga de contenedores. La información aquí presente ha sido extraída de los procedimientos de manipulación del contenedor de la central nuclear. Por motivos de confidencialidad, la información se presenta de forma neutra, sin citar la nomenclatura ni los detalles específicos de estructuras, sistemas, y componentes. El anexo O contiene figuras e imágenes que acompañan a las descripciones proporcionadas en este anexo.

A.1. Fase 1: Carga

Las tareas aquí presentes siguen el orden secuencial estipulado en los procedimientos de manipulación del contenedor. Cada párrafo contiene una tarea.

Recordar a la sección de Química que ha de obtener dos muestras de la concentración de boro en el MPC cuatro horas antes de que se cargue el primer elemento de combustible gastado. Recordar a Química que ha de obtener una muestra de la concentración de boro en el MPC cada 48 horas en el periodo de tiempo que abarca desde la carga del primer elemento de combustible hasta que el agua del MPC se drena.

Verificar con el responsable de la carga y con el supervisor independiente del contenedor que todos los requisitos de vigilancia se han llevado a cabo positivamente.

Asegurar que no hay obstáculos, a todas las cotas, en el camino por el que se llevan elementos de combustible gastado mediante la grúa polar antes de comenzar un movimiento.

Obtener los resultados de las dos muestras de concentración de boro en el interior del MPC y verificar que sean más altas o iguales que la de referencia.

Anunciar al personal con licencia de movimiento de combustible que la carga del MPC comienza.

Llevar a cabo los siguientes pasos para introducir los elementos de combustible en el MPC:

- Trasladar los 32 elementos de combustible gastado desde su posición en la piscina a otra sección de la piscina donde se pueden colocar en la misma configuración que tendrán en el interior del MPC. Solo es posible si hay espacio suficiente en la piscina de combustible gastado.
- Trasladar los elementos de combustible gastado desde la piscina al MPC.
- Verificar la condición de los elementos de combustible gastado cargados en el contenedor. Una cámara acuática se utiliza para realizar esta tarea.

A.2. Fase 2: Instalación de la tapa del MPC y alzamiento del HI-TRAC

Retirar los tapones de las penetraciones de venteo y drenaje de la tapa del MPC.

Instalar los espaciadores de combustible superiores en la tapa del MPC. Verificar el correcto posicionamiento de los espaciadores con respecto a la configuración de los elementos de combustible en el MPC.

Anclar el yugo de alzamiento del HI-TRAC al gancho principal de la grúa puente. El yugo se ha de alinear correctamente con respecto a la tapa del MPC para asegurar que está correctamente alineado con las articulaciones del HI-TRAC.

Anclar el sistema de eslingas de piscina de la tapa del MPC a la propia tapa y al yugo.

Verificar que el alineamiento entre la tapa del MPC y el yugo del HI-TRAC es correcto.

Elevar y nivelar la tapa del MPC. Verificar que la tapa del MPC está horizontal.

Instalar la línea de drenaje del MPC en la tapa del MPC. Apretar hasta conseguir el espacio libre deseado.

Verificar que la linea de drenaje del MPC se ha colocado correctamente.

Mover y bajar la tapa del MPC hasta que esté justo por encima del MPC.

Rociar la tapa del MPC con agua desmineralizada la parte superior de la tapa del MPC mientras se baja la tapa.

Notificar la cantidad de agua rociada al responsable del proceso de carga y al supervisor independiente del contenedor.

Colocar la tapa del MPC encima del MPC. La correcta alineación entre la tapa y el contenedor ha de mantenerse en todo momento para evitar dañar la linea de drenaje u otras partes del MPC. Hay marcas de alineamiento tanto en la tapa como en el MPC. Se utilizan cámaras acuáticas, cuerdas y poleas para mantener la alineación correcta.

Verificar visualmente que la tapa del MPC se ha colocado correctamente.

Determinar el tiempo hasta ebullición (en este momento del proceso no hay circulación de agua en el MPC así que la temperatura del agua en su interior aumenta y se podría producir ebullición. La ebullición del agua en el interior del MPC no es deseable porque impediría significativamente la extracción de calor). Si se llegase al tiempo hasta ebullición, se debería restablecer la circulación del agua en el interior del MPC. La preparación del proceso de circulación de agua tarda entre 4 y 6 horas.

Notificar el tiempo hasta ebullición al responsable del proceso de carga y al supervisor independiente del contenedor.

Anclar el yugo de alzamiento a las articulaciones del HI-TRAC utilizando, si es necesario, una cámara acuática para confirmar el alineamiento.

Notificar al responsable del proceso de carga y al supervisor independiente del contenedor que comienza la operación de alzado del HI-TRAC.

Alzar el HI-TRAC hasta que su extremo superior esté justo por debajo del nivel de agua.

La sección de Protección Radiológica inspecciona el HI-TRAC para detectar partículas radiactivas. Se mide la tasa de dosis a 75 y 90 cm de la tapa del MPC. El contenedor se introduce otra vez en el pozo del contenedor si la tasa de dosis es superior a un cierto valor umbral.

Limpiar con agua a presión desmineralizada la superficie superior del HI-TRAC y el MPC.

Notificar la cantidad de agua consumida.

Continuar el alzamiento del HI-TRAC mientras se rocía su superficie con agua desmineralizada siguiendo las instrucciones de Protección Radiológica. Seguir las instrucciones de Protección Radiológica al respecto de la velocidad de alzamiento para facilitar las tareas de inspección y revisión.

Notificar la cantidad de agua consumida.

Utilizar una bomba de vacío para aspirar el agua acumulada en el extremo del contenedor HI-TRAC cuando el éste se encuentre al nivel de plataforma de la grúa polar. De la misma manera, aspirar agua del MPC mediante la penetración de venteo hasta que no salga más agua de su interior (la penetración de venteo está en el extremo superior del MPC así que se la cantidad de agua aspirada es pequeña).

Cerrar la válvula de drenaje del espacio anular del HI-TRAC y apagar el sistema de presurización del espacio anular del HI-TAC cuando el HI-TRAC esté fuera del pozo.

Finalmente, inspeccionar el extremo inferior del HI-TRAC para asegurar que no haya partículas calientes.

A.3. Fase 3: Traslado del contenedor a la zona de preparación

Asegurar que el contenedor se traslade a la menor altura posible para minimizar la dosis proveniente del extremo inferior del HI-TRAC. El personal, principalmente observadores, han de alejarse del contenedor. El contenedor se ha de volver a posar sobre el suelo tan pronto como sea posible.

Trasladar el contenedor y posarlo en la zona de descontaminación. Realizar una descontaminación y secado preliminares de la superficie del HI-TRAC.

Desanclar los dispositivos de izado de la tapa del MPC. Verificar el correcto desenganche de la tapa y los dispositivos de izado.

Desanclar los brazos del yugo de alzamiento de las articulaciones del HI-TRAC. Asegurar que el desenganche se ha realizado correctamente.

Retirar el yugo de alzamiento y preparar la plataforma de trabajo para las actividades de preparación.

A.4. Fase 4: Actividades de preparación

Solo se describen los pasos más importantes de esta fase porque no se ejecuta ni una acción humana que pueda causar la caída del contenedor o la carga errónea del mismo (el contenedor está posado en el suelo y ya ha sido cargado).

Descontaminar la superficie exterior del HI-TRAC y del extremo superior del MPC que presenten una actividad superficial superior a un valor umbral.

Instalar un blindaje temporal alrededor del HI-TRAC si es necesario.

Drenar parcialmente el interior del MPC.

Examinar el espacio entre la tapa del MPC y los bordes del MPC. Utilizar cuñas para conseguir un espaciado uniforme si es necesario.

Instalar el sistema automático de soldadura.

Noticar al supervisor independiente del conteneor que empiezan las operaciones de soldado de la tapa.

Purgar el aire del interior del MPC con gas argón para asegurar que se evita el límite explosivo inferior (comúnmente conocido como Lower Explosive Limit (LEL)).

Ejecutar una soldadura por puntos entre la tapa y el borde del MPC.

Completar la soldadura base entre la tapa y el borde del MPC. Realizar un test de penetración mediante tinte.

Realizar todos los pasos de soldadura que sean necesarios para conseguir una soldadura de 9,5 mm de espesor. Realizar de nuevo una supervisión visual y un test de penetración mediante tinte.

Soldar hasta que se consiga un espesor de 19 mm. Realizar, otra vez, una supervisión visual y un test de penetración mediante tinte. El proceso de soldadura ha acabado.

Confirmar que hay tiempo suficiente para acabar las tareas de preparación antes de llegar a la ebullición del agua en el interior del MPC.

Instalar los conectores de venteo y drenaje. Realizar un test hidrostático con un sistema específicamente diseñado para ese propósito.

Utilizar un sistema de deshidratación por convección forzada de helio para drenar el agua del MPC. Al drenar el agua la tasa de dosis aumenta. El personal ha de mantenerse alejado del HI-TRAC durante esta operación.

Secar el interior del MPC con el mismo sistema. Rellenar el MPC con helio utilizando el mismo sistema.

Retirar el sistema de deshidratación por convección forzada de helio y los conectores de venteo y drenaje. Colocar y apretar los tapones de las penetraciones de venteo y drenaje.

Limpiado y secado de las penetraciones de venteo y drenaje de la tapa del MPC.

Finalmente, se revisa la soldadura mediante técnicas no destructivas.

A.5. Fase 5: Trasladar el HI-TRAC, cargado, hasta el HI-STORM 100

Instalar el yugo de alzado en el gancho principal de la grúa puente. Colocar el yugo puente sobre el HI-TRAC y anclar los brazos del yugo a las articulaciones del HI-TRAC. Verificar la correcta colocación y anclaje del dispositivo de alzamiento.

Alzar y trasladar el HI-TRAC hasta que este por encima del HI-STORM 100.

Instalar los dispositivos de alineación en el sistema de acoplamiento para facilitar el posicionamiento del HI-TRAC (El sistema de posicionamiento se ha colocado previamente encima del HI-STORM). Poco a poco, bajar el HI-TRAC sobre el sistema de acoplamiento verificando en todo momento la posición del contenedor al respecto del sistema. Finalmente, el HI-TRAC reposa sobre el dispositivo de acoplamiento.

Confirmar que el HI-TRAC se ha alineado correctamente con respecto al sistema de acoplamiento.

Asegurar y confirmar mediante inspección visual que el equilibrio y el nivel del conjunto dispositivo de acoplamiento y HI-TRAC es correcto. Comprobar que el dispositivo de alzamiento del yugo no soporta ninguna carga. Desanclar el yugo de alzamiento del HI-TRAC.

Retirar el yugo de alzamiento del gancho principal de la grúa puente.

A.6. Fase 6: Transferencia del MPC al HI-STORM 100

Instalar el dispositivo de bloqueo de izado en el MPC.

Instalar el adaptador del dispositivo de bloqueo de izado en el gancho principal de la grúa puente. Colocar el gancho sobre el MPC. Bajar el adaptador hasta que este en posición para poderse anclarse al dispositivo de bloqueo de izado.

Anclar el MPC a la grúa mediante el dispositivo de bloqueo de izado y el adaptador colocado en el yugo. Asegurar que el MPC esté correctamente anclado para poder empezar el movimiento de transferencia.

Alzar ligeramente el MPC para dejar 2,5 cm entre el extremo inferior del MPC y la tapa inferior del HI-TRAC. Si el MPC saliese del blindaje que ofrece el HI-TRAC los niveles de dosis podrían ser peligrosos.

Presurizar los amortiguadores del dispositivo de acoplamiento y verificar que entran en contacto con la tapa inferior del HI-TRAC. Soltar y retirar los pernos de la tapa inferior del HI-TRAC. Los niveles de radiación en los alrededores del dispositivo de alzamiento son altos. Personal de Protección Radiológica debe estar presente durante esta fase y el personal encargado de otras tareas debe alejarse tanto como sea posible del dispositivo de acoplamiento.

Despresurizar los amortiguadores del dispositivo de acoplamiento para que la tapa inferior del HI-TRAC descanse sobre la bandeja del dispositivo. Asegurar que la tapa quede nivelada sobre la bandeja.

Asegurar que las herramientas de fijación de la bandeja del dispositivo de acoplamiento se han retirado. Retirar la bandeja del dispositivo de acoplamiento.

Utilizar la grúa para bajar el MPC hasta que descanse sobre la base del HI-STORM. Realizar la aproximación a la base del HI-STORM lentamente para evitar golpear el contenedor.

Medir la tasa de dosis alrededor del dispositivo de acoplamiento durante el descenso del MPC. Pedir al personal que no esté involucrado en la operación que despejen la zona.

Desanclar el MPC del adaptador del dispositivo de bloqueo de alzado. Alzar el gancho principal de la grúa puente.

Retirar el adaptador del dispositivo de bloqueo de alzado del gancho principal de la grúa e instalar el yugo de alzamiento. Colocar la grúa encima del HI-TRAC. Anclar el yugo de alzamiento a las articulaciones del HI-TRAC.

Retirar el HI-TRAC del dispositivo de acoplamiento. Alzar el HI-TRAC hasta que no interfiera con el dispositivo de acoplamiento y trasladarlo a la zona de almacenamiento del contenedor.

Retirar el dispositivo de bloqueo de alzamiento del MPC. Cerrar parcialmente la bandeja del sistema de acoplamiento para proporcionar blindaje adicional mientras se retira el dispositivo de bloqueo de alzamiento.

Instalar tapones en los agujeros de izado de la tapa del MPC en los que se anclaba el dispositivo de bloqueo de izado. Insertar completamente la bandeja del dispositivo de acoplamiento (la tapa inferior del HI-TRAC permanece en su interior).

Instalar el dispositivo de alzamiento multipropósito en el gancho principal e la grúa puente y retirar el dispositivo de acoplamiento. El HI-STORM queda preparado para la fase de transferencia.

Apéndice B

Árboles de sucesos del modelo APS de ATI

A continuación se incluyen los árboles de sucesos de cada suceso iniciador incluido en el modelo APS de ATI. Estos árboles de sucesos han sido extraídos directamente del modelo APS creado en el software *RiskSpectrum® PSA*.

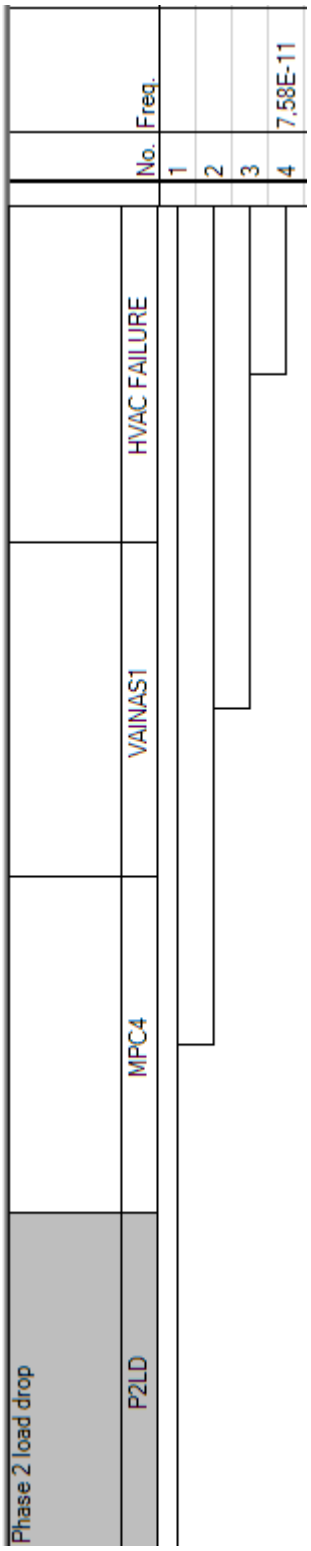


Figura B.1: Árbol de sucesos del suceso iniciador Caída4 / LDP2.

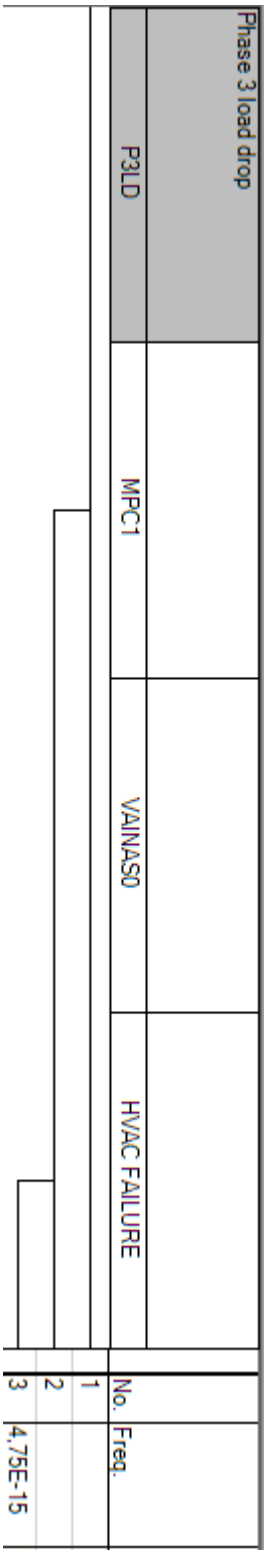


Figura B.2: Árbol de sucesos del suceso iniciador Caída1 / LDP3.

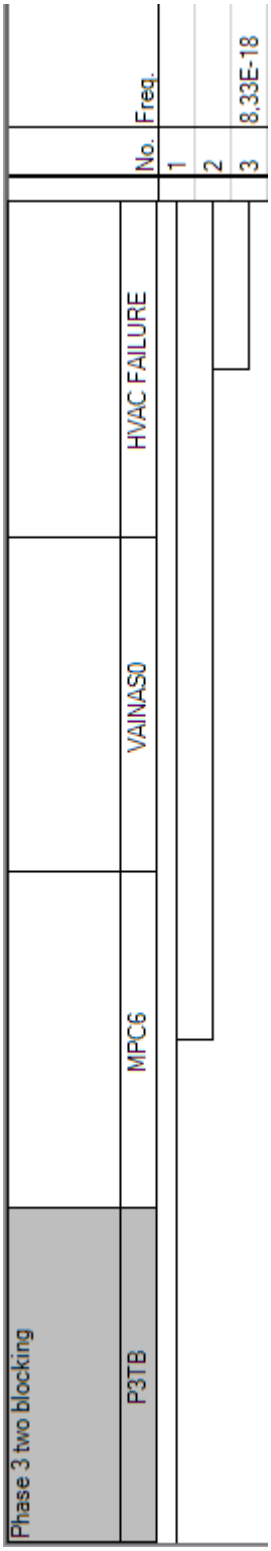


Figura B.3: Árbol de sucesos del suceso iniciador Caída2 / TBP3

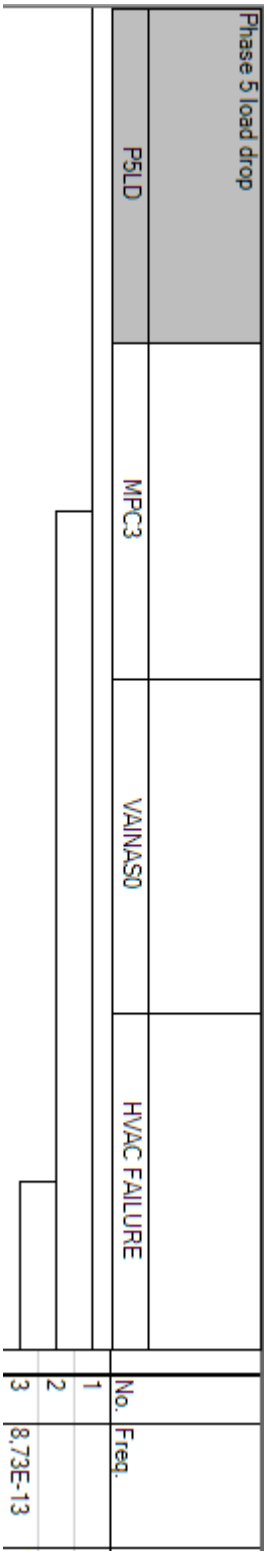


Figura B.4: Árbol de sucesos del suceso iniciador Caída3 / LDP5

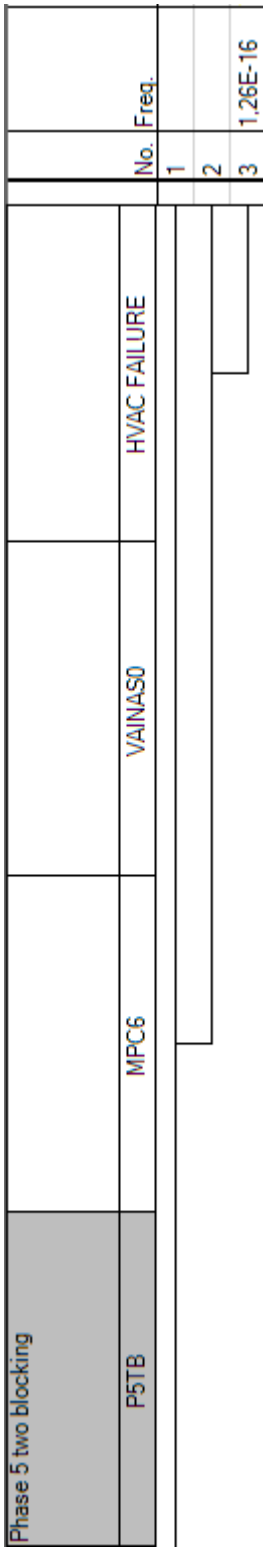


Figura B.5: Árbol de sucesos del suceso iniciador Caída2 / TBP5

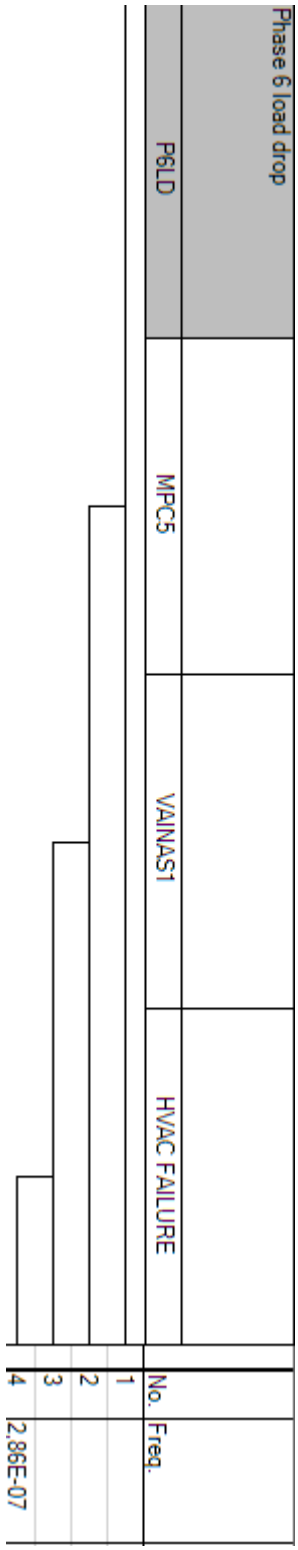


Figura B.6: Árbol de sucesos del suceso iniciador Caída5 / LDP6

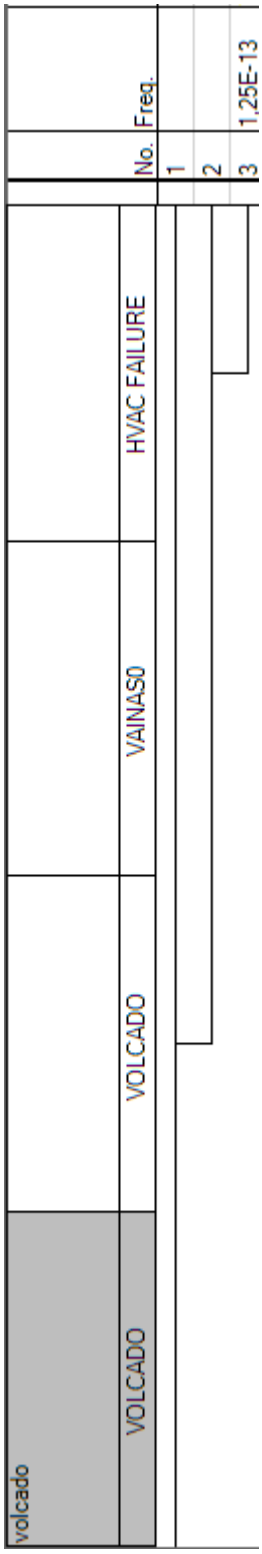


Figura B.7: Árbol de sucesos del suceso iniciador Volcado / Tip-over

Apéndice C

Análisis del sistema de ventilación. Árbol de fallos del sistema

Toda la información presente en este anexo ha sido extraída de documentación de la central nuclear. Por motivos de confidencialidad, la información se presenta de forma neutra, sin citar la nomenclatura ni los detalles específicos de algunas estructuras, sistemas, y componentes.

C.1. Funciones del sistema

El Sistema de Ventilación HVAC del Edificio de Combustible realiza cuatro funciones diferenciadas:

- Suministrar aire exterior al Edificio de Combustible para atemperarlo durante la época invernal y distribuir aire por su interior con especial atención a la zona de la PCG. El aire suministrado se filtra antes de su impulsión y distribución.
- Extraer aire captado en diferentes puntos del Edificio evacuando el calor sensible procedente de pérdidas en todos los equipos y tuberías y especialmente el calor latente de evaporación del agua de la PCG.
- Filtrar el aire captado mediante prefiltro, filtro HEPA (*High-efficiency particulate arrestance*), filtro de carbón activo y filtro HEPA antes de su transporte y expulsión a través del plénum de descarga del Edificio Auxiliar, durante las condiciones de Operación Normal, Manejo de Combustible y Accidente en el Manejo de Combustible.
- Mantener el Edificio de Combustible en depresión respecto al exterior.
- Aportar calefacción en la época invernal en la zona de ubicación de las unidades de tratamiento de aire.

El Sistema de Ventilación HVAC del Edificio de Combustible consta de cuatro subsistemas separados:

- Unidad suministradora de aire.
- Unidad extractora de aire A.
- Unidad extractora de aire B.
- Compuertas de aislamiento del Edificio de Combustible.

C.1.1. Unidad suministradora de aire

Su función principal es la de suministrar aire exterior al Edificio de Combustible atemperado para mantener la temperatura interior del Edificio dentro de unos límites. El aire pasa por un sistema de filtrado como el descrito anteriormente para que quede totalmente limpio. Contribuye a la generación de la depresión estipulada.

C.1.2. Unidades extractoras

Ambas unidades existentes son iguales, se utilizan dos siguiendo el criterio de redundancia. La principal función de estas unidades es extraer el aire del interior del Edificio de Combustible pasándolo por un sistema de filtraje que asegura la no liberación de radionúclidos al ambiente. Además, estas unidades también contribuyen a la generación de la depresión estipulada.

C.1.3. Compuertas de aislamiento

La función de estas compuertas es mantener la depresión estipulada en casos especiales. Estas compuertas comunican con el exterior, y son utilizadas cuando la depresión en el interior del Edificio de Combustible es mayor de lo estipulado.

C.2. Descripción general del sistema

El Sistema de Ventilación HVAC del Edificio de Combustible está organizado como un circuito semicerrado, siendo el subsistema de suministro de aire el que realiza el aporte y el subsistema de extracción el que realiza la extracción de aire. A continuación se describe cada subsistema.

C.2.1. Subsistema de suministro de aire

El sistema consta de una unidad de suministro de aire del 100 %. La unidad de suministro tiene mando y señalización de estado en Sala de Control y dispone de ventilador con motor de dos velocidades, alta o baja, para acomodarse al funcionamiento en verano o invierno, en operación normal o en manejo de combustible, si bien operará en alta velocidad en el caso de funcionamiento de las dos unidades de filtración de aire. También dispone de:

- Dos compuertas motorizadas de aislamiento redundantes en la aspiración de aire exterior, que abren/cierran automáticamente siempre que la unidad arranque/pare manual o automáticamente. Tienen señalización en Sala de Control.
- Prefiltro y filtro de alta eficiencia y batería eléctrica de calefacción controlada por un programador con termostato limitador.
- Los filtros (PF y HEF) de la unidad de suministro disponen de presostatos de presión diferencial al igual que el ventilador de la unidad para alarma de malfuncionamiento en Sala de Control.
- En el caso de producirse señal de Aislamiento del Edificio de Combustible, señal que se producida por el Sistema de Vigilancia de Radiación en caso de detectarse alto nivel de radiación, la unidad de suministro se dispara automáticamente y se aísla la aspiración de aire exterior. Por ello, la alimentación eléctrica a las compuertas de aspiración se ha previsto desde barras de Emergencia redundantes.
- El suministro de aire al Edificio se realiza a partir de rejillas situadas en dos niveles, a nivel de PCG y a nivel superior.

C.2.2. Subsistema de extracción de aire

El sistema consta de dos unidades de extracción en emergencia. Estas unidades tienen mando y señalización de estado individual en Sala de Control y disponen cada una de ellas de:

- Compuerta motorizada de regulación de caudal de aire, en la descarga del ventilador de la unidad.
- Sendas compuertas motorizadas de aislamiento en la aspiración y en la descarga de cada unidad con señalización individual en Sala de Control.
- Batería de calefacción para disminuir la humedad de entrada a los filtros de carbón activo. Esta calefacción es muy importante pues si la humedad está por encima de 70 % el filtro de carbón activo no trabaja correctamente.
- Las compuertas motorizadas abren/cierran y las baterías de calefacción conectan/desconectan automáticamente siempre que las unidades respectivas arranquen/paren manual o automáticamente.
- Los filtros de las unidades disponen de interruptores de presión diferencial al igual que los ventiladores de las unidades para alarma de malfuncionamiento.
- Los filtros de carbón activo de las unidades disponen de detectores de temperatura para alarma de malfuncionamiento por alta temperatura, con objeto de vigilar el posible aumento de temperatura del lecho debido al calor de desintegración de los iodos absorbidos por el carbón activo.
- En la descarga común de las unidades de extracción se encuentran situadas las dos compuertas de sobrepresión redundantes, que se mantienen cerradas por un contrapeso y que se posicionarán para abrir cuando el conducto aguas abajo esté bloqueado.
- El aire se aspira a través de una ramificación de rejillas situadas a dos alturas. Unas están situadas a nivel de la PCG y otras a nivel superior.

C.2.3. Subsistema de alivio de presión

El subsistema de alivio de presión está formado por dos compuertas que se encuentran normalmente cerradas mediante un sobrepeso y que solo se abrirán al darse la señal de depresión excesiva en el Edificio de Combustible.

C.3. Criterios de diseño

A continuación se presentan los criterios de diseño procedentes del documento de Bases de Diseño del sistema:

- El Sistema de Ventilación HVAC del Edificio de Combustible está diseñado para mantener la temperatura interior del Edificio entre 38 ºC y 20 ºC con temperaturas en el exterior entre 32,2 ºC y 0,6 ºC. La máxima temperatura interior del edificio tras un accidente de manejo de combustible es 50 ºC.
- El sistema está diseñado para mantener una depresión de 6,35 mm.c.a en el edificio, siempre que exista combustible gastado en la piscina. En caso de presurización dispone de dos compuertas de alivio de presión que abrirían si por alguna causa se superase ese valor de depresión en el Edificio de Combustible.

- El sistema está diseñado para proporcionar un barrido de aire en la superficie de la piscina (cuando exista combustible gastado) que controla los vapores desprendidos. En la aspiración de la zona de barrido se dispone de una compuerta motorizada, y de otra en la descarga del suministro de aire con mando y señalización ambas en Sala de Control.
- El sistema está diseñado para controlar la emisión de aire al ambiente después de purificarlo a través de filtros.
- Los componentes del sistema cuya operabilidad se requiere durante y después de un accidente de manejo de combustible están diseñados como clase sísmica 1.
- Las compuertas de sobrepresión para alivio de presiones de Categoría Sísmica 1 impiden que la presión negativa en el interior del Edificio de Combustible llegue a ser excesiva. El resto del equipo y de las canalizaciones son de Categoría Sísmica 2, disponiéndose soportes de Categoría Sísmica 1 donde un conducto caído pudiera caer en la piscina de combustible o dañar los equipos de Categoría 1.
- Se proporciona la redundancia apropiada en los componentes y porciones del sistema cuya operación se requiere durante y después de un accidente de manejo de combustible.
- Para la detección del accidente de manejo de combustible (Suceso Condición IV) se dispone de dos trenes redundantes de vigilancia de la radiación de Clase 1E en el Edificio de Combustible. Estos trenes generan la acción de Aislamiento del Edificio de Combustible.
- El sistema está diseñado para que la dosis gamma (a todo el cuerpo), beta (a la piel) y al tiroides en el radio de exclusión y zona de baja población, sean inferiores a las especificadas en el 10CFR100 en el supuesto de un accidente de manejo de combustible. Para ello se necesita una unidad de extracción de aire del Edificio de Combustible que tiene un 100 % de capacidad de filtración, en caso de este accidente, permaneciendo la otra en reserva.
- Todas las penetraciones en las paredes y el techo del Edificio de Combustible estarán completamente selladas de forma que se asegure que la infiltración máxima sea de 2573 m^3/h.
- A las unidades de extracción se les da crédito para limitar las consecuencias radiológicas del Accidente de Manejo de Combustible, por lo que están alimentadas, junto con sus compuertas de regulación, de aislamiento y baterías calefactoras desde las barras de alimentación eléctrica de emergencia redundantes.
- El sistema se requiere en operación en caso de Pérdida de Potencia Exterior (PPE), por lo que están conectadas al secuenciador de PPE en el escalón 25 segundos.
- Los lechos de carbón activo se diseñan para un tiempo de residencia media (tiempo de contacto entre el gas y el carbón) de 0,25 segundos. En los 5 cm de espesor del lecho.
- El Sistema de Ventilación HVAC del Edificio de Combustible debe estar diseñado y ubicado de manera que se minimice la probabilidad de fuegos o explosiones y sus efectos.
- El sistema deberá estar diseñado para soportar los efectos derivados de, y para ser compatible con, las condiciones ambientales asociadas a la operación normal, a los trabajos de mantenimiento a la realización de pruebas y a los accidentes base de diseño, incluidos los accidentes con pérdida de refrigerante, durante toda la vida de la central.
- El sistema deberá estar convenientemente protegido frente a los efectos dinámicos, incluyendo los debidos a proyectiles, al efecto látigo en tuberías y a las descargas de fluidos, que pudieran producirse por fallos de equipos, así como frente a sucesos y condiciones que ocurran en el exterior de la central.

- En caso de producirse la señal de Aislamiento del Edificio de Combustible la unidad de suministro se para automáticamente y se aísla la aspiración de aire exterior. En consecuencia la alimentación eléctrica a las compuertas de aspiración se ha previsto desde barras de emergencia redundante.
- La aportación de aire al sistema, durante la operación de extracción de emergencia, con la unidad de suministro detenida, procederá únicamente de infiltraciones, o en el supuesto caso de excesiva presión negativa en el edificio, procedente de las compuertas de alivio de presión.

C.4. Operación del sistema

Se estipulan 3 modos de operación:

- Operación de manejo de combustible: Se define como operación de manejo de combustible maniobras en las que deba estar en funcionamiento la grúa con cargas por encima de la PCG, operaciones de recarga de combustible del reactor, operaciones de movimiento de combustible de la propia PCG, descontaminación del canal de transferencia o descontaminación y manejo de herramientas.
- Operación en accidente de manejo de combustible: Se define como operación en accidente de manejo de combustible (Condición IV) a todas aquellas acciones a realizar a partir del momento en el que se detecta alto nivel de radiación en el Edificio de Combustible.
- Operación normal: Se define como operación normal cualquier otro situación operativa no recogida en las definidas como operaciones de manejo de combustible ni la producida por la actuación de los transmisores de radiación, ya sea por un accidente en el manejo de combustible o por la activación de éstos.

En cualquier modo de operación siempre deben cumplirse las siguientes condiciones iniciales:

- Las barras de salvaguardias están energizadas.
- Los centros de potencia están energizados.
- Los generadores Diésel están disponibles.
- Los monitores de radiación estarán en servicio.

Sea cual sea el modo de operación se deben tener en cuenta las siguientes precauciones:

- Poner en servicio, siempre que sea posible, primero una unidad de extracción de aire, para evitar someter al Edificio de Combustible a una presión positiva.
- En el caso de parada del sistema se procederá primero a la parada de la unidad de suministro del aire.
- Limitar como máximo a 3 arranques de las unidades ventilación por hora.
- Por señal de PPE se producirá señal de DCNE (Disparo de Cargas NO Esenciales) y el posterior arranque de las unidades de extracción de aire.

A continuación se presentan los procedimientos para poner en servicio y mantener en operación el Sistema de Ventilación HVAC del Edificio de Combustible en los modos de operación definidos anteriormente.

C.4.1. Puesta en servicio en operación normal

C.4.1.1. Condiciones iniciales particulares

- La situación operativa para el funcionamiento del Sistema de Ventilación es la definida como Operación Normal en el apartado anterior.
- El ventilador de la unidad de suministro de aire está disponible.
- Los prefiltros y filtros de alta eficiencia de la unidad están limpios y disponibles.
- Las baterías eléctricas de la unidad están energizadas.
- Las compuertas de aislamiento de aspiración de aire exterior del sistema de suministro de aire, de aspiración de aire del foso de combustible gastado, y de impulsión de aire a la PCG están cerradas.
- Las unidades de extracción están paradas y las compuertas de dichas unidades están cerradas.
- Las baterías eléctricas de las unidades están energizadas.

C.4.1.2. Precauciones particulares

Verificar la disponibilidad y buenas condiciones de funcionamiento del prefiltro y filtro de alta eficiencia, de la unidad de suministro.

C.4.1.3. Maniobras

1. Poner los selectores en la posición reposición, con lo que quedan repuestas para actuar las cadenas lógicas A y B de aislamiento del Sistema HVAC y desenclavadas las unidades del sistema.
2. Abrir la compuerta de aislamiento del colector de aspiración de aire de la PCG, mediante el botón pulsador.
3. Abrir la compuerta de aislamiento del colector de suministro de aire de la PCG, mediante el botón pulsador.
4. Arranca la unidad de extracción de aire A o B mediante su selector de mando y verificar que abren las compuertas asociadas.
5. Verificar que permanecen apagadas las alarmas: [AL-22 (6.1)], "Anomalía unidades extracción Edificio Combustible". [AL-22 (6.2)], "Posición incorrecta compuertas unidades extracción Edificio Combustible". [AL-22 (6.3)], "Anomalía filtros unidades extracción Edificio Combustible.
6. Verificar que el caudal suministrado por la unidad de extracción en funcionamiento está comprendido entre 7200 y 8800 CFM mediante los indicadores de caudal.
7. Arrancar la unidad de suministro en baja velocidad mediante el selector. Verificar que abren las compuertas de aspiración y que los calentadores de la unidad se conectan para mantener la temperatura al punto de consigna de 23 ºC.
8. Verificar que permanecen apagadas las alarmas: "Anomalía unidad suministro Edificio Combustible". "Alta presión diferencial unidad suministro Edificio Combustible".
9. Verificar que si la temperatura del Edificio de Combustible es inferior a 20 ºC arrancan automáticamente las unidades de calefacción por medio de interruptores de temperatura.

C.4.2. Puesta fuera de servicio en Operación Normal

C.4.2.1. Condiciones iniciales particulares

- En el Edificio de Combustible no se está realizando ninguna operación de manejo de combustible.
- La temperatura es inferior a 38 ºC, límite superior según las Bases de Diseño.
- Las unidades de suministro y extracción (A o B) están en servicio.

C.4.2.2. Precauciones particulares

Parar en primer lugar la unidad de suministro de aire para mantener la presión dentro del edificio ligeramente negativa.

C.4.2.3. Maniobras

1. Parar la unidad de suministro de aire mediante el selector y verificar las siguientes actuaciones: Verificar cerradas las compuertas de aspiración de la unidad en servicio. Verificar localmente que las resistencias de calefacción quedan desconectadas.
2. Verificar que permanece apagada la alarma "Anomalía unidad suministro Edificio Combustible".
3. Parar la unidad de extracción de aire en servicio mediante su selector de mando y verificar que cierran las compuertas asociadas.
4. Verificar que permanece apagada la alarma "Posición incorrecta compuertas unidades extracción Edificio Combustible".
5. Cerrar la compuerta de aislamiento del colector de la descarga de aire a la superficie de la PCG mediante el botón pulsador.
6. Cerrar la compuerta de aislamiento del colector de aspiración de aire de la superficie de la PCG mediante el botón pulsador.

C.4.3. Puesta en servicio para operaciones de manejo de combustible

C.4.3.1. Condiciones iniciales particulares

- La situación operativa para el funcionamiento del Sistema de Ventilación es la definida como Operaciones de Manejo de Combustible anteriormente.
- El sistema está operando con la unidad de suministro de aire funcionando a baja velocidad y una unidad de extracción en funcionamiento.

C.4.3.2. Precauciones particulares

- En caso de inoperabilidad de una unidad d extracción de aire, consultar las Condiciones Límite de Operación (CLO).
- No poner la unidad de suministro en alta velocidad a menos que estén en marcha las dos unidades de extracción.

C.4.3.3. Maniobras

1. Cerrar la compuerta de aislamiento del colector de descarga de aire a la superficie de la PCG mediante un botón pulsador. Cerrar totalmente esta compuerta a solicitud de PR para los trabajos de descontaminación del canal de transferencia y de herramientas en la PCG.
2. Arrancar la unidad de extracción de aire A o B que esté parada mediante su selector de mando y verificar que abren las compuertas asociadas.
3. Verificar que permanecen apagadas las alarmas: "Anomalía unidades extracción Edificio Combustible", "Posición incorrecta compuertas unidades extracción Edificio Combustible", y "Anomalía filtros unidades extracción Edificio Combustible.
4. Las compuertas de regulación, a la descarga de las unidades de extracción, mantendrán un caudal entre 7200 y 8800 CFM. Verificar localmente que se mantiene el caudal de aire en los interruptores indicadores de caudal.
5. Pasar la unidad de suministro a Alta velocidad mediante su selector.
6. Verificar que permanecen apagadas las alarmas: "Anomalía unidad suministro Edificio Combustible" y "Alta presión diferencial unidad suministro Edificio Combustible".

C.4.4. Puesta en servicio en Operación Normal después de las Operaciones de Manejo de Combustible

C.4.4.1. Condiciones iniciales particulares

- El sistema se encuentra operando de la siguiente forma: Unidad de suministro de aire operando en alta velocidad. Unidades de extracción de aire A y B en marcha.

C.4.4.2. Maniobras

1. Verificar abierta la compuerta de aislamiento del colector de aspiración de aire de la superficie de la PCG mediante el botón pulsador.
2. Abrir la compuerta de aislamiento del colector de descarga de aire a la superficie de la PCG, mediante el botón pulsador.
3. Pasar la unidad de suministro de aire a la posición baja velocidad mediante el selector.
4. Parar una unidad de extracción mediante su selector de mando y verificar que cierran las compuertas asociadas.

C.4.5. Operación durante un accidente de manejo de combustible o activación de los monitores de radiación

C.4.5.1. Condiciones iniciales particulares

- El sistema de Ventilación del Edificio de Combustible se encuentra en funcionamiento en modo de operación normal o en modo de operación para operaciones de manejo de combustible.
- En el instante t se produce una señal de alta radiación en el Edificio de Combustible dada por los lazos de radiación.

C.4.5.2. Maniobras

1. Verificar la unidad de suministro parada.
2. Verificar cerradas las compuertas de aspiración de la unidad de suministro mediante su luz verde indicadora.
3. Verificar que las dos unidades de extracción se encuentran en funcionamiento.
4. Reponer la señal de aislamiento del Edificio de Combustible mediante los selectores llevándolos a la posición reposición.
5. Parar una unidad de extracción.
6. Cuando la radiación del Edificio de Combustible sea normal, arrancar la unidad de suministro en baja velocidad.

C.5. Instrumentación

A continuación se describe la instrumentación asociada al Sistema de Ventilación HVAC del Edificio de Combustible dividiéndola en las diferentes unidades anteriormente presentadas. La información ha sido extraída de los documentos de diseño y del esquema lógico de funcionamiento del sistema.

C.5.1. Unidad de suministro de aire

La instrumentación asociada a esta unidad se puede dividir en varios grupos, cada uno de los cuales está relacionado con los siguientes componentes del sistema:

- Ventilador (motor).
- Filtros.
- Resistencias.
- Compuertas.

C.5.1.1. Ventilador

La unidad de suministro de aire contiene un único ventilador que tiene 100 % de capacidad. Este ventilador es de tipo centrífugo y puede funcionar a dos velocidades, 725 (baja velocidad) y 1475 (alta velocidad) rpm. Su presión estática de diseño es 77,8 mm.c.a y el caudal efectivo que puede impulsar es de 24480 o 12240 m^3/h dependiendo de la velocidad. La potencia consumida por el ventilador es 12 o 17 CV, también dependiendo de la velocidad a la que se utiliza, y es alimentado a 380 V 50 Hz. El suministro de energía se realiza a partir de un centro de distribución, concretamente, el centro de control de motores (CCM) 6C7-X. El control del ventilador se realiza desde Sala de Control mediante el interruptor/selector IC/SM-81XX. No existe la posibilidad de ejercer control local o automático sobre el ventilador. En el propio panel de control en el que está el interruptor/selector existen lámparas de señalización para indicar parada, alta velocidad o baja velocidad.

Respecto a los elementos auxiliares asociados, se destacan los siguientes:

- Relé R3/KB76 contacto 3 de Aislamiento de Edificio de Combustible, que daría orden de desconexión en caso de haber un Aislamiento de Edificio de Combustible.

- Relé R1, que da orden de apertura o cierre de la compuerta de suministro A.
- Relé R2, que da orden de apertura o cierre de la compuerta de suministro B.
- Interruptores de baja presión diferencial.

Por disparo del disyuntor 52, actuación del térmico 49 o fusión de los fusibles de mando, actúa una alarma en Sala de Control. Por alta presión diferencial de filtros actúa otra alarma. Por mal funcionamiento de la unidad, se activa una alarma. Los interruptores de fin de carrera o baja presión diferencial y alta o baja velocidad activan el relé R3 para actuar una alarma en Sala de Control. Las señales de alta o baja velocidad y baja temperatura, ponen en funcionamiento un programador de cuatro etapas para las resistencias de calefacción.

C.5.1.2. Filtros

En la unidad de suministro de aire existen 2 filtros. Un prefiltro de 5 cm de espesor de tipo No regenerable con una eficiencia de eliminación de partículas del 50 % y un filtro de alta eficiencia (HEF) de tipo No regenerable con eficiencia del 90 %.

C.5.1.3. Resistencias

A continuación de la unidad de los filtros hay una batería de cuatro resistencias que realiza la función de atemperar el aire. Esta batería tiene una potencia de 4 x 75 kW y en condiciones de máximo caudal es capaz de aumentar la temperatura del aire de entrada de 0,6 ºC a 34 ºC. La totalidad de las resistencias se alimentan a 380 V 50 Hz desde el centro de control de motores 6C7-X. El control de las resistencias es realizado automáticamente por el programador en caja local de la unidad y no tienen lámparas de señalización en Sala de Control. Por disparo del disyuntor 52 o fusión de los fusibles de mando, actúa una alarma en Sala de Control.

C.5.1.4. Compuertas

Las compuertas, situadas entre la captación de aire exterior y los filtros, que son redundantes en su función para asegurar el aislamiento del Edificio de Combustible en caso de señal de Aislamiento, son alimentadas a 380 V 50 Hz desde centros de distribución diferentes. Concretamente, la compuerta A es alimentada mediante el CCM AC3-X y la compuerta B mediante el CCM BC4-X. En ambas el control de la compuerta se realiza por medio de la unidad y para ambas existen lámparas de señalización en Sala de Control que indican el cierre o apertura de la compuerta.

Los elementos auxiliares asociados a las compuertas son:

- Relé R2/KB76 contacto 7 o relé R1/KB67 contacto 2 dan orden de cierre de la compuerta A.
- Relé R2/KB77 contacto 7 o relé R1/KB67 contacto 2 dan orden de cierre de la compuerta B.
- Relé R1/KB67 contacto 1 y el relé R2/KB76 contacto 8 dan orden de apertura a la compuerta A.
- Relé R1/KB67 contacto 1 y el relé R2/KB77 contacto 8 dan orden de apertura a la compuerta B.
- Fines de carrera y limitadores de par incorporados en la compuerta.

Por disparo del disyuntor 52, actuación del térmico 49 o fusión de los fusibles de mando, actúa una alarma en Sala de Control.

C.5.2. Unidad de extracción de aire

La instrumentación asociada a estas unidades se puede dividir en varios grupos, cada uno de los cuales está relacionado con los siguientes componentes del sistema:

- Ventilador (motor).
- Filtros.
- Resistencias.
- Compuertas.

Destacar que la instrumentación es la misma en las 2 unidades, cambia la distribución de energía y los elementos de control asociados.

C.5.2.1. Ventilador

Ambos ventiladores son centrífugos y con 100 % de capacidad cada uno. El caudal efectivo de cada ventilador es 13600 m^3/h y su presión estática es 220 mm.c.a. Ambos consumen una potencia de 25 CV y son alimentados a 380 V 50 Hz. Ambos ventiladores están situados después de la sección de filtrado.

Ventilador A El suministro de energía hacia este ventilador es redundante puesto que se realiza desde tres centros de distribución diferentes: CCM AC5-X, CCM 5H4-1, CCM AH5-X. El control de este ventilador se puede realizar remotamente desde un selector en Sala de Control o bien automáticamente por un contacto del SIS en el armario del secuenciador o por un contacto del relé R2/KB76 de Aislamiento de Edificio de Combustible o por un contacto del R3/KB70 (DCNE). No existe control local, y tiene lámparas de señalización en Sala de Control de parada y marcha incorporadas al selector.

Los elementos auxiliares asociados a este ventilador son:

- Relé R3/CN09 contacto 4 de sistema DNCE, da orden de desconexión por medio del relé biestable R3 contacto 2.
- Relé R2 temporizado en armario de relés auxiliares.
- Interruptor de baja presión diferencial en unidad A.
- Interruptores alta presión diferencial en unidad A.
- Relé R1 y R4 temporizado en panel de relés auxiliares.

Por disparo del disyuntor 52, actuación del térmico 49 o fusión de los fusibles de mando, actúa una alarma en Sala de Control. Con alta presión diferencial en filtros actúa una alarma en Sala de Control. Por mal funcionamiento de la unidad activa una alarma también en Sala de Control. Por baja presión diferencial en el ventilador actúa una alarma en Sala de Control. Con alta temperatura actúa una alarma en Sala de Control. Con marcha de la unidad, baja temperatura y alta humedad entra en funcionamiento una batería de calentadores.

Ventilador B El suministro de energía hacia este ventilador es redundante puesto que se realiza desde tres centros de distribución diferentes: CCM BC3-X, CCM 6H6-1 y CCM BH3-X. El control de este ventilador se puede realizar remotamente desde un selector en Sala de Control o bien automáticamente por un contacto del SIS en el armario del secuenciador o por un contacto del relé R2/KB77 de Aislamiento de Edificio de Combustible o por un contacto del R3/KB77 (DCNE). No existe control local, y tiene lámparas de señalización en Sala de Control de parada y marcha incorporadas al selector.

Los elementos auxiliares asociados a este ventilador son:

- Relé R3/CN10 contacto 4 de sistema DNCE, da orden de desconexión por medio del relé biestable R3 contacto 2.
- Relé R2 temporizado en armario de relés auxiliares.
- Interruptor de baja presión diferencial en unidad B.
- Interruptores alta presión diferencial en unidad B.
- Relé R1 y R4 temporizado en panel de relés auxiliares.

Por disparo del disyuntor 52, actuación del térmico 49 o fusión de los fusibles de mando, actúa una alarma en Sala de Control. Con alta presión diferencial en filtros actúa una alarma en Sala de Control. Por mal funcionamiento de la unidad se activa una alarma en Sala de Control. Por baja presión diferencial en el ventilador actúa una alarma en Sala de Control. Con alta temperatura actúa una alarma en Sala de Control. Con marcha de la unidad, baja temperatura y alta humedad entra en funcionamiento una batería de calentadores.

C.5.2.2. Filtros

Los filtros de ambas unidades son los mismos. En cada unidad hay 4 filtros: 1 prefiltro No regenerable de eficiencia 80 %. 1 filtro HEPA No regenerable de eficiencia 99,97 %. Un filtro de carbón activo, con espesor de lecho de 5 cm, con una eficiencia para Iodos (elemental y orgánico) de 95 %. Finalmente, otro filtro HEPA con una eficiencia para partículas de diámetro menor a 3 micras de 99,97 %.

C.5.2.3. Resistencias

Antes de la sección de filtraje hay una batería de 4 resistencias que realiza la función de atemperar el aire y reducir su humedad. Cada batería tiene una potencia de 4 x 42 kW. La totalidad de las resistencias se alimentan a 380 V 50 Hz. Las de la unidad A lo hacen desde el CCM A5-X y las de la unidad B lo hacen desde el CCM BC3-X. El control de las resistencias es realizado automáticamente por el programador en caja local de la unidad A o B y no tienen lámparas de señalización en Sala de Control. Por disparo del disyuntor 52 o fusión de los fusibles de mando, actúa una alarma en Sala de Control diferente para cada unidad.

C.5.2.4. Compuertas

Compuertas de la unidad de extracción A Las compuertas, situadas antes de la batería de resistencias y después del ventilador respectivamente, consumen 0,28 CV y son alimentadas a 380 V 50 Hz desde el CCM AC3-X. En ambas el control de la compuerta se realiza por medio de la unidad de extracción y para ambas existen lámparas de señalización en Sala de Control que indican el cierre o apertura de la compuerta.

Los elementos auxiliares asociados a las compuertas son:

- Relé R1/KB70 da orden de apertura o cierre a la compuerta B.
- Fines de carrera y limitadores de par incorporados en la compuerta.
- Fines de carrera y limitadores de par incorporados en la compuerta.

Por disparo del disyuntor 52, actuación del térmico 49 o fusión de los fusibles de mando, actúa una alarma en Sala de Control.

Compuertas de la unidad de extracción B Las compuertas, situadas antes de la batería de resistencias y después del ventilador respectivamente, consumen 0,28 CV y son alimentadas a 380 V 50 Hz desde el CCM BC4-X. En ambas el control de la compuerta se realiza por medio de la unidad de extracción y para ambas existen lámparas de señalización en Sala de Control que indican el cierre o apertura de la compuerta.

Los elementos auxiliares asociados a las compuertas son:

- Relé R1/KB73 da orden de apertura o cierre a las compuertas A y B.
- Fines de carrera y limitadores de par incorporados en la compuerta.
- Fines de carrera y limitadores de par incorporados en la compuerta.

Por disparo del disyuntor 52, actuación del térmico 49 o fusión de los fusibles de mando, actúa una alarma en Sala de Control.

Compuerta de regulación de la unidad de extracción A Situada entre el ventilador y la compuerta aguas abajo de la unidad, esta compuerta permite regular el flujo de aire que pasa por la unidad de extracción A. El suministro de energía a esta compuerta es redundante y se realiza mediante el CCM AC5-X o bien el CCM 5C4-X. La compuerta se controla automáticamente por un interruptor de caudal que actúa sobre R5-KB70 o R6-KB70. Por R4-KB76 en caso de señal de aislamiento.

Compuerta de regulación de la unidad de extracción B Situada entre el ventilador y la compuerta aguas abajo de la unidad, esta compuerta permite regular el flujo de aire que pasa por la unidad de extracción B. El suministro de energía a esta compuerta es redundante y se realiza mediante el CCM BC3-X o bien el CCM 6C6-X. La compuerta se controla automáticamente por un interruptor de caudal que actúa sobre R5-KB73 o R6-KB73. Por R3-KB77 en caso de señal de aislamiento.

C.6. Inspecciones y Especificaciones técnicas de funcionamiento

Se omite este apartado por motivos de confidencialidad.

C.7. Interfase con otros sistemas

La tabla C.1 muestra las diferentes interfases del Sistema de Ventilación HVAC del Edificio de Combustible con otros sistemas y componentes.

Sistema	Interacción
Sistema de vigilancia de radiación (Áreas)	Señal de Aislamiento del Edificio de Combustible por alta radiación, orden de parada de la unidad de suministro y de arranque de las unidades de filtrado.
Sistema de baja tensión. Barras de emergencia	Alimentación a los motores de los ventiladores de las unidades de filtrado y compuertas asociadas a dichas unidades y a las asociadas con el aislamiento del edificio.
Sistema de corriente continua	Alimentación de corriente continua a cuadros asociados a las unidades de filtrado.
Sistema del secuenciador	Señal de Pérdida de Potencia Exterior para el arranque secuenciado de las unidades de filtrado.
Sistema de baja tensión. Barras normales	Alimentación a los motores de la unidad de suministro, de extracción normal, aerotermos y compuertas no relacionadas de las unidades de filtración y aislamiento del edificio.
Sistema de corriente continua	Alimentación de corriente continua a cuadros asociados a las unidades de suministro.
Sistema de alarmas de Sala de Control	Señalización de alarmas en Sala de Control.

Tabla C.1: Interfase del sistema de ventilación con otros sistemas.

C.8. Árbol de fallos

El árbol de fallos del sistema de ventilación se crea a partir de las bases de modelización definidas en la memoria de la tesis. El árbol de fallos del sistema está formado por los sub-árboles listados a continuación. En caso que se llegue a fallo en alguno de estos sub-árboles, se considera que el sistema ha fallado (véase la figura C.1).

C.8.1. Sub-árboles de fallo del sistema de ventilación

C.8.1.1. VENTFAIL: Fallo en la descarga del sistema de ventilación

Se modeliza el caso en el que el plénum de descarga del Edificio Auxiliar está bloqueado y las compuertas de alivio han de abrirse. Se considera la hipótesis que en caso de existir una acumulación de aire a la salida del ventilador y las secciones de filtrado, alguno de estos componentes podría fallar dejando inutilizadas las unidades de extracción. Se trata de una inclusión conservadora pues no se conoce con seguridad si la acumulación de aire podría provocar fallo de alguno de los componentes aguas arriba.

La modelización del bloqueo del plénum de descarga del Edificio Auxiliar se realiza mediante el fallo de obturación de compuertas motorizadas al no disponerse de un suceso específico de bloqueo de conducto. Las compuertas de alivio se modelizan como compuertas de retención.

C.8.1.2. EXTSISTFAIL: Fallo en la extracción del sistema de ventilación

Se modeliza el fallo de ambas unidades teniendo en cuenta que se necesita el fallo combinado de ambas para que se dé fallo en la extracción. En cada unidad se modeliza el fallo de las compuertas, ventilador,

filtros y batería de resistencias de tal manera que el fallo de uno de estos grupos supone el fallo de la unidad de extracción. Tanto en compuertas como en el ventilador se modela el fallo al arrancar por los motivos que se han comentado en las condiciones. En aquellos componentes en los que ha sido necesario se les ha acoplado el fallo del CCM correspondiente. Conservadoramente, si un componente recibe suministro de más de un CCM solo se le ha aplicado uno. De forma conservadora, las baterías de resistencias se han modelado mediante el fallo de una de ellas.

C.8.1.3. SSUM: Fallo en el suministro de aire del sistema de ventilación

Tal y como se ha comentado en las bases de modelización, se modeliza el fallo de las dos compuertas redundantes de aislamiento del exterior. En caso de fallo combinado de ambas al cerrar o a permanecer cerradas se considerará fallado el Sistema de Ventilación.

C.8.1.4. DETFAIL: Fallo en los trenes de detectores del sistema de vigilancia de radiación

Debido a la falta de información sobre la sección de este sistema que actúa en el Edificio de Combustible se ha decidido actuar conservadoramente y modelizar cada tren con un único detector. El fallo combinado de ambos trenes, es decir el fallo combinado de dos detectores, lleva a fallo del sistema de ventilación.

C.8.2. Límites del sistema

El límite del flujo de aire se establece en el propio sistema de ventilación. Concretamente, los límites de la unidad de suministro sobre los que se aplica la modelización son las compuertas y el ventilador. Para las unidades de extracción de aire, los límites de las unidades sobre los que se aplica la modelización son la batería de calentadores y el plénum de descarga del Edificio Auxiliar. Estos límites se observan de forma clara en el diagrama de tubería e instrumentación del Sistema de Ventilación. El resto se considera una caja negra a efectos del estudio probabilista de seguridad.

En cuanto a los detectores, solo se modeliza el propio aparato en sí, la electrónica y sistema eléctrico asociado es una caja negra.

Finalmente, los límites del Sistema de Ventilación con los de suministro de energía eléctrica para el accionamiento de los componentes se establecen en la conexión del cable de suministro con el centro de distribución correspondiente a cada componente. Gracias a la Base de Datos Genérica de la central nuclear se ha podido modelizar el fallo de los CCM citados anteriormente teniendo en cuenta los modos de fallo locales y todos los modos de fallo aguas arriba que pueden llevar a fallo del CCM.

C.8.3. Descripción de los componentes, límites y modos de fallo aplicados en la modelización del fallo del sistema de ventilación

Se describen los componentes considerados en la modelización mediante árbol de fallos del sistema de ventilación en cuanto a límites físicos y modos de fallo aplicables. Los componentes se clasifican como mecánicos, eléctricos o de instrumentación y control. En este estudio, no se contemplan componentes de control. Para la realización de este apartado se ha utilizado la Base de Datos Genérica de la centra nuclear, principalmente, y el IAEA-TECDOC-478 *Component reliability data for use in probabilistic risk assessment* [82] y el *Savannah River Site Generic Data Base Development* [83]. En las siguientes descripciones se indica que modos de fallo han sido añadidos a la Base de Datos Genérica de la central nuclear.

C.8.3.1. Componentes mecánicos

Ventilador Los límites físicos considerados para los ventiladores incluyen el cuerpo de éste, el acoplamiento y el motor accionador. No está incluido el interruptor o contactor de alimentación ni su circuito de control asociado.

Los modos de fallo locales aplicados a los ventiladores son el "fallo al arranque" y el "fallo en operación".

Filtro Los límites físicos considerados para los filtros incluyen el cuerpo y el elemento filtrante tipo malla, cesta o cartucho. El modo de fallo postulado a los filtros es la "obturación". Además, en la base de datos de *Savannah River Site* se han encontrado los fallos por “fuga” y “rotura” en filtro.

Compuerta motorizada Se consideran las compuertas de ventilación motorizadas de los sistemas de HVAC.

Los límites físicos considerados para las compuertas motorizadas incluyen el cuerpo de ésta, la propia compuerta obturadora, el motor actuador, fines de carrera propios, el contactor (contactos principales y auxiliares) así como el circuito de control local asociado (circuito de apertura y cierre, protecciones, mandos e indicaciones locales, transformador de alimentación para el control) y el interruptor de acoplamiento a barra.

Los modos de fallo locales aplicados a las compuertas motorizadas son el "fallo a la apertura", el "fallo al cierre", el "fallo a permanecer abierta" y el "fallo a permanecer cerrada". Además, en la base de datos de *Savannah River Site* se han encontrado modos de fallo relacionados con los “fallo a permanecer abierta” y “fallo a permanecer cerrada”. Estos fallos son “operación espuria”, “obturación”, “fuga” y “rotura”.

Compuerta de retención Se consideran las compuertas de ventilación de retención de los sistemas de HVAC.

Los límites físicos considerados para las compuertas de retención incluyen el cuerpo de ésta y la propia compuerta.

Los modos de fallo aplicables a las compuertas de retención son el "fallo a la apertura", "fallo al cierre" y el "fallo a permanecer cerrada". Además, en la base de datos de *Savannah River Site* se han encontrado modos de fallo relacionados con el “fallo a permanecer cerrada”. Estos fallos son “operación espuria”, “obturación”, “fuga” y “rotura”.

Resistencia eléctrica No se han encontrado datos en la Base de Datos Genérica de la central nuclear. A partir de IAEA-TECDOC-478 se considera el modo de fallo “fallo en operación, fallo al calentar”.

C.8.3.2. Componentes eléctricos

Detector de radiación De manera similar al caso de la resistencia eléctrica, no se han encontrado datos para este componente en la Base de Datos Genérica. Mediante la base de datos de *Savannah River Site* se han obtenido datos para modo de fallo “fallo en operación”.

Barra eléctrica Los límites físicos considerados para las barras eléctricas son la propia barra (incluidas sus protecciones) hasta el primer interruptor. Se consideran dos tipos de barras; las comprendidas entre niveles de tensión de 600 V hasta 15000 V, y las barras con un nivel de tensión inferior a 500 V. No se distingue entre barras de continua y barras de corriente alterna.

El modo de fallo aplicado a las barras es el "Fallo local", considerándose todos los posibles fallos catastróficos mecánicos y eléctricos del componente (circuito abierto, puestas a tierra y cortocircuitos).

Interruptor de potencia Los límites físicos considerados para los interruptores de potencia son el propio interruptor (contactos principales) y su circuito local asociado (bobinas de arranque y disparo, protecciones, mandos e indicaciones locales,...). Se consideran dos tipos de interruptores de potencia; los de media potencia, comprendidos entre niveles de tensión de 6000 V hasta 10000 V, y los interruptores de baja potencia, con un nivel de tensión inferior a 600 V. No se distingue entre interruptores de continua e interruptores de alterna. En el caso de contactores de pequeñas bombas o ventiladores de sala o de torre de refrigeración, alimentados éstos de 380 V, se han considerado como interruptores de baja potencia. De allí la necesidad de realizar dos estimaciones para este componente eléctrico en función de la potencia.

Los modos de fallo aplicados a los interruptores de potencia son el "Fallo a la apertura", el "fallo al cierre" y la "apertura prematura".

Interruptor manual Los límites físicos considerados para los interruptores manuales son el propio interruptor y las conexiones y contactos entre entrada y salida de cables.

El modo de fallo aplicado a los interruptores manuales es el "Fallo a la transferencia".

Relé Los límites físicos considerados para los relés incluyen la bobina y los contactos asociados.

Los modos de fallo aplicables a los relés son el "fallo a la energización del relé", el "fallo a la desenergización" y la "desenergización espúrea del relé". Se consideran incluidos en este apartado los relés temporizados de tipo electro-mecánico, a los cuales se aplicarán los tres modos de fallo definidos.

Contactos de relé Los límites físicos considerados son los propios contactos del relé.

El modo de fallo aplicado a los contactos de relés es el "Fallo a la transferencia".

C.8.4. Parámetros de fallo de los componentes del sistema

Las tablas C.2 y C.3 contienen los parámetros de fallo de los diferentes componentes del sistema de ventilación del edificio de combustible. Cada parámetro de fallo está asociado a diversos sucesos básicos del árbol de fallos del sistema de ventilación.

Código	Descripción	Indisp.	Distribución	Modelo	Tasa de fallo [h^{-1}]	T.de misión [h]
FANFOP	Fallo en operación de ventilador	3,26E-03	Gamma	Mission Time (MT)	1,36E-04	24
FANFRUN	Fallo al arrancar un ventilador	3,04E-04	Beta	Probability	-	-
FMANT	Mantenimiento ventilador	2,45E-05	Lognormal	Probability	-	-
RESFOP	Fallo en operación de resistencia eléctrica	3,07E-04	Lognormal	MT	1,28E-05	24
CFSPU	Operación espuria de una compuerta	8,16E-06	Gamma	MT	3,40E-07	24
CMANT	Mantenimiento de compuerta	1,16E-02	Lognormal	Probability	-	-
CFOPEN	Fallo a la apertura de compuerta	1,14E-03	Beta	Probability	-	-
CFLEAK	Fuga en compuerta	3,34E-06	Gamma	MT	1,39E-07	24

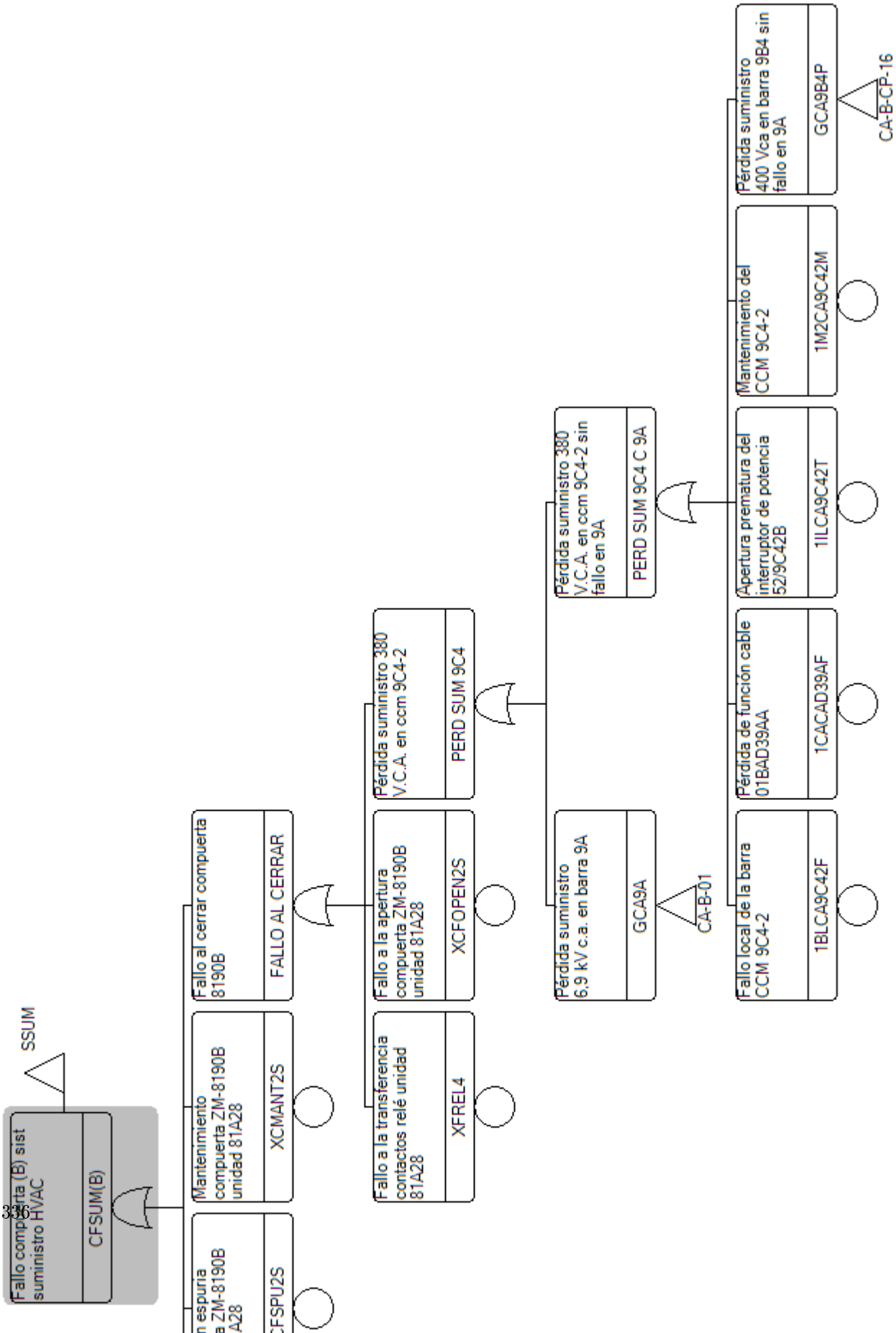
Tabla C.2: Parámetros de fallo de los componentes del sistema de ventilación.

Código	Descripción	Indisp.	Distribución	Modelo	Tasa de fallo [h^{-1}]	T.de misión [h]
FFBLOQ	Obturación de filtro	7,44E-06	Gamma	MT	3,10E-07	24
FFLEAK	Fuga en filtro	3,36E-06	Gamma	MT	1,40E-07	24
FFMANT	Mantenimiento de filtro	7,79E-06	Lognormal	Probability	-	-
RDFAIL	Fallo en operación de tren detectores	1,20E-04	Lognormal	MT	5,00E-06	24
FREL	Fallo de transferencia de relé	5,33E-06	Beta	Probability	-	-

Tabla C.3: Parámetros de fallo de los componentes del sistema de ventilación (2).

C.8.5. Modelo del árbol de fallos introducido en el APS de ATI

Las siguientes figuras muestran el modelo de árbol de fallos del sistema de ventilación del edificio de combustible introducido en el modelo APS de ATI.


SSUM
Fallo compuerta (B) sist suministro HVAC
CFSUM(B)
Mantenimiento compuerta ZM-8190B unidad 81A28
XCMANT2S
Fallo al cerrar compuerta 8190B
FALLO AL CERRAR
Fallo a la apertura compuerta ZM-8190B unidad 81A28
XCFOPEN2S
Pérdida suministro 380 V.C.A. en ccm 9C4-2
PERD SUM 9C4
Fallo a la transferencia contactos relé unidad 81A28
XFREL4
Pérdida suministro 6,9 kV c.a. en barra 9A
GCA9A
CA-B-01
Pérdida suministro 380 V.C.A. en ccm 9C4-2 sin fallo en 9A
PERD SUM 9C4 C 9A
Fallo local de la barra CCM 9C4-2
1BLCA9C42F
Pérdida de función cable 01BAD39AA
1CACAD39AF
Apertura prematura del interruptor de potencia 52/9C42B
1ILCA9C42T
Mantenimiento del CCM 9C4-2
1M2CA9C42M
Pérdida suministro 400 Vca en barra 9B4 sin fallo en 9A
GCA9B4P
CA-B-CP-16

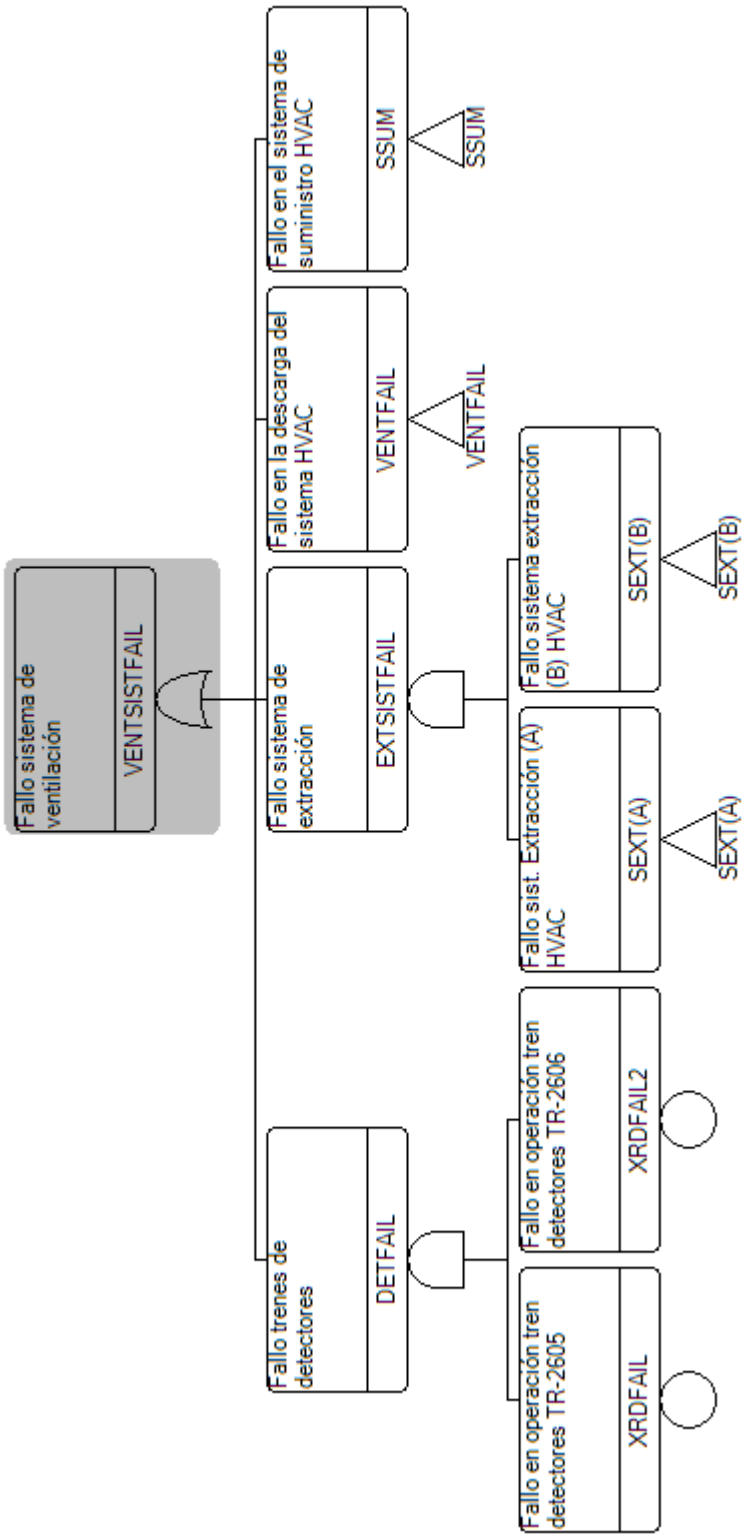


Figura C.1: Árbol de fallos del sistema de ventilación. *Top gate* y módulos principales.

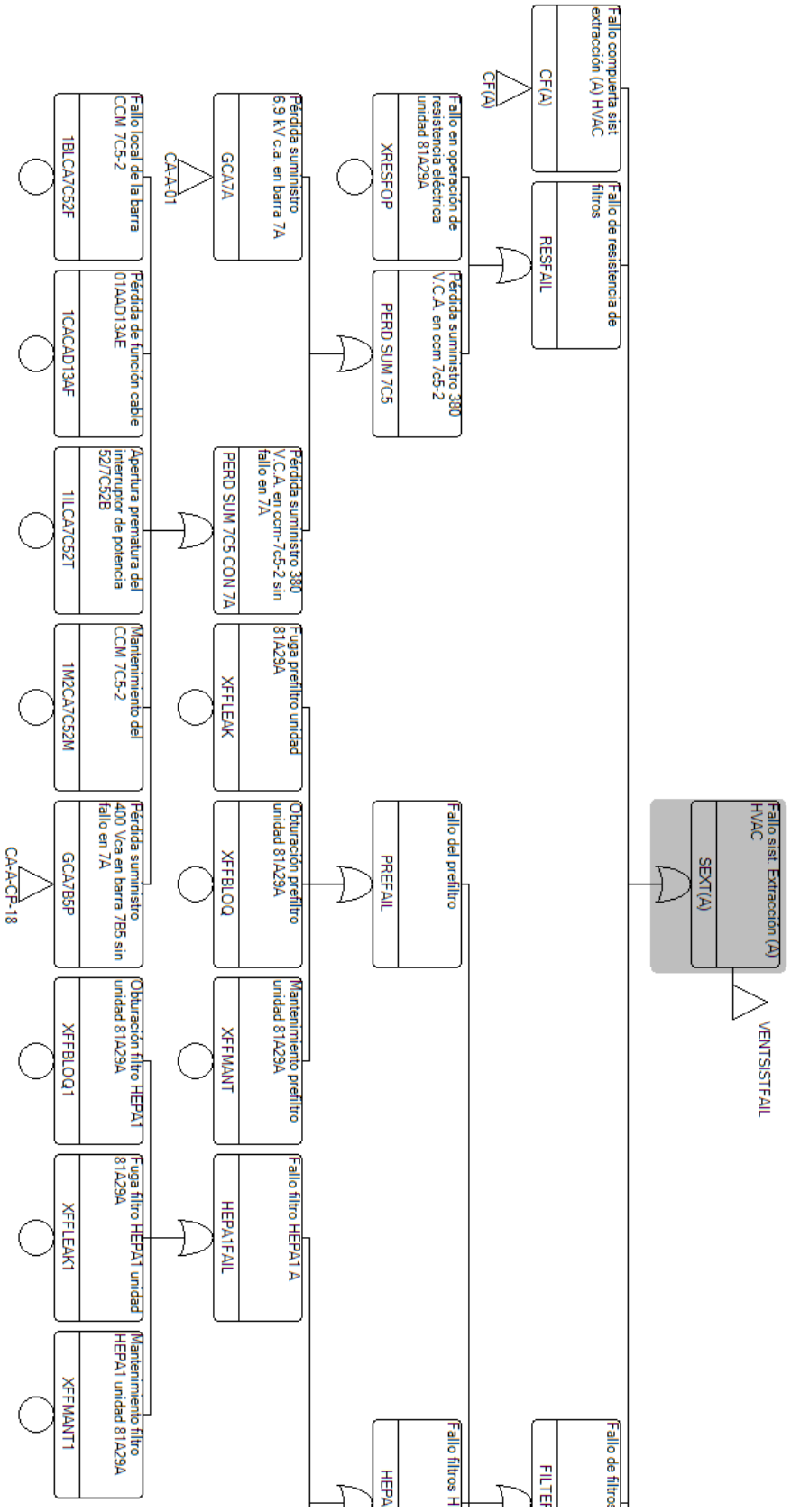


Figura C.2: Módulo SEXT(A) que representa la unidad de extracción A

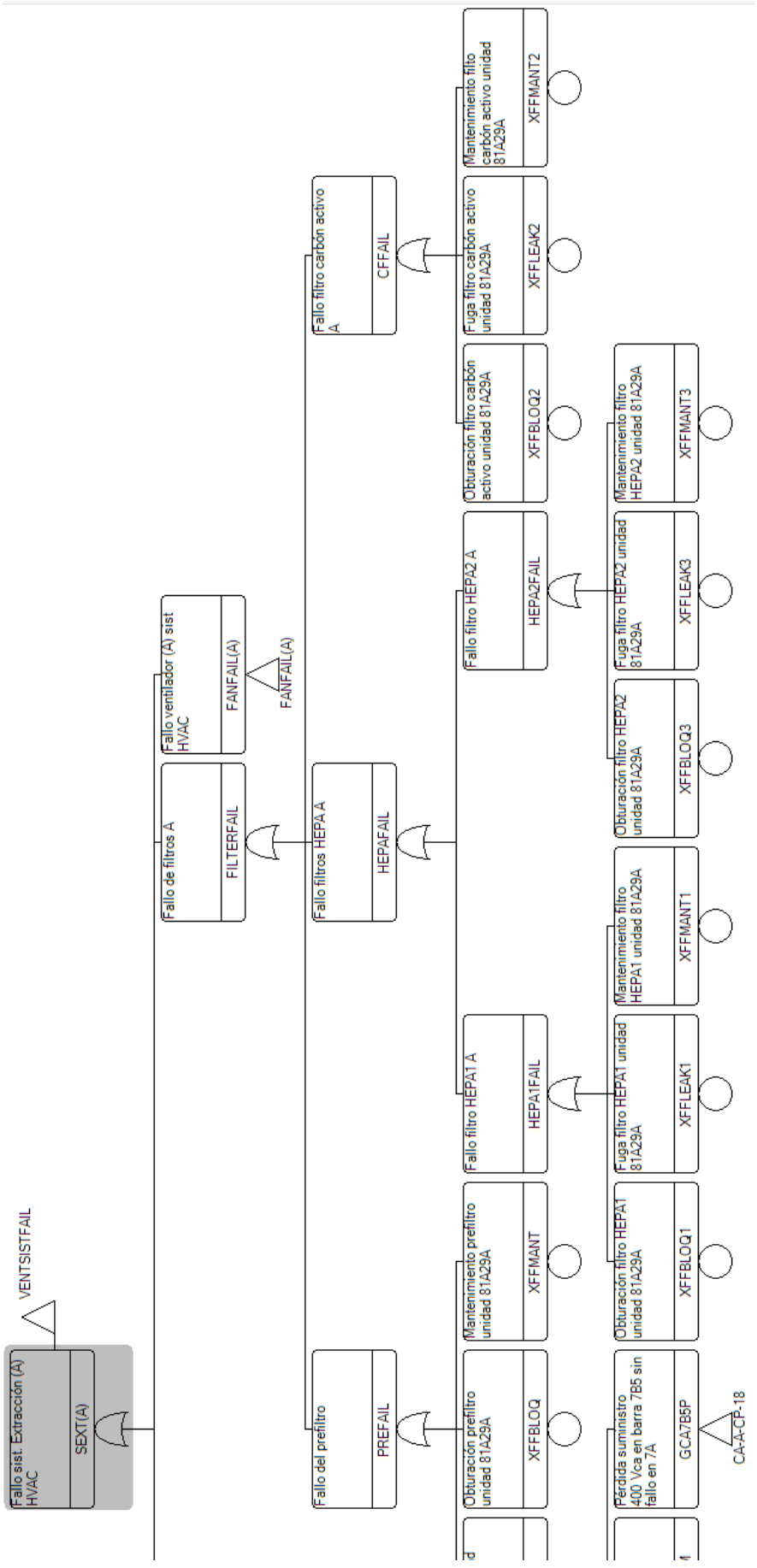


Figura C.3: Módulo SEXT(A) que representa la unidad de extracción A (2)

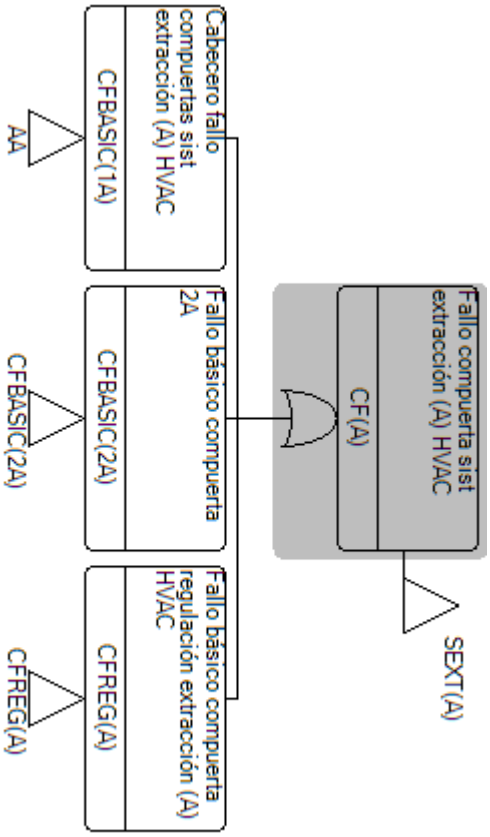


Figura C.4: Módulo CF(A) que representa el fallo de compuertas de la unidad de extracción A

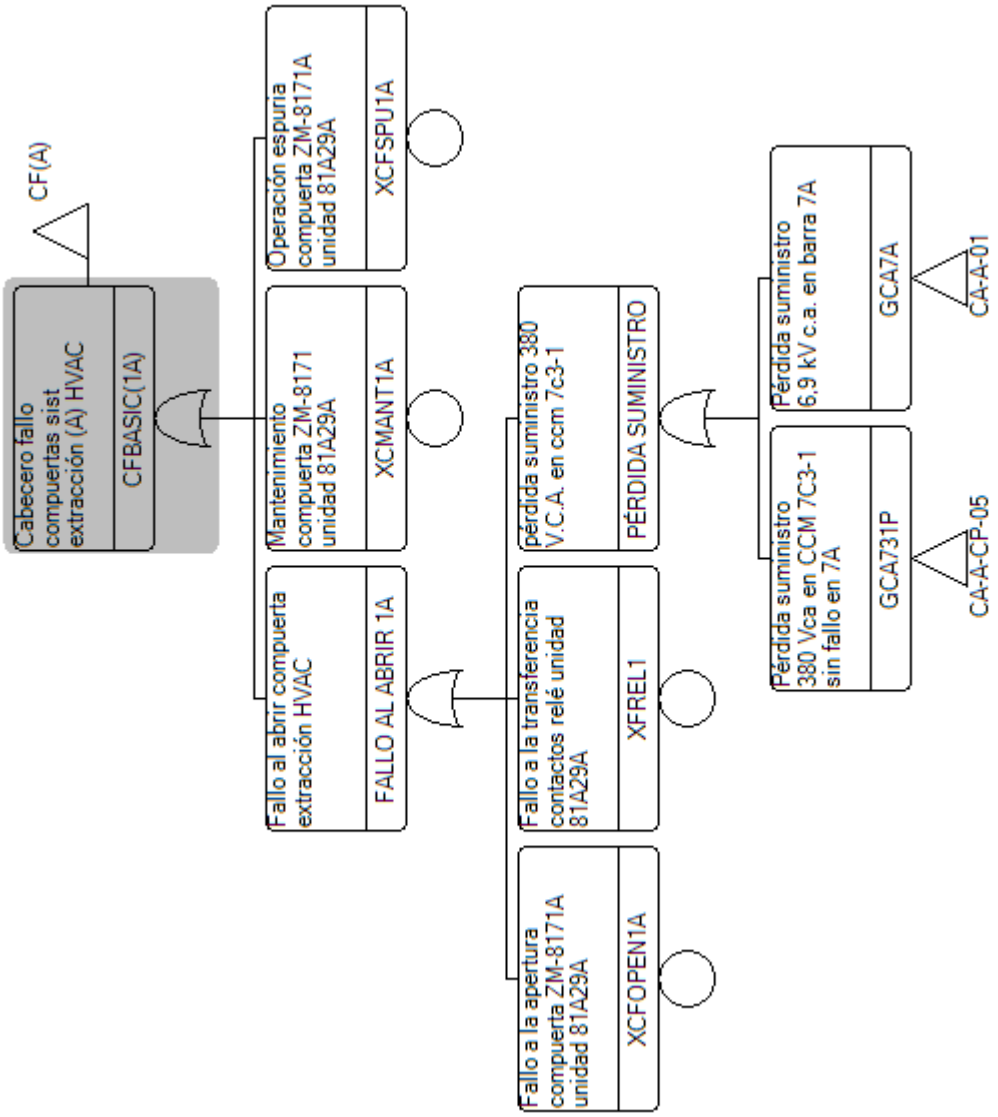


Figura C.5: Módulo CFBASIC(1A) que representa el fallo de la compuerta de extracción A de la unidad de extracción A

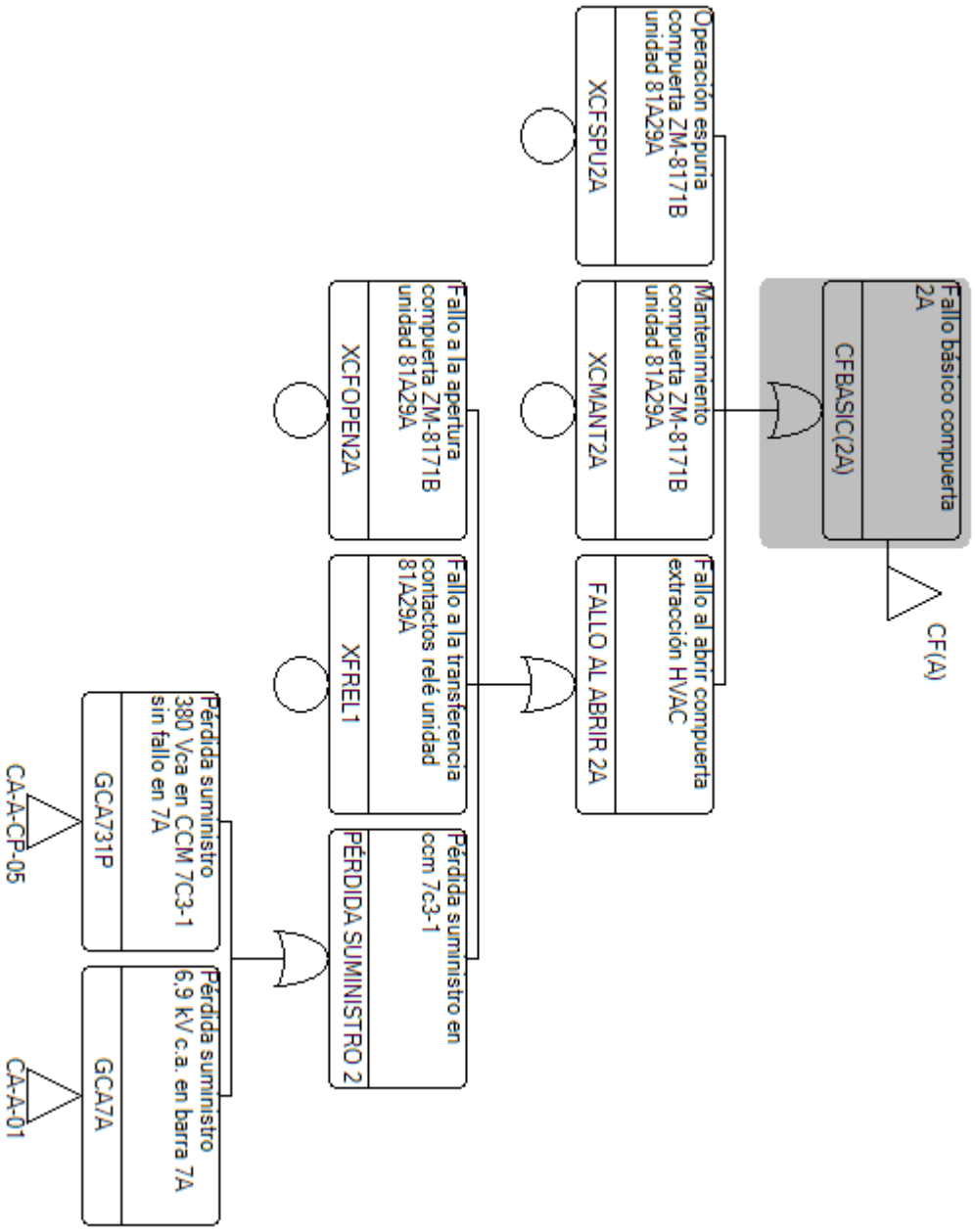


Figura C.6: Módulo CFBASIC(2A) que representa el fallo de la compuerta de extracción B de la unidad de extracción A

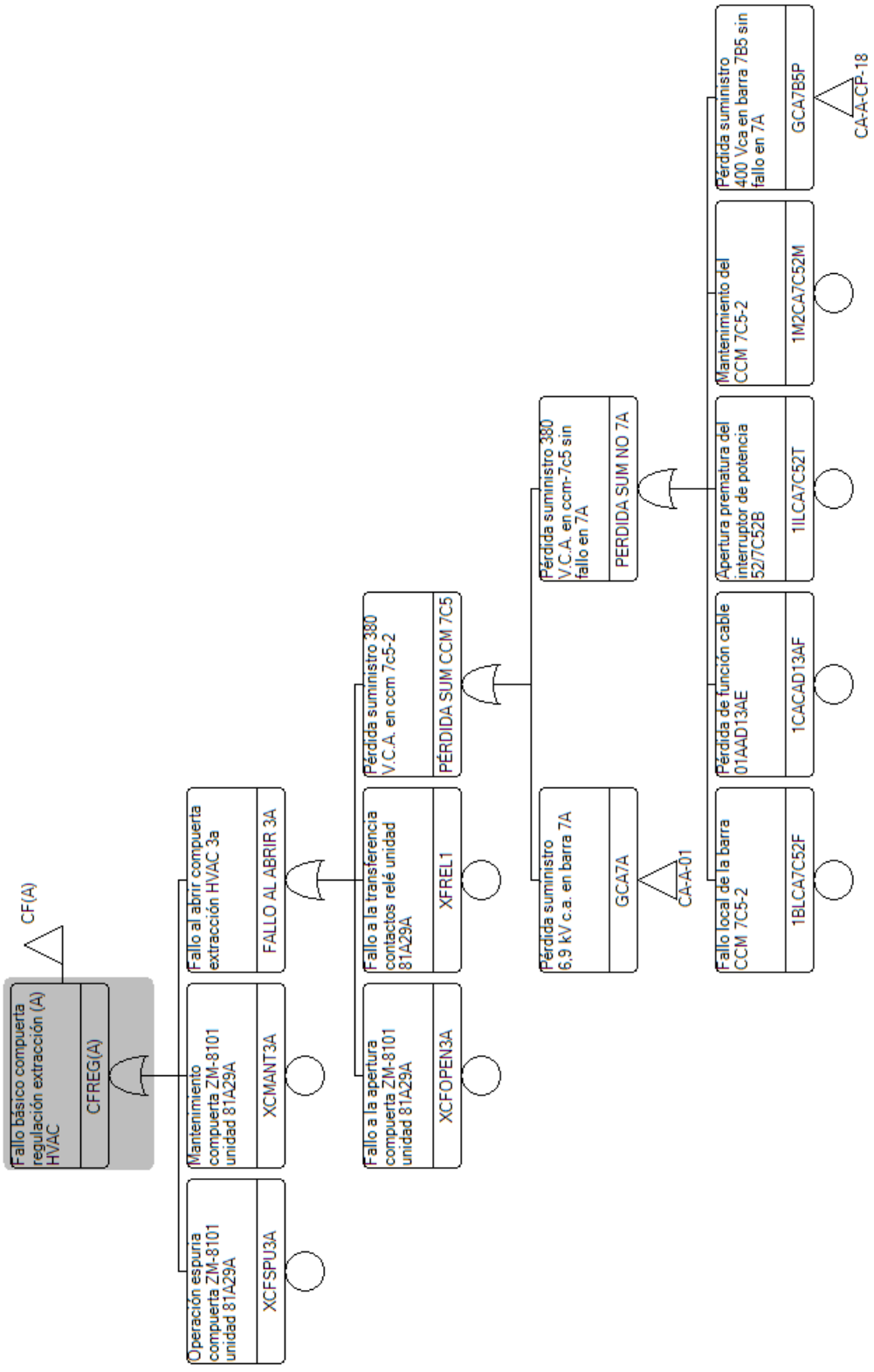


Figura C.7: Módulo CFREG(A) que representa el fallo de la compuerta de extracción común de la unidad de extracción A

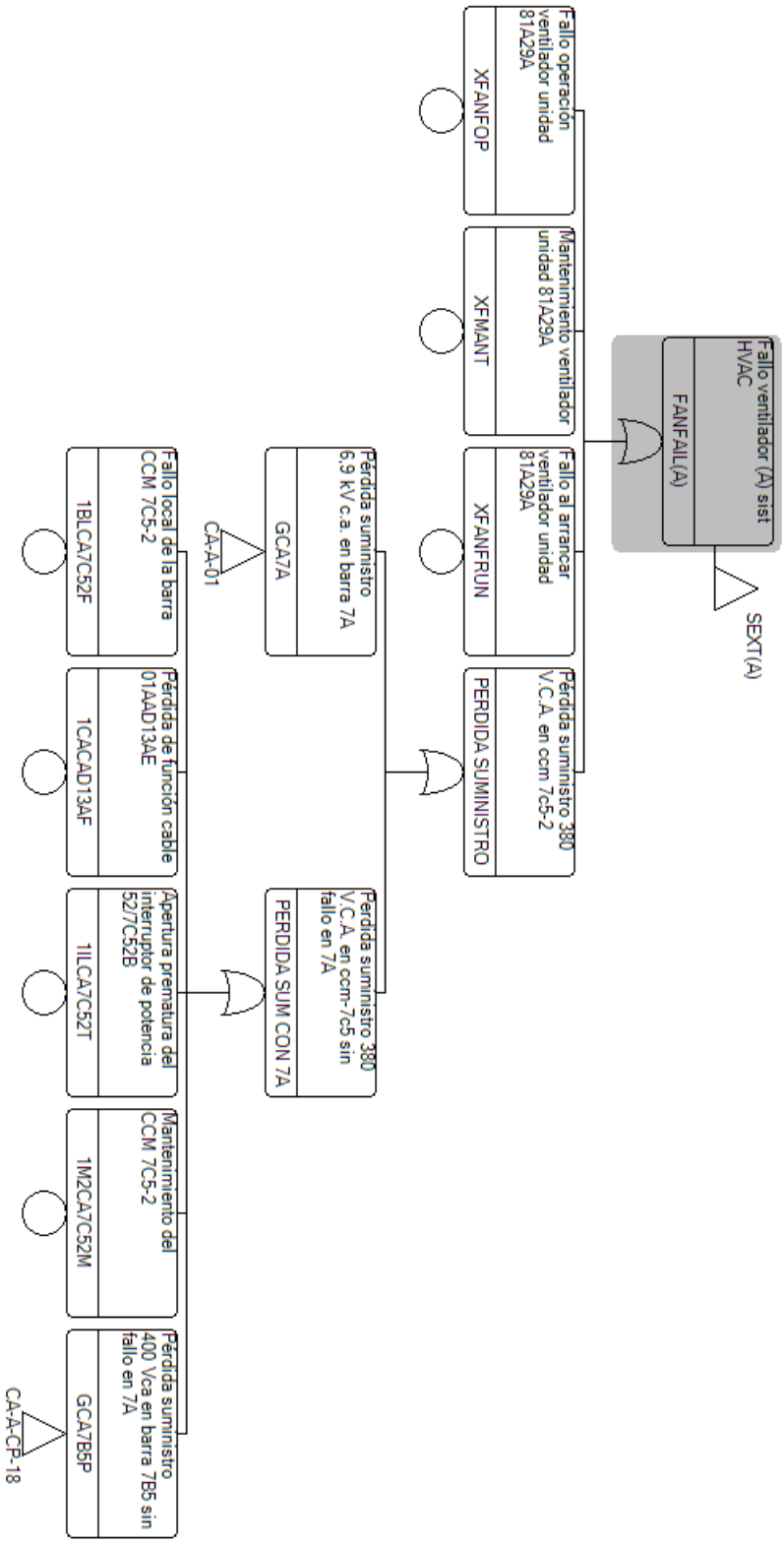


Figura C.8: Módulo FANFAIL(A) que representa el fallo del ventilador de la unidad de extracción A

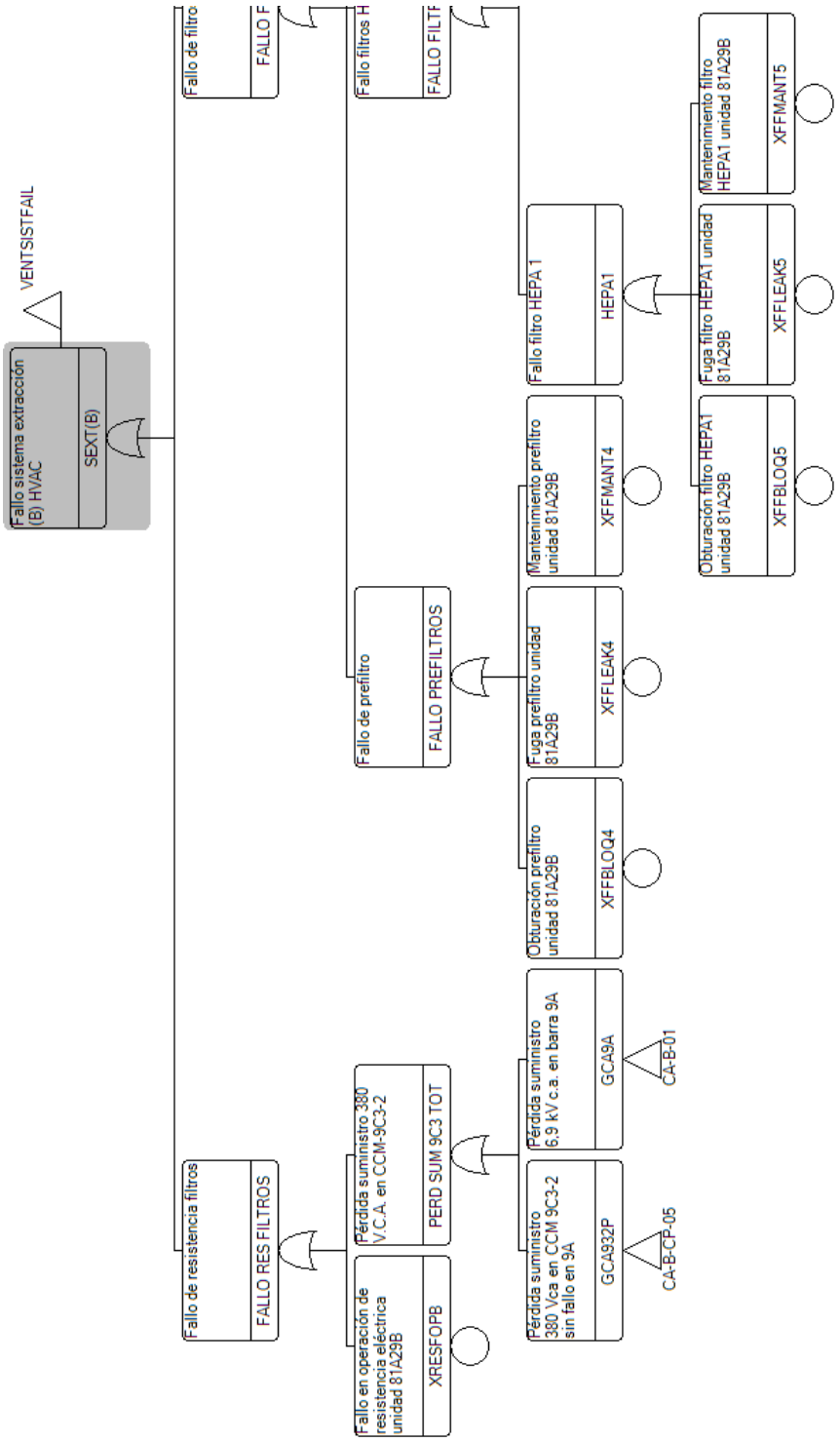


Figura C.9: Módulo SEXT(B) que representa la unidad de extracción B

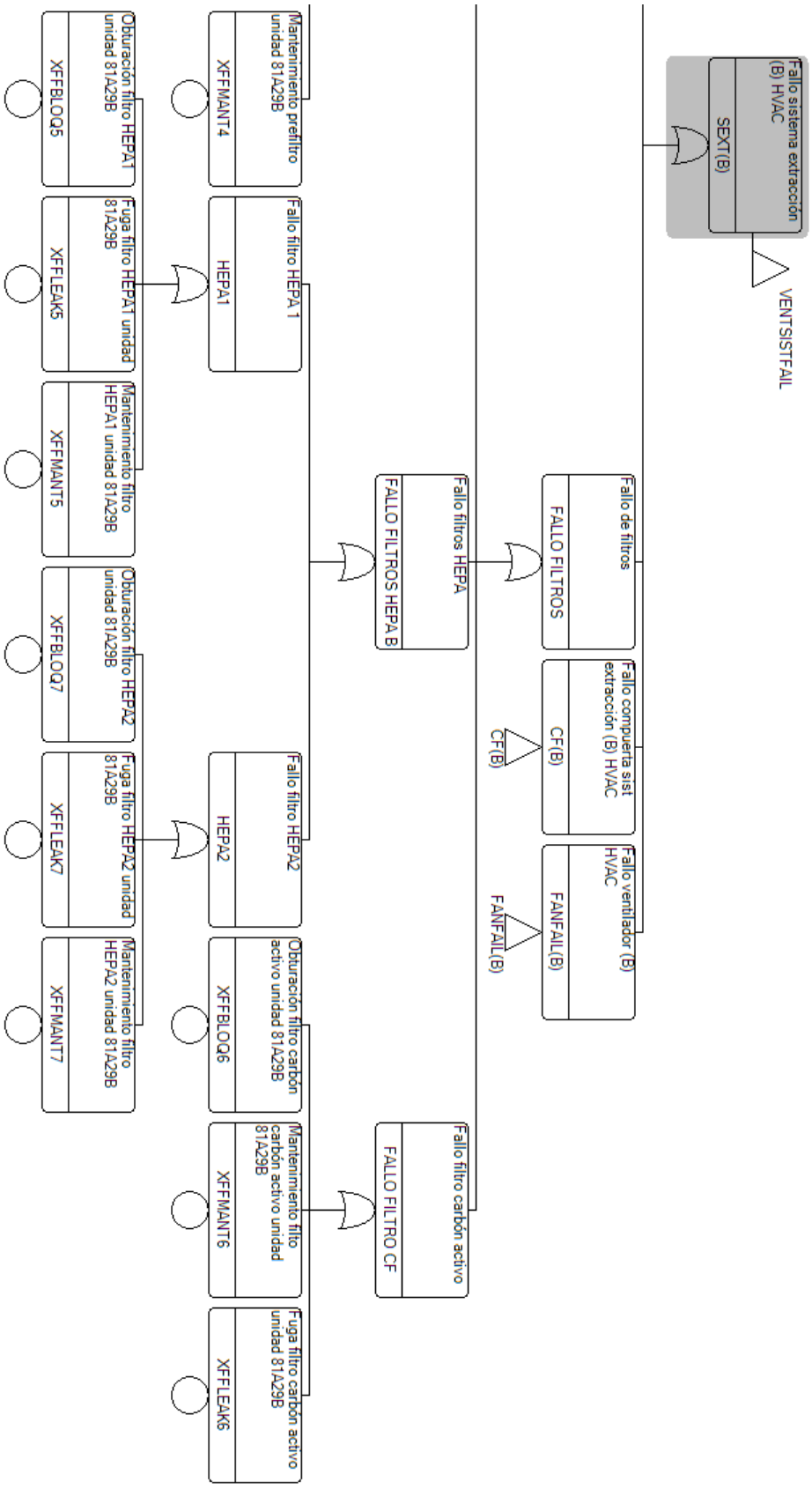


Figura C.10: Módulo SEXT(B) que representa la unidad de extracción B (2)

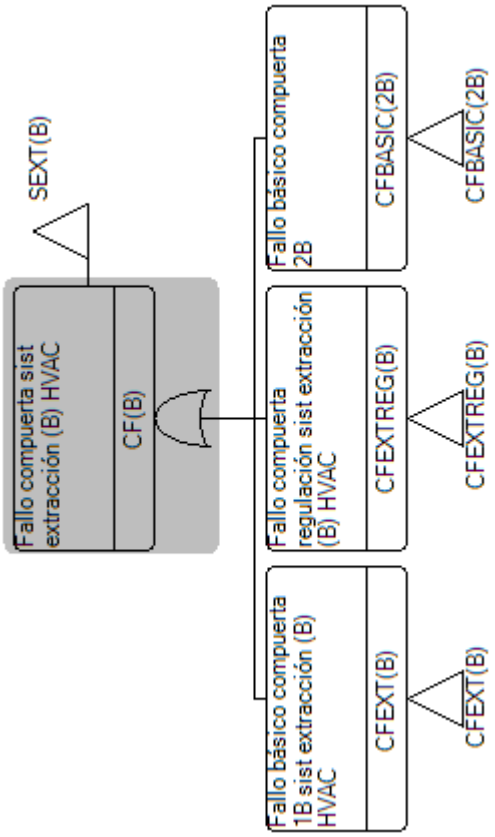


Figura C.11: Módulo CF(B) que representa el fallo de compuertas de la unidad de extracción B

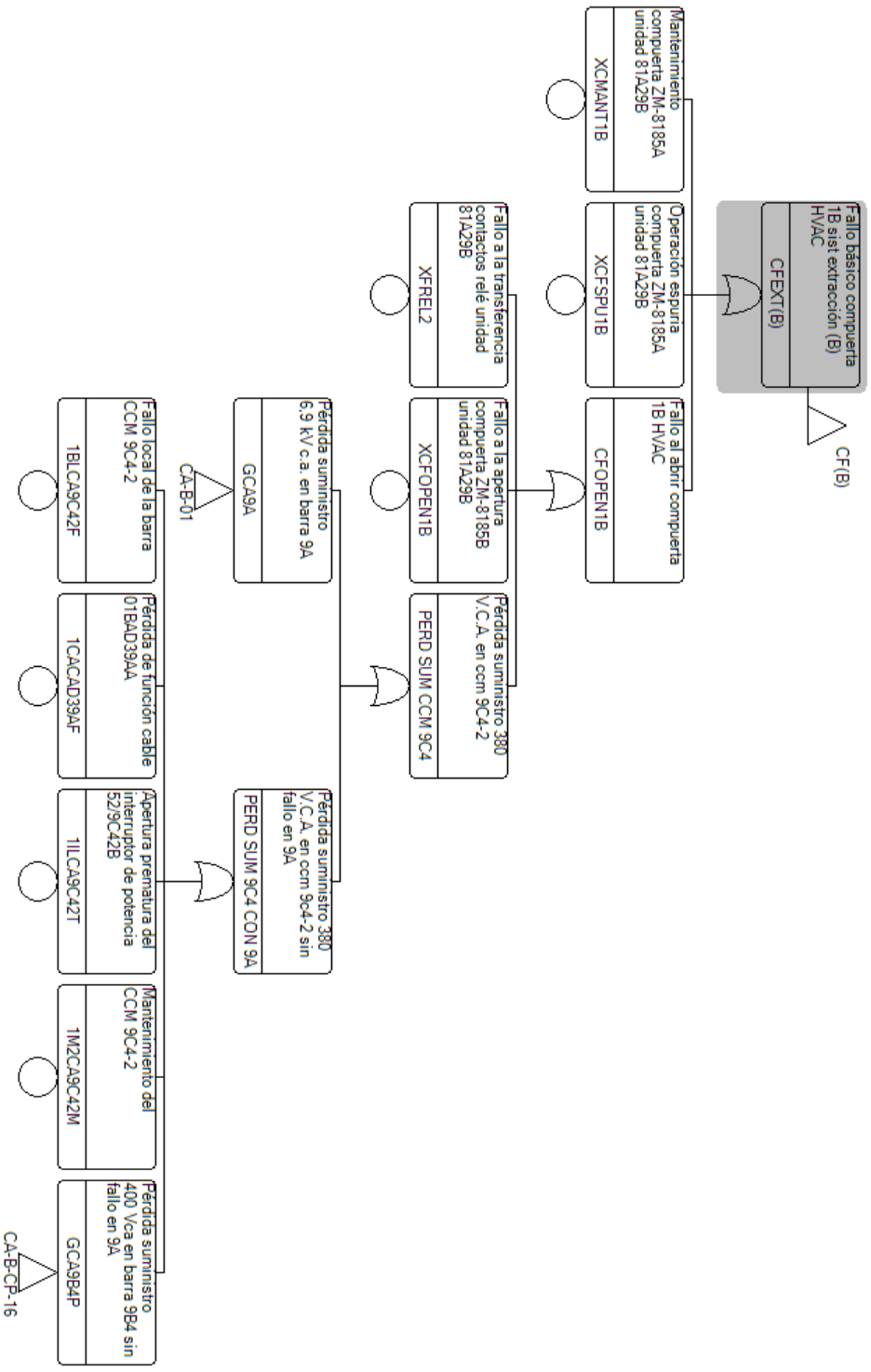


Figura C.12: Módulo CFEXT(B) que representa el fallo de la compuerta A de la unidad de extracción B

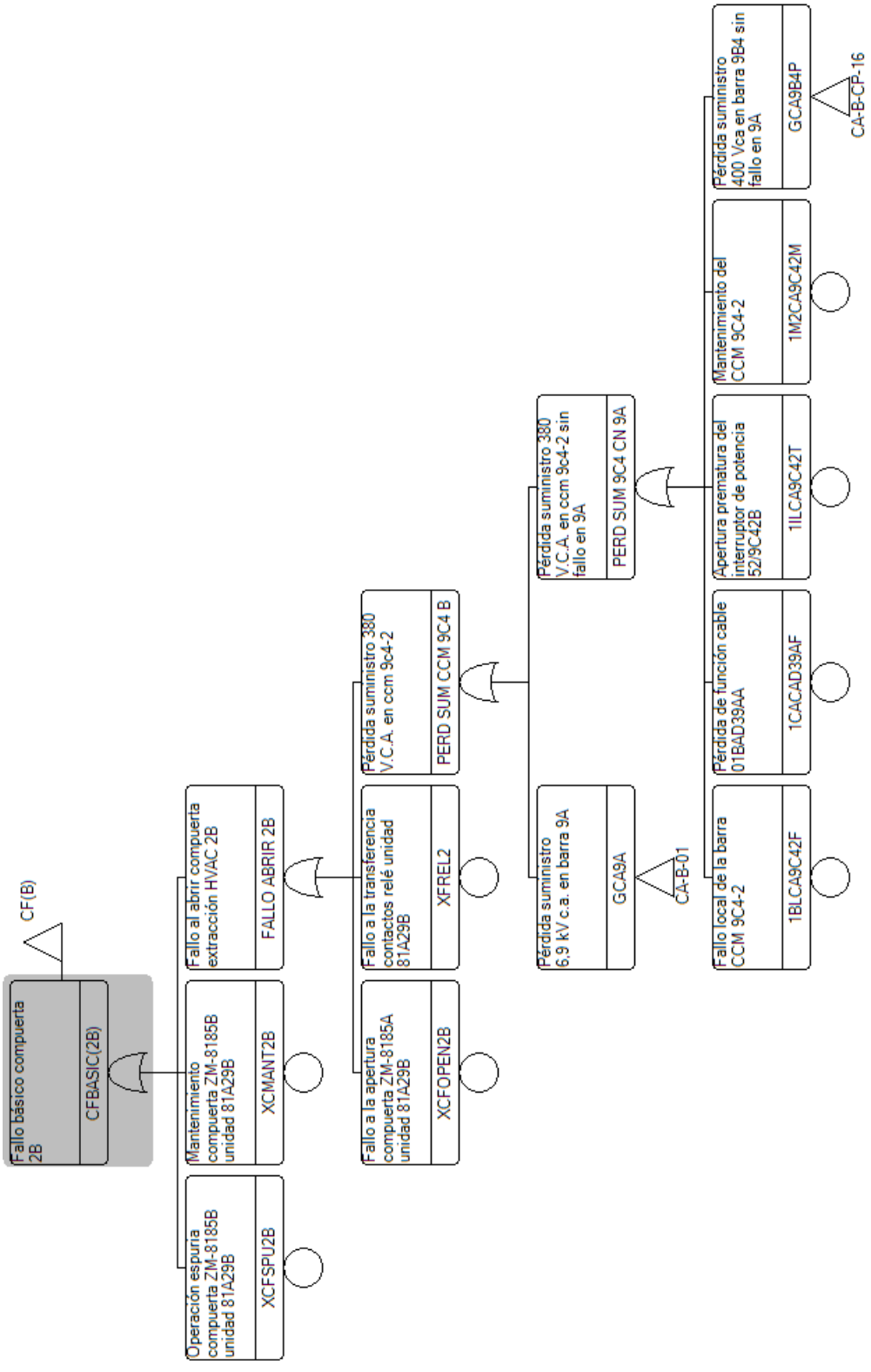


Figura C.13: Módulo CFBASIC(2B) que representa el fallo de la compuerta B de la unidad de extracción B

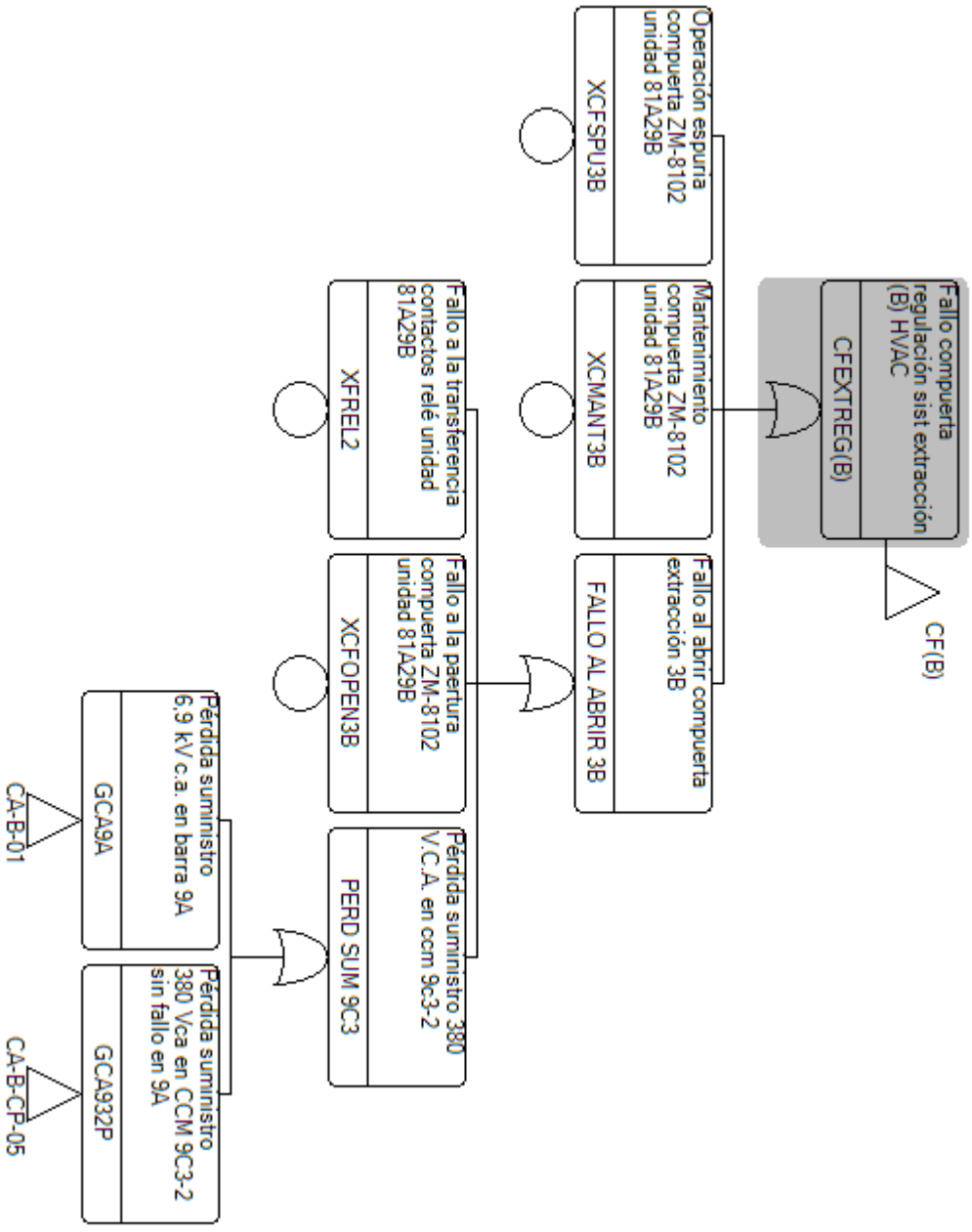


Figura C.14: Módulo CFEXTREG(B) que representa el fallo de la compuerta común de la unidad de extracción B

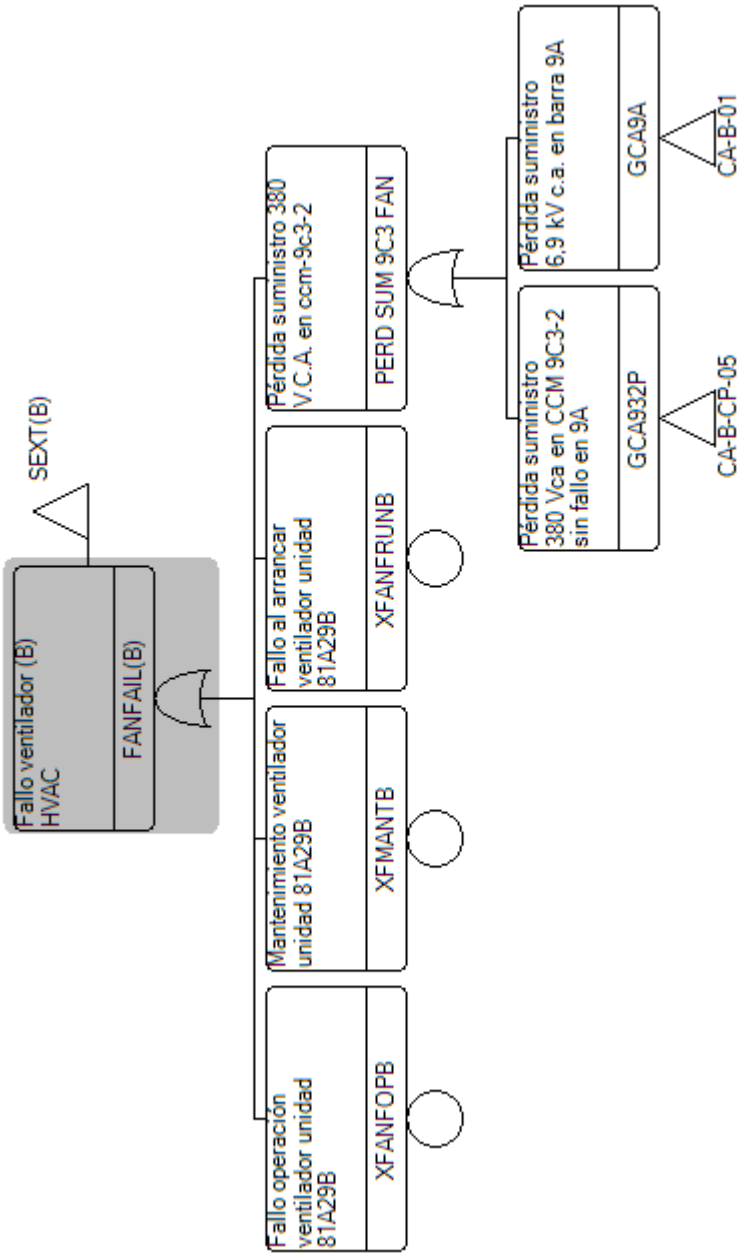


Figura C.15: Módulo FANFAIL(B) que representa el fallo del ventilador de la unidad de extracción B

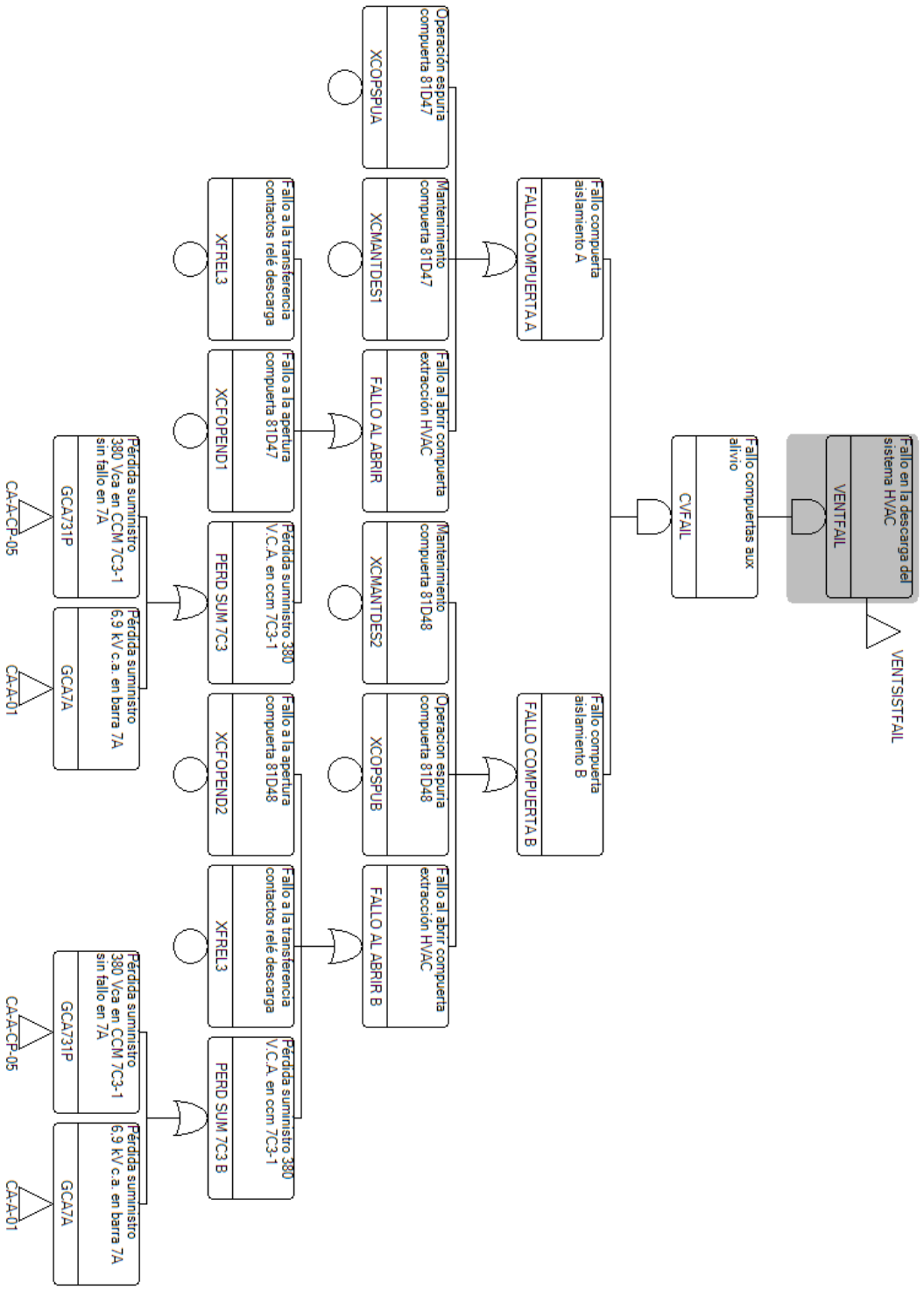


Figura C.16: Módulo VENTFAIL que representa el fallo en la descarga del Sistema de Ventilación

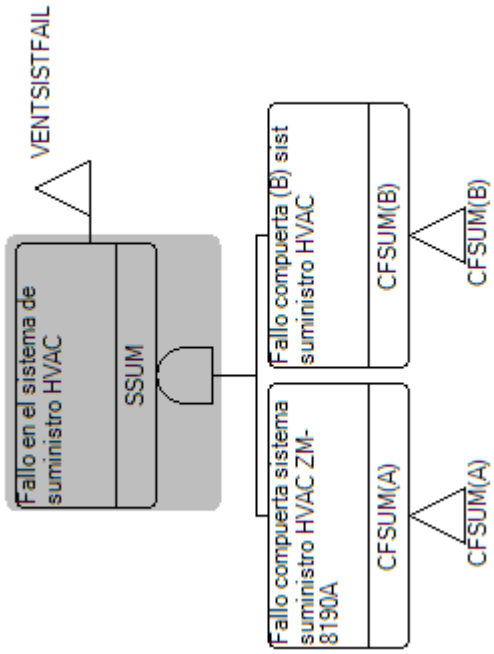


Figura C.17: Módulo SSUM que representa el fallo de la unidad de suministro

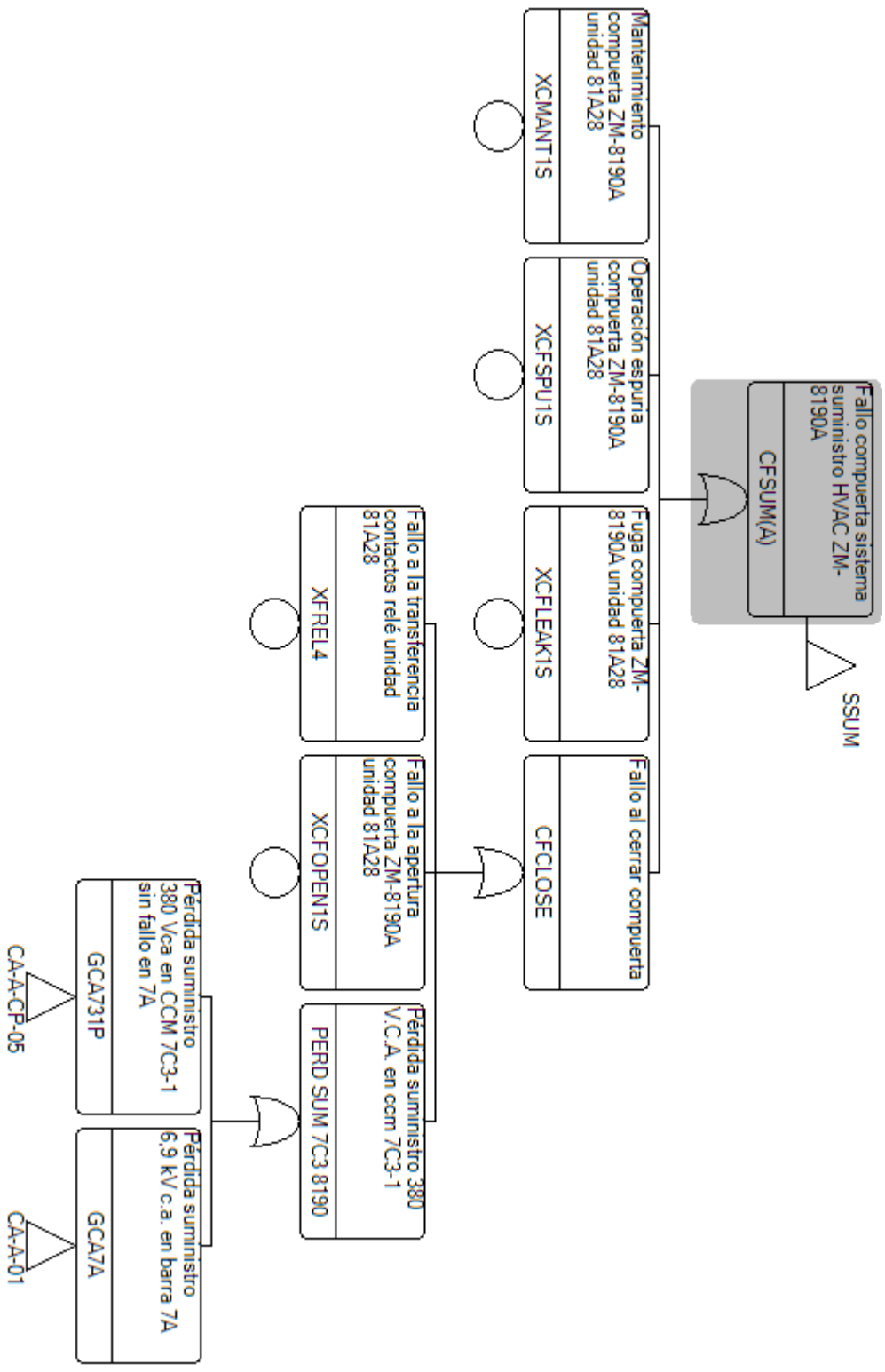


Figura C.18: Módulo CFSUM(A) que representa el fallo de la compuerta de suministro A

Apéndice D

Frecuencia de sucesos iniciadores

Este anexo contiene información adicional que amplia el detalle de las explicaciones al respecto de la frecuencia de sucesos iniciadores incluidas en la memoria de tesis. En aquellos casos en los que es conveniente se adjuntan también los cálculos realizados.

D.1. Frecuencia de caída del contenedor

La figura D.1, extraída del NUREG-1864, muestra las nueve plantas estudiadas en el NUREG-1774 [76]. Cada una de las plantas representa un tipo de NSSS. El tipo de NSSS refleja el tipo de cargas que se alzan en cada caso. Por lo tanto, los datos presentes en el NUREG-1774 son transversales y son representativos de la industria nuclear americana. Las 9 plantas seleccionadas tienen, en total, 19 reactores. La cantidad de levantamientos de cargas muy pesadas realizados en cada reactor se obtiene de los registros de mantenimiento.

Group	Type of Plant	Representative Site and Units	Number of Very Heavy Load Lifts
1	BWR, Mark I, G4	Browns Ferry 1, 2, 3	980
2	PWR, Westinghouse, 4-loop	Comanche Peak 1, 2	230
3	PWR, Westinghouse, 4-loop	Diablo Canyon 1, 2	344
4	BWR, Mark-I, G3	Dresden 2, 3	554
5	BWR, Mark-III, G6	Grand Gulf	118
6	BWR, Mark-II, G4	Limerick 1, 2	950
7	PWR, B&W	Oconee 1, 2, 3	1656
8	BWR, Mark-I, G2	Oyster Creek	504
9	PWR, CE80	Palo Verde 1, 2, 3	2277

Figura D.1: Datos recopilados en el NUREG-1774 al respecto del levantamiento de cargas pesadas. Fuente: [5]

La mayoría de los levantamientos recopilados en el NUREG-1774 se realizaron durante paradas de recarga. En consecuencia, el numero total de paradas de recarga realizadas en las centrales estadounidenses durante el periodo de tiempo 1968 a 2002 se utiliza para extrapolar los datos y obtener una aproximación del número total de levantamientos llevados a cabo en el periodo de tiempo analizado. Se obtiene que el

número total de levantamientos de cargas muy pesadas realizados en el periodo de 1968 a 2002 es de aproximadamente 54000.

El número de caídas de cargas muy pesadas en el periodo de tiempo que va de 1968 a 2002 se ha obtenido, en el NUREG-1864, de registros y de *Licensee Event Reports* (LER) de todas las plantas estadounidenses. El número de caídas ocurridas durante el periodo de tiempo de 1968 a 2002 es de tres (3).

D.2. Frecuencia de explosión cercana

El análisis de explosiones se basa en 4 casos: plantas industriales en un radio de 8 km, sustancias explosivas transportadas por carretera, sustancias explosivas transportadas por ferrocarril y sustancias explosivas almacenadas en el propio emplazamiento de la central.

D.2.1. Plantas industriales cercanas

En un radio de 8 km solo se ha encontrado una planta industrial, concretamente química, a una distancia de 3,8 km. Del análisis de las sustancias explosivas con las que se trabaja en esta planta se obtiene que la máxima distancia de seguridad de todas ellas es 1,822 km, inferior a los 3,8 km de distancia entre la planta y la central. En consecuencia, la contribución de este caso al suceso iniciador ha sido cribada.

D.2.2. Sustancias explosivas transportadas por carretera

En este caso, la distancia de seguridad de todas las sustancias explosivas transportadas por carretera, de todas se transporta la misma cantidad, es de 705 m. Para evaluar si una explosión de estas sustancias puede afectar al ATI se ha de conocer la distancia entre éste y la carretera. Para ello se utiliza un mapa cartográfico mediante el cual se determina que la distancia mínima entre la carretera y la instalación ATI es de 630 m. Al ser esta distancia menor que la distancia de seguridad es necesario evaluar la sobrepresión generada en el ATI mediante el procedimiento explicitado en la *Regulatory Guide* 1.91 de la NRC [81]. El procedimiento consiste en obtener la presión *Ps* externa generada en la distancia D utilizando un gráfico[1] en el cual el input es Z. La ecuación I.1 es la propuesta por la RG 1.91 para calcular el input Z. D es la distancia respecto al punto de la explosión en la cual se quiere calcular la sobrepresión, y W es la masa equivalente de TNT de la sustancia estudiada[2].

$$Z = \frac{D}{W^{1/3}} \tag{D.1}$$

La sobrepresión obtenida para la distancia mínima, 630 m, es de 4 psi, que es inferior a los 10 psi de diseño que soporta el contenedor. En consecuencia, la contribución de este caso al suceso iniciador ha sido cribada.

D.2.3. Sustancias explosivas transportadas por ferrocarril

La distancia máxima de seguridad para el caso del transporte por ferrocarril es de 1224 m. Mediante un mapa cartográfico se mide la mínima distancia entre la instalación ATI y la vía de ferrocarril, resultando de 491 m, inferior a todas las distancias de seguridad de las sustancias transportadas por ferrocarril. Así

[1] El gráfico no se presenta en el análisis de externos. Se puede encontrar el gráfico en la referencia [99].

[2] La RG 1.91 estipula que la masa equivalente de TNT es igual a 2,4 veces la masa de la sustancia explosiva considerada en el caso de las sustancias gaseosas y líquidas, e igual a la masa de sustancia explosiva considerada en el caso de sólidos.

Substancia	Frecuencia de explosión
Cloruro de vinilo estabilizado	6,19E-07
Acrilonitrilo estabilizado	2,49E-07
Hidrocarburos gaseosos licuados en mezcla	4,15E-07
Estireno estabilizado	3,77E-07

Tabla D.2: Frecuencia de explosión de las sustancias cuya explosión puede dañar el contenedor.

pues, de la misma manera que en el apartado anterior, se ha de calcular, para cada sustancia, el valor de la sobrepresión generada sobre el ATI. En este caso se transportan cantidades diferentes. La tabla D.1 contiene el input Z y la sobrepresión a la distancia de 491 m para todas las substancias estudiadas.

Nombre de la sustancia	Z	Ps [psi]
Butadienos estabilizados	10,92	9
Cloruro de vinilo estabilizado	7,35	19
Acrilonitrilo estabilizado	7,44	19
Disulfuro de carbono	12,36	6,5
Metacrilato de metilo inhibido	11,77	6,5
Hidrocarburos gaseosos licuados en mezcla	7,75	19
Estireno estabilizado	7,22	21
Naftaleno fundido	12,04	6,5
Bebidas alcohólicas	11,77	6,5

Tabla D.1: Sobrepresión de las substancias transportadas en ferrocarril a la distancia de 491 m. Datos de 2010.

Cuatro de las sustancias transportadas por ferrocarril generarían una presión externa mayor que la de diseño en el contenedor. Por lo tanto, existe la posibilidad de que se genere daño al contenedor. Para estos cuatro casos hay que completar el análisis calculando la frecuencia de explosión mediante la ecuación L.2. En la ecuación L.2, F es la frecuencia de explosión (explosiones/año), f es la frecuencia de accidente (accidentes/año), n es el ratio de explosión para cada substancia y cada modo de transporte (explosiones/milla), y s es la distancia de exposición, es decir, la porción de vía ferroviaria que está a menos espacio del ATI que la distancia de seguridad.

$$F = f * n * s \tag{D.2}$$

Los parámetros f y n se obtienen del análisis de sucesos externos de la central, que a su vez los obtiene de datos de experiencia operativa. El parámetro s se calcula mediante un mapa cartográfico. Como las distancias de seguridad de las cuatro sustancias son similares, se ha decido establecer como distancia de seguridad para el cálculo de s un valor de 1220 m, que es la máxima distancia de seguridad de las cuatro. Teniendo en cuenta este valor, s es 2946,15 m. Las frecuencias de explosión obtenidas se presentan en la tabla D.2.

La suma de las cuatro frecuencias, cuyo valor es 1,66E-06 (año·contenedor)$^{-1}$, es la frecuencia total de explosión externa.

D.2.4. Frecuencia de accidente de avión

La metodología propuesta en el *Standard Review Plan* para la estimación de la frecuencia de accidente de avión divide el tránsito aéreo cercano a la central en aerovías y en rutas de llegada o salida a aeropuertos

cercanos [100]. La ecuación L.3 es la formulación propuesta en el *Standard Review Plan* para estimar la frecuencia anual de accidente de avión.

$$P_{fa} = \frac{C * N * A_{eff}}{W} \tag{D.3}$$

Donde:

- P_{fa} es la probabilidad anual de impacto, es decir, la frecuencia de impacto de avión.
- C es la tasa de accidentes aéreos. Se utiliza el valor de 4E-10 accidentes por milla y por avión propuesto en el propio *Standard Review Plan* para aviones comerciales.
- N es el número de vuelos por año. Este dato se obtiene del análisis de sucesos externos de la central.
- A_{eff} es el área efectiva de la instalación a tener en cuenta. Se introduce en millas al cuadrado.
- W es la anchura de la aerovía más dos veces la distancia desde el límite de la aerovía al emplazamiento en millas. La anchura de la aerovía se toma igual a ocho millas náuticas siguiendo el ejemplo del análisis de sucesos externos de la central.

El valor de los parámetros C, N, y W es el mismo tanto para el APS de ATI como para el análisis de sucesos externos de la central. Por lo tanto, la única diferencia entre la estimación de la frecuencia de accidente de avión para la central y para el ATI es el valor del área efectiva de la instalación.

D.2.5. Frecuencia de accidente por vientos fuertes

La velocidad de viento con periodo de retorno de 1,0E+6 en la cota del emplazamiento del ATI se estima asumiendo que el perfil de velocidades del viento en recinto de la central es logarítmico. Concretamente, se utiliza la ecuación L.4 para estimar la velocidad de viento en la cota del ATI:

$$\frac{v_{h_2}}{v_{h_1}} = \frac{ln\left(\frac{h_2}{z_0}\right)}{ln\left(\frac{h_1}{z_0}\right)} \tag{D.4}$$

Donde:

- v_{h_2}. es la velocidad a la altura h_2. En este caso la altura h_2 es la cota del ATI, es decir, 57 metros.
- v_{h_1} es la velocidad del viento a la altura h_1. En este caso, v_{h_1} es la velocidad del viento con periodo de retorno de 1,0E+06 correspondiente a la cota 30 metros.
- z_0 es la rugosidad del terreno. Este valor, que se extrae del análisis de sucesos externos, es de 0,042.
- h_{x} es la propia altura de la cota x.

A partir de esta fórmula se obtiene la velocidad con período de retorno 1,0E+06 a la altura de 57 metros, que es de 114,16 m/s. En los resultados del análisis estructural se explicita que es necesaria una velocidad de 179 m/s y otra de 268,3 m/s para deslizar o volcar el contenedor, respectivamente. Por lo tanto, la frecuencia de ocurrencia de estas velocidades sería sustancialmente inferior a 1,0E-06 por año. Además, para calcular la frecuencia de liberación de radionúclidos se debería aplicar la probabilidad de rotura de las barreras de confinamiento, que, en el caso volcado, es de 1,0E-06. En consecuencia, este suceso iniciador es cribado porque su FLR sería despreciable.

D.2.6. Frecuencia de impacto de meteorito

La frecuencia de ocurrencia de la caída de un meteorito en un contenedor se obtiene siguiendo la metodología detallada en el documento NUREG-1864. El NUREG-1864 presenta los resultados de un estudio que determina qué tipo de meteorito podría provocar la ruptura del contenedor. El contenedor ha de ser golpeado por un meteorito rocoso de al menos 1542 kg de peso para que el primero sufra un fallo estructural. De manera similar, el contenedor ha de ser golpeado por un meteorito ferroso de al menos 1088,6 kg para que el contenedor sufra daño estructural. Teniendo en cuenta que existe una relación entre el peso y el diámetro de los meteoritos, el NUREG-1864 estima la frecuencia de que un meteorito de estas características atraviese la atmósfera terrestre. La frecuencia de que un meteorito rocoso como el que haría fallar el contenedor golpee la Tierra es de uno por año. A su vez, la frecuencia de que un meteorito ferroso como el que dañaría el contenedor golpee la tierra es de uno cada año y medio. El NUREG-1864 considera, conservadoramente, que la frecuencia de que un meteorito que pueda dañar el contenedor atraviese la atmósfera terrestres es de dos por año.

Teniendo en cuenta que la superficie de la Tierra es de 5,08E+08 km^2, la frecuencia por unidad de superficie con la que un meteorito de las características necesarias golpea la Tierra es de 4,0E-09 por año y por km^2. Multiplicando este valor por la superficie de un contenedor que puede ser golpeada por un meteorito[3], se estima la frecuencia de impacto de un meteorito en un contenedor.

[3] En este caso, se considera que es la superficie del extremo superior y el área cilíndrica.

Apéndice E

Extensión del análisis estructural y termohdráulico

El presente anexo extiende la explicación del análisis estructural y el análisis termohidráulico proporcionada en la memoria de tesis. El anexo se divide en los diferentes sucesos iniciadores estudiados en el análisis probabilista de seguridad.

E.1. Caída del contenedor en el interior del edificio de combustible

E.1.1. Respuesta del contenedor

La figura E.1 muestra el modelo de elementos finitos utilizado para calcular la *Effective Plastic Strain* máxima del MPC en eventos de caída. El modelo de elementos finitos se crea mediante el código LS-DYNA. LS-DYNA es un código de elementos finitos de propósito general que se utiliza para analizar la respuesta dinámica de estructuras ante grandes deformaciones.

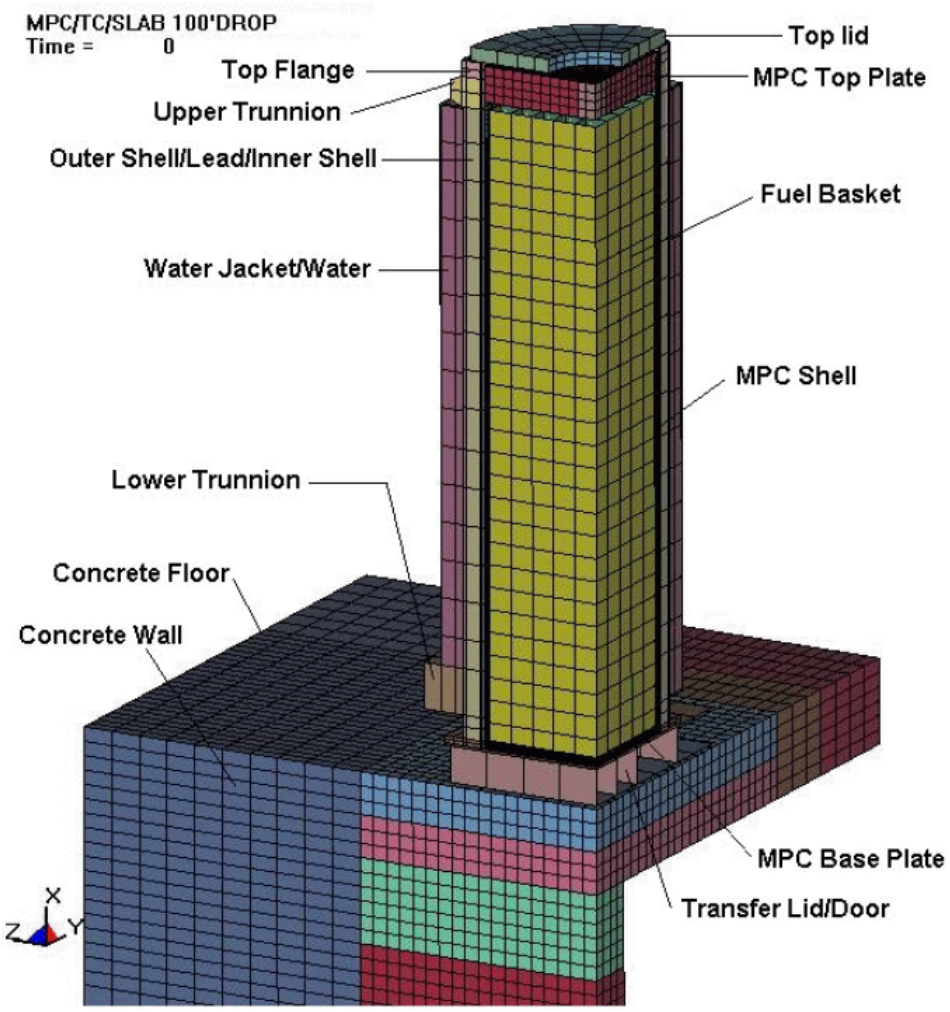


Figura E.1: Modelo de elementos finitos utilizado para calcular la deformación plástica del contenedor en sucesos de caída. Fuente: [5]

El contenedor descansa sobre la superficie de impacto en el inicio de la simulación. La altura de caída se simula introduciendo una velocidad inicial al conjunto del contenedor. La velocidad inicial del contenedor se calcula mediante la ecuación E.1.

$$Velocidad = \sqrt{2gh} \tag{E.1}$$

El modelo de elementos finitos sobrestima la deformación plástica dado que las curvas tensión-deformación de los materiales introducidas en el modelo son ingenieriles en lugar de reales. Las EPS obtenidas para los casos de caída del contenedor de transferencia sobre una superficie de hormigón como la del edificio de combustible se plasman en la tabla E.1.

Altura de caída [m]	EPS máxima [cm/cm]	Elemento de máxima EPS	Mínima deformación verdadera al fallo [cm/cm]
1,52	0,024	16539	0,92
12,2	0,195	15973	0,92
21,3	0,24	15997	0,92
30,5	0,256	15997	0,92

Tabla E.1: EPS máxima en el MPC de los casos de caída del NUREG-1864.

Los elementos de máxima deformación se encuentran en la parte inferior del casco del MPC, entre los soportes de los elementos de combustible y la superficie base del contenedor, en la soldadura que une el casco con su base. La figura E.2 muestra la máxima deformación del casco del MPC y de los soportes de los elementos de combustible para la caída de 30,5 metros.

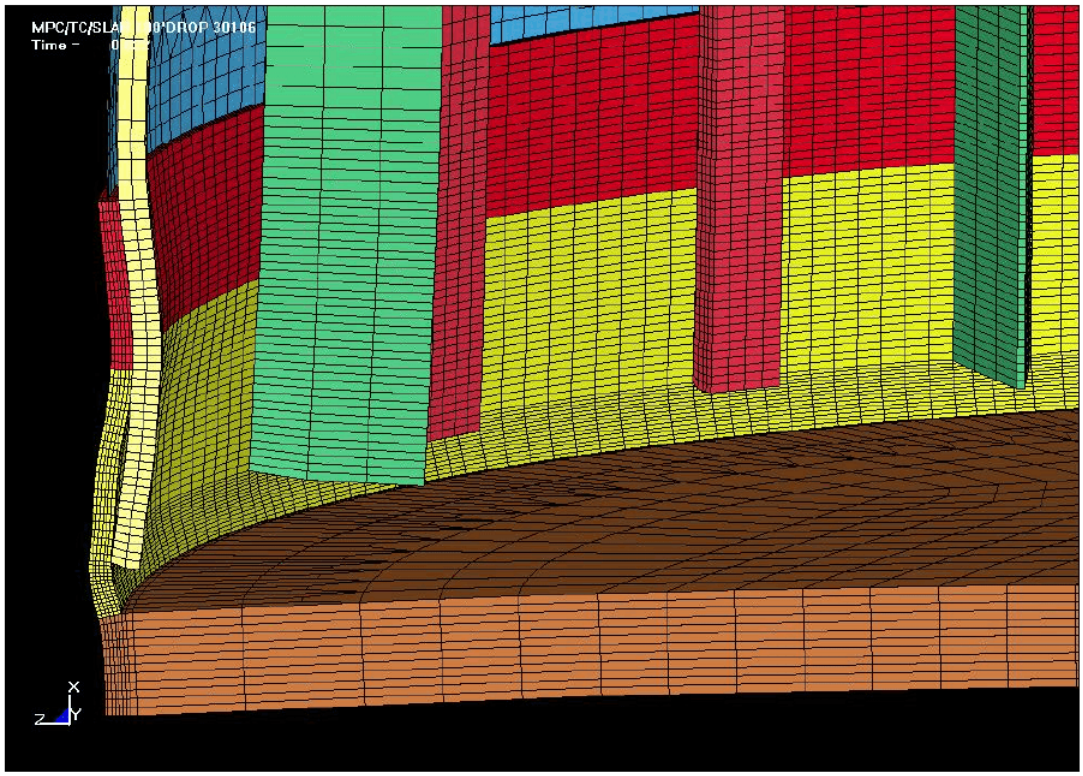


Figura E.2: Máxima deformación en el casco del MPC para la caída de 30,5 metros. Fuente: [5]

En el caso del suceso de volcado, la máxima tensión a la que se somete el contenedor, que es de aproximadamente 406,8 MPa, se obtiene del estudio final de seguridad del HI-STORM 100. Dicha tensión se obtiene mediante un análisis elástico lineal. NUREG obtiene la EPS máxima del caso de volcado mediante LS-DYNA, aplicando un balance de energías. Se impone, en el modelo de elementos infinitos, que la energía de deformación absorbida por unidad de volumen debida a la deformación elástica y plástica en el elemento de máxima tensión es igual a la energía de deformación absorbida por unidad de volumen calculada en el punto de máxima tensión mediante el modelo lineal elástico. Es decir, se introduce la energía calculada en el estudio final de seguridad en el modelo LS-DYNA como input para la calcular la EPS. La máxima EPS calcualda en el caso de volcado es de 0,0031 cm/cm.

La máxima EPS del MPC se ha de comparar con un criterio apropiado de fallo por deformación para determinar si la integridad de la propia barrera de confinamiento se ve comprometida por la caída. Las condiciones postuladas para el cálculo de la EPS y las condiciones en las que se mide o se calcula el límite de fallo por deformación han de ser consecuentes para que la comparación sea valida. Por lo tanto, se han detener en cuenta factores como el efecto de la tasa de deformación, la temperatura, y el estado de tensión a la hora de comparar ambos valores.

E.1.1.1. Deformación al fallo

El código LS-DYNA considera la reducción de la sección transversal de los elementos finitos en el cálculo de la tensión y la deformación del elemento. Por lo tanto, el programa espera que el usuario introduzca curvas de tensión-deformación verdaderas[1]. Como el cálculo de la EPS está basado en deformación verdadera, el criterio de fallo también ha de estar basado en una medida de la deformación verdadera [5]. La deformación verdadera al fallo se calcula mediante la ecuación L.2 en el NUREG-1864. RA hace referencia al porcentaje de reducción de la sección en el momento del fallo.

$$\varepsilon_t = ln\left(\frac{1}{1-RA}\right) \tag{E.2}$$

La RA utilizada para el material de la soldadura, acero inoxidable 308, en el NUREG es de media igual a 59,0 % con desviación estándar de 9,7 % (Distribución normal). Esta RA proviene de la combinación de los resultados de diferentes tests realizados con probetas de acero 308, algunas provenientes de soldaduras y otras no, a temperatura ambiente y con cargas estáticas. La RA se multiplica por 0,88 para tener en cuenta que la temperatura del MPC es mayor que la temperatura ambiente y que la deformación no es constante, es decir, existe una tasa de deformación. 0,88 es el resultado de multiplicar 0,90, el ratio de reducción de la RA a la temperatura del MPC respecto a la temperatura ambiente, por 0,98, que es un ajuste conservador utilizado en el NUREG para tener en cuenta el efecto de la tasa de deformación. Finalmente, la RA utilizada tiene una media de 52 % y una desviación estándar de 5,7 %.

Al disponer de una distribución de probabilidad para la RA, se dispone también de la distribución de probabilidad de la deformación al fallo. En consecuencia, al comparar la máxima EPS con la distribución acumulada de probabilidad de la deformación al fallo se obtiene la probabilidad de que la soldadura del elemento finito estudiado falle. La tabla E.2 presenta alguno de los valores de la distribución de probabilidad de la deformación verdadera al fallo.

Desviación estándar	Deformación verdadera al fallo [cm/cm]	Probabilidad de que la deformación verdadera al fallo sea menor que el valor tabulado
0,0 (media)	0,73	0,5
0,5	0,64	0,3085
1	0,55	0,1587
1,5	0,47	0,0668
2	0,44	0,0228

Tabla E.2: Distribución de probabilidad de la deformación verdadera al fallo [5].

E.1.1.2. Ajuste de la EPS

Incluso después de aplicar los factores de ajuste de la temperatura y la tasa de deformación, la máxima EPS y la deformación verdadera al fallo aún no se pueden comparar. La razón es que la máxima EPS

[1] Como ya se ha comentado, en el caso del análisis realizado en el marco del NUREG-1864 esto no es así. Se introducen curvas ingenieriles para que así los resultados sean conservadores.

se ha obtiene de estado de tensión tridimensional complejo, mientras que la deformación verdadera al fallo proviene de pruebas de probetas en las que la tensión era unidimensional. Un estado tridimensional de tensión puede contener la deformación plástica de material y reducir la EPS a la cual se produce el fallo del material [5]. La pérdida de ductilidad producto de un estado tridimensional de tensión se puede representar mediante el llamado *Triaxility factor* (TF)[2]. El TF permite calcular el ratio de ductilidad, llamado DR, véase la ecuación L.3, que es el cociente entre la EPS al fallo y la deformación verdadera al fallo en un estado uniaxial de tensión.

$$DR = 2^{(1-TF)} \tag{E.3}$$

Por lo tanto, la EPS calculada mediante el modelo de LS-DYNA se divide por el DR para poder compararla con la deformación verdadera al fallo. Al dividir por el DR, se calcula la deformación equivalente de un estado de tensión uniaxial, que sí que se puede comparar con la deformación verdadera al fallo. El cálculo de la EPS ajustada se lleva a cabo para todo elemento finito puesto que, al depender del estado de tensión, es posible que el elemento con la máxima EPS ajustada no sea el mismo que el de la máxima EPS. La tabla E.3 presenta los valores ajustados de EPS para los casos de caída del NUREG-1864 y la probabilidad de fallo de cada caso, que se obtiene al comparar las EPS ajustadas con la distribución de probabilidad de la tabla E.2.

Altura de caída [m]	EPS máxima [cm/cm]	Máxima EPS ajustada [cm/cm]	Probabilidad de grieta en soldadura
1,52	0,024	0,048	<1,0E-06
12,2	0,195	0,213	3,6E-04
21,3	0,24	0,285	2,6E-03
30,5	0,256	0,385	1,96E-02

Tabla E.3: EPS ajustada y probabilidad de fallo de los casos de caída analizados en el NUREG-1864.

E.1.2. Respuesta de las vainas de combustible

NUREG-1864 estudia el posible fallo debido a pandeo de las vainas de combustible en los casos de caída analizados anteriormente. Cabe destacar que para eventos dinámicos de impacto, como es el caso de las caídas, donde la carga dura del orden de milisegundos, pasar el límite crítico de pandeo no causa, por si mismo, fallo de la vaina. Es la combinación de tiempo y carga la que determina si la vaina llega al fallo por deformación.

Para analizar el pandeo se ha planteado un modelo en el cual se ha simulado una vaina PWR. El acercamiento utilizado consiste en analizar la vaina como una columna-haz elástica y plástica con una curvatura inicial y bajo un impacto dinámico. Las rejillas espaciadoras de los elementos de combustible están simuladas con muelles, al igual que la interacción entre las vainas, el contenedor y el suelo. Las vainas están simuladas mediante un único elemento al igual que el contenedor, que es un punto con la masa equivalente de todo el contenedor. La posible interacción de las vainas, con las paredes del contenedor, o con otras vainas, está simulada mediante una pared a la distancia correcta. La figura E.3 muestra el modelo utilizado para estimar el pandeo de la vaina de combustible.

[2]Si el TF es igual a la unidad el estado de tensión es uniaxial, si es mayor que la unidad el estado de tensión contiene la deformación plástica, y si es menor que la unidad el estado de tensión facilita la deformación, con lo que se incrementa la ductilidad.

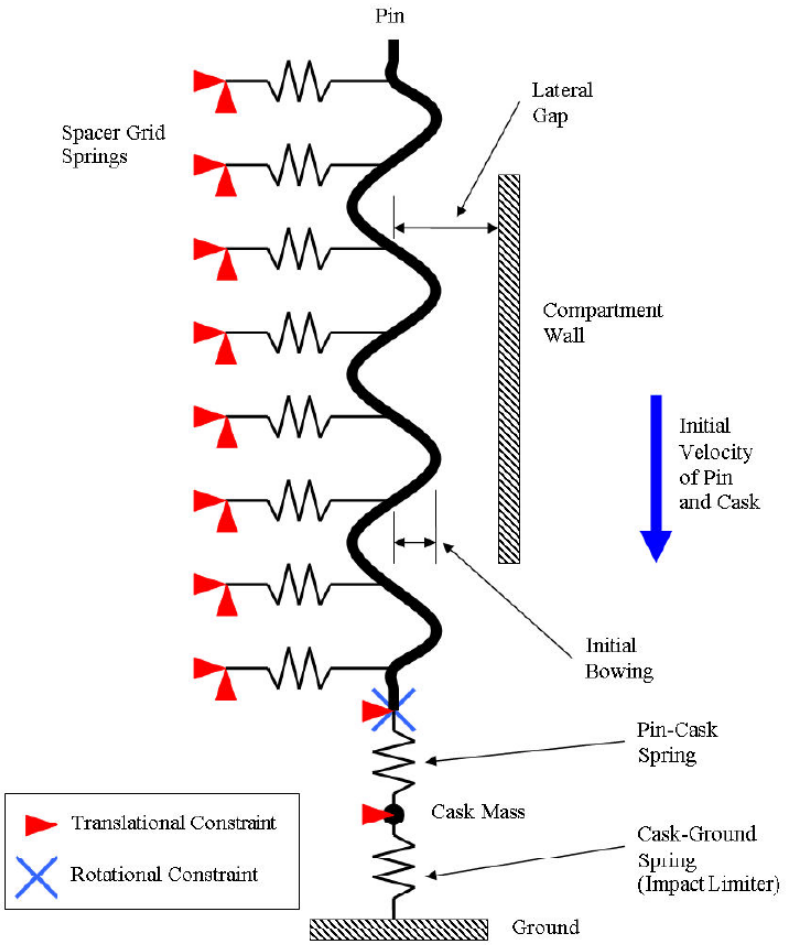


Figura E.3: Modelo de estimación del pandeo de una vaina de combustible en un suceso de caída. Fuente: [5]

El fallo de las vainas se determina comparando la máxima deformación en la vaina con el límite de deformación basado en datos experimentales. La tabla E.4 presenta los resultados obtenidos en el NUREG-1864. Si la máxima deformación de la vaina es mayor que la deformación al fallo se considera que la vaina modelo falla y, por extensión, todas las vainas en el interior del MPC.

Suceso	Altura de caída [m]	Máxima deformación en la vaina	Deformación al fallo	Rotura
Caída vertical del contenedor de transferencia	0,305	0,0043	0,01	No
	1,524	0,0062	0,01	No
	6,096	0,0072	0,01	No
	12,19	0,011	0,01	Sí
	16,76	0,025	0,01	Sí
	21,34	0,037	0,01	Sí
	30,48	0,052	0,01	Sí
Caída del MPC en el interior del HI-STORM	5,79	0,09	0,01	Sí

Tabla E.4: Análisis del fallo de las vainas de combustible del NUREG-1864.

Para el caso de volcado, el NUREG utiliza un resultado externo en el que se detalla que, para un caso de carga lateral de 63 g, la deformación plástica máxima de las vainas es 0,0077 cm/cm. Debido a que el análisis realizado para obtener este valor es lineal, la deformación para 45 g sería de 0,0055 cm/cm, muy por debajo del límite de 0,01 cm/cm. En consecuencia, en los casos de volcado se desestima la rotura de vainas.

Se ha de destacar que el fallo de las vainas al que se hace referencia en el NUREG se trata de poros o agujeros en vaina o de pequeñas grietas. En ningún caso se relaciona el fallo con brechas o rotura de la vaina en múltiples trozos.

E.2. Caída del contenedor durante la transferencia

En el NUREG-1864 se estudia la caída del contenedor HI-STORM 100 cargado con el MPC sobre tres posibles superficies: asfalto, gravilla, y la losa de hormigón de la zona de almacenamiento. La caída simulada es de 30,5 cm, que es la altura a la que se transporta el contenedor. El análisis de estos casos de impacto no lineal se realiza otra vez mediante el código LS-DYNA, aunque, para este caso, se utilizan modelos ya existentes del contenedor de almacenamiento proporcionados por HOLTEC International®. Como estos modelos no incluyen el casco del contenedor MPC, se calcula mediante el código LS-DYNA la mayor aceleración a la que se somete el centro del extremo inferior del contenedor de almacenamiento. Posteriormente, se estima la tensión sufrida por el casco del MPC mediante una tabla que relaciona valores de aceleración con la tensión sufrida por las diferentes partes del MPC. Dicha tabla proviene del documento *Dynamic Impact Effects on Spent Fuel Assemblies*, escrito por Ramsey Chun et al, del Lawrence Livermore National Laboratory, en octubre del 1987. La tabla E.5 resume los resultados obtenidos en el NUREG-1864.

Superficie de impacto	Espesor [cm]	Módulo elástico [MPa]	Aceleración máxima [g]	Tensión máxima [MPa]
Hormigón	61	641	41,2	53,3
Asfalto	30,5	4482	23,2	45,6
Gravilla	30,5	345	15,8	28,6

Tabla E.5: Resultados del análisis de caída del contenedor sobre las superficies de transferencia. Fuente: [5]

Los valores de máxima tensión presentados en la tabla E.5 están muy por debajo de la tensión elástica de

pandeo y del límite elástico. En consecuencia, la ocurrencia de este tipo de sucesos no tiene consecuencias negativas sobre el contenedor.

Apéndice F

Elemento de combustible utilizado en el cálculo del inventario

El presente anexo contiene las características principales del modelo de elemento de combustible utilizado en el cálculo del inventario del contenedor mediante simulación de irradiación y post-irradiación con el código ORIGEN-S. El anexo también presenta los principales inputs de la simulación.

F.1. Características principales del modelo de elemento de combustible

El modelo de elemento de combustible utilizado en la obtención del inventario del contenedor es un elemento PWR 17x17 formado por Zircaloy-4, Inconel 690, acero inoxidable 304L, y el propio combustible en forma de UO_2. La tabla F.1 presenta las principales características estructurales del modelo de elemento de combustible.

Característica	Valor
Longitud total [m]	4,059
Sección transversal [cm^2]	21,4 x 21,4
Longitud de la vaina [m]	3,851
Altura activa de combustible [m]	3,658
Diámetro exterior de la vaina [cm]	0,950
Vainas de combustible por elemento	264
Peso total [kg]	657,9
Peso de uranio [kg]	461,4
Peso de UO_2 [kg]	523,4
Peso de Zircaloy [kg]	108,4
Peso de elementos estructurales [kg]	26,1
Peso total de metal [kg]	134,5
Volumen nominal [m^3]	0,186

Tabla F.1: Características principales del elemento de combustible.

Se considera que el porcentaje en peso del Inconel y del acero inoxidable es equivalente. Por lo tanto, el elemento de combustible simulado contiene 108,4 kg de Zircaloy-4, 13,05 kg de Inconel, y 13,05 kg de acero

inoxidable. El resto del peso del elemento de combustible corresponde al combustible UO_2, lo que implica la existencia de 461,4 kg de uranio y 62 kg de oxigeno por elemento de combustible. La tabla F.2 muestra la composición del Zircaloy-4, el Inconel, y el acero inoxidable. Dichas composiciones, conjuntamente con la cantidad de oxigeno y uranio, se introducen en ORIGEN-S para definir el elemento de combustible.

Elemento	304L [% peso]	Inconel-690 [% peso]	Zircaloy-4 [% peso]
Al	0	0	0,0075
B	0	0	0,00005
C	0,33	0,04	0,027
Cd	0	0	0,0005
Co	0	0	0,002
Cr	19	29	0,09855
Cu	0	0,45	0,005
Fe	67	10,5	0,2
H	0	0	0,0025
Hf	0	0	0,01
Mg	0	0	0,002
Mn	2	0,5	0,005
Mo	0	0	0,005
N	0,1	0	0,008
Ni	11,1	59	0
P	0,04	0	0
S	0,03	0,01	0
Si	0,7	0,5	0,012
Sn	0	0	1,3
Ti	0	0	0,005
U	0	0	0,00035
W	0	0	0,01
Zr	0	0	98,3
Total	100	100	100

Tabla F.2: Composición del Zircaloy-4, Inconel, y acero inoxidable

F.2. Principales inputs de la simulación

La tabla F.3 presenta los principales inputs de la simulación con ORIGEN-S.

Input	Valor
Enriquecimiento	5 %
Grado de quemado total	55000 MWd/tU
Grado de quemado por ciclo de irradiación	18333,5 MWd/tU (quemado simétrico)
Potencia	33,95 MW
Ciclos de irradiación	3 ciclos, separados por ciclos de post-irradiación de 40 días
Duración de un ciclo de irradiación	18 meses separados en los siguientes pasos de tiempo (días): 54, 108, 162, 216, 270, 324, 378, 432, 486, 540.
Duración de la post-irradiación final	7 años
Pasos de tiempo de la post-irradiación	0,001, 0,003, 0,01, 0,03, 0,1, 0,3, 1, 3, 5, 7 años

Tabla F.3: Principales inputs de la simulación.

Apéndice G

Conjuntos mínimos de fallo de la Fase I

Las siguientes tablas contienen los conjuntos mínimos de fallo de cada suceso iniciador[1] estudiado en la etapa de carga del modelo APS en fase I.

CMF	FLR [(año·contenedor)$^{-1}$]	%	Ecuación			
1	1,37E-15	6,74	CAÍDA	CMANT1S	CMANT2S	MPC1
2	1,37E-15	6,74	CAÍDA	1M9GDA38BM	CMANT1B	MPC1
3	1,37E-15	6,74	CAÍDA	1M9GDA38BM	CMANT3B	MPC1
4	1,37E-15	6,74	CAÍDA	1M9GDA38BM	CMANT2B	MPC1
5	1,37E-15	6,74	CAÍDA	CMANT1B	CMANT3A	MPC1
6	1,37E-15	6,74	CAÍDA	CMANT	CMANT1B	MPC1
7	1,37E-15	6,74	CAÍDA	CMANT3A	CMANT3B	MPC1
8	1,37E-15	6,74	CAÍDA	CMANT	CMANT3B	MPC1
9	1,37E-15	6,74	CAÍDA	CMANT2B	CMANT3A	MPC1
10	1,37E-15	6,74	CAÍDA	CMANT	CMANT2B	MPC1
11	1,20E-15	5,91	CAÍDA	FALLORELES	MPC1	

Tabla G.1: CMFs de mayor contribución del Suceso Iniciador Caída1

[1] Entiéndase aquí que los conjuntos mínimos de fallo provienen de las secuencias de accidente que llevan a liberación de radionúclidos.

CMF	FLR [(año·contenedor)$^{-1}$]	%	Ecuación			
1	2,37E-13	6,59	CAÍDA	1M9GDA38BM	CMANT1B	MPC2
2	2,37E-13	6,59	CAÍDA	CMANT1B	CMANT3A	MPC2
3	2,37E-13	6,59	CAÍDA	1M9GDA38BM	CMANT2B	MPC2
4	2,37E-13	6,59	CAÍDA	CMANT3A	CMANT3B	MPC2
5	2,37E-13	6,59	CAÍDA	CMANT	CMANT1B	MPC2
6	2,37E-13	6,59	CAÍDA	CMANT1S	CMANT2S	MPC2
7	2,37E-13	6,59	CAÍDA	CMANT	CMANT3B	MPC2
8	2,37E-13	6,59	CAÍDA	CMANT	CMANT2B	MPC2
9	2,37E-13	6,59	CAÍDA	CMANT2B	CMANT3A	MPC2
10	2,37E-13	6,59	CAÍDA	1M9GDA38BM	CMANT3B	MPC2
11	2,07E-13	5,78	CAÍDA	FALLORELES	MPC2	

Tabla G.2: CMFs de mayor contribución del Suceso Iniciador Caída2

CMF	FLR [(año·contenedor)$^{-1}$]	%	Ecuación			
1	7,78E-14	6,61	CAÍDA	1M9GDA38BM	CMANT2B	MPC3
2	7,78E-14	6,61	CAÍDA	CMANT	CMANT1B	MPC3
3	7,78E-14	6,61	CAÍDA	CMANT	CMANT3B	MPC3
4	7,78E-14	6,61	CAÍDA	CMANT1B	CMANT3A	MPC3
5	7,78E-14	6,61	CAÍDA	1M9GDA38BM	CMANT3B	MPC3
6	7,78E-14	6,61	CAÍDA	CMANT3A	CMANT3B	MPC3
7	7,78E-14	6,61	CAÍDA	CMANT1S	CMANT2S	MPC3
8	7,78E-14	6,61	CAÍDA	1M9GDA38BM	CMANT1B	MPC3
9	7,78E-14	6,61	CAÍDA	CMANT	CMANT2B	MPC3
10	7,78E-14	6,61	CAÍDA	CMANT2B	CMANT3A	MPC3
11	6,82E-14	5,79	CAÍDA	FALLORELES	MPC3	

Tabla G.3: CMFs de mayor contribución del Suceso Iniciador Caída3

CMF	FLR [(año·contenedor)$^{-1}$]	%	Ecuación				
1	1,56E-12	6,61	CAÍDA	CMANT1S	CMANT2S	MPC4	VAINAS1
2	1,56E-12	6,61	CAÍDA	CMANT	CMANT2B	MPC4	VAINAS1
3	1,56E-12	6,61	CAÍDA	1M9GDA38BM	CMANT2B	MPC4	VAINAS1
4	1,56E-12	6,61	CAÍDA	CMANT2B	CMANT3A	MPC4	VAINAS1
5	1,56E-12	6,61	CAÍDA	CMANT	CMANT1B	MPC4	VAINAS1
6	1,56E-12	6,61	CAÍDA	CMANT	CMANT3B	MPC4	VAINAS1
7	1,56E-12	6,61	CAÍDA	CMANT1B	CMANT3A	MPC4	VAINAS1
8	1,56E-12	6,61	CAÍDA	1M9GDA38BM	CMANT1B	MPC4	VAINAS1
9	1,56E-12	6,61	CAÍDA	CMANT3A	CMANT3B	MPC4	VAINAS1
10	1,56E-12	6,61	CAÍDA	1M9GDA38BM	CMANT3B	MPC4	VAINAS1
11	1,36E-12	5,79	CAÍDA	FALLORELES	MPC4	VAINAS1	

Tabla G.4: CMFs de mayor contribución del Suceso Iniciador Caída4

CMF	FLR [(año·contenedor)$^{-1}$]	%	Ecuación				
1	9,58E-10	6,53	CAÍDA	CMANT1B	CMANT3A	MPC5	VAINAS1
2	9,58E-10	6,53	CAÍDA	1M9GDA38BM	CMANT1B	MPC5	VAINAS1
3	9,58E-10	6,53	CAÍDA	CMANT3A	CMANT3B	MPC5	VAINAS1
4	9,58E-10	6,53	CAÍDA	CMANT2B	CMANT3A	MPC5	VAINAS1
5	9,58E-10	6,53	CAÍDA	CMANT	CMANT2B	MPC5	VAINAS1
6	9,58E-10	6,53	CAÍDA	CMANT	CMANT3B	MPC5	VAINAS1
7	9,58E-10	6,53	CAÍDA	1M9GDA38BM	CMANT2B	MPC5	VAINAS1
8	9,58E-10	6,53	CAÍDA	CMANT	CMANT1B	MPC5	VAINAS1
9	9,58E-10	6,53	CAÍDA	CMANT1S	CMANT2S	MPC5	VAINAS1
10	9,58E-10	6,53	CAÍDA	1M9GDA38BM	CMANT3B	MPC5	VAINAS1
11	8,40E-10	5,73	CAÍDA	FALLORELES	MPC5	VAINAS1	

Tabla G.5: CMFs de mayor contribución del Suceso Iniciador Caída5

CMF	FLR [(año·contenedor)$^{-1}$]	%	Ecuación			
1	3,40E-15	6,74	CAÍDA	CMANT1S	CMANT2S	VOLCADO
2	3,40E-15	6,74	CAÍDA	1M9GDA38BM	CMANT1B	VOLCADO
3	3,40E-15	6,74	CAÍDA	1M9GDA38BM	CMANT3B	VOLCADO
4	3,40E-15	6,74	CAÍDA	1M9GDA38BM	CMANT2B	VOLCADO
5	3,40E-15	6,74	CAÍDA	CMANT1B	CMANT3A	VOLCADO
6	3,40E-15	6,74	CAÍDA	CMANT	CMANT1B	VOLCADO
7	3,40E-15	6,74	CAÍDA	CMANT3A	CMANT3B	VOLCADO
8	3,40E-15	6,74	CAÍDA	CMANT	CMANT3B	VOLCADO
9	3,40E-15	6,74	CAÍDA	CMANT2B	CMANT3A	VOLCADO
10	3,40E-15	6,74	CAÍDA	CMANT	CMANT2B	VOLCADO
11	2,98E-15	5,91	CAÍDA	FALLORELES	VOLCADO	

Tabla G.6: CMFs de mayor contribución del Suceso Iniciador Volcado

Apéndice H

Análisis de incertidumbre del modelo APS

El presente anexo contiene el análisis de incertidumbre del modelo APS de ATI en fase I obtenido mediante el software *RiskSpectrum® PSA*. La aplicación *RiskSpectrum® PSA* realiza el análisis de incertidumbre de la figura indiciada, en este caso, la frecuencia de liberación de radionúclidos, mediante una simulación Monte Carlo en la que propaga la incertidumbre epistémica de los sucesos básicos presentes en el modelo APS. Tal y como se ha comentado en la memoria de tesis, el análisis de incertidumbre aquí presentado es únicamente representativo de la incertidumbre epistémica de los parámetros de fallo de los sucesos básicos presentes en el árbol de fallos del sistema de ventilación. La tabla H.1 muestra la distribución estadística de la FLR de los diferentes sucesos iniciadores. Las figuras H.1 y H.2 muestran, respectivamente, la función de distribución de probabilidad acumulada y la función de densidad de probabilidad de la FLR del suceso Caída5, el suceso predominante de la etapa de carga.

Suceso Iniciador	Percentil 5 %	Mediana	Media	Percentil 95 %
Caída1	3,39E-15	1,47E-14	2,03E-14	8,06E-14
Caída2	6,36E-13	2,51E-12	3,59E-12	1,84E-11
Caída3	1,90E-13	8,65E-13	1,18E-12	4,80E-12
Caída4	3,76E-12	1,72E-11	2,38E-11	1,06E-10
Caída5	2,51E-09	1,05E-08	1,47E-08	6,88E-08
Volcado	7,89E-15	3,57E-14	5,05E-14	2,24E-13

Tabla H.1: Distribución estadística de la FLR de sucesos iniciadores.

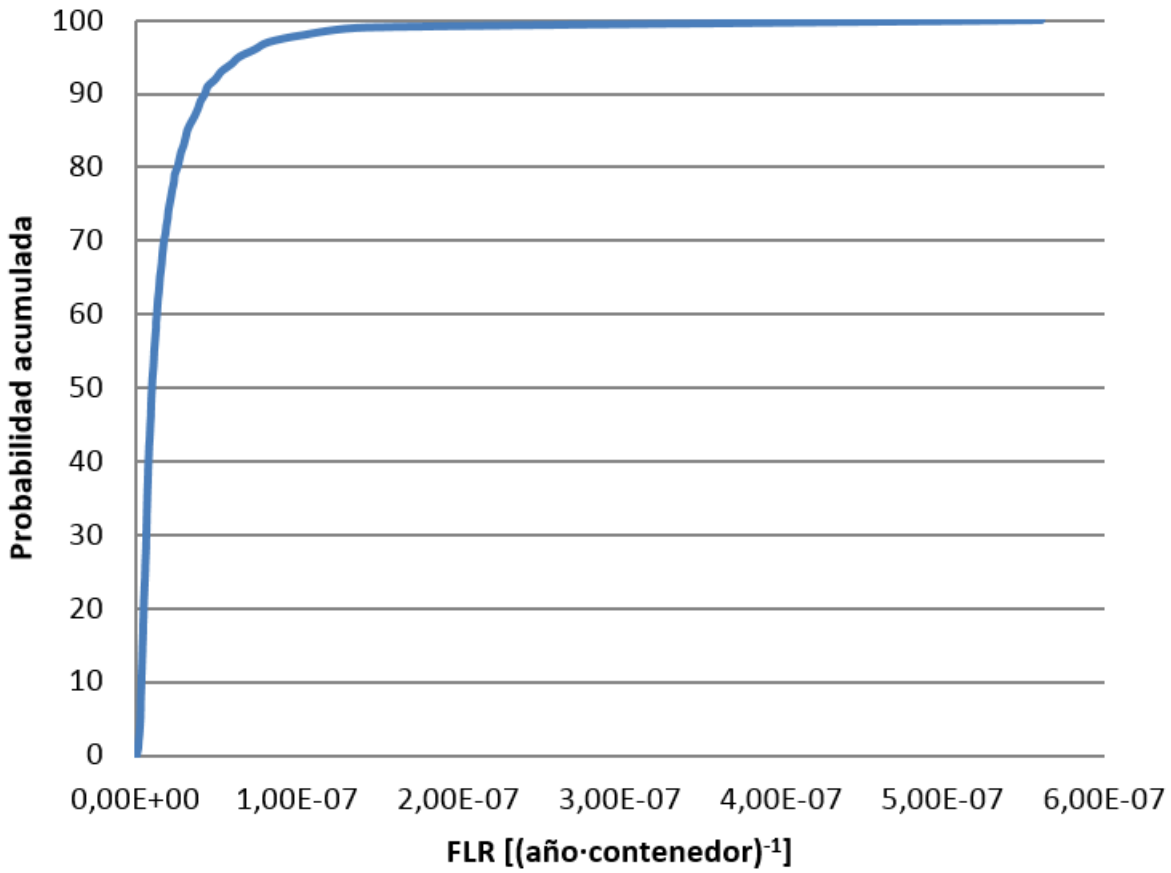


Figura H.1: Distribución de probabilidad acumulada de la FLR del suceso Caída5.

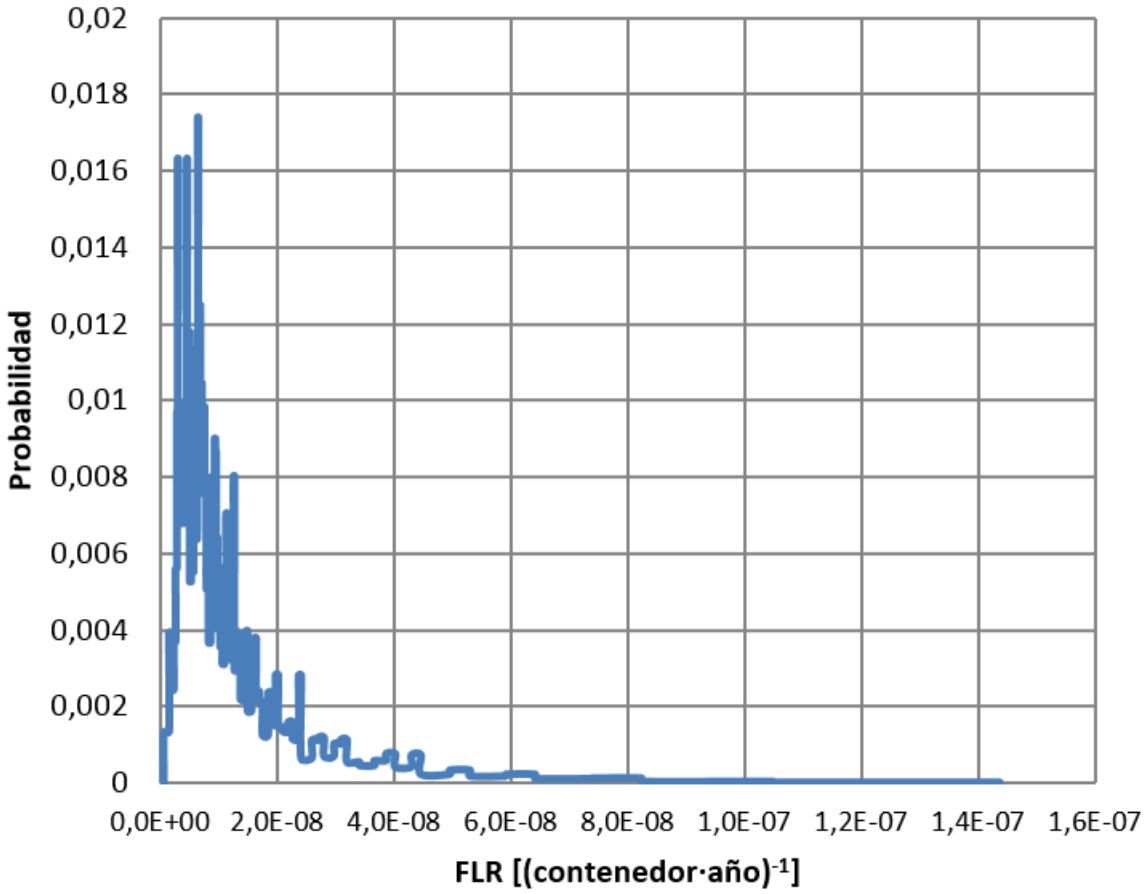


Figura H.2: Función densidad de probabilidad acumulada de la FLR del suceso Caída5.

Apéndice I

Glosario del análisis de fiabilidad humana

La definición de los siguientes conceptos es importante para la comprensión del análisis de fiabilidad humana desarrollado y presentado en la segunda parte de la memoria de tesis. Se definen también los diferentes tipos de error humano.

Evento de fallo humano Un suceso básico en los modelos lógicos de un APS que representa el fallo de una función, un sistema, o un componente a causa de una o más acciones no seguras [74].

Probabilidad de error humano La probabilidad de fallo de un operador al llevar a cabo una acción.

Fallo cognitivo Hace referencia a la probabilidad de éxito o fallo de un operador en el momento de decidir qué acción debe hacer a continuación. El resultado del fallo cognitivo puede ser la no realización de ninguna acción o la realización de una acción incorrecta o inadecuada. El fallo cognitivo está estrechamente relacionado con la detección y el diagnóstico de situaciones y es especialmente importante en situaciones en las que el tiempo es un factor crítico. Uno de los métodos utilizados para analizar el fallo cognitivo es el *Human Cognitive Reliability* model descrito en el documento NUS-4531 [87].

Fallo manual Hace referencia a la probabilidad de éxito o fallo de un operador al realizar una acción manual. El resultado del fallo puede ser la no realización de una acción o la realización incorrecta de una acción.

Comportamiento basado en la habilidad Comportamiento que requiere ningún, o muy poco, control consciente para realizar una acción. Las acciones realizadas bajo un comportamiento basado en la habilidad se llevan a cabo de manera prácticamente automática debido a la experiencia y entrenamiento del operador. Las acciones basadas en la habilidad implican secuencias preprogramadas de comportamiento separadas por revisiones momentáneas para asegurar que la acción en cuestión se está realizando correctamente. Un conductor experimentado conduciendo un coche en un ambiente familiar, un operador de grúa experimentado moviendo cargas que le son familiares por caminos que le son familiares, y tareas de anclaje son ejemplos de acciones compuestas primordialmente por comportamientos basados en la habilidad. En el caso del ATI, la mayoría de acciones manuales son de este tipo.

Comportamiento basado en reglas Comportamiento basado en el uso de procedimientos y reglas para decidir el curso de las acciones en un ambiente de trabajo familiar una vez se ha detectado la necesidad de desviarse de la ejecución basada en la habilidad. Un ejemplo común de comportamiento basado en reglas es un conductor experimentado que responde a interacciones inesperadas con otros coches o señales de tránsito. El conductor detecta conscientemente un problema, selecciona una [9] norma a seguir, y, una vez pasado el problema, vuelve al comportamiento basado en la habilidad.

Comportamiento basado en el conocimiento Comportamiento que confía en la capacidad de resolución de problemas del individuo, que utiliza procesos lentos, secuenciales, y de recursos limitados para seleccionar el curso de las acciones apropiados en situaciones inesperadas o nuevas. El comportamiento basado en el conocimiento actúa cuando las normas y reglas fallan a resolver un problema que ha surgido durante la ejecución de acciones basadas en la habilidad o las reglas. La necesidad de utilizar el comportamiento basado en el conocimiento implica una gran incertidumbre al respecto de la consecución del éxito. Aprender a conducir un coche es un buen ejemplo de este tipo de comportamiento.

Error de omisión (EOO) Un evento de fallo humano producto del fallo a realizar una acción requerida, que deriva en una situación de planta igual o peor con la consecuencia de una degradación de la seguridad de la planta [9]. Hace referencia a omisiones al realizar de acciones que causan, la omisión, un efecto negativo en la seguridad de la planta. Se puede aplicar a acciones manuales.

Error de comisión (EOC) Un evento de fallo humano producto de una evidente acción no segura que, cuando se realiza, deriva en la degradación de la seguridad de la planta [9]. EOC hace referencia a cometer un error al realizar una acción. El resultado de la ejecución incorrecta de la acción es un efecto negativo en la seguridad de la planta. Solo es aplicable a acciones manuales.

Acción no segura Una acción llevada a cabo incorrectamente, o no llevada a cabo cuando es necesario, por el personal de planta que resulta en una degradación de la seguridad de la planta [3]. Hace referencia tanto a EOO como a EOC. La combinación de acciones no seguras puede llevar a la ocurrencia de un evento de fallo humano.

Performance shaping factors Un conjunto de influencias sobre la actuación del personal de operación que derivan de las características de la planta, el grupo de trabajo, y de operadores individuales. Algunos ejemplos son la bonanza de los procedimientos, el estrés, el tiempo disponible, y la experiencia.

Tipos de error humano El tipo de error humano depende de la etapa de la secuencia de accidente en la que se da el fallo humano:

- Tipo 1: Hace referencia a aquellos errores humanos que ocurren antes del suceso iniciador. Estos errores contribuyen a la indisponibilidad de componentes y sistemas.
- Tipo 2: Errores humanos que inducen o causan un suceso iniciador. Incrementan la probabilidad de ocurrencia de los sucesos iniciadores.
- Tipo 3: Después de la ocurrencia de un suceso iniciador, errores humanos que podrían producirse al seguir los procedimientos de operación en emergencia. Se trata, normalmente, de fallos a seguir el procedimiento cuando éstos están basados en síntomas.

- Tipo 4: Después de la ocurrencia de un suceso iniciador, errores humanos que podrían producirse al seguir los procedimientos de operación en emergencia. De forma diferente a las de tipo 3, las acciones en las que se produce el fallo requieren cierto diagnóstico. Acostumbran a ser acciones de recuperación y/o mitigación sugeridas por el procedimiento.
- Tipo 5: Después de la ocurrencia de un suceso iniciador, errores humanos que podrían producirse al realizar acciones no previstas en los procedimientos de operación en emergencia. Fallos al realizar acciones de recuperación y/o mitigación que no están anotadas en los procedimientos de operación en emergencia.

Apéndice J

Metodologías de análisis de fiabilidad humana

El presente anexo contiene la descripción de las metodologías mencionadas y/o utilizadas en el desarrollo del análisis de fiabilidad humana de las operaciones asociadas al almacén temporal individualizado del caso de estudio. Concretamente, se presentan las metodologías THERP, HCR, y SPAR-H.

J.1. Technique for Human Error Rate Prediction

La *Technique for Human Error Rate Prediction* es la metodología de análisis de fiabilidad humana más antigua y una de las comúnmente más utilizadas. Fue creada por Swain y Gutmann en 1983 y fue incluida en el NUREG/CR-1278, llamado *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications.*

THERP describe una metodología cuyas tareas son similares a las realizadas en análisis de fiabilidad convencionales. La diferencia radica en que los equipos o componentes mecánicos son reemplazados por acciones humanas. La característica más representativa de THERP es el uso de árboles de eventos de fallo humano, comúnmente conocidos como *Human Failure Event Trees.* Estos árboles de eventos son una herramienta visual que se utiliza para descomponer los eventos de fallo humano en acciones simples llamadas acciones no seguras, comúnmente conocidas como *Unsafe Actions.* La figura J.1 presenta un árbol de fallos tal y como está descrito en THERP. Cada bifurcación del árbol corresponde a una acción no segura y cada rama describe el éxito (letra minúscula) o el fallo (letra mayúscula) del operador al realizar la acción no segura de la bifurcación.

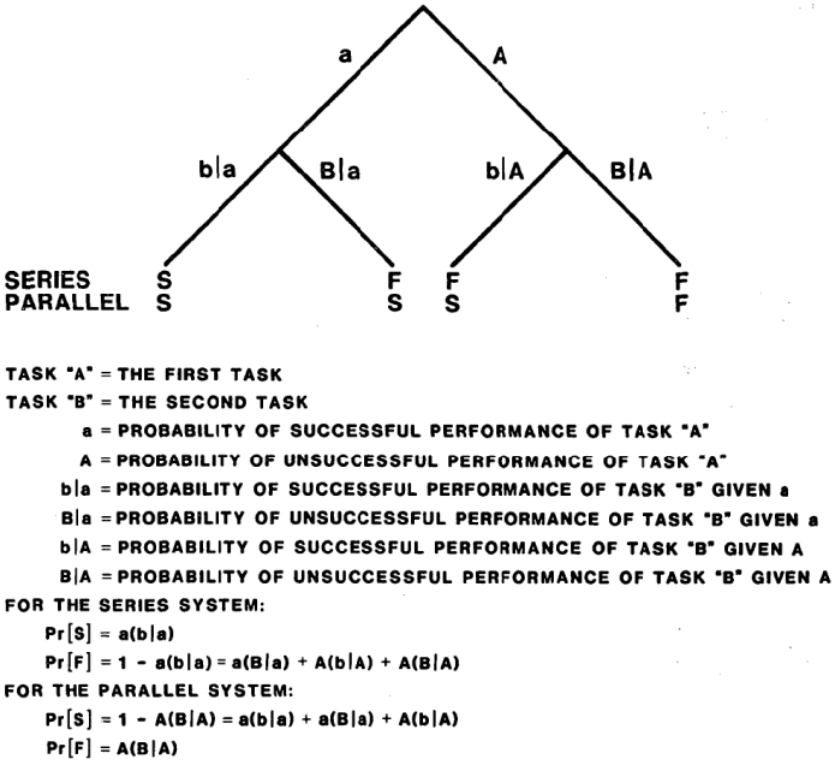


Figura J.1: Árbol de eventos de fallo humano extraído de THERP. Fuente: [6]

La figura J.1 muestra también como se pueden utilizar estos árboles de eventos para estimar la probabilidad de fallo humano. Se han de tomar las hipótesis necesarias para estimar la probabilidad de ocurrencia de cada acción no segura. Por ejemplo, la probabilidad de ocurrencia de las UAs se puede obtener de la base de datos de valores de probabilidad de fallo humano presente en el NUREG/CR-1278. THERP también proporciona herramientas, principalmente tablas con valores aplicables, para tener en cuenta las dependencias entre acciones no seguras consecutivas y la influencia de factores externos.

La metodología THERP fue diseñada para estimar la probabilidad de fallo manual. Es necesario utilizar otros métodos si la parte cognitiva del fallo humano necesita ser evaluada.

J.2. Human Cognitive Reliability

La metodología HCR está dedicada al análisis de la parte cognitiva del fallo humano. El método postula que la probabilidad de éxito o fallo de un operador a realizar correctamente una acción en la que el tiempo es un factor crítico depende del proceso cognitivo, que depende del tipo de acción, es decir, si está basada en la habilidad, reglas, o conocimiento, usado para tomar las decisiones críticas que determinan el resultado final. Para aplicar HCR se han de determinar el tiempo disponible para realizar una acción, el tiempo necesario para ejecutar manualmente la acción, y el tiempo necesario para decidir qué acción hay que tomar. El tiempo necesario para realizar una acción es la suma del tiempo necesario para decidir qué acción hay que tomar y el tiempo necesario para ejecutar manualmente la acción. La metodología HCR también postula el uso de PSFs para evaluar la influencia del contexto en el tiempo promedio necesario para realizar una acción. La combinación de estos factores, los PSFs y el tiempo necesario para realizar una acción, permite calibrar curvas de tiempo de respuesta, que se comparan con el tiempo disponible para realizar la acción objeto de estudio. Las curvas se utilizan para estimar la probabilidad de que un

operador realice la acción correcta dentro del tiempo disponible para su realización. La relación entre las probabilidades de fallo cognitivo y la comparación entre tiempo de respuesta y tiempo disponible se basa en datos experimentales obtenidos en simulador y depende del tipo de la acción: basada en la habilidad, basada en reglas, y basada en el conocimiento. El anexo L presenta la aplicación del método HCR al caso de estudio.

J.3. Standardized Plant Analysis Risk - Human Reliability Analysis

SPAR-H es una metodología de análisis de fiabilidad humana creada por la NRC, que la publicó en 2005 en el NUREG/CR-6883 [88]. SPAR-H es una metodología simple de análisis que se fundamenta en una extensa y detallada descripción de muchos PSFs. El propósito de SPAR-H es describir y cuantificar eventos de fallo humano a partir de una completa definición del contexto en el que pueden ocurrir. Con este objetivo, el NUREG/CR-6883 proporciona una extensa tabla que contiene niveles cualitativos de PSFs y sus correspondientes multiplicadores cuantitativos. La sección presenta cada uno de los PSFs y sus diferentes niveles cualitativos. Los niveles cualitativos de PSFs que se ajustan mejor al contexto de estudio se seleccionan para representar al evento de fallo humano objeto de estudio.

La metodología SPAR-H presenta un modelo de cuantificación que combina los multiplicadores de PSFs con valores de probabilidad de fallo humano. El modelo de cuantificación fue desarrollado para no proporcionar resultados imposibles[1]. La ecuación L.1 representa el modelo de cuantificación postulado en SPAR-H.

$$HEP = \frac{NHEP * PSF_{composite}}{NHEP * (PSF_{composite} - 1) + 1} \tag{J.1}$$

NHEP hace referencia a una probabilidad de fallo humano nominal, es decir, una probabilidad de fallo que no ha sido ajustada según la influencia del contexto en la actuación humana. El término $\text{PSF}_{\text{composite}}$ representa el producto de los multiplicadores de todos los PSFs. El resultado es un valor de probabilidad de fallo humano único que tiene en consideración el contexto en el que se realiza la acción analizada.

J.3.1. PSFs: niveles cualitativos

Se definen a continuación los PSFs presentados en SPAR-H y sus niveles cualitativos. Los multiplicadores cuantitativos asociados a los niveles cualitativos de los PSFs ya se han presentado en la memoria de la tesis doctoral.

J.3.1.1. Tiempo disponible

Este PSF hace referencia a la cantidad de tiempo de la que dispone un operario o un grupo para actuar en reacción a la ocurrencia de un suceso anormal de planta. Se establecen los siguientes niveles para este PSF:

- Tiempo inadecuado: si el operador no puede ejecutar la acción adecuada en la cantidad de tiempo disponible para su ejecución el fallo es inevitable. En este caso, la probabilidad de fallo de la acción en cuestión es 1.

[1] Básicamente, probabilidades de fallo humano mayores a 1.

- El tiempo disponible es igual al tiempo necesario: El tiempo del que dispone el operario para realizar la acción es equivalente al tiempo necesario para realizar dicha acción.
- Tiempo nominal: El tiempo disponible es ligeramente superior al mínimo tiempo necesario para realizar una acción.
- Tiempo disponible al menos cinco veces superior al tiempo necesario para realizar una acción.
- Tiempo disponibe al menos cincuenta veces superior al tiempo necesario para realizar una acción.
- Información insuficiente.

J.3.1.2. Estrés y elementos estresantes

Fuerzas, tanto positivas como negativas, que motivan e influencian la actuación humana [88]. El nivel de condiciones y circunstancias indeseables que impiden que un operador realice fácilmente la acción en cuestión. El término estrés incluye el estrés mental, el estrés físico y la carga excesiva de trabajo. Se entiende como elementos estresantes a el calor, el ruido, una ventilación ineficaz, y la dosis de radiación ente otros. Una pequeña cantidad de estrés se considera nominal y puede favorecer la actuación humana. Se establecen los siguientes niveles para este PSF:

- Extremo: Un nivel de estrés perjudicial que deteriora drásticamente la capacidad de trabajo de la mayoría de individuos.
- Alto: Un nivel de estrés superior al nominal. Por lo tanto, su efecto sobre la actuación humana es negativo.
- Nominal: El nivel de estrés que es positivo para la actuación humana.
- Información insuficiente.

J.3.1.3. Complejidad

Como su propio nombre indica, el PSF de complejidad hace referencia a lo difícil de realizar que es una acción en el contexto de estudio. El PSF complejidad tiene en cuenta tanto la acción a realizar como el contexto en el que se ha de realizar. El PSF también tiene en cuenta el esfuerzo mental necesario, como, por ejemplo, si es necesario realizar operaciones matemáticas, entender modelos, y memorizar datos entre otros. La complejidad derivada de requisitos físicos y/o de habilidad también es tenida en cuenta por este PSF. Se establecen los siguientes niveles para este PSF:

- Complejidad alta: La ejecución de la acción en cuestión es muy complicada. Se aplica también en acciones en que el grado de ambigüedad al respecto de qué se ha de hacer es alto.
- Complejidad moderada: La ejecución de la acción en cuestión es complicada. Se aplica también en acciones en las que existe ambigüedad al respecto de qué se ha de hacer.
- Complejidad nominal: La ejecución de la acción en cuestión no es complicada. Se aplica también en acciones en que el grado de ambigüedad al respecto de qué se ha de hacer es bajo.
- Diagnóstico obvio: El diagnóstico de qué acción se ha de ejecutar es muy simple.
- Información insuficiente.

J.3.1.4. Experiencia y entrenamiento

Este PSF hace referencia a la experiencia y entrenamiento de los operadores involucrados en la realización de la acción. Se tienen en cuenta en este PSF los años de experiencia del individuo o grupo que realiza la acción, si se ha entrenado la acción a realizar, cuanto tiempo ha pasado desde el entrenamiento, y los sistemas involucrados en la acción y el escenario de utilizado. Se establecen los siguientes niveles para este PSF:

- Bajo: Menos de seis meses de experiencia y/o entrenamiento.
- Nominal: Más de seis meses de experiencia y/o entrenamiento.
- Alto: gran experiencia, maestría.

J.3.1.5. Procedimientos

El PSF de procedimientos tiene en consideración la existencia y uso de procedimientos de operación formales para la realización de la acción objeto de estudio. Procedimientos mal diseñados pueden proporcionar información inadecuada o equivocada al respecto de una acción específica. Otro problema común es la ambigüedad de los pasos en los que está dividido el procedimiento. Se establecen los siguientes niveles para este PSF:

- No disponible: El procedimiento que se debería consultar para ejecutar la acción de estudio en el contexto de estudio no está disponible o no existe.
- Incompleto: El procedimiento no incluye información necesaria para ejecutar la acción objeto de estudio.
- Disponible, pero pobre: Se dispone de procedimientos pero estos son ambiguos y contienen información equivocada o inadecuada.
- Nominal: Se dispone de procedimientos que favorecen la actuación humana.
- Información insuficiente.

J.3.1.6. Ergonomía e interfaz hombre-máquina

El PSF de ergonomía incluye el equipamiento, las pantallas y controles, los planos, la calidad y cantidad de información disponible al respecto de la instrumentación, y la interacción entre el individuo y el equipamiento necesario para llevar a cabo la acción objeto de estudio. Se establecen los siguientes niveles para este PSF:

- Ausente / engañosa: La instrumentación necesaria para ejecutar una acción falla a facilitar el diagnóstico o postdiagnóstico, o la instrumentación es imprecisa. La información necesaria para entender la instrumentación no existe o no está disponible.
- Pobre: El diseño de la instrumentación a utilizar tiene un impacto negativo en la actuación humana.
- Nominal: El diseño de la instrumentación a utilizar facilita la actuación correcta, pero no favorece a la actuación humana o no hace que la ejecución de la acción a realizar sea más sencilla de lo esperado.
- Buena: El diseño de la instrumentación a utilizar tiene un impacto positivo en la ejecución de la acción a realizar. La instrumentación proporciona la información y capacidad necesaria para reducir la posibilidad de cometer errores.
- Información insuficiente

J.3.1.7. Aptitud para el trabajo

El PSF de aptitud para el trabajo evalúa si un individuo está física y mentalmente preparado para realizar la acción de estudio. La aptitud para el trabajo se ve afectada por la fatiga, la enfermedad, el uso de drogas, el exceso de confianza, los problemas personales, y las distracciones, entre otros. Se establecen los siguientes niveles para este PSF:

- No apto: El individuo no está preparado para llevar a cabo la acción requerida.
- Aptitud degradada: El individuo puede llevar a cabo la acción requerida, aunque la actuación humana se ve afectada negativamente por la condición del individuo. La actuación física y mental del individuo puede verse afectada por enfermedades o estados, como la fiebre. La aptitud de un individuo también puede considerarse como degradada si confía excesivamente en sus posibilidades.
- Aptitud nominal: El individuo es capaz de llevar a cabo la acción requerida. La actuación del individuo no se ve degradada por ningún factor.
- Información insuficiente.

J.3.1.8. Procesos de trabajo

El PSF en cuestión hace referencia a aspectos inter-organizacionales, la cultura de seguridad, la gestión y planteamiento de tareas, y las políticas de comunicación y de soporte de la gestión, entre otros. Se establecen los siguientes niveles para este PSF:

- Pobre: La actuación humana se ve afectada negativamente por los procesos de trabajo de la planta en cuestión.
- Nominal: La actuación humana no se ve afectada por los procesos de trabajo de la planta, o los procesos de trabajo no juegan un papel importante en la acción objeto de estudio.

Apéndice K

Potential vulnerabilities de la actuación humana

El presente anexo resume las potenciales vulnerabilidades de la actuación humana en el contexto ATI definidas y descritas en el documento NUREG/CR-7017. Las potenciales vulnerabilidades aquí presentes derivan del análisis del proceso de almacenamiento y de la opinión de expertos en el proceso de almacenamiento. Se incluye también un listado de las citas y comentarios específicos de expertos en la materia que han llevado al desarrollo de la lista de las potenciales vulnerabilidades.

K.1. Actividades que no suponen un desafío

Las acciones y actividades llevadas a cabo en contextos de manejo de combustible son, en general, bastante sencillas. Los movimientos, de combustible o contenedores, son lentos, por lo que se tarda un tiempo considerable en terminarlos. Por lo tanto, el contexto es propicio para que haya distracciones, y para que se instaure un ambiente de informalidad y complacencia en los miembros del equipo. Desde el punto de vista psicológico, la actividad no es lo suficientemente dinámica como para generar un nivel de estrés óptimo. La falta de estímulo, combinada con la gran experiencia[1] del personal que lleva a cabo la tarea puede derivar en la omisión en el uso de procedimientos. La transición desde el uso estricto de procedimientos a la violación rutinaria de procedimientos genera reglas informales que el personal acepta como normales pasado un tiempo.

K.2. Dificultades visuales

Diferentes tipos de indicaciones y/o señales visuales son primordiales en la realización de operaciones de combustibles gastado. En muchos casos, la observación de dichas indicaciones y/o señales se complica por el posicionamiento del personal observador en relación a la actividad a observar. Las operaciones a realizar en el interior de la piscina de combustible pueden ser particularmente complicadas. La refracción del agua y el reflejo de la superficie pueden distorsionar la visión de la operaciones que requieren un posicionamiento preciso. La observación de señales de daño en vainas de combustible que se encuentran en el interior del contenedor puede verse seriamente dificultada por elementos estructurales.

Las operaciones de grúa presentan dificultades visuales ya se realicen en el agua o no. El operador de grúa se ha de inclinar sobre el puente de la grúa para poder tener una visión cenital de las operaciones.

[1] Se supone que han realizado las operaciones motivo de estudio muchas veces sin que haya incidencias.

Muchos de los errores que se pueden cometer en el movimiento de cargas con la grúa puente no pueden ser detectados desde arriba. Además, la visión desde el puente grúa puede verse obstruida por el yugo de alzamiento o por la propia carga. En consecuencia, el operario de grúa se encuentra en una situación en el que es las manos de otros ojos, con lo que la operación es vulnerable a dificultades de comunicación.

Finalmente, en muchos casos, los operarios observadores han de seguir la actividad que vigilan desde la distancia para cumplir con el criterio ALARA. En estos casos, es posible que el personal observador no detecte pequeñas desviaciones y errores que pueden llevar a problemas significativos en etapas posteriores.

K.3. Dificultades de comunicación

Las dificultades de comunicación entre los miembros del equipo de trabajo al realizar operaciones de movimiento de combustible gastado son significativas. El ambiente del edificio de combustible presenta una gran cantidad de ruido de fondo, especialmente ruido de maquinaria. Aunque los miembros del equipo de trabajo utilizan auriculares para comunicarse, éstos no son suficiente como para eliminar potenciales malentendidos. La comunicación mediante auriculares puede estar distorsionada[2] y es posible que, en algunos casos, no se pueda determinar claramente quien es el operario que transmite un mensaje. La creencia de que un operario está hablando, cuando realmente no lo está, puede influenciar al oyente y hacerle pensar que está escuchando lo que espera escuchar.

Los miembros de los equipos de trabajo utilizan, principalmente, señales gestuales para comunicarse entre sí, pero no existe ninguna garantía de que el operario objetivo vea las señales dirigidas a él. El uso de comunicación gestual complica captar rápidamente la atención del individuo objetivo. Además, también es posible que las señales gestuales se interpreten de forma errónea, especialmente en aquellos casos en los que el significado de las señales no está firmemente establecido.

K.4. Presión temporal

Aunque la presión temporal de las campañas de carga es generalmente menor que las de las paradas de recarga, no cumplir con los hitos de la planificación puede incrementar los gastos y la incertidumbre en la planificación de futuras paradas de recarga. Los expertos en la materia consultados comentan que la presión temporal puede dispararse rápidamente, incluso en el traslado de los elementos de combustible gastado. La percepción de que la mayoría de errores cometidos durante las etapas de carga y transferencia tienen una consecuencia baja puede empeorar la actuación humana en situaciones en las que se dispara la presión temporal. Los operarios son conscientes de que la caída de un contenedor cargado de elementos de combustible puede tener graves consecuencias, así que todas las operaciones relacionadas son mucho menos susceptibles a la presión temporal. Sin embargo, la percepción al respecto del movimiento individual de elementos de combustible es diferente. Los operarios pueden considerar que no es necesario realizar estas operaciones lentamente, siguiendo un procedimiento. El tono establecido por la dirección de la central al respecto del beneficio que supone primar la seguridad por encima de cumplir con la planificación predeterminada tiene un gran impacto en la percepción de la presión temporal entre los operarios que llevan a cabo el proceso de almacenamiento.

K.5. Otros aspectos ergonómicos

Aspectos como trabajar en entornos inhóspitos como, por ejemplo, entornos de calor extremo o lugares de espacio reducido, pueden afectar negativamente a la actuación humana en las operaciones del contexto

[2] Debido a interferencias o al ruido de fondo.

ATI. Dichos entornos pueden afectar al ritmo de trabajo ya sea, por ejemplo, por la necesidad de evacuar rápidamente el lugar por motivos de seguridad o por el poco confort que presentan. Otros aspectos como la necesidad de llevar equipamiento protector también pueden afectar negativamente a la actuación humana al restringir el movimiento de los operarios y causar incomodidad.

K.6. Confianza

La confianza es una componente esencial de cualquier actividad realizada en equipo. Los miembros del equipo han poder esperar, y depender, del adecuado comportamiento de otros miembros al realizar acciones. Sin embargo, la confianza puede tener también una variable negativa. Por ejemplo, un supervisor confía en el personal observador y el personal encargado del movimiento de cargas, siendo alta la experiencia de ambos, lo que le lleva a verificar de forma rápida la carga de elementos de combustible. Se les ha de recordar a los miembros del equipo la adecuada orientación de la confianza. En el caso de ejemplo, la correcta orientación de la confianza es que el personal observador y el personal encargado del movimiento de carga confían en que el el supervisor revisará cuidadosamente la carga de elementos de combustible.

K.7. Citas y comentarios de los expertos en la materia

Los siguientes párrafos contienen observaciones de expertos en la materia extraídas de entrevistas y otros documentos. Estas observaciones pueden resultar beneficiosas para entender e identificar contextos en los que la actuación humana puede tender al fallo.

Es posible retirar elementos de combustible de posiciones equivocadas y colocar elementos de combustible en posiciones equivocadas. El observador puede revisar los números de serie con binoculares, pero es posible que omita algunos movimientos. A veces, se mueve más de un elemento de combustible antes de anotar los movimientos realizados en una hoja de movimientos.

La refracción de la luz en el agua es un gran problema. El personal observa desde la grúa pórtico los movimientos realizados a una profundidad de entre seis y quince metros y trata de garantizar el adecuado posicionamiento del dispositivo de izado. Las dificultades visuales contribuyen a que haya problemas de identificación de los elementos de combustible.

Las actividades realizadas se basan en la habilidad. Los procedimientos no se siguen paso a paso sino que los operarios ejecutan los pasos que han aprendido como si fuese una rutina basada en la habilidad. Los errores al realizar estas actividades suelen ser deslices o lapsos / omisiones. El uso laxo de los procedimientos puede dar lugar a distracciones y alteraciones.

Los errores de carga no se manifiestan hasta pasadas semanas o meses, o incluso años, después de que se haya cargado erróneamente el contenedor. Los errores de carga pueden ocurrir al trasladar elementos de combustible gastado desde el núcleo del reactor a la piscina de combustible gastado, al trasladar elementos de combustible entre posiciones de la piscina, o al trasladar los elementos de combustible desde la piscina hasta el contenedor.

El ritmo y la naturaleza de las actividades llegadas a cabo durante el movimiento de elementos de combustible es muy lento y repetitivo. Rápidamente se transforma en una tarea monótona. El hecho de que las actividades no sean desafiantes puede contribuir a la ocurrencia de errores.

Es posible que se den distracciones durante las operaciones del contenedor. La planificación de una parada de recarga justo después de una campaña de carga de contenedores puede ser un problema realmente importante para muchas centrales. Un solapamiento entre una CLC y una parada de recarga podría suponer un gran problema por falta de personal.

Las operaciones de grúa son altamente repetitivas y monótonas.

Apéndice L

Aplicación del análisis de fiabilidad humana

El presente anexo contiene todas aquellas características y resultados de la aplicación del análisis de fiabilidad humana a las operaciones del contexto ATI que no se han incluido en la memoria de la tesis. Concretamente, el anexo incluye la definición de eventos de fallo humano, la descripción de DHFET, la asignación de PSFs, y la cuantificación de probabilidades de los eventos de fallo humano postulados en las fases de la etapa de carga que no son la quinta fase.

L.1. Definición de eventos de fallo humano

La definición detallada de los eventos de fallo humano se apoya en la descripción de las tareas y acciones a realizar en las diferentes fases de la etapa de carga según los procedimientos de operación proporcionados por la central nuclear.

L.1.1. Fase 1: Carga del contenedor MPC con elementos de combustible gastado

La única causa raíz considerada en la fase 1 es la carga errónea. El término carga errónea hace referencia a un evento de fallo humano en el que el MPC o bien es cargado con elementos de combustible incorrectos, o bien es cargado con los elementos de combustible correctos pero en una configuración errónea. El procedimiento utilizado en la central nuclear estipula que el traslado de elementos de combustible se realiza en dos fases. Primero, se trasladan los elementos de combustible seleccionados a un espacio vacío de la piscina, donde se colocan en la misma configuración que tendrán en el contenedor. A continuación, los elementos de combustible se trasladan al interior del contenedor. Se asume, por simplicidad de análisis, que en el traslado de elementos de combustible desde la piscina al contenedor no se cometen errores. Por lo tanto, el evento de carga errónea se acota al traslado de elementos de combustible en el interior de la piscina. Las principales características del movimiento de elementos de combustible son:

- Tres operarios son los responsables del movimiento elementos de combustible gastado: el operario de grúa, el observador, y el supervisor. El supervisor no tiene porqué estar presente durante el movimiento del combustible.
- El procedimiento obliga a los operarios a seguir una hoja de movimientos que explicita qué elementos de combustible han de trasladarse y dónde han de colocarse.

- Se utiliza la comunicación a tres vías[1] por las dificultades de comunicación presentes en el edificio.
- El observador revisa que el operador de grúa esté siguiendo la hoja de movimientos. Él también revisa el elemento de combustible que va a ser trasladado y la posición en la que se coloca.
- Una vez el contenedor queda cargado el supervisor revisa la configuración de combustible en su interior.

El análisis del evento de carga errónea se divide en dos eventos de fallo humano. Uno evalúa la posibilidad de colocar elementos de combustible en posiciones incorrectas, y el otro evalúa la posibilidad de seleccionar elementos de combustible equivocados. La definición de ambos HFE es conservadora porque consideran como fallo humano la colocación incorrecta de tan solo un elemento de combustible gastado. Estudios recientes concluyen que se han de colocar incorrectamente al menos seis elementos de combustible para que produzcan consecuencias negativas [2]. El resultado cuantitativo de los HFE propuestos dictaminará si la situación real debiera ser analizada o si puede ser despreciada.

L.1.1.1. HFE1.1: Colocar un elemento de combustible correcto en una posición incorrecta

El evento HFE1.1 define el fallo de humano en el que se coloca un elemento de combustible que está en la hoja de movimientos en una posición que no es la suya. Este evento puede estar causado por el fallo del operario de grúa a seleccionar, o entender, la posición objetivo en la hoja de movimientos, o por el fallo del operario de grúa a colocar la herramienta de brazo de largo de la grúa, y, por extensión, el elemento de combustible, encima de la posición objetivo. El observador ha de omitir o realizar incorrectamente la acción de revisión para que el evento pueda ocurrir. La definición del HFE1.1 tiene en cuenta que es posible que se omita el uso de procedimientos.

L.1.1.2. HFE1.2: Seleccionar un elemento de combustible incorrecto

El evento HFE1.2 define el fallo humano en el que se traslada un elemento de combustible que no está presenta en la hoja de movimientos. Este evento puede estar causado por el fallo del operario a seleccionar, o entender, la posición objetivo desde la cual se ha de extraer un elemento de combustible, o por el fallo del operario de grúa a colocar la herramienta de brazo de largo de la grúa encima de la posición en la que descansa el elemento de combustible objetivo. El observador ha de omitir o realizar incorrectamente la acción de revisión para que el evento pueda ocurrir. La definición del HFE1.2 tiene en cuenta que es posible que se omita el uso de procedimientos.

L.1.2. Fase 2: Alzamiento del contenedor cargado desde el pozo del contenedor

Se evalúan dos posibles causas raíz en esta fase de la etapa de carga: el fallo al anclaje o la obstaculización del contenedor. Al respecto de la obstaculización, se desestima su análisis por los siguientes motivos:

- El pozo del contenedor está rodeado de operarios que realizan tareas de observación y/o descontaminación. Es altamente improbable que éstos no notificasen la existencia de un obstáculo en el camino de ascenso del contenedor.
- Estos mismos operarios deberían dejar utillaje en el borde del contenedor para que realmente existiese la posibilidad de que el contenedor se viese obstaculizado.

[1] Comunicación en la que la persona objetivo repite el mensaje y el emisor confirma o desmiente la correcta interpretación del receptor.

- Si el operario de grúa sigue los procedimientos, el contenedor se ha de colocar en el centro del pozo del contenedor. Si es así, se evitaría que este chocase con algún objeto colocado en el borde del pozo.
- Si el operario de grúa sigue los procedimientos, el movimiento ascendente del contenedor se ha de parar justo antes de que su extremo superior salga del agua. En consecuencia, en caso de chocar con un obstáculo inmediatamente después, la poca velocidad a la que se alzaría el contenedor no causaría la caída del mismo y facilitaría a los observadores la tarea de notificar con tiempo al operario de grúa que cese el movimiento.

El fallo al anclaje se produciría al conectar los brazos del yugo de alzamiento con las articulaciones del contenedor HI-TRAC. El mencionado anclaje se lleva a cabo bajo el agua, siendo el operario de la grúa puente el principal responsable del mismo. Los brazos del yugo de alzamiento se abren para rodear las articulaciones del HI-TRAC y, posteriormente, se cierran para ajustarse a ellas. Una vez anclado, el HI-TRAC, con el MPC cargado, se extrae del pozo del contenedor. Las principales características del anclaje y posterior alzamiento son:

- El pozo está rodeado de operarios cuya misión es observar la realización del anclaje y/o descontaminar la superficie del contenedor HI-TRAC con agua desmineralizada.
- El operario de la grúa puente ve el movimiento del contenedor con mucha dificultad.
- La tapa del MPC también se encuentra anclada al yugo de alzamiento, pero no se utiliza para alzar el contenedor.

L.1.2.1. HFE2.1: El contenedor cae debido a un fallo al anclaje del dispositivo de izado

El evento HFE2.1 define un fallo humano en el que el contenedor cae al pozo debido al fallo del operario de grúa a anclar correctamente el yugo de alzamiento con el HI-TRAC. Los operarios observadores han de omitir, o realizar de forma incorrecta, su tarea de supervisión del anclaje para que se de el HFE. El evento HFE2.1 tiene en cuenta una posible recuperación: es posible que los observadores oigan el sonido chirriante que producirían los brazos del yugo al desanclarse, y que, acto seguido, le comuniquen al operario de grúa que ha de cesar el movimiento ascendente. La definición del HFE2.1 tiene en cuenta que es posible que se omita el uso de procedimientos. Conservadoramente, se considera que le contenedor caería cuando su extremo inferior estuviese justo por encima de la superficie del pozo. Esto supone una distancia de caída de 13 metros.

L.1.3. Fase 3: Traslado del contenedor hasta la zona de preparación

La única causa raíz estudiada en esta fase es el suceso de *two-blocking*. Un suceso de *two-blocking* hace referencia al izado inadvertido e incontrolado del contenedor que causa la caída del contenedor debido a la rotura de los cables de izado si fallan, a su vez, componentes de seguridad de la grúa. La rotura de los cables de izado de la grúa se produciría cuando el bloque del gancho principal chocase con la grúa y su vehículo. Las principales características del traslado en esta fase son:

- Los procedimientos de manipulación del contenedor no especifican la altura máxima a la que se puede trasladar el contenedor. La única mención de los procedimientos en referencia a este aspecto es que el contenedor ha de trasladarse lo más cerca posible del suelo. Por lo tanto, un suceso de *two-blocking* no representa la violación de los procedimientos.
- Los procedimientos no especifican ni la máxima velocidad de traslado, ni la máxima velocidad de alzamiento del contenedor. Sin embargo, se conoce por el procedimiento de operación de la grúa que la máxima velocidad de alzado de cargas críticas es de 1,54 m/min.

- Si el caso se trasladase a 0,5 m del suelo, hipótesis tomada en el análisis, habría ocho metros de distancia entre el extremo superior del contenedor y el vehículo de la grúa. Por lo tanto, serían necesarios cinco minutos y 12 segundos para que el contenedor golpease el vehículo si se respeta la máxima velocidad de la grúa.
- Es posible que el operador de grúa deje el *joystick* de mando en la posición de movimiento continúo en lugar de en la posición de *Stop* debido a la configuración del mismo.
- El contenedor está rodeado por observadores / limpiadores que se darán cuenta de si el contenedor se alza más de lo esperado.
- La posibilidad de que ocurra este tipo de suceso es mayor si se han de esquivar obstáculos.
- Se asume que el operario de grúa tiene dificultades para seguir con precisión el movimiento del contenedor en todo momento.

El evento de *two-blocking* se modela con un único evento de fallo humano.

L.1.3.1. HFE3.1: suceso de *two-blocking*

El evento HFE3.1 define el fallo humano en el cual el operador de grúa falla a parar el movimiento ascendente del contenedor. Existe la posibilidad de que el operador de grúa deje el *joystick* de mando en la posición de movimiento continúo en lugar de en la posición de *Stop* debido a la configuración del mismo. Además, se asume que el operario de grúa no puede seguir con la vista el movimiento del contenedor. No obstante, los observadores que siguen el movimiento se darán cuenta, seguro, de que el contenedor está siendo alzado más de los esperado. Sin embargo, puede que haya problemas de comunicación entre los observadores y los operarios de grúa.

L.1.4. Fase 4: Test, soldadura, y rellenado con helio

No existen causas raíces aplicables a esta fase.

L.1.5. Fase 5: Traslado del contenedor desde la zona de soldadura hasta la plataforma de traslado. El contenedor HI-TRAC se coloca encima del HI-STORM

Desarrollado en la memoria de la tesis.

L.1.6. Fase 6: Traslado del MPC al HI-STORM 100

La única causa raíz postulada en la fase 6 es el fallo al anclaje. No obstante, el fallo al anclaje postulado en la fase 6 es sustancialmente diferente con respecto a los estudiados en la fase 2 y en la fase 5. En la fase 6 se realizan tres anclajes en serie: el anclaje de la tapa del MPC con el dispositivo de bloqueo de izado, el anclaje del adaptador del dispositivo de bloqueo de izado con el gancho principal de la grúa puente y, finalmente, el anclaje del dispositivo de bloqueo de izado con el adaptador del dispositivo del bloqueo de izado, que cierra la conexión entre el gancho principal y el MPC. La figura L.1 muestra los tres anclajes mencionados. Al estar en serie, si cualquiera de estos tres anclajes se realiza incorrectamente se podría producir la caída del contenedor MPC. La función principal del dispositivo de bloqueo de izado es la de permitir el descenso controlado del contenedor a la vez que se restringe el ascenso inadvertido del mismo[2].

[2] En consecuencia, no se estudia la causa raíz de *two-blocking*.

No obstante, ni el diseño del dispositivo ni el detalle del procedimiento seguido para realizar los diversos anclajes son conocidos porque no se incluyen en los procedimientos de manipulación del contenedor. Los anclajes se llevan a cabo de forma manual. Las principales características del traslado del MPC son:

- El anclaje del dispositivo de bloqueo de izado con el MPC y el anclaje del adaptador del dispositivo de bloqueo de izado con el propio dispositivo se han de llevar a cabo encima del MPC. La temperatura y la tasa de dosis encima del MPC son más altas que en cualquier otro lugar del edificio de combustible.
- El espacio en el que se realizan los anclajes es reducido.
- Los operarios que realizan los anclajes han de vestirse con equipos especiales para protegerse de la radiación y la temperatura. Su capacidad de movimiento está restringida y no están cómodos.

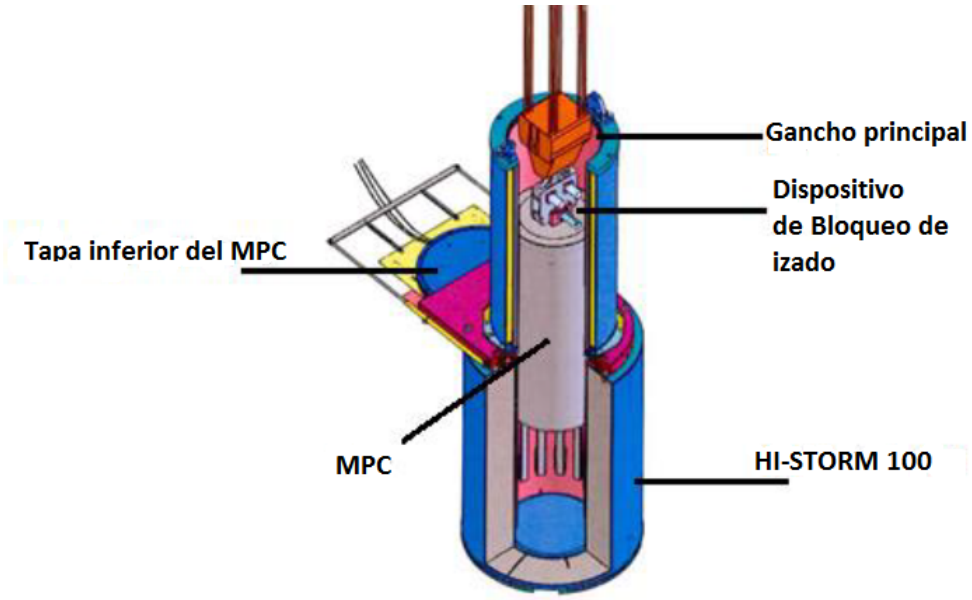


Figura L.1: Anclaje entre el gancho principal y el MPC.

El evento de fallo al anclaje se modela con un único evento de fallo humano.

L.1.6.1. HFE6.1: Fallo al anclaje que provoca la caída del MPC en el interior del HI-STORM 100

El evento HFE6.1 define el fallo humano al anclaje del MPC con el gancho principal de la grúa puente que provoca la caída del MPC en el interior del HI-STORM 100. La conexión entre el MPC y el gancho principal está formada por los tres anclajes descritos anteriormente. El fallo de cualquiera de los anclajes provocaría la caída del MPC. Conservadoramente, el fallo a anclar, en cada uno de los tres casos, se modela como el fallo a anclar un único perno. El procedimiento sugiere que se ha de anclar más de un perno, pero no detalla cantidad total. El observador ha de omitir o realizar incorrectamente la acción de revisión para que el evento pueda ocurrir. La definición del HFE6.1 tiene en cuenta que es posible que se omita el uso de procedimientos.

L.2. Delineación de DHFETs

Este anexo se limita a reproducir los DHFET de los eventos de fallo humano no incluidos en la memoria de tesis. No se incluyen descripciones detalladas de los DHFET puesto que se considera que los árboles son fácilmente interpretables, más teniendo en cuenta los ejemplos incluidos en la memoria de tesis. La tabla L.1 contiene todas las acciones no seguras utilizadas en la delineación de los DHFET.

ID	Descripción
A	Omisión del uso de procedimientos
B	Fallo al seleccionar la posición objetivo en la hoja de movimientos
C	Fallo al seleccionar la posición objetivo en la hoja de movimientos omitiendo el uso de procedimientos
D	Fallo a seleccionar la posición en la que se ha de colocar el elemento de combustible
E	Fallo a seleccionar la posición en la que se ha de colocar el elemento de combustible omitiendo el uso de procedimientos
F	Omisión de revisión
G	Omisión de supervisión omitiendo el uso de procedimientos
H	Fallo al ejecutar la revisión
I	Fallo al ejecutar la supervisión omitiendo el uso de procedimientos
J	Fallo a colocar la herramienta de brazo largo sobre la posición objetivo
K	Fallo a colocar la herramienta de brazo largo sobre la posición objetivo omitiendo el uso de procedimientos
L	Error de comunicación
M	El operario de grúa falla a parar
N	Fallo a anclar el dispositivo de izado
O	Fallo a anclar el dispositivo de izado omitiendo el uso de procedimientos
P	Fallo a darse cuenta de un sonido chirriante
Q	El operario de grúa falla a parar el ascenso del contenedor
E	El operario de grúa falla a parar el movimiento del contenedor a tiempo
S	Fallo a anclar el dispositivo de bloqueo de izado con la tapa del MPC
T	Fallo a anclar el dispositivo de bloqueo de izado con la tapa del MPC omitiendo el uso de procedimientos
U	Fallo a anclar el adaptador del dispositivo de bloqueo de izado con el gancho principal
V	Fallo a anclar el adaptador del dispositivo de bloqueo de izado con el gancho principal omitiendo el uso de procedimientos
W	Fallo a anclar el dispositivo de bloqueo de izado con su adaptador
X	Fallo a anclar el dispositivo de bloqueo de izado con su adaptador omitiendo el uso de procedimientos

Tabla L.1: Acciones no seguras identificadas en el análisis de fiabilidad humana.

Los DHFET delineados y las ecuaciones de los caminos de fallo presentes en los DHFET se presentan a continuación.

L.2.1. DHFET de los eventos de fallo humano de la fase 1

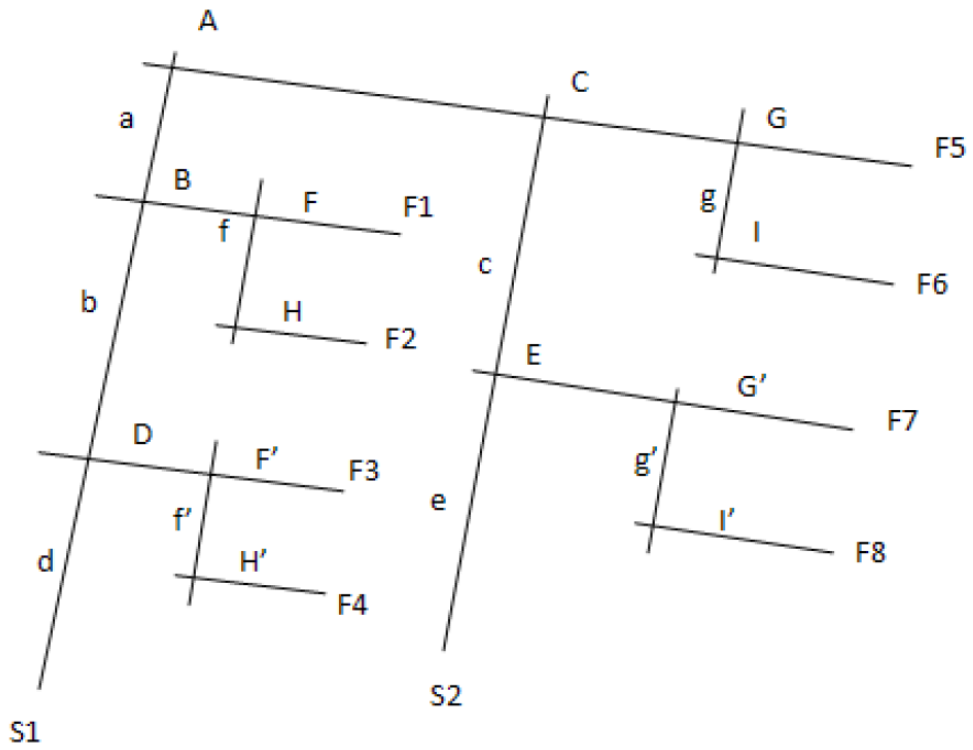


Figura L.2: DHFET del evento de fallo humano HFE1.1

$$F1 = a \cdot B \cdot F \qquad F2 = a \cdot B \cdot f \cdot H \qquad F3 = a \cdot J \cdot F' \qquad F4 = a \cdot J \cdot f' \cdot H'$$

$$F5 = A \cdot C \cdot G \qquad F6 = A \cdot C \cdot g \cdot I \qquad F7 = A \cdot K \cdot G' \qquad F8 = A \cdot K \cdot g' \cdot I'$$

Figura L.3: Ecuaciones de los caminos de fallo del DHFET del evento HFE1.1

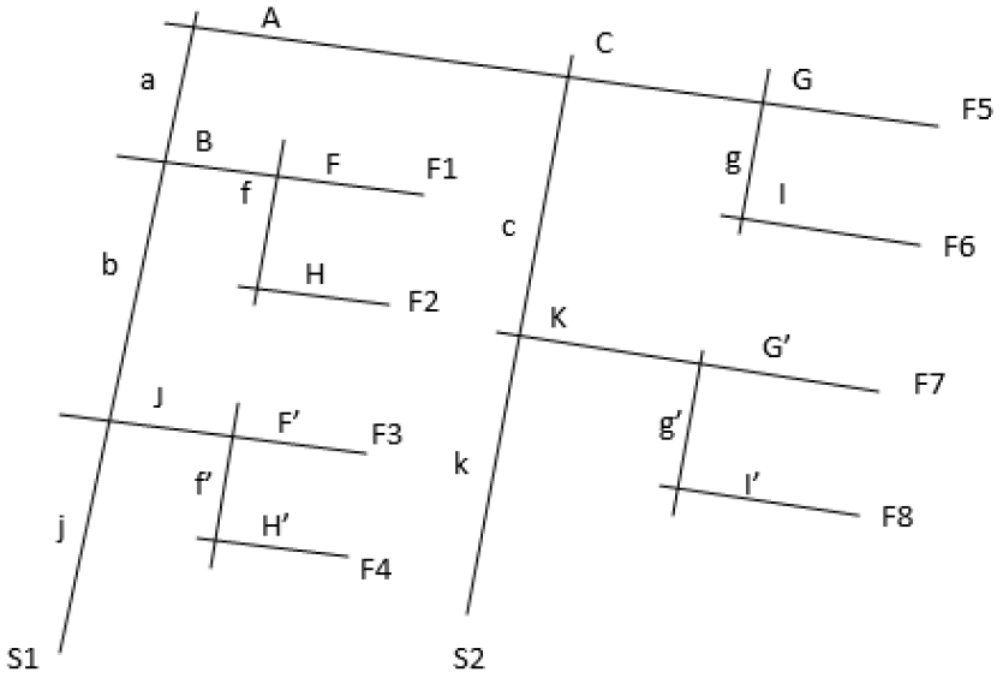


Figura L.4: DHFET del evento de fallo humano HFE1.2

$$F1 = a \cdot B \cdot F \qquad F2 = a \cdot B \cdot f \cdot H \qquad F3 = a \cdot J \cdot F' \qquad F4 = a \cdot J \cdot f' \cdot H'$$

$$F5 = A \cdot C \cdot G \qquad F6 = A \cdot C \cdot g \cdot I \qquad F7 = A \cdot K \cdot G' \qquad F8 = A \cdot K \cdot g' \cdot I'$$

Figura L.5: Ecuaciones de los caminos de fallo del DHFET del evento HFE1.2

L.2.2. DHFET de los eventos de fallo humano de la fase 2

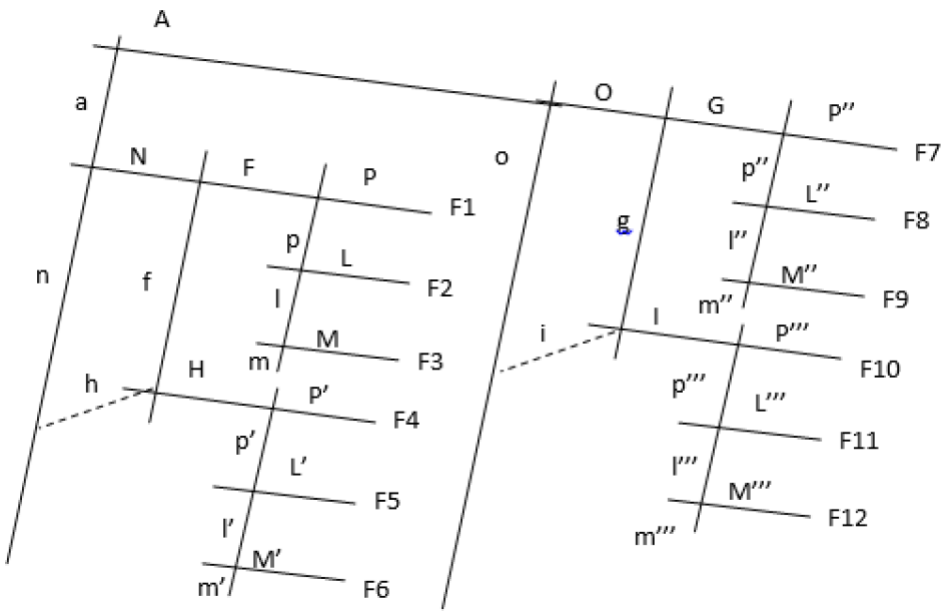


Figura L.6: DHFET del evento de fallo humano HFE2.1

$$F1 = a \cdot N \cdot F \cdot P \quad F2 = a \cdot N \cdot F \cdot p \cdot L \quad F3 = a \cdot N \cdot F \cdot p \cdot l \cdot M \quad F4 = a \cdot N \cdot f \cdot H \cdot P'$$

$$F5 = a \cdot N \cdot f \cdot H \cdot p' \cdot L' \quad F6 = a \cdot N \cdot f \cdot H \cdot p' \cdot l' \cdot M' \quad F7 = A \cdot O \cdot G \cdot P\ ''$$

$$F8 = A \cdot O \cdot G \cdot p'' \cdot L'' \quad F9 = A \cdot O \cdot G \cdot p'' \cdot l'' \cdot M'' \quad F10 = A \cdot O \cdot g \cdot I \cdot P'''$$

$$F11 = A \cdot O \cdot g \cdot I \cdot p''' \cdot L''' \quad F12 = A \cdot O \cdot g \cdot I \cdot p''' \cdot l''' \cdot M'''$$

Figura L.7: Ecuaciones de los caminos de fallo del DHFET del evento HFE2.1

L.2.3. DHFET de los eventos de fallo humano de la fase 3

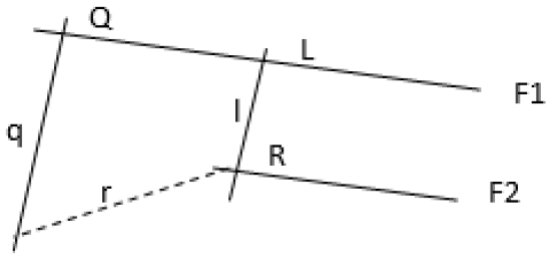


Figura L.8: DHFET del evento de fallo humano HFE3.1

$$F1 = Q \cdot L \quad F2 = Q \cdot l \cdot R$$

Figura L.9: Ecuaciones de los caminos de fallo del DHFET del evento HFE3.1

L.2.4. DHFET de los eventos de fallo humano de la fase 6

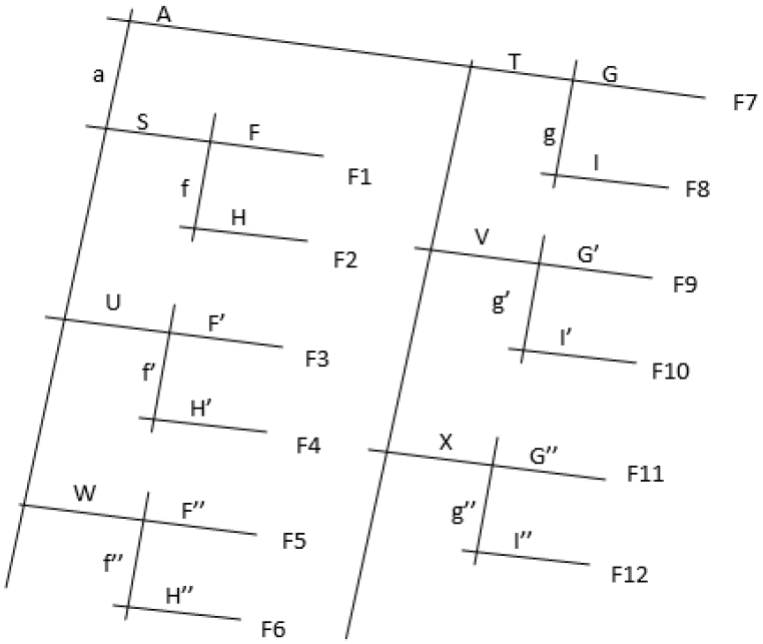


Figura L.10: DHFET del evento de fallo humano HFE6.1

$$F1 = a \cdot S \cdot F \quad F2 = a \cdot S \cdot f \cdot H \quad F3 = a \cdot U \cdot F' \quad F4 = a \cdot U \cdot f' \cdot H'$$

$$F5 = a \cdot W \cdot F'' \quad F6 = a \cdot W \cdot f'' \cdot H'' \quad F7 = A \cdot T \cdot G \quad F8 = A \cdot T \cdot g \cdot I$$

$$F9 = A \cdot V \cdot G' \quad F10 = A \cdot V \cdot g' \cdot I' \quad F11 = A \cdot X \cdot G'' \quad F12 = A \cdot X \cdot g'' \cdot I''$$

Figura L.11: Ecuaciones de los caminos de fallo del DHFET del evento HFE6.1

L.3. Análisis de PSFs

El análisis de PSFs consiste en seleccionar qué niveles cualitativos describen el contexto en el que se realizan cada una de las UAs. Los niveles cualitativos se han de ajustar lo máximo posible a las condiciones reales en las que se realizan las acciones humanas. Las condiciones en la que se realizan las acciones de la fases de la etapa de carga están descritas en la sección de descripción del contexto nominal de la memoria de tesis y en el anexo A.

El nivel cualitativo Nominal se ha elegido por defecto en dos PSFs para toda UA en el contexto nominal: procesos de trabajo y experiencia / entrenamiento. La influencia de ambos sobre la ejecución de las UAs es nula en el contexto nominal por la propia definición del contexto. El resto de niveles cualitativos elegidos para los eventos de fallo humano no descritos en la memoria se presentan a continuación.

L.3.1. HFE1.1: Colocar un elemento de combustible correcto en una posición incorrecta

La tabla L.2 contiene los multiplicadores, y, por lo tanto, índica los niveles cualitativos, seleccionados para las UAs que forman el HFE1.1.

	PSFs					
UA ID	AT	Estrés	Complejidad	Procedimientos	Ergo/HMI	Aptitud
A	0,1	1	1	1	1	1
B	0,1	1	1	1	1	1
C	0,1	1	2	1	1	1
D	1	2	1	1	1	1
E	1	2	2	1	1	1
F	0,1	1	1	1	1	1
F'	0,1	1	1	1	1	1
G	0,1	1	1	1	1	1
G'	0,1	1	1	1	1	1
H	1	2	1	1	1	1
H'	1	2	1	1	1	1
I	1	2	2	1	1	1
I'	1	2	2	1	1	1

Tabla L.2: Multiplicadores de PSF para el evento HFE1.1.

Se detallan a continuación las razones por las cuales se han elegido multiplicadores diferentes a Nominal para algunas de las UAs del suceso HFE1.1:

- Se considera que el tiempo disponible para identificar y leer la posición objetivo en la hoja de movimientos es cinco veces más grande que el tiempo requerido para ello. El tiempo disponible para ejecutar acciones en un contexto de omisión de procedimientos también se considera cinco veces mayor que el tiempo requerido para realizarlas. De esta manera, se tiene en cuenta que la decisión de no utilizar procedimientos no viene condicionada por la presión temporal del contexto.
- Se considera que el tiempo disponible es nominal para el movimiento de elementos de combustible gastado sobre la piscina y para la ejecución de revisiones. El movimiento de elementos de combustible requiere mucho tiempo así que las revisiones se realizan lo más rápido posible para pasar al siguiente movimiento.
- La dificultad visual se introduce como elemento estresante. Se utiliza el nivel cualitativo Alto en todas las acciones realizadas en la piscina de combustible.
- La complejidad de las acciones es más elevada cuando los procedimientos no se utilizan. Por lo tanto, se selecciona el nivel cualitativo Moderadamente Complejo para las UAs que representan la ejecución de acciones sin utilizar procedimientos.
- Se desconoce el formato de la hoja de movimientos. En consecuencia, el PSF de ergonomía se mantiene en nominal.

L.3.2. HFE1.2: Seleccionar un elemento de combustible incorrecto

La tabla L.3 contiene los multiplicadores, y, por lo tanto, índica los niveles cualitativos, seleccionados para las UAs que forman el HFE1.2.

	PSFs					
UA ID	AT	Estrés	Complejidad	Procedimientos	Ergo/HMI	Aptitud
A	0,1	1	1	1	1	1
B	0,1	1	1	1	1	1
C	0,1	1	2	1	1	1
J	1	1	1	1	1	1
K	1	1	1	1	1	1
F	0,1	1	1	1	1	1
F'	0,1	1	1	1	1	1
G	0,1	1	1	1	1	1
G'	0,1	1	1	1	1	1
H	1	2	1	1	1	1
H'	1	2	1	1	1	1
I	1	2	2	1	1	1
I'	1	2	2	1	1	1

Tabla L.3: Multiplicadores de PSF para el evento HFE1.2.

Se detallan a continuación las razones por las cuales se han elegido multiplicadores diferentes a Nominal para algunas de las UAs del suceso HFE1.2:

- Se considera que el tiempo disponible para identificar y leer qué elemento de combustible se ha de trasladar en la hoja de movimientos es cinco veces más grande que el tiempo requerido para ello. El tiempo disponible para ejecutar acciones en un contexto de omisión de procedimientos también se considera cinco veces mayor que el tiempo requerido para realizarlas. De esta manera, se tiene en cuenta que la decisión de no utilizar procedimientos no viene condicionada por la presión temporal del contexto.
- Se considera que el tiempo disponible es nominal para el movimiento de elementos de combustible gastado sobre la piscina y para la ejecución de revisiones. El movimiento de elementos de combustible requiere mucho tiempo así que las revisiones se realizan lo más rápido posible para pasar al siguiente movimiento.
- La dificultad visual se introduce como elemento estresante. Se utiliza el nivel cualitativo Alto en todas las acciones realizadas en la piscina de combustible.
- La complejidad de las acciones es más elevada cuando los procedimientos no se utilizan. Por lo tanto, se selecciona el nivel cualitativo Moderadamente Complejo para las UAs que representan la ejecución de acciones sin utilizar procedimientos.
- Se desconoce el formato de la hoja de movimientos. En consecuencia, el PSF de ergonomía se mantiene en nominal.

L.3.3. HFE2.1: El contenedor cae debido a un fallo al anclaje del dispositivo de izado

La tabla L.4 contiene los multiplicadores, y, por lo tanto, índica los niveles cualitativos, seleccionados para las UAs que forman el HFE2.1.

	PSFs					
UA ID	AT	Estrés	Complejidad	Procedimientos	Ergo/HMI	Aptitud
A	1	1	1	1	1	1
F	1	1	1	1	1	1
G	1	1	1	1	1	1
H	1	1	1	1	10	1
I	1	1	2	1	10	1
L	1	2	1	1	1	1
L’	1	2	1	1	1	1
L”	1	2	1	1	1	1
L”’	1	2	1	1	1	1
M	10	1	1	1	0,5	1
M’	10	1	1	1	0,5	1
M”	10	1	1	1	0,5	1
M”’	10	1	1	1	0,5	1
N	1	1	2	1	1	1
O	1	1	5	1	1	1
P	1	2	1	1	1	5
P’	1	2	1	1	1	5
P”	1	2	1	1	1	5
P”’	1	2	1	1	1	5

Tabla L.4: Multiplicadores de PSF para el evento HFE2.1.

Se detallan a continuación las razones por las cuales se han elegido multiplicadores diferentes a Nominal para algunas de las UAs del suceso HFE2.1:

- Se utiliza el nivel cualitativo Aptitud degradada para introducir el concepto de pérdida (véase el anexo K). El concepto de pérdida hace referencia al hecho que las personas tienden a rechazar la existencia de un problema cuando escuchan o ven algo que no entienden. En el caso de la UA llamada P, los operarios oyen un ruido metálico y lo asocian al uso de maquinaria en otro lugar del edificio de combustible en lugar de pensar que se está desenganchando el contenedor.
- Se escoge el nivel Bueno para el PSF de ergonomía en la UA llamada M, fallo del operario de grúa a parar el movimiento. De esta manera se tiene en cuenta que la grúa puente del edificio de combustible ha sido mejorada recientemente, incluyendo el cambio del puesto de mando.
- Se escoge el nivel cualitativo Nominal para el PSF Tiempo disponible como valor de referencia porque la fase 2 está restringida temporalmente por el tiempo hasta ebullición. En esta fase, el agua que está en el interior del contenedor se calienta paulatinamente debido al calor producido por los elementos de combustible. Todas las acciones a realizar en esta fase han de terminar antes de que el agua del interior del contenedor entre en ebullición.
- Se escoge el nivel cualitativo Alto del PSF de elementos estresantes para la UA de error de comunicación con la intención de tener en cuenta las dificultades de comunicación existentes en el edificio de combustible.
- Se escoge el nivel cualitativo Tiempo disponible = tiempo necesario para la UA de fallo del operario de grúa a parar el movimiento porque el tiempo disponible para parar la grúa en caso de desenganche es corto. El nivel cualitativo de este PSF también tiene en cuenta posibles distracciones y el hecho que el operario de grúa tiene dificultades para ver el contenedor.

- Se utiliza el nivel cualitativo Pobre del PSF de ergonomía en la UA de fallo a ejecutar la revisión porque se ha de realizar bajo el agua mediante cámaras acuáticas.
- Se considera que realizar el anclaje sin seguir procedimientos es una operación más complicada que la nominal. En consecuencia, se selecciona el nivel Altamente complejo para la UA llamada O.

L.3.4. HFE3.1: Evento de *two-blocking*

La tabla L.5 contiene los multiplicadores, y, por lo tanto, índica los niveles cualitativos, seleccionados para las UAs que forman el HFE3.1.

	PSFs					
UA ID	AT	Estrés	Complejidad	Procedimientos	Ergo/HMI	Aptitud
L	1	2	1	1	1	1
Q	1	1	1	1	0,5	1
R	0,1	1	1	1	0,5	1

Tabla L.5: Multiplicadores de PSF para el evento HFE3.1.

Se detallan a continuación las razones por las cuales se han elegido multiplicadores diferentes a Nominal para algunas de las UAs del suceso HFE3.1:

- Se escoge el nivel cualitativo Alto del PSF de elementos estresantes para la UA de error de comunicación con la intención de tener en cuenta las dificultades de comunicación existentes en el edificio de combustible.
- Se utiliza el nivel cualitativo Bueno del PSF de ergonomía en las UAs relacionadas con operaciones de grúa con la intención de tener en cuenta que se han instalado nuevos controles y pantallas recientemente.
- Se escoge el nivel tiempo disponible = 5 veces el tiempo requerido para la UA de fallo del operario de grúa a parar el izado a tiempo (R). El tiempo disponible para realizar esta acción es de tres minutos, y el tiempo requerido para realizarla es de 2 segundos. No se ha escogido el nivel 50 veces superio para tener en cuenta posibles distracciones y el hecho que es posible que el operario de grúa no vea el contenedor.

L.3.5. HFE6.1: Fallo al anclaje que provoca la caída del MPC en el interior del HI-STORM 100

La tabla L.6 contiene los multiplicadores, y, por lo tanto, índica los niveles cualitativos, seleccionados para las UAs que forman el HFE6.1.

	PSFs					
UA ID	AT	Estrés	Complejidad	Procedimientos	Ergo/HMI	Aptitud
A	1	1	1	1	1	1
F	1	1	1	1	1	1
F'	1	1	1	1	1	1
F"	1	1	1	1	1	1
G	1	1	1	1	1	1
G'	1	1	1	1	1	1
G"	1	1	1	1	1	1
H	1	1	1	1	10	1
H'	1	1	1	1	1	1
H"	1	1	1	1	10	1
I	1	1	2	1	10	1
I'	1	1	2	1	1	1
I'	1	1	2	1	10	1
S	1	2	1	1	10	1
T	1	2	2	1	10	1
U	1	1	1	1	1	1
V	1	1	2	1	1	1
W	1	2	1	1	10	1
X	1	2	2	1	10	1

Tabla L.6: Multiplicadores de PSF para el evento HFE6.1.

Se detallan a continuación las razones por las cuales se han elegido multiplicadores diferentes a Nominal para algunas de las UAs del suceso HFE6.1:

- Se considera que el tiempo disponible es Nominal porque las UAs postuladas se ejecutan en la zona superior del contenedor MPC.
- Se utiliza el nivel Alto para el PSF de elementos estresantes con el objetivo de introducir la influencia de los altos niveles de temperatura y radiación en la zona de trabajo.
- Se escoge el nivel cualitativo Pobre del PSF de ergonomía para tener en cuenta que la zona en la que los operarios han de realizar las UAs es de espacio reducido.
- Se considera que la realización de anclajes sin seguir procedimientos es una tarea más compleja que su realización usando procedimientos. En consecuencia, se selecciona el nivel Moderadamente complejo del PSF Complejidad para las UAs relacionadas.

L.4. Cuantificación de HFEs

En el caso de la cuantificación de HFEs, el presente anexo contiene los siguientes ítems:

- Los cálculos realizados para estimar la componente cognitiva del fallo humano del modelo clásico.
- La justificación de los valores de probabilidad seleccionados para conformar la base de datos de fallo manual.
- Tablas con la probabilidad de ocurrencia de los caminos de fallo de los HFE no incluidos en la memoria de tesis.

L.4.1. Análisis del fallo cognitivo

L.4.1.1. Definición de tiempos

A continuación se definen los diferentes tiempos a considerar en el análisis del fallo cognitivo a realizar una acción:

- t_{d1}: tiempo disponible (nominal): máximo tiempo disponible para realizar la acción objeto de estudio.
- t_{mnom}: tiempo de acción manual (nominal): estimación del tiempo necesario para ejecutar la acción.
- $t_{1/2nom}$: tiempo de detección y diagnosis (nominal): estimación del tiempo necesario para detectar que algo va mal y para diagnosticar qué esta yendo mal.
- t_{mbasic}: tiempo de acción manual (básico): Estimación del tiempo, en minutos, necesario para ejecutar la acción alterado por los PSFs de HCR (k_1,k_2,k_3). La ecuación L.1 es la utilizada para introducir la influencia de los PSFs. Los PSFs de HCR se presentan en la figura L.12.

$$t_{mbasic} = t_{mnom} * (1 + k_1) * (1 + k_2) * (1 + k_3) \tag{L.1}$$

Operator experience (K_1)	
1. Expert, well trained	−0.22
2. Average knowledge training	0.00
3. Novice, minimum training	0.44
Stress level (K_2)	
1. Situation of grave emergency	0.44
2. Situation of potential emergency	0.28
3. Active, no emergency	0.00
4. Low activity	0.28
Quality of operator/plant interface (K_3)	
1. Excellent	−0.22
2. Good	0.00
3. Fair	0.44
4. Poor	0.78

Figura L.12: PSFs del método HCR. Fuente: [7]

- $t_{1/2basic}$: tiempo de detección y diagnosis (básico): Estimación del tiempo necesario para detectar y diagnosticar alterado por los PSFs de HCR. Se substituye t_{mnom} por $t_{1/2nom}$ en la ecuación L.1 para estimar $t_{1/2basic}$.

El tiempo disponible para diagnosticar la acción, es decir, el tiempo durante el cual el operario puede no reaccionar y, aún así, no se consideraría fallo cognitivo, se estima mediante la ecuación L.2. Si el operario

permanece inactivo o toma la decisión de actuar una vez superado este tiempo, siendo el origen temporal el inicio del evento, la acción no se podrá ejecutar a tiempo para corregir el curso de los eventos.

$$t_{d2} = t_{d1} - t_{mbasic} - t_{1/2basic} \tag{L.2}$$

La probabilidad de fallo cognitivo se calcula mediante la ecuación L.3. Se utilizan los tiempos t_{d2} y $t_{1/2basic}$. Los parámetros alfa, beta, y gamma se seleccionan según si la acción a realizar está basada en la habilidad, las reglas, o el conocimiento.

$$FP_{cog} = e^{-\left\{\frac{\frac{t_d}{t_{1/2}}-\gamma}{\alpha}\right\}^{\beta}} \tag{L.3}$$

L.4.1.2. Operario de grúa falla a parar el movimiento de HFE2.1 y HFE5.1

Se le ha comunicado al operador de grúa que ha de detener inmediatamente el izado del contenedor porque éste está a punto de caer debido a un anclaje defectuoso entre el yugo de alzamiento y el HI-TRAC. Los tiempos considerados son los siguientes:

- t_{d1}: Conservadoramente, se asume que pasan solo diez segundos entre la orden de parada y la caída del contenedor.
- t_{mnom}: Se tarda dos segundos en presionar el botón de parada de emergencia (localizar el botón con la vista y mover el brazo).
- $t_{1/2nom}$: Se considera que se tarda un solo segundo en entender que alguien te ordena detener la grúa.
- t_{mbasic}: 1,75 segundos (K_1 = -0,22, K_2 = 0,44, K_3 = -0,22).
- $t_{1/2basic}$: 0,876 segundos.
- t_{d2}: El valor final es 7,374 segundos.

Esta acción está basada en la habilidad. La FP_{cog} es:

$$FP_{cog} = e^{-\left\{\frac{\frac{t_d}{t_{1/2}}-\gamma}{\alpha}\right\}^{\beta}} = e^{\left\{\frac{\frac{7,374}{0,876}-0,7}{0,407}\right\}^{1,2}} = 1,47E-15 \tag{L.4}$$

L.4.1.3. El operario de grúa falla a parar el movimiento a tiempo de HFE3.1

El operario de grúa olvida o falla a parar el movimiento de izado del contenedor. Por lo tanto, el contenedor sigue ascendiendo y se acerca al gancho principal. El operario no ve el contenedor. Se da la posibilidad de *two-blocking*. Los tiempos considerados son los siguientes:

- t_{d1}: Si el contenedor se transporta a 0,5 m del suelo la distancia entre el extremo superior del contenedor y el raíl de la grúa puente es de ocho metros. Considerando que la altura de la grúa puente es de un metro, el contenedor ha de ascender siete metros antes de que ocurra el *two-block*. A la velocidad máxima de 1,54 m/min, se necesita que el contenedor ascienda durante 272 segundos para que golpee la grúa.

- t_{mnom}: Se tarda dos segundos en presionar el botón de parada de emergencia (localizar el botón con la vista y mover el brazo).
- $t_{1/2nom}$: Se considera que se tarda un solo segundo en entender que alguien te ordena detener la grúa.
- t_{mbasic}: 1,558 segundos (K_1 = -0,22, K_2 = 0,28, K_3 = -0,22).
- $t_{1/2basic}$: 0,779 segundos.
- t_{d2}: El valor final es 270,39 segundos.

Esta acción está basada en la habilidad. La FP_{cog} es:

$$FP_{cog} = e^{-\left\{\frac{\frac{t_d}{t_{1/2}}-\gamma}{\alpha}\right\}^{\beta}} = e^{\left\{\frac{\frac{270,39}{0,779}-0,7}{0,407}\right\}^{1,2}} = \varepsilon \tag{L.5}$$

L.4.1.4. El operario de grúa falla a parar el movimiento a tiempo de HFE5.2

El operario de grúa olvida o falla a parar el movimiento de izado del contenedor. Por lo tanto, el contenedor sigue ascendiendo y se acerca al gancho principal. El operario se centra en observar el extremo inferior del contenedor, pues lo ha de colocar sobre el HI-STORM. Se da la posibilidad de *two-blocking*. Los tiempos considerados son los siguientes:

- t_{d1}: El contenedor se alza hasta que queda por encima del HI-STORM. Se considera que el contenedor se alza hasta que su extremo inferior está a una altura de 6,1 m. En esta situación, el espacio libre entre el extremo superior del contenedor y el raíl de la grúa es de 2,66 m, lo que significa que el espacio libre entre el contenedor y el gancho principal es de 1,66 m. A la velocidad máxima de 1,54 m/min, se necesita que el contenedor ascienda durante 65 segundos para que golpee la grúa.
- t_{mnom}: Se tarda dos segundos en presionar el botón de parada de emergencia (localizar el botón con la vista y mover el brazo).
- $t_{1/2nom}$: Se considera que se tarda un solo segundo en entender que alguien te ordena detener la grúa.
- t_{mbasic}: 1,75 segundos (K_1 = -0,22, K_2 = 0,44, K_3 = -0,22).
- $t_{1/2basic}$: 0,876 segundos.
- t_{d2}: El valor final es 62,05 segundos.

Esta acción está basada en la habilidad. La FP_{cog} es:

$$FP_{cog} = e^{-\left\{\frac{\frac{t_d}{t_{1/2}}-\gamma}{\alpha}\right\}^{\beta}} = e^{\left\{\frac{\frac{62,05}{0,876}-0,7}{0,407}\right\}^{1,2}} = 2,56E-210 \tag{L.6}$$

L.4.2. Justificación de los valores de probabilidad seleccionados para formar la base de datos de fallo manual

En esta sección se repasan y se justifican uno a uno los valores de probabilidad seleccionados para representar la probabilidad de fallo manual de las UAs consideradas en el análisis de fiabilidad humana. Se proporciona, para cada valor, la mediana de la probabilidad de fallo y el factor de error, entre paréntesis, si no se indica lo contrario.

L.4.2.1. Omisión del uso de procedimientos

Se podrían utilizar tres elementos de la tabla 20-6 anexa al NUREG/CR-1278:

- Ítem 1: Fallo a llevar a cabo una política o una tarea planificada como, por ejemplo, un test periódico o un mantenimiento semanal. Probabilidad: 0,01(5).
- Ítem 3: Fallo a utilizar procedimientos de operación escritos en:
  - Condiciones normales de operación. Probabilidad: 0,01(3).
  - Condiciones anormales de operación. Probabilidad: 0,005(10).

En el documento SHED, por otra parte, se propone utilizar un valor nominal promedio de 5,0E-03(10) para la probabilidad de fallo a utilizar procedimientos en circunstancias normales.

Se considera que el valor presente en SHED es el que mejor se adecua al caso de estudio. De hecho, el valor de SHED es el resultado de modificarlos ítems del NUREG/CR-1278 teniendo en cuenta que el procedimiento a utilizar no está relacionado con operaciones de reactor. El valor de SHED se utiliza para representar la probabilidad de fallo a utilizar procedimientos tanto en el contexto nominal como en los EFCs.

L.4.2.2. Fallo a seleccionar la posición objetivo en la hoja de movimientos

La tabla 20-6 del NUREG/CR-1278 propone una probabilidad de fallo de 0,5(5) al utilizar una lista de control correctamente. Este ítem valora la posibilidad de no utilizar la lista, y no representa la probabilidad de cometer un error al utilizarla.

En SHED se presenta una acción que nombran como Lectura incorrecta. Descomponen esta acción en dos, un error de comisión y un error de omisión. La probabilidad de ocurrencia del error de comisión viene del ítem 5 de la tabla 20-10 del NUREG/CR-1278. El valor de probabilidad del error de comisión es 1,02E-02(3). La probabilidad de ocurrencia del error de omisión proviene del ítem 2 de la tabla 20-7 del NUREG/CR-1278. El valor de probabilidad del error de omisión es 3,03E-03(3). SHED obtiene el valor de probabilidad deseado sumando ambos valores presentados, dando como resultado una probabilidad de 1,30E-02(3). Se utiliza este valor para representar la probabilidad de fallo manual de esta UA tanto si se usan procedimientos como si no[3].

L.4.2.3. Fallo a seleccionar la posición correcta en la que colocar el elemento de combustible

Se asume que el operario de grúa percibe las posiciones de la piscina de combustible gastado como un operador de sala de control percibe grupos de *displays* para poder obtener un valor de probabilidad de fallo de esta UA. Por lo tanto, se utilizan los datos de la tabla 20-9 del NUREG/CR-1278 *Estimated probabilities of errors in selecting unannunciated displays for quantitative or qualitative readings*. Concretamente, se selecciona el ítem 4: *from an array of similar-appearing displays identified by labels only*. El valor de probabilidad de fallo seleccionada es 3,0E-03(3). Se modifican los PSFs asociados a la UA para modelar la omisión en el uso de procedimientos.

L.4.2.4. Omisión de la revisión

La tabla 20-7 del NUREG/CR-1278 se puede utilizar para proporcionar probabilidades de omisión de un paso escrito en un procedimiento. El ítem 1 proporciona la probabilidad de fallo cuando se utiliza el procedimiento. El valor de probabilidad del ítem 1 es 1,0E-03(3). El ítem 5 proporciona la probabilidad de fallo cuando no se utiliza el procedimiento. El valor de probabilidad del ítem 5 es 5,0E-02(5).

[3] Se modifican los multiplicadores de los PSF para representar la situación en la que se omite el uso de procedimientos.

L.4.2.5. Fallo a ejecutar la revisión

El documento SHED recomienda utilizar la tabla 20-22 del NUREG/CR-1278 *Estimated probabilities that a checker will fail to detect errors made by others* para valorar la probabilidad de fallo a ejecutar una revisión. Específicamente, SHED recomienda utilizar el ítem 3 *checker checking an action in which he is not an active participant will be alerted.* El valor de probabilidad del ítem 3 es 5,0E-02(5). Este valor de probabilidad se utiliza para todas las UAs de fallo a ejecutar una revisión, a excepción de las relacionadas con la revisión del anclaje entre el dispositivo de bloqueo de izado y la MPC, y la revisión del anclaje entre el dispositivo de bloqueo de izado y su adaptador. Se utiliza el ítem 9, *Checking the status of equipment if that status affects one's safety when performing its tasks*, para valorar la probabilidad de fallar al realizar los anclajes mencionados. Se considera que el ítem 9 es el adecuado porque los anclajes son críticos para la correcta, y segura, introducción del MPC en el HI-STORM. Los revisores han de llevar a cabo la revisión de estos anclajes con todo el cuidado posible. El valor de probabilidad del ítem 9 es 3,0E-03(3). Se modifican los PSFs de estas UAs para modelar el fallo a ejecutar la revisión cuando se omite el uso de procedimientos.

L.4.2.6. Fallo a colocar la herramienta de brazo largo encima de la posición objetivo

Aplica el mismo análisis que para la UA de fallo a seleccionar la posición correcta en la que colocar el elemento de combustible, sección L.4.2.3 anterior.

L.4.2.7. Error de comunicación

El documento SHED recomienda utilizar la tabla 20-8 del NUREG/CR-1278 *Estimated probabilities of error in recalling oral instruction items not written down*, aunque no es lo mismo que un malentendido. En el caso de estudio solo se ha de entender una palabra, *Stop*. En consecuencia, se utiliza el ítem 1c de la tabla 20-8. El valor de probabilidad proporcionado por el ítem 1c es 1,0E-03(3). Las dificultades de comunicación producto del ambiente ruidoso en el que se realizan las operaciones, o producto de la falta de contacto visual, se tienen en cuenta en forma de PSFs.

L.4.2.8. El operario de grúa falla a parar el movimiento a tiempo

El ítem de SHED que valora el fallo al seleccionar un control o una válvula fuera de sala de control puede utilizarse para este tipo de UAs porque incluye operar incorrectamente un control fuera de control cuando se pide su actuación. La acción postulada en SHED está compuesta de un error de omisión y un error de comisión. Utiliza ítems de las tablas 20-12, 20-13, 20-14, y 20-15 del NUREG/CR-1278. El valor nominal promedio sugerido por SHED es 1,0E-02(5).

Sin embargo, se considera que en este caso es más adecuado utilizar un único valor de las tablas del NUREG/CR-1278. Concretamente, se sugiere utilizar el ítem 11 de la tabla 20-12. Este ítem proporciona la probabilidad de seleccionar un interruptor incorrecto de entre un grupo densamente poblado de interruptores que solo están marcados con etiquetas. Este ítem describe con cierta precisión la situación en la que se encuentra el botón de parada de emergencia en la cabina de control principal de la grúa. El valor de probabilidad del ítem 11 de la tabla 20-12 es 5,0E-03(3).

L.4.2.9. Fallo a anclar

Esta UA incluye el fallo a anclar el dispositivo de bloqueo de izado a la tapa del MPC, el fallo a anclar el adaptador del dispositivo de bloqueo de izado con el gancho principal de la grúa, y el fallo a anclar el

dispositivo de bloqueo de izado con el adaptador. Si es necesario, se puede diferenciar entre ellos mediante PSFs.

El documento EEG-74 utiliza el ítem 13 de la tabla 20-12 del NUREG/CR-1278, *Improperly mate a connector, including failure to test the locking feature for engagement*, para modelar el fallo a ejecutar correctamente el anclaje entre dos dispositivos. El valor de probabilidad de este ítem es 3,0E-03(3).

L.4.2.10. Fallo a darse cuenta de la existencia de un sonido chirriante

El documento SHED presenta un ítem similar al fallo a darse cuenta de la existencia de un sonido chirriante: el fallo a responder a una señal apremiante. Es similar porque una señal apremiante puede ser una alarma sonora. SHED obtiene la probabilidad de este ítem de la tabla 20-23 del NUREG/CR-1278. El documento SHED presenta tres valores, uno bajo, uno nominal, y uno alto, dependiendo de la cantidad de señales apremiantes en paralelo. Se escoge el valor nominal para el caso de estudio porque los operarios pueden estar realizando otras tareas que atraigan su atención y rivalicen con el sonido chirriante. El valor de probabilidad promedio nominal proporcionado por SHED es 1,0E-02(5). Este valor se utiliza en los tres escenarios en los que se postula esta UA.

L.4.2.11. El operario de grúa falla a parar el movimiento

Esta UA no es una omisión de un procedimiento porque el procedimiento no específica la altura máxima a la cual se puede trasladar el contenedor. Esta UA describe la situación en la que el operador deja el *joystick* de mando en una posición activa sin darse cuenta. El ítem 10 de la tabla 20-10 del NUREG/CR-1278 describe una situación similar: *failure to complete a change of state of a component if switch must be held until change is completed*. El valor de probabilidad del ítem 10 de la tabla 20-10 es 3,0E-03(3). Este valor se utiliza en todos los escenarios en los que se postula esta UA.

L.4.2.12. Revisión de supervisor

La revisión de supervisor es una acción de recuperación. Se escoge el ítem *Supervisor verification error* postulado en el documento SHED para representar a esta acción. Se explicita, en la descripción del ítem mencionado, que la dependencia es la principal influencia sobre la probabilidad de ocurrencia de este ítem. Cuanto más distraído esté el supervisor, más depende de que los operarios realicen correctamente la tarea a revisar y mayor es la probabilidad de que la revisión sea incorrecta. El documento SHED propone una probabilidad de fallo nominal promedio de 3,1E-1(5) para el ítem en cuestión. Se considera que este valor es muy alto en el marco de una campaña de carga porque las configuraciones a revisar son importantes para la seguridad. Los supervisores estarán en un estado de alerta mayor que el que describe el valor nominal propuesto en SHED. En consecuencia, se escoge el valor de probabilidad bajo propuesto en el SHED, de valor promedio 1,6E-01(5).

L.4.2.13. Medida de la dosis de radiación

La medida de dosis de radiación es una acción de recuperación. Se utiliza la tabla 20-3 del NUREG/CR-1278, *Nominal model of estimated HEPs and EFs for diagnosis within time T by control room personnel of abnormal events annunciated closely in time*, para modelar el fallo del personal de protección de la radiación a diagnosticar que la dosis es más alta de lo esperado. Se asume que el personal de protección de la radiación y el personal de sala de control tienen comportamientos similares. Se escoge el ítem 4 de la tabla 20-3 para representar la probabilidad de fallo de la acción en cuestión por dos razones. En primer lugar, porque específicamente representa sucesos individuales, como, por ejemplo, aquel en el que la dosis exterior de un contenedor es más alta de lo esperado. En segundo lugar, porque el tiempo disponible para

diagnosticar es treinta minutos, que es probable que sea el tiempo necesario para trasladar el contenedor desde el pozo del contenedor hasta la zona de descontaminación. El valor de probabilidad de este ítem es 1,0E-03(10).

L.5. Cuantificación de probabilidades de eventos de fallo humano

Las siguientes tablas contienen la probabilidad de ocurrencia de los caminos de fallo y la probabilidad de fallo humano de cada uno de los eventos de fallo humano estudiados en el análisis. No se tiene en cuenta el potencial de recuperación.

Camino de fallo	Nominal	EFC1	EFC2	EFC3	EFC4
F1	2,06E-07	9,86E-05	2,06E-07	1,02E-06	2,07E-09
F2	2,46E-04	4,80E-03	2,46E-04	3,82E-03	2,89E-07
F3	9,34E-07	1,12E-04	9,34E-07	4,53E-06	9,42E-10
F4	1,11E-03	5,46E-03	1,11E-03	1,69E-02	1,32E-07
F5	1,44E-08	2,39E-04	1,44E-08	1,71E-06	1,46E-11
F6	2,13E-07	1,29E-04	2,13E-07	1,25E-05	2,90E-11
F7	6,48E-08	2,71E-04	6,48E-08	7,38E-06	6,63E-12
F8	1,92E-06	2,89E-04	1,92E-06	1,07E-04	2,64E-11
Supervisor	1,87E-02	2,76E-01	1,87E-02	1,01E-01	1,90E-03
PR	2,67E-04	5,31E-03	2,67E-04	6,67E-04	2,67E-05
HEP	**6,81E-09**	**1,67E-05**	**6,81E-09**	**1,41E-06**	**2,15E-14**

Tabla L.7: Probabilidad de ocurrencia del evento de fallo humano HFE1.1

Camino de fallo	Nominal	EFC1	EFC2	EFC3	EFC4
F1	2,06E-07	9,86E-05	2,06E-07	1,02E-06	2,07E-09
F2	2,46E-04	4,80E-03	2,46E-04	3,82E-03	2,89E-07
F3	4,69E-07	4,53E-05	4,69E-07	2,31E-06	4,71E-10
F4	5,60E-04	2,21E-03	5,60E-04	8,61E-03	6,59E-08
F5	1,44E-08	2,39E-04	1,44E-08	1,71E-06	1,46E-11
F6	4,26E-07	2,55E-04	4,26E-07	2,49E-05	5,80E-11
F7	1,64E-08	5,59E-05	1,64E-08	1,95E-06	1,66E-12
F8	4,85E-07	5,59E-05	4,85E-07	2,83E-05	6,61E-12
Supervisor	1,87E-02	2,76E-01	1,87E-02	1,01E-01	1,90E-03
RP	2,67E-04	5,31E-03	2,67E-04	6,67E-04	2,67E-05
HEP	**4,03E-09**	**1,14E-05**	**4,03E-09**	**8,41E-07**	**1,82E-14**

Tabla L.8: Probabilidad de ocurrencia del evento de fallo humano HFE1.2

Camino de fallo	Nominal	EFC1	EFC2	EFC3	EFC4
F1	8,52E-07	8,25E-06	8,52E-07	2,20E-07	6,57E-10
F2	2,11E-08	2,04E-07	2,11E-08	5,44E-09	1,62E-11
F3	2,57E-07	2,48E-06	2,57E-07	3,17E-07	1,85E-10
F4	3,18E-04	8,40E-04	3,18E-04	1,21E-04	1,35E-06
F5	7,87E-06	2,08E-05	7,87E-06	2,99E-06	3,31E-08
F6	9,58E-05	2,53E-04	9,58E-05	1,74E-04	3,80E-07
F7	6,84E-07	2,49E-05	6,84E-07	1,61E-05	5,78E-12
F8	1,69E-08	6,15E-07	1,69E-08	4,00E-07	1,42E-13
F9	2,06E-07	7,49E-06	2,06E-07	2,33E-05	1,63E-12
F10	4,96E-06	4,41E-05	4,96E-06	3,00E-05	3,30E-10
F11	1,23E-07	1,09E-06	1,23E-07	7,42E-07	8,11E-12
F12	1,49E-06	1,33E-05	1,49E-06	4,32E-05	9,30E-11
Supervisor	1,60E-01	2,76E-01	1,60E-01	8,70E-02	5,68E-03
HEP	**6,89E-05**	**3,36E-04**	**6,89E-05**	**3,58E-05**	**1,00E-08**

Tabla L.9: Probabilidad de ocurrencia del evento de fallo humano HFE2.1

Camino de fallo	Nominal	EFC1	EFC2	EFC3	EFC4
F1	4,69E-06	9,36E-06	4,69E-06	5,85E-06	4,18E-05
F2	5,89E-07	1,18E-06	5,89E-07	3,67E-06	5,25E-06
HEP	**5,28E-06**	**1,05E-05**	**5,28E-06**	**9,53E-06**	**4,71E-05**

Tabla L.10: Probabilidad de ocurrencia del evento de fallo humano HFE3.1

Camino de fallo	Nominal	EFC1	EFC2	EFC3	EFC4
F1	8,57E-08	8,25E-06	8,57E-08	2,25E-08	6,57E-10
F2	2,12E-09	2,04E-07	2,12E-09	5,57E-10	1,62E-11
F3	2,58E-08	2,48E-06	2,58E-08	3,24E-08	1,85E-10
F4	5,53E-05	1,97E-04	5,53E-05	3,24E-05	1,38E-07
F5	1,37E-06	4,87E-06	1,37E-06	8,01E-07	3,39E-09
F6	1,66E-05	5,93E-05	1,66E-05	4,66E-05	3,89E-08
F7	7,41E-09	2,49E-05	7,41E-09	2,28E-07	5,78E-12
F8	1,83E-10	6,15E-07	1,83E-10	5,63E-09	1,42E-13
F9	2,23E-09	7,49E-06	2,23E-09	3,28E-07	1,63E-12
F10	1,26E-07	1,47E-05	1,26E-07	1,58E-06	3,45E-11
F11	3,11E-09	3,64E-07	3,11E-09	3,91E-08	8,49E-13
F12	3,79E-08	4,43E-06	3,79E-08	2,28E-06	9,74E-12
Supervisor	1,60E-01	2,76E-01	1,60E-01	3,23E-01	5,68E-03
HEP	**1,18E-05**	**8,95E-05**	**1,18E-05**	**2,72E-05**	**1,03E-09**

Tabla L.11: Probabilidad de ocurrencia del evento de fallo humano HFE5.1

Camino de fallo	Nominal	EFC1	EFC2	EFC3	EFC4
F1	8,71E-05	7,94E-04	5,34E-04	4,42E-05	2,31E-06
F2	1,11E-03	3,97E-03	1,04E-01	1,37E-03	8,52E-03
F3	4,66E-06	9,00E-05	4,66E-06	2,29E-06	1,41E-09
F4	3,01E-04	2,15E-03	3,01E-04	3,29E-04	2,96E-07
F5	8,71E-05	7,94E-04	5,34E-04	4,42E-05	2,31E-06
F6	1,11E-03	3,97E-03	1,04E-01	1,37E-03	8,52E-03
F7	5,28E-05	1,73E-03	2,42E-04	2,04E-03	1,37E-08
F8	1,88E-05	2,39E-04	1,08E-03	3,48E-04	1,38E-06
F9	3,01E-06	2,19E-04	3,01E-06	1,38E-04	9,95E-12
F10	5,13E-06	1,29E-04	5,13E-06	9,60E-05	5,94E-11
F11	5,28E-05	1,73E-03	2,42E-04	2,04E-03	1,37E-08
F12	1,88E-05	2,39E-04	1,08E-03	3,48E-04	1,38E-06
Supervisor	1,60E-01	4,32E-01	6,56E-01	1,83E-01	3,64E-01
HEP	**4,55E-04**	**6,94E-03**	**1,39E-01**	**1,50E-03**	**6,20E-03**

Tabla L.12: Probabilidad de ocurrencia del evento de fallo humano HFE6.1

Apéndice M

Parámetros de fallo de los componentes de la grúa puente

Las siguientes tablas contienen los parámetros de fallo de componentes de grúa puente utilizados en el modelo de árbol de fallos de los sucesos iniciadores del APS en fase II. Los parámetros de fallo utilizados han sido extraídos del documento *Probability Risk Assessment of Bolted Storage Casks. Updated Quantification and Analysis Report* de EPRI. Los parámetros de fallo introducidos son valores puntuales. Por lo tanto, no están asociados a ninguna distribución estadística de probabilidad.

Descripción	Media	Modelo
Fallo del freno #1	1,00E-05	Probabilidad
Fallo del freno #2	1,00E-05	Probabilidad
Fallo de causa común de los frenos mecánicos	8,00E-07	Probabilidad
Fallo de causa común de cables	2,00E-06	Probabilidad
Fallo catastrófico del gancho principal	2,00E-09	Probabilidad
Fallo del eje de la caja de cambios	2,00E-07	Probabilidad
Rotura de engranaje de la caja de cambios	1,00E-06	Probabilidad
Fallo del soporte del tambor de la caja de cambios	4,00E-08	Probabilidad
Rotura por cizallamiento del freno del eje de la caja de cambios	8,00E-07	Probabilidad
Rotura por cizallamiento del freno de la caja de cambios	2,00E-07	Probabilidad
Fallo del acoplamiento del tambor de la caja de cambios	2,00E-07	Probabilidad
Caída de la carga debido a un fallo estructural	1,00E-09	Probabilidad
Rotura del cable #1	2,00E-06	Probabilidad
Rotura del cable #2	2,00E-06	Probabilidad
Rotura de la cuerda del tambor de la grúa por desenhebrado	4,00E-08	Probabilidad

Tabla M.1: Parámetros de fallo de los componentes de la grúa puente (1).

Descripción	Media	Modelo
Fallo del final de carrera #1	1,25E-04	Probabilidad
Fallo del final de carrera #2	1,25E-04	Probabilidad
Fallo de causa común de los finales de carrera	6,00E-06	Probabilidad
Rotura mecánica del freno #1	1,00E-05	Probabilidad
Rotura mecánica del freno #2	1,00E-05	Probabilidad
Fallo de causa común de los frenos	8,00E-07	Probabilidad
Rotura del acoplamiento del motor	1,00E-05	Probabilidad
Rotura del freno del eje	1,00E-05	Probabilidad
Fallo del final de carrera de seguridad #1	1,25E-04	Probabilidad
Fallo del final de carrera de seguridad #2	1,25E-04	Probabilidad
Fallo de causa común de los finales de carrera de seguridad	6,00E-06	Probabilidad
Rotura por cizallamiento del freno del eje	2,00E-07	Probabilidad

Tabla M.2: Parámetros de fallo de los componentes de la grúa puente (2).

Apéndice N

Árboles de fallo de los sucesos iniciadores

El siguiente anexo presenta los árboles de fallo creados para obtener la frecuencia de ocurrencia de los sucesos iniciadores de la etapa de carga postulados en el modelo APS en fase II. En dichos árboles de fallo se introduce tanto el fallo humano como el fallo de la grúa puente del edificio de combustible.

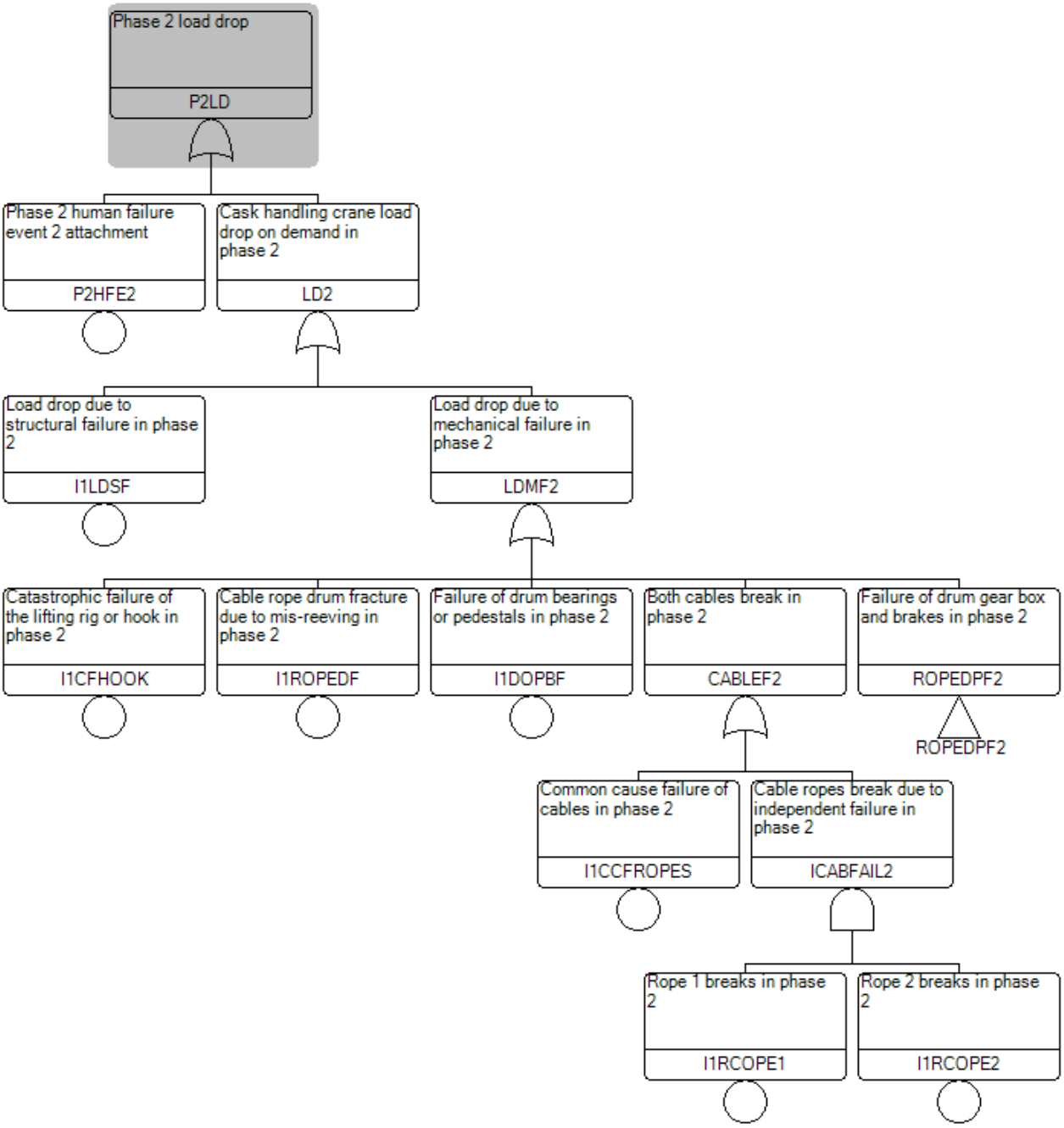


Figura N.1: Árbol de fallos del suceso iniciador LDP2.

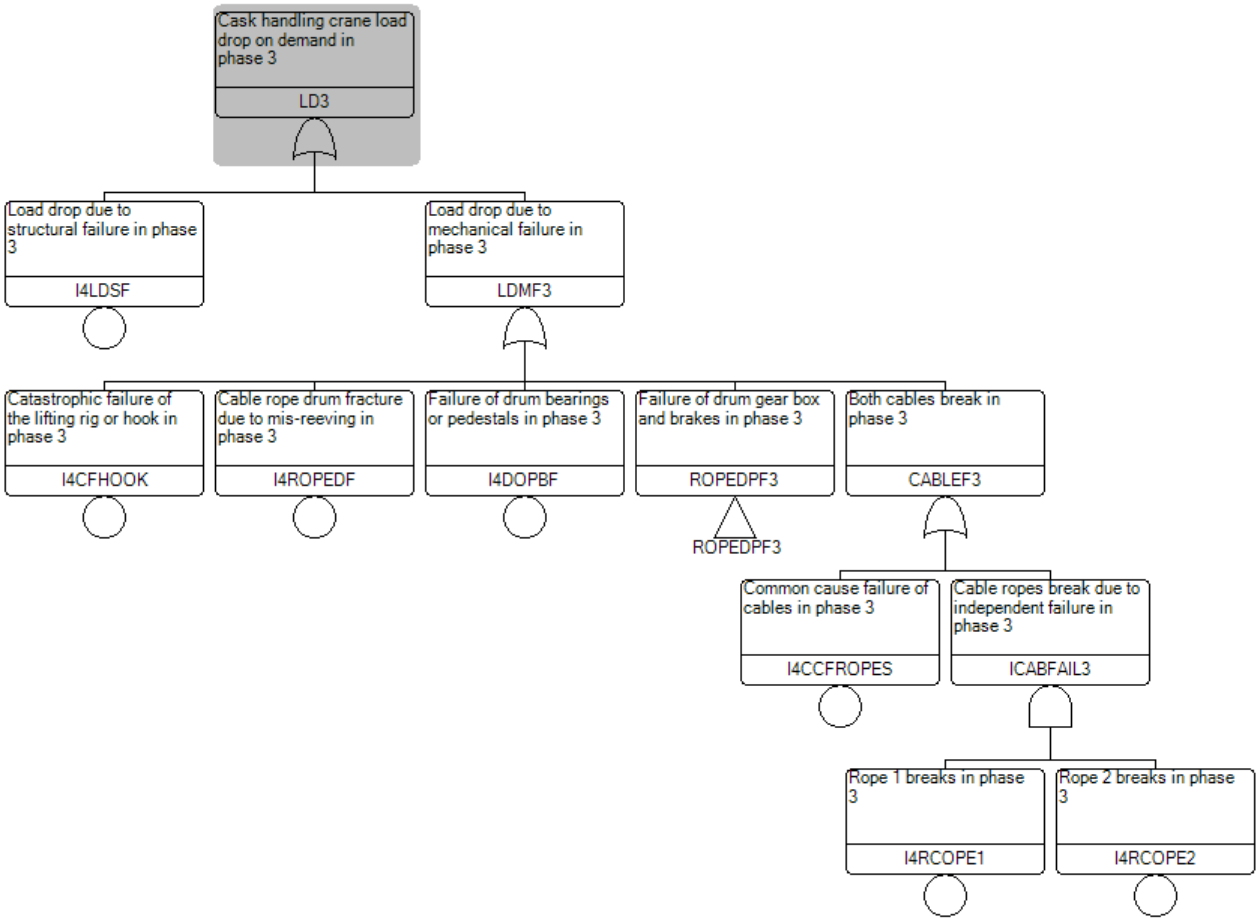


Figura N.2: Árbol de fallos del suceso iniciador LDP3.

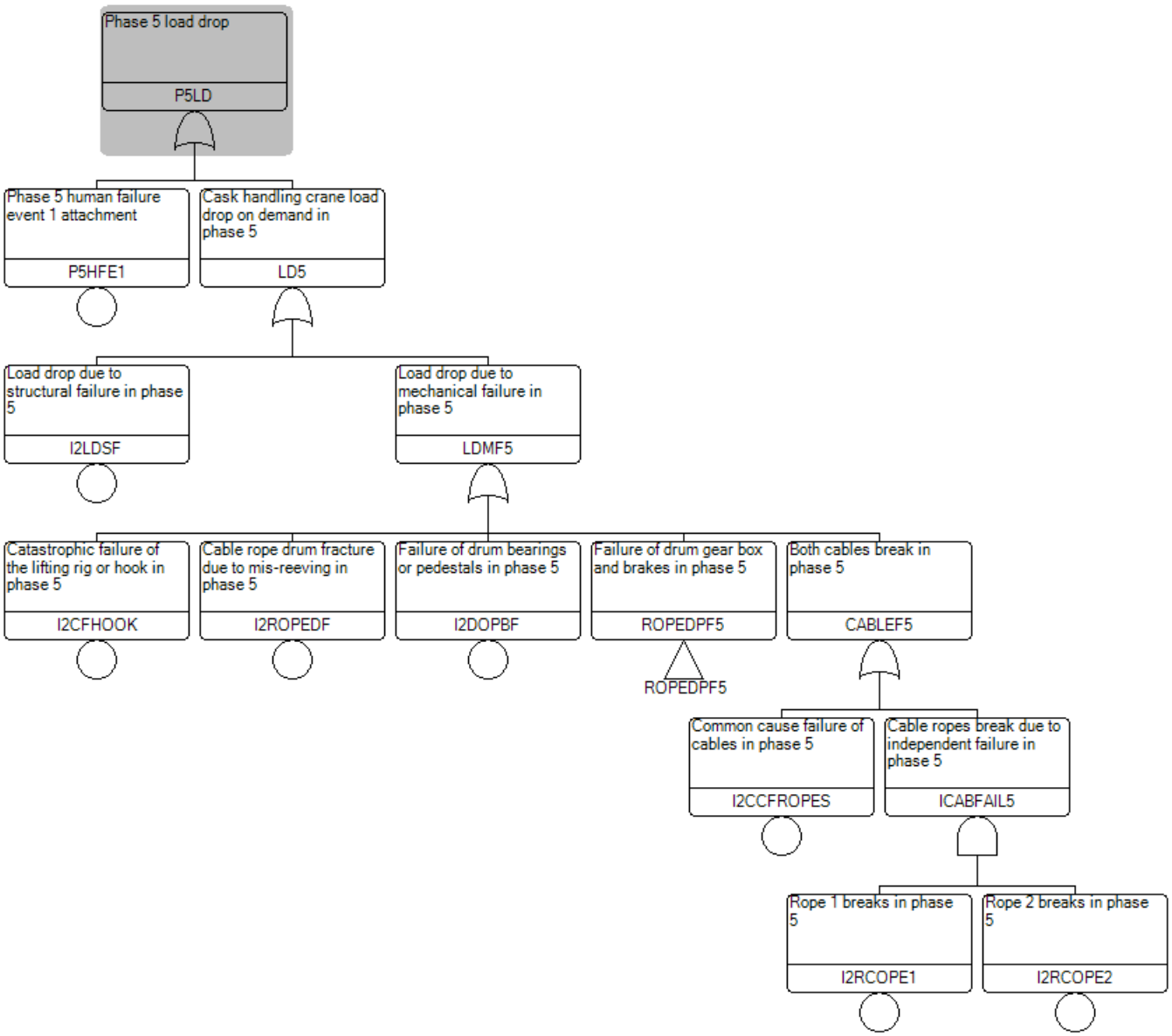


Figura N.3: Árbol de fallos del suceso iniciador LDP5.

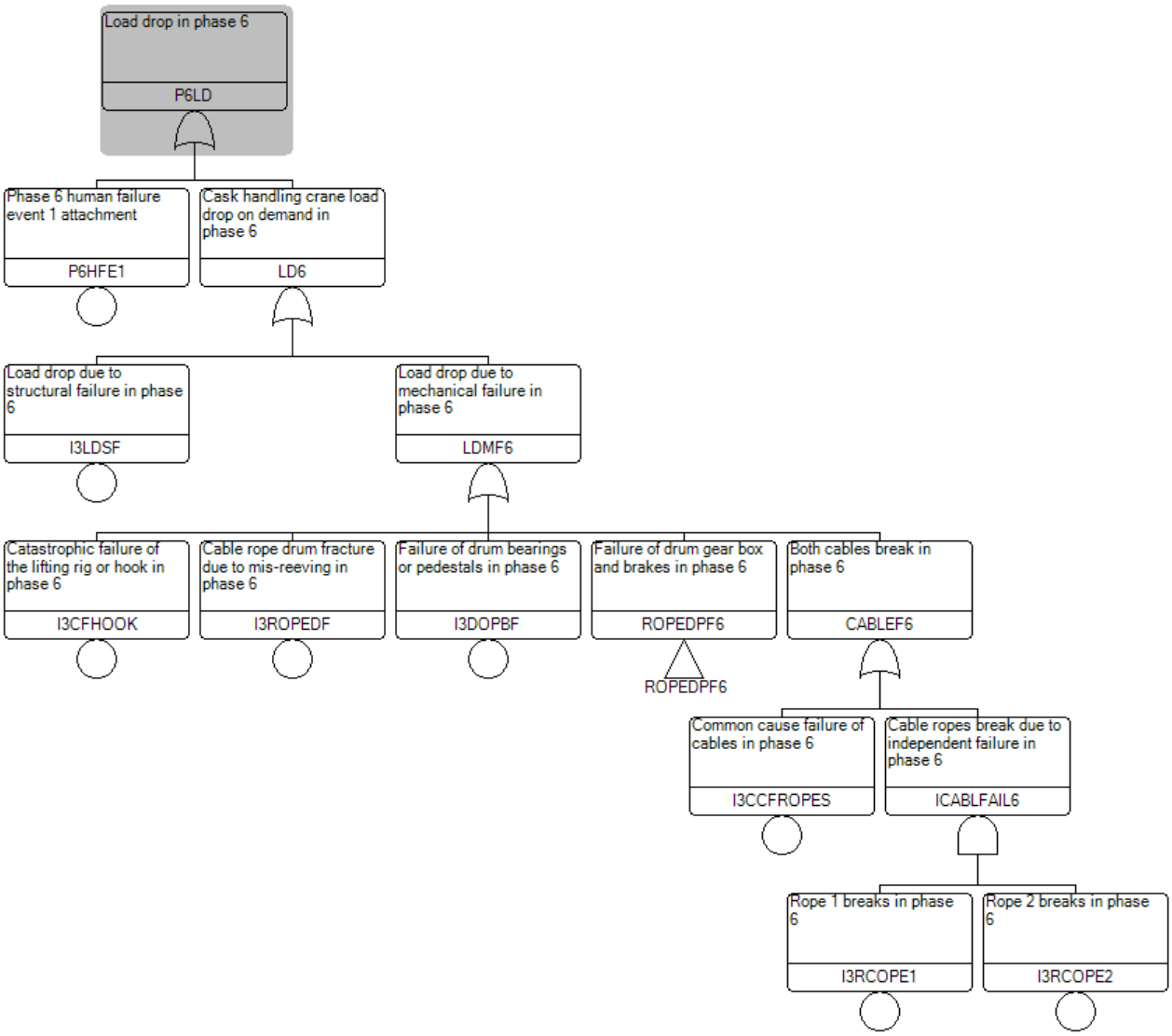
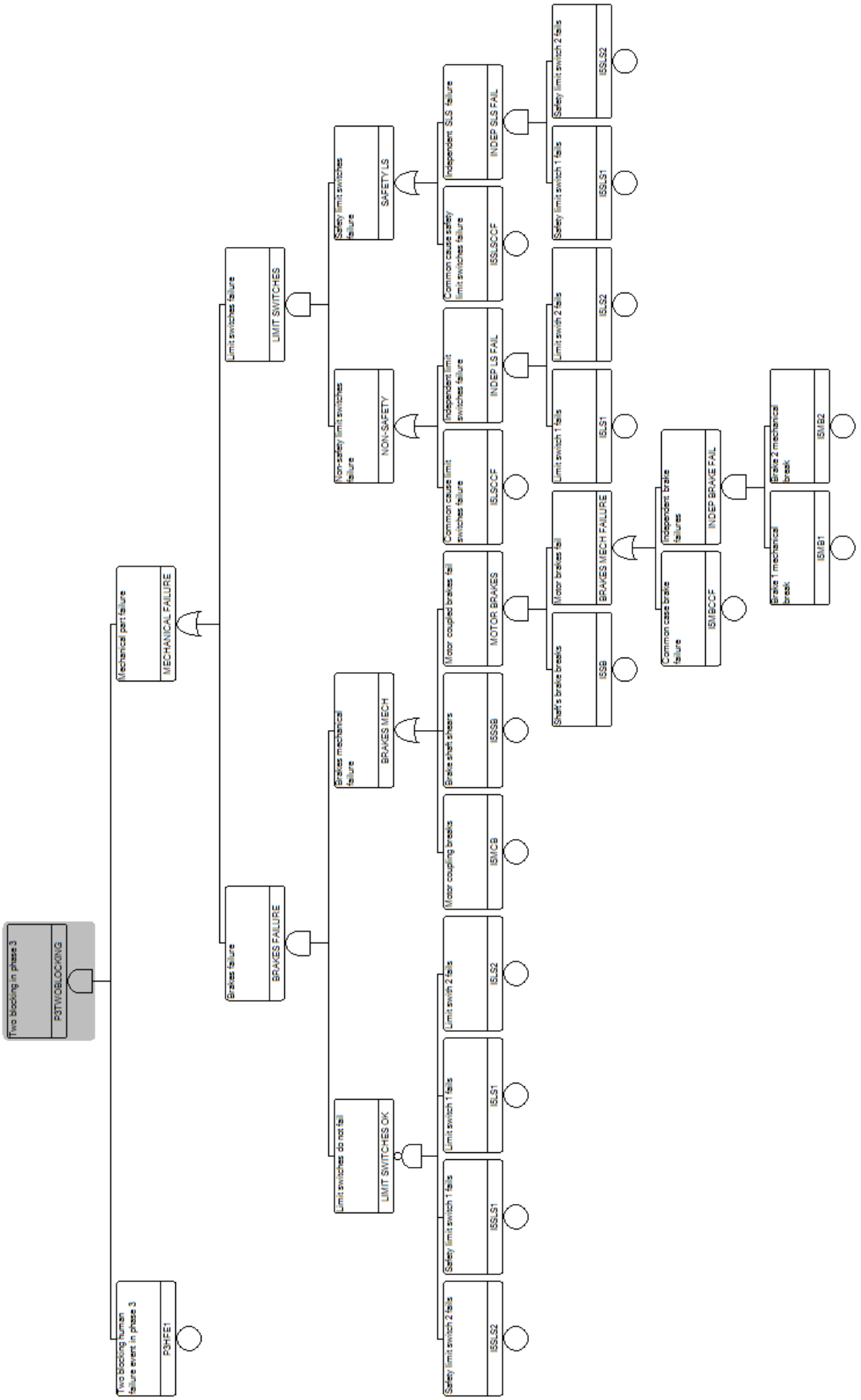


Figura N.4: Árbol de fallos del suceso iniciador LDP6.


Two blocking in phase 3
P3TWOBLOCKING
Two blocking human failure event in phase 3
P3HFE1
Mechanical part failure
MECHANICAL FAILURE
Brakes failure
BRAKES FAILURE
Limit switches failure
LIMIT SWITCHES
Brakes mechanical failure
BRAKES MECH
Limit switches do not fail
LIMIT SWITCHES OK
Safety limit switch 2 fails
ISSLS2
Safety limit switch 1 fails
ISSLS1
Limit switch 1 fails
ISLS1
Limit swith 2 fails
ISLS2
Motor coupling breaks
ISMCB
Brake shaft shears
ISSSB
Motor coupled brakes fail
MOTOR BRAKES
Shaft's brake breaks
ISSB
Motor brakes fail
BRAKES MECH FAILURE
Common cause limit switches failure
ISLSCCF
Independent limit switches failure
INDEP LS FAIL
Non-safety limit switches failure
NON-SAFETY
Safety limit switches failure
SAFETY LS
Common cause safety limit switches failure
ISSLSCCF
Independent SLS failure
INDEP SLS FAIL
Safety limit switch 2 fails
ISSLS2
Safety limit switch 1 fails
ISSLS1
Limit swith 2 fails
ISLS2
Limit switch 1 fails
ISLS1
Common case brake failure
ISMBCCF
Independent brake failures
INDEP BRAKE FAIL
Brake 1 mechanical break
ISMB1
Brake 2 mechanical break
ISMB2

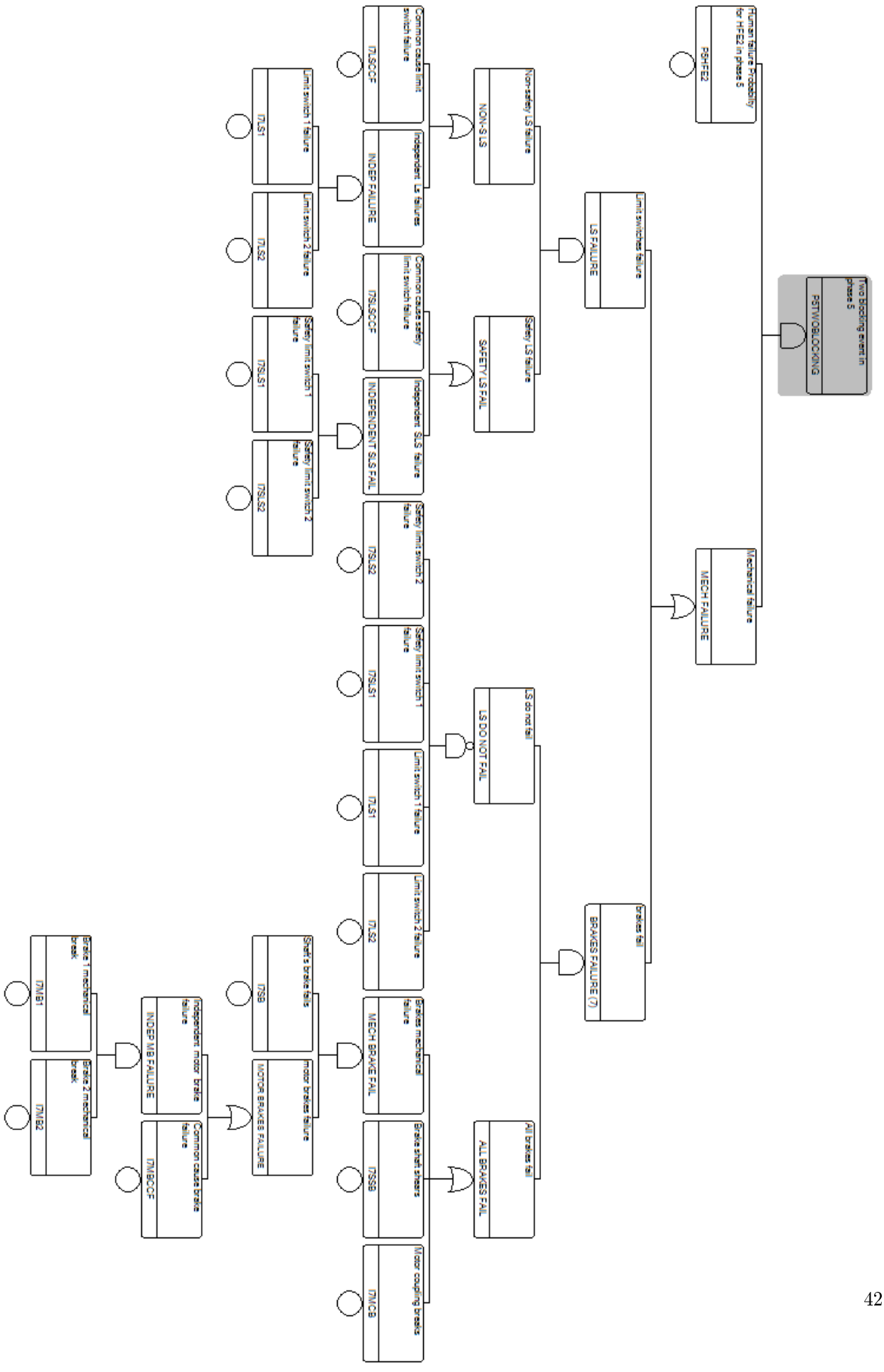


Figura N.6: Árbol de fallos del suceso iniciador TBP5.

Apéndice Ñ

Análisis de importancia

El objeto de este tipo de análisis es la obtención de las distintas medidas de importancia que facilitan la interpretación de los resultados obtenidos en la tarea de cuantificación. A continuación se describen las diferentes medidas de importancia proporcionadas por *RiskSpectrum® PSA*.

La medida de importancia de Fussell-Vesely de un suceso básico (o conjunto mínimo de fallo) se calcula como el cociente entre la frecuencia de la ecuación de referencia menos la frecuencia que tendría la misma si se asignase cero a la probabilidad del suceso (o conjunto mínimo de fallo), dividido por la frecuencia de la ecuación de referencia. Los valores que adopta esta medida de importancia van de cero a uno y puede interpretarse como la contribución del suceso o conjunto mínimo de fallo a la frecuencia de la ecuación de referencia, expresada en tanto por uno.

La medida de importancia del Reducción de Riesgo *Risk Reduction Worth (Risk decrease factor* (RDF) en *RiskSpectrum PSA®*) se obtiene haciendo el cociente entre la frecuencia de la ecuación de referencia y la que se obtendría al asignar cero a un suceso básico. Adopta valores entre uno e infinito. Se interpreta como el número por el que se dividiría la frecuencia de la ecuación si desapareciese (probabilidad cero) el suceso básico. El concepto es equivalente al de FV, aunque la expresión matemática sea diferente; así, a un suceso con FV igual a uno le corresponderá una RR infinito (lo que indica que dicho suceso está contenido en todos los conjuntos de la ecuación), mientras que si FV valiese cero RR valdría uno (que sería el hipotético caso de un suceso que no estuviese contenido en la ecuación).

La medida de importancia de Incremento del Riesgo *Risk Achievement Worth* (Risk increase factor (RIF) en *RiskSpectrum PSA®*) se calcula como la frecuencia que adoptaría la ecuación si se asignase el valor uno de probabilidad a un suceso (suceso seguro) dividida por la frecuencia de la ecuación de referencia. Al igual que RR, adopta valores entre uno e infinito, pero el concepto es el opuesto. Se puede interpretar como el factor por el que habría que multiplicar la frecuencia de la ecuación de referencia si el suceso fuese cierto.

En las siguientes tablas se presentan los sucesos básicos más significativos, según las medidas de importancia obtenidas mediante *RiskSpectrum® PSA*, de las ecuaciones booleanas de cada suceso iniciador. Se presentan en el mismo anexo los resultados de la fase I y los de la fase II.

Ñ.1. Análisis de importancia del modelo APS fase I

Suceso básico	Probabilidad	FV	RDF	RIF
CAÍDA	5,60E-05	1,00E+00	9,99E+99	9,99E+99
MPC1	4,03E-07	1,00E+00	9,99E+99	2,48E+06
1M9GDA38BM	7,79E-03	2,42E-01	1,32E+00	3,19E+01
CMANT	7,79E-03	2,42E-01	1,31E+00	3,15E+01
CMANT3A	7,79E-03	2,42E-01	1,31E+00	3,15E+01
CMANT2B	7,79E-03	2,38E-01	1,30E+00	3,07E+01
CMANT1B	7,79E-03	2,38E-01	1,30E+00	3,07E+01
CMANT3B	7,79E-03	2,38E-01	1,30E+00	3,07E+01
CMANT2S	7,79E-03	7,54E-02	1,08E+00	1,06E+01
CMANT1S	7,79E-03	7,54E-02	1,08E+00	1,06E+01
FALLORELES	5,32E-05	5,91E-02	1,06E+00	1,11E+03

Tabla Ñ.1: Sucesos básicos más importantes de la ecuación de FLR del suceso Caída1

Suceso básico	Probabilidad	FV	RDF	RIF
CAÍDA	5,60E-05	1,00E+00	9,99E+99	9,99E+99
MPC6	6,96E-05	1,00E+00	9,99E+99	1,44E+04
1M9GDA38BM	7,79E-03	2,38E-01	1,321E+00	3,13E+01
CMANT	7,79E-03	2,38E-01	1,31E+00	3,09E+01
CMANT3A	7,79E-03	2,38E-01	1,31E+00	3,09E+01
CMANT1B	7,79E-03	2,38E-01	1,30E+00	3,08E+01
CMANT2B	7,79E-03	2,38E-01	1,30E+00	3,08E+01
CMANT3B	7,79E-03	2,38E-01	1,30E+00	3,08E+01
CMANT1S	7,79E-03	7,43E-02	1,08E+00	1,04E+01
CMANT2S	7,79E-03	7,39E-02	1,08E+00	1,04E+01
FALLORELES	5,32E-05	5,78E-02	1,06E+00	1,09E+03

Tabla Ñ.2: Sucesos básicos más importantes de la ecuación de FLR del suceso Caída2

Suceso básico	Probabilidad	FV	RDF	RIF
CAÍDA	5,60E-05	1,00E+00	9,99E+99	9,99E+99
MPC2	2,29E-05	1,00E+00	9,99E+99	4,37E+04
1M9GDA38BM	7,79E-03	2,38E-01	1,321E+00	3,13E+01
CMANT	7,79E-03	2,38E-01	1,31E+00	3,09E+01
CMANT3A	7,79E-03	2,38E-01	1,31E+00	3,09E+01
CMANT1B	7,79E-03	2,39E-01	1,31E+00	3,08E+01
CMANT2B	7,79E-03	2,39E-01	1,31E+00	3,08E+01
CMANT3B	7,79E-03	2,39E-01	1,31E+00	3,08E+01
CMANT1S	7,79E-03	7,40E-02	1,08E+00	1,04E+01
CMANT2S	7,79E-03	7,40E-02	1,08E+00	1,04E+01
FALLORELES	5,32E-05	5,79E-02	1,06E+00	1,09E+03

Tabla Ñ.3: Sucesos básicos más importantes de la ecuación de FLR del suceso Caída3

Suceso básico	Probabilidad	FV	RDF	RIF
CAÍDA	5,60E-05	1,00E+00	9,99E+99	9,99E+99
MPC4	2,29E-05	1,00E+00	9,99E+99	2,18E+03
VAINAS1	1,00E+00	1,00E+00	9,99E+99	1,00E+00
1M9GDA38BM	7,79E-03	2,36E-01	1,31E+00	3,11E+01
CMANT	7,79E-03	2,36E-01	1,30E+00	3,08E+01
CMANT3A	7,79E-03	2,36E-01	1,30E+00	3,08E+01
CMANT1B	7,79E-03	2,38E-01	1,30E+00	3,07E+01
CMANT2B	7,79E-03	2,38E-01	1,30E+00	3,07E+01
CMANT3B	7,79E-03	2,38E-01	1,30E+00	3,07E+01
CMANT1S	7,79E-03	7,40E-02	1,08E+00	1,04E+01
CMANT2S	7,79E-03	7,37E-02	1,08E+00	1,04E+01
FALLORELES	5,32E-05	5,73E-02	1,06E+00	1,09E+03

Tabla Ñ.4: Sucesos básicos más importantes de la ecuación de FLR del suceso Caída4

Suceso básico	Probabilidad	FV	RDF	RIF
CAÍDA	5,60E-05	1,00E+00	9,99E+99	9,99E+99
MPC5	2,82E-01	1,00E+00	9,99E+99	3,55E+00
VAINAS1	1,00E+00	1,00E+00	9,99E+99	1,00E+00
1M9GDA38BM	7,79E-03	2,36E-01	1,31E+00	3,11E+01
CMANT	7,79E-03	2,36E-01	1,30E+00	3,07E+01
CMANT3A	7,79E-03	2,36E-01	1,30E+00	3,07E+01
CMANT1B	7,79E-03	2,38E-01	1,30E+00	3,06E+01
CMANT2B	7,79E-03	2,38E-01	1,30E+00	3,06E+01
CMANT3B	7,79E-03	2,38E-01	1,30E+00	3,06E+01
CMANT1S	7,79E-03	7,39E-02	1,08E+00	1,04E+01
CMANT2S	7,79E-03	7,38E-02	1,08E+00	1,04E+01
FALLORELES	5,32E-05	5,73E-02	1,06E+00	1,08E+03

Tabla Ñ.5: Sucesos básicos más importantes de la ecuación de FLR del suceso Caída5

Suceso básico	Probabilidad	FV	RDF	RIF
CAÍDA	5,60E-05	1,00E+00	9,99E+99	9,99E+99
VOLCADO	1,00E-06	1,00E+00	9,99E+99	1,00E+06
1M9GDA38BM	7,79E-03	2,42E-01	1,32E+00	3,19E+01
CMANT	7,79E-03	2,42E-01	1,31E+00	3,15E+01
CMANT3A	7,79E-03	2,42E-01	1,31E+00	3,15E+01
CMANT1B	7,79E-03	2,38E-01	1,30E+00	3,07E+01
CMANT2B	7,79E-03	2,38E-01	1,30E+00	3,07E+01
CMANT3B	7,79E-03	2,38E-01	1,30E+00	3,07E+01
CMANT1S	7,79E-03	7,54E-02	1,08E+00	1,06E+01
CMANT2S	7,79E-03	7,54E-02	1,08E+00	1,06E+01
FALLORELES	5,32E-05	5,91E-02	1,06E+00	1,11E+03

Tabla Ñ.6: Sucesos básicos más importantes de la ecuación de FLR del suceso Volcado

Aparte de los sucesos iniciadores y los sucesos de fallo de las barreras de confinamiento, los sucesos relacionados con el mantenimiento de las compuertas del sistema HVAC son los más importantes del modelo.

Ñ.2. Análisis de importancia del modelo APS fase II

Suceso básico	Probabilidad	FV	RDF	RIF
VAINA1	1,00E+00	1,00E+00	9,99E+99	1,00E+00
MPC4	4,58E-04	1,00E+00	9,99E+99	2,18E+03
P2HFE2	6,89E-05	9,29E-01	1,40E+01	1,35E+04
CMANT2A	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT1A	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT3A	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT2B	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT1B	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT3B	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT1S	1,16E-02	6,68E-02	1,07E+00	6,69E+00

Tabla Ñ.7: Sucesos básicos más importantes de la ecuación de FLR del suceso LDP2

Suceso básico	Probabilidad	FV	RDF	RIF
MPC1	4,03E-07	1,00E+00	9,99E+99	2,48E+06
I4CCFROPES	2,00E-06	3,79E-01	1,61E+00	1,89E+05
CMANT3A	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT2A	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT1A	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT3B	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT2B	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT1B	1,16E-02	2,18E-01	1,27E+00	1,90E+01
I4DGGBF	1,00E-06	1,89E-01	1,23E+00	1,89E+05
I4CCFBRK	8,00E-07	1,51E-01	1,18E+00	1,89E+05

Tabla Ñ.8: Sucesos básicos más importantes de la ecuación de FLR del suceso LDP3

Suceso básico	Probabilidad	FV	RDF	RIF
MPC3	2,29E-05	1,00E+00	9,99E+99	4,37E+04
P5HFE1	1,18E-05	6,91E-01	3,23E+00	5,85E+04
CMANT2A	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT3A	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT1A	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT2B	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT1B	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT3B	1,16E-02	2,18E-01	1,27E+00	1,90E+01
I2CCFROPES	2,00E-06	1,17E-01	1,13E+00	5,85E+04
CMANT1S	1,16E-02	6,68E-02	1,07E+00	6,69E+00

Tabla Ñ.9: Sucesos básicos más importantes de la ecuación de FLR del suceso LDP5

Suceso básico	Probabilidad	FV	RDF	RIF
VAINA1	1,00E+00	1,00E+00	9,99E+99	1,00E+00
MPC5	2,82E-01	1,00E+00	9,99E+99	3,55E+00
P6HFE1	4,55E-04	9,89E-01	8,71E+01	2,17E+03
CMANT3A	1,16E-02	2,19E-01	1,27E+00	1,91E+01
CMANT2A	1,16E-02	2,19E-01	1,27E+00	1,91E+01
CMANT1A	1,16E-02	2,19E-01	1,27E+00	1,91E+01
CMANT2B	1,16E-02	2,19E-01	1,27E+00	1,91E+01
CMANT1B	1,16E-02	2,19E-01	1,27E+00	1,91E+01
CMANT3B	1,16E-02	2,19E-01	1,27E+00	1,91E+01
CMANT2S	1,16E-02	6,72E-02	1,07E+00	6,72E+00

Tabla Ñ.10: Sucesos básicos más importantes de la ecuación de FLR del suceso LDP6

Suceso básico	Probabilidad	FV	RDF	RIF
MPC6	6,96E-05	1,00E+00	9,99E+99	1,44E+04
P3HFE1	5,28E-06	1,00E+00	9,99E+99	1,89E+05
I5MCB	1,00E-05	9,80E-01	5,10E+01	9,80E+04
CMANT3A	1,16E-02	2,19E-01	1,27E+00	1,90E+01
CMANT1A	1,16E-02	2,19E-01	1,27E+00	1,90E+01
CMANT2A	1,16E-02	2,19E-01	1,27E+00	1,90E+01
CMANT2B	1,16E-02	2,19E-01	1,27E+00	1,90E+01
CMANT3B	1,16E-02	2,19E-01	1,27E+00	1,90E+01
CMANT1B	1,16E-02	2,19E-01	1,27E+00	1,90E+01
CMANT1S	1,16E-02	6,72E-02	1,07E+00	6,72E+00

Tabla Ñ.11: Sucesos básicos más importantes de la ecuación de FLR del suceso TBP3

Suceso básico	Probabilidad	FV	RDF	RIF
MPC6	6,96E-05	1,00E+00	9,99E+99	1,44E+04
P5HFE2	7,98E-05	1,00E+00	9,99E+99	1,25E+04
I7MCB	1,00E-05	9,80E-01	5,10E+01	9,80E+04
CMANT3A	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT1A	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT2A	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT2B	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT3B	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT1B	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT1S	1,16E-02	6,68E-02	1,07E+00	6,69E+00

Tabla Ñ.12: Sucesos básicos más importantes de la ecuación de FLR del suceso TBP5

Suceso básico	Probabilidad	FV	RDF	RIF
VOLCADO	5,60E-05	1,00E+00	9,99E+99	9,99E+99
TIPOVER	1,00E-06	1,00E+00	9,99E+99	1,00+06
CMANT1A	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT2A	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT3A	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT3B	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT2B	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT1B	1,16E-02	2,18E-01	1,27E+00	1,90E+01
CMANT2S	1,16E-02	6,68E-02	1,07E+00	6,68E+00
CMANT1S	1,16E-02	6,68E-02	1,07E+00	6,68E+00

Tabla Ñ.13: Sucesos básicos más importantes de la ecuación de FLR del suceso Tip-over

Aparte de los sucesos iniciadores y los sucesos de fallo de las barreras de confinamiento, los sucesos relacionados con el mantenimiento de las compuertas del sistema HVAC, algunos de los sucesos del modelo de fallo de la grúa puente, y los sucesos de fallo humano son los más importantes del modelo.

Apéndice O

Figuras y planos

El presente anexo contiene figuras y planos de soporte a la memoria de tesis y a otros anexos. Concretamente, este anexo contiene figuras e imágenes de los contenedores, del utillaje utilizado para transportar los contenedores, y del edificio de combustible.

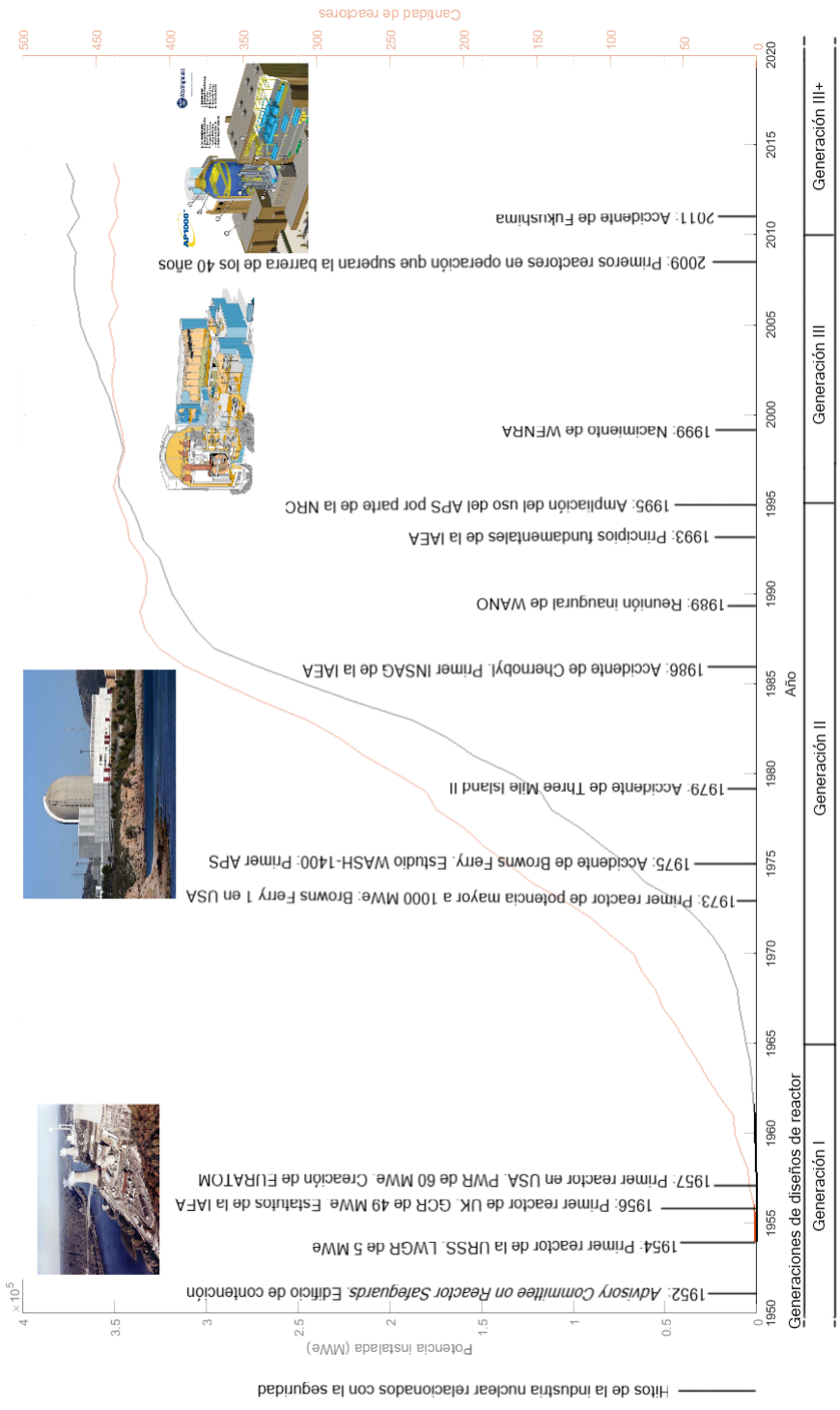


Figura O.1: Hitos de la evolución de la industria nuclear y la seguridad nuclear. Fuente: Elaboración propia.

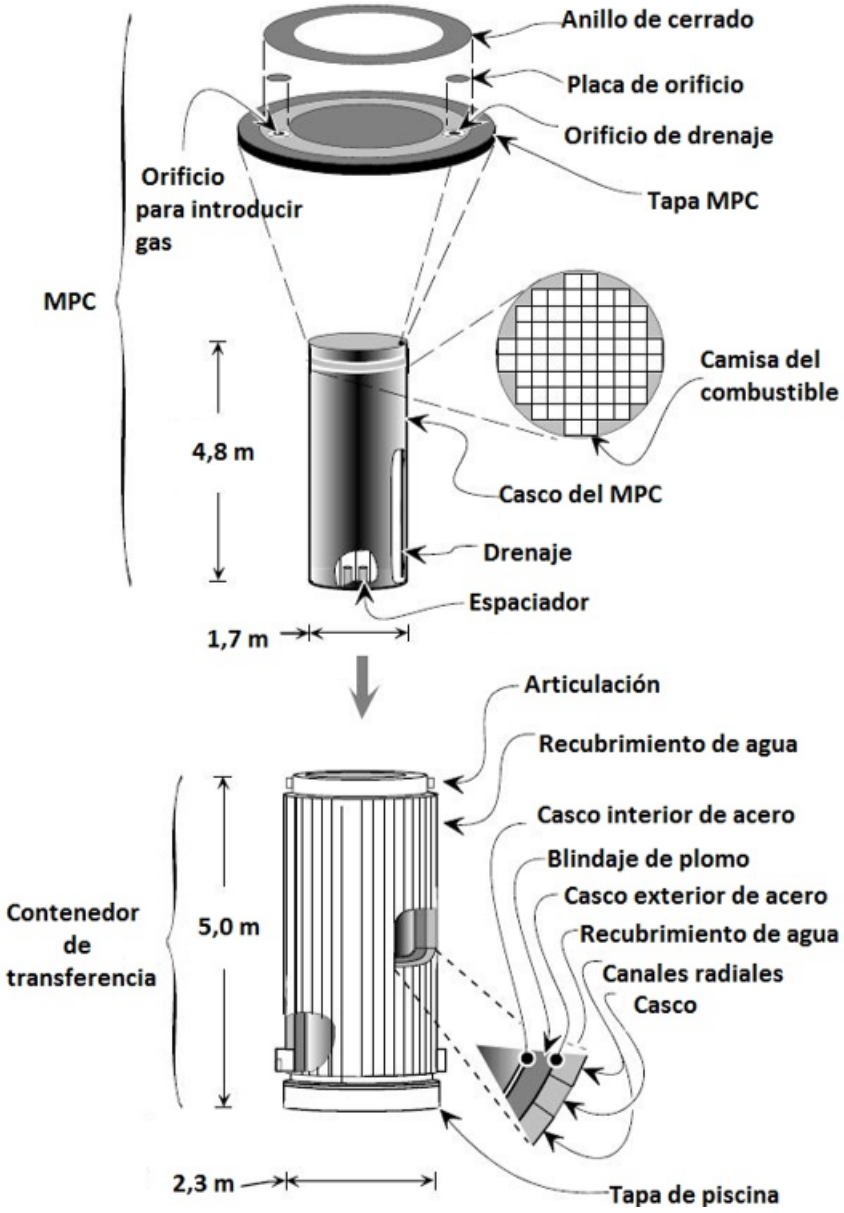


Figura O.2: Desglose del MPC y del HI-TRAC. Fuente: [5]

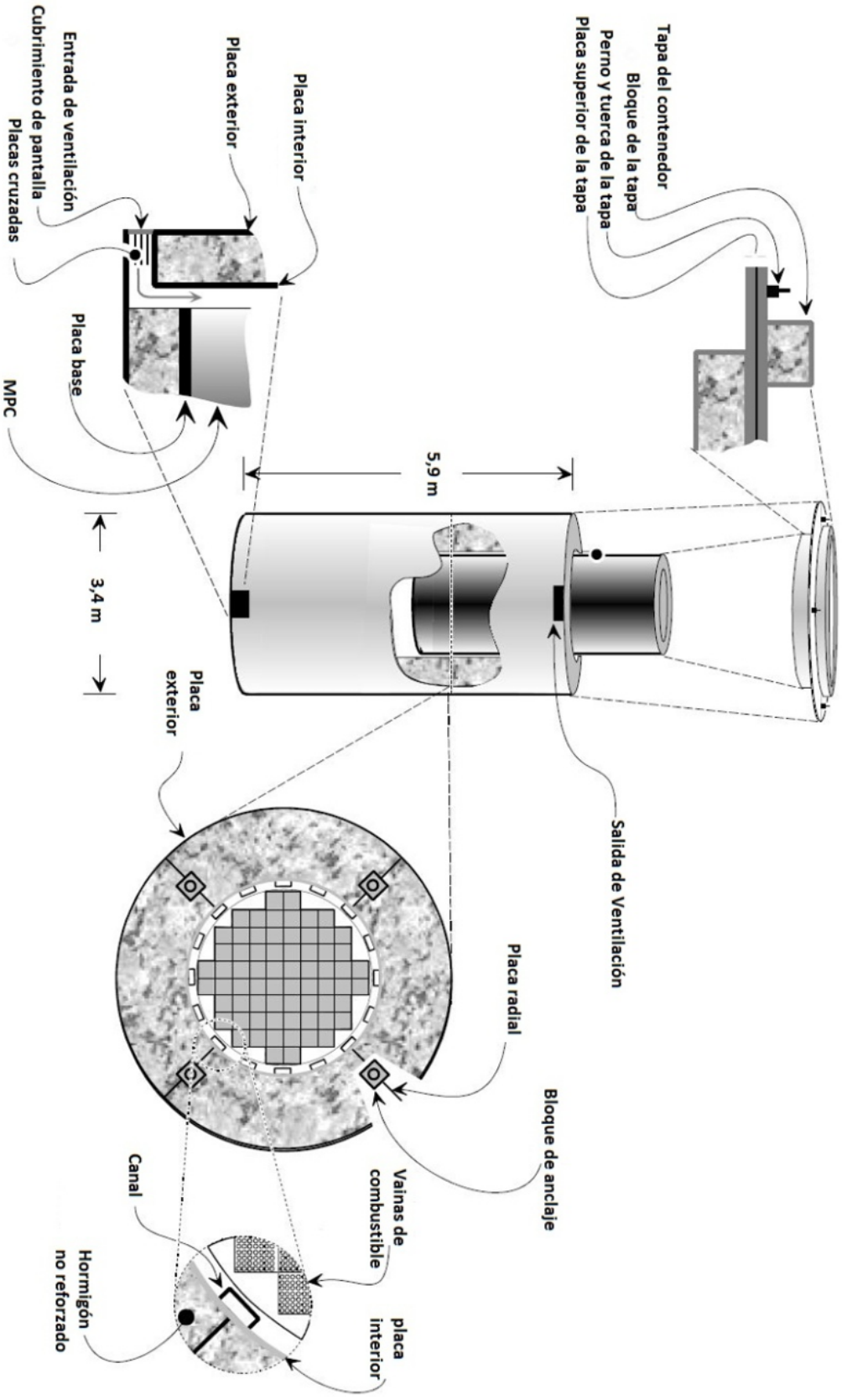


Figura O.3: Desglose del contenedor HI-STORM. Fuente: [5]

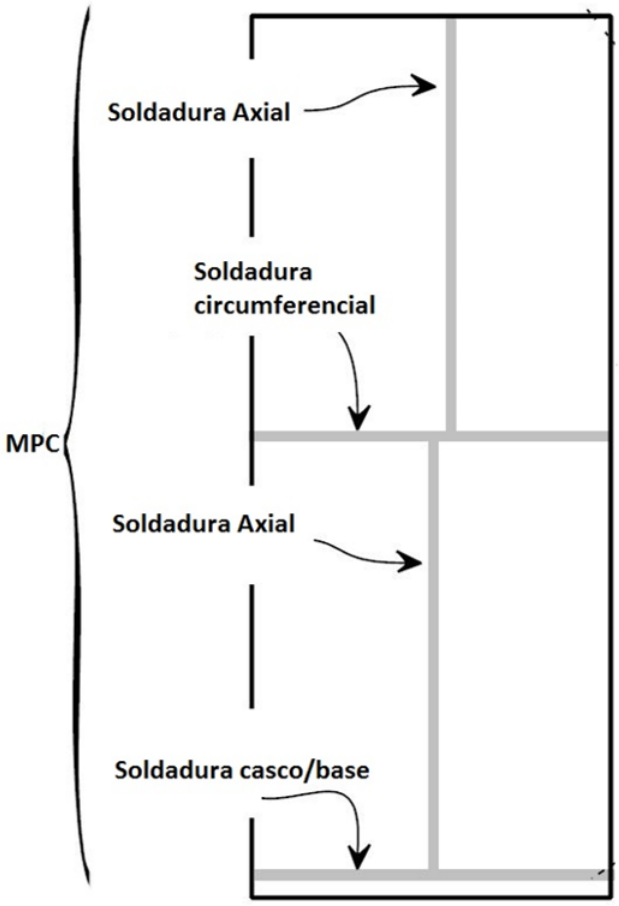


Figura O.4: Soldaduras del casco del MPC. Fuente: [5]

Figura O.5: Ejemplo de descenso de la tapa del MPC.Fuente: [8]

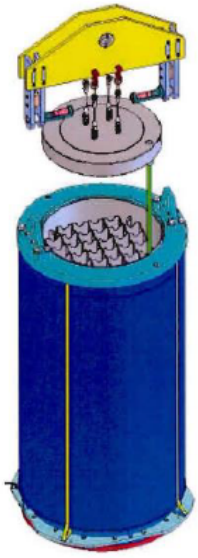


Figura O.6: Ejemplo de yugo de alzamiento, tapa de MPC, y HI.TRAC. Fuente: [9]

Figura O.7: Vehículo oruga.

Figura O.8: Contenedores HI-STORM en un ATI.

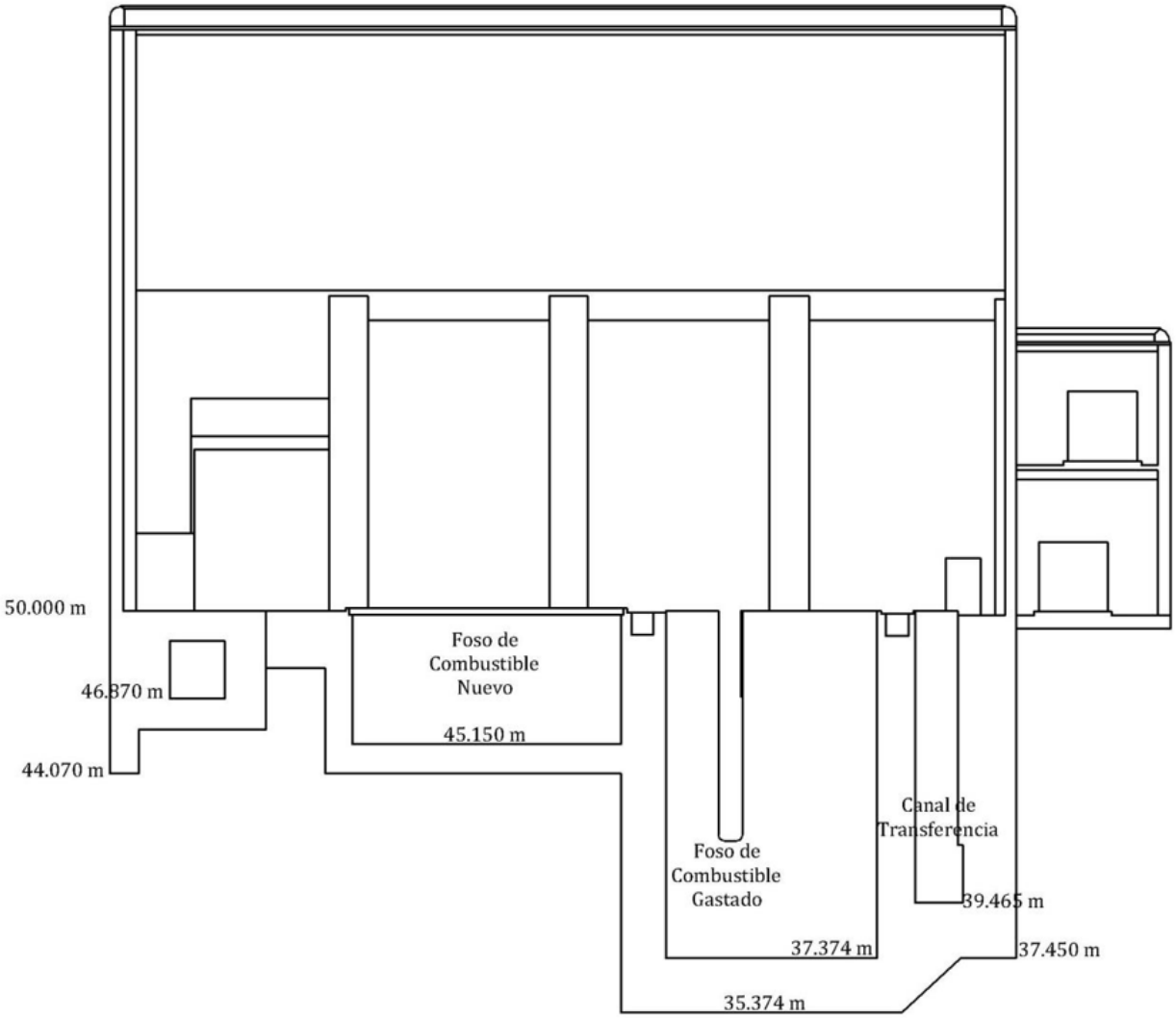


Figura O.9: Sección del edificio de combustible.

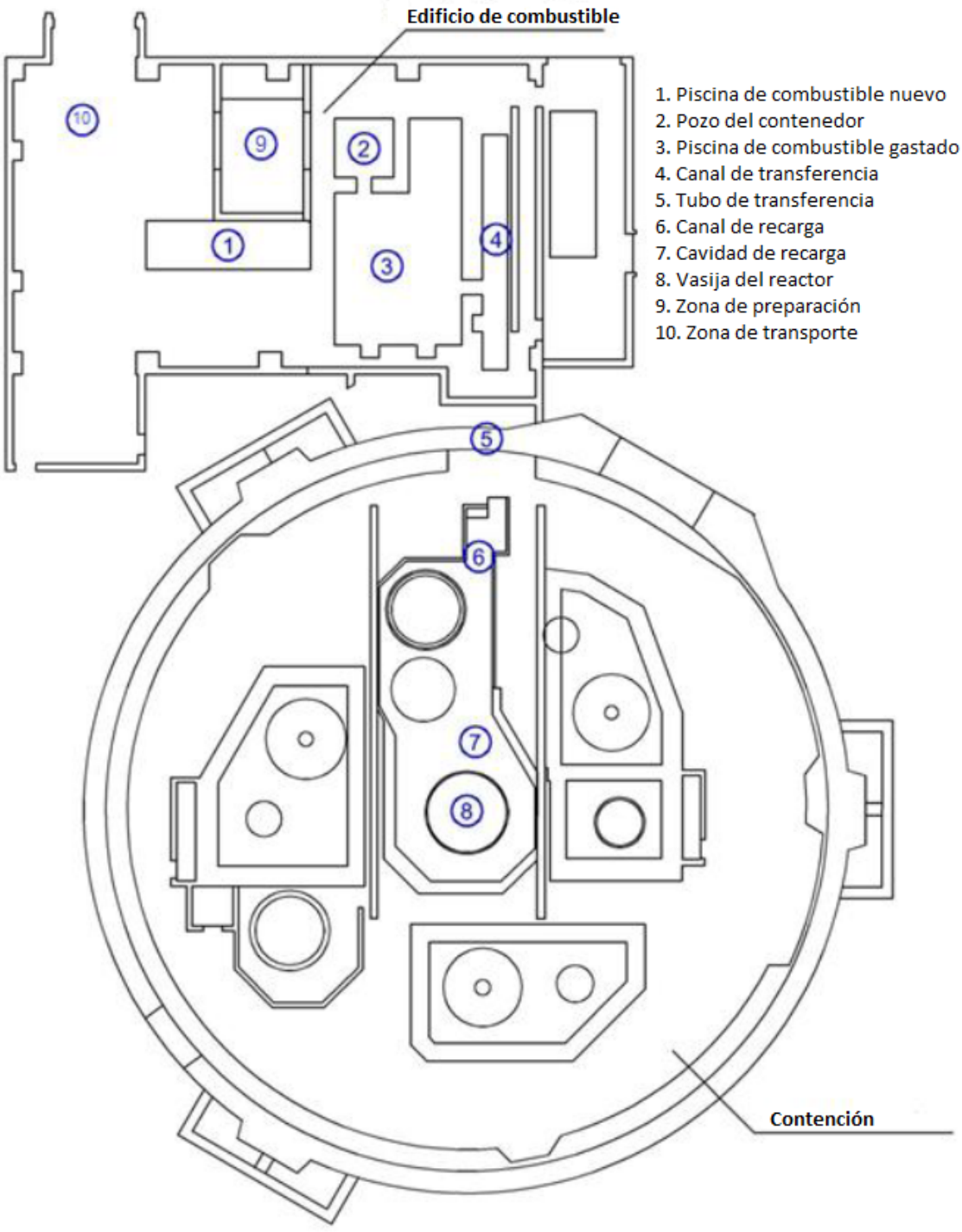


Figura O.10: Planta del edificio de combustible.

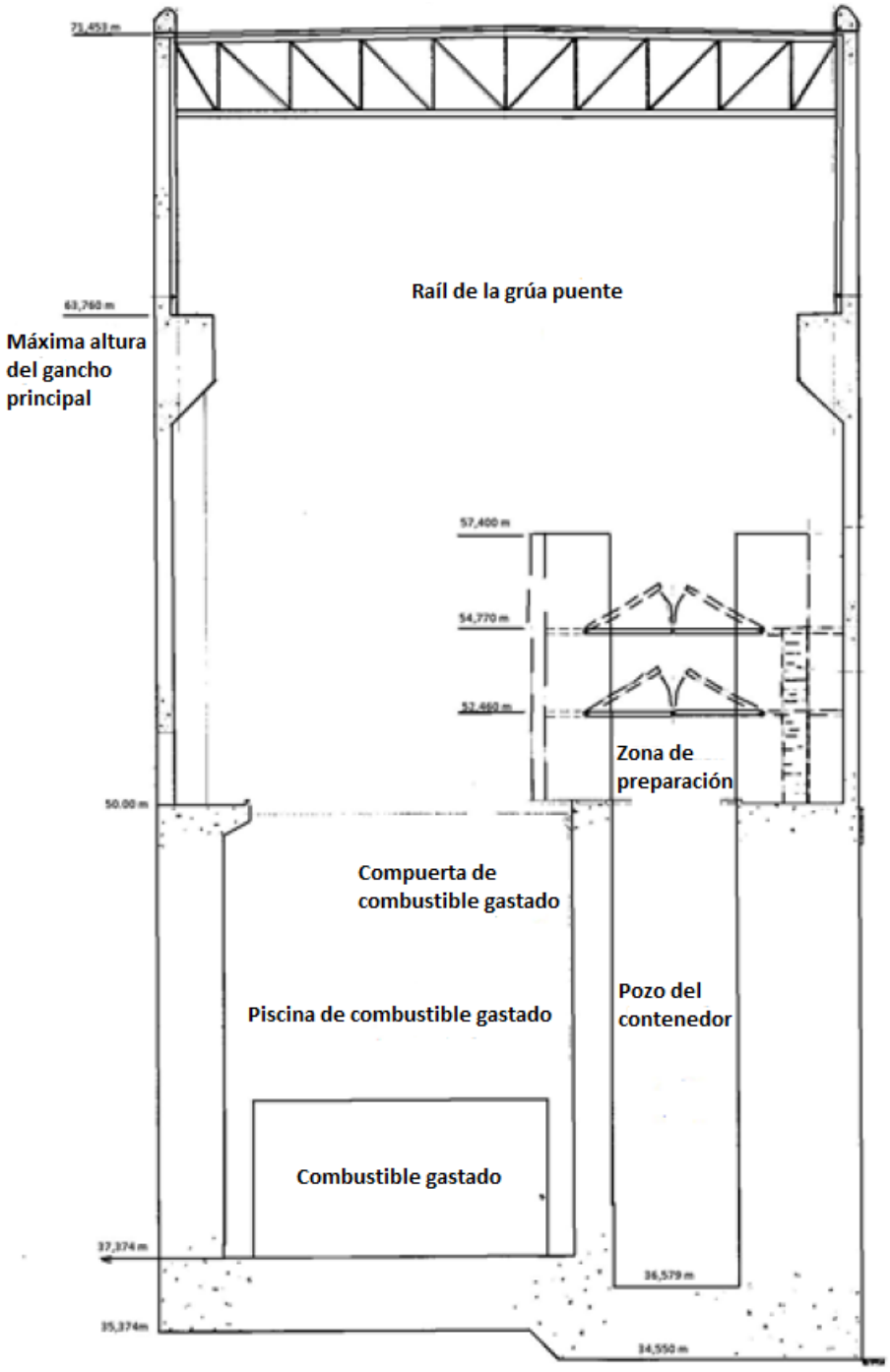


Figura O.11: Sección del edificio de combustible.

Parte V

Anexos asociados a la parte III

Apéndice P

Exchange events de sistemas contra incendio

Tal y como se ha explicado en el capítulo 12 de la tercera parte de la memoria de tesis, el APS de incendios detallado está enfocado de forma genérica, ya que para representar a los 384 casos de análisis repartidos en 41 zonas de incendio se usan solamente dos tipos de árboles de eventos de mitigación de incendios (excepto en contadas ocasiones) para modelizar la probabilidad de que un incendio genere un suceso interno o de ser detectado y extinguido. Estos dos árboles contemplan fuegos iniciados por actividades de corte y soldadura (árboles CI-CYS-) y fuegos originados por otras causas (árboles CI-A-). Los sistemas de detección y extinción a los que se les da crédito en la mitigación de incendios son la detección inicial (PS, cuando el fuego tiene origen de corte y soldadura, porque los trabajadores se encuentran en la zona), la detección automática (PDA, cuando no hay operarios en la zona), la extinción automática (PEA) y la brigada contra incendios (PFB).

La tabla P.1 contiene las características y probabilidades de fallo genéricas de los sistemas contra incendios de los árboles de mitigación de incendios. En pocos casos del modelo de APS de incendios detallado se dejan todos los cabeceros simultáneamente en su situación por defecto, es decir, lo más común es que en cada caso algún *Exchange Event* sustituya a algún cabecero.

Nombre (y código) del cabecero	Nombre usado en la matriz	Nombre del suceso básico del cabecero	Probabilidad de fallo	Descripción del suceso básico en el modelo
Detección automática (ADA)	PDA	INC-PDA	5,00E-02	Probabilidad de fallo en la detección automática
Extinción inicial (PS)	PS	INC-PS	1,00E+00	Probabilidad fallo extinción inicial para tiempo t=0
Extinción automática (AS)	PEA	INC-PEA	1,00E+00	Probabilidad de fallo cuando no existe extinción automática
Brigada (FB)	PFB	INC-PFB	2,00E-02	Probabilidad de fallo de la brigada con factor 2 %

Tabla P.1: Características de los sucesos básicos genéricos de los sistemas contra incendio.

La figura P.1 muestra qué *Exchange Events* sustituyen a los sucesos básicos de los cabeceros indicados en la tabla P.1 . Al hacer el análisis y poner en estado *True* a algún sistema contra incendios es necesario poner también a *True* todos los sucesos básicos que se encuentran en la figura P.1 debajo del sistema deseado. Si sólo se quisiera analizar la indisponibilidad en la mitigación de incendios de una zona, o de un edificio, no sería necesario ponerlos todos a *True*, puesto que no se usan todos los *Exchange Events* en todas las zonas.

INC-PDA	**INC-PS**	**INC-PEA**	**INC-PFB**
INC-DA-NO	INC-PS-2	INC-EA-AGUA	INC-ACEITE-2
INC-DA-ARCO	INC-PS-2%	INC-EA-CO2	INC-FB-0
*INC-SCONT-SIST-ASP	INC-PS-24	INC-EA-MAN	INC-CABLE-2
	INC-PS-4	INC-EA-MAN1	INC-CABLE-4
	INC-PS-9	*INC-SCONT-HUM	INC-CABLE-9
	INC-PS-12		INC-CON-2
	INC-CYS-2		INC-CYS-0
	INC-CYS-10		INC-ELECT-***
	*INC-SCONT-EXT-ASP		INC-TRANS-2
			INC-TRANS-24
			INC-TRANS-A

Figura P.1: *Exchange events* asociados a cada suceso básico genérico de sistema contra incendios.

INC-SCONT-SIST-ASP, INC-SCONT-EXT-ASP e INC-SCONT-HUM no son propiamente *Exchange Events*. Por ese motivo van acompañados de un asterisco (*). Estos tres sucesos básicos se añaden a la lista para facilitar el cálculo de las contribuciones dFDN dadas por las zona especial CXXX1. También cabe destacar que INC-ELECT-*** representa a 35 sucesos básicos con la misma raíz en el nombre.

Apéndice Q

Scripts utilizados en el proceso de cuantificación de la matriz MCI

Q.1. Introducción

Se han programado dos scripts en lenguaje *Python™* para la organización de los datos (script 1) y el cálculo de las matrices dFDN y MCI (script 2). Los scripts están programados para ser ejecutados por la versión 2.7.X de *Python™*, por lo tanto su ejecución bajo *Python™* 3.X no es posible a menos que se adapte el código. En el presente anexo se detalla el funcionamiento de los scripts.

Q.2. Jerarquía de carpetas y archivos

La figura Q.1 muestra la disposición de carpetas y archivos establecida para una correcta ejecución y funcionamiento de los scripts.

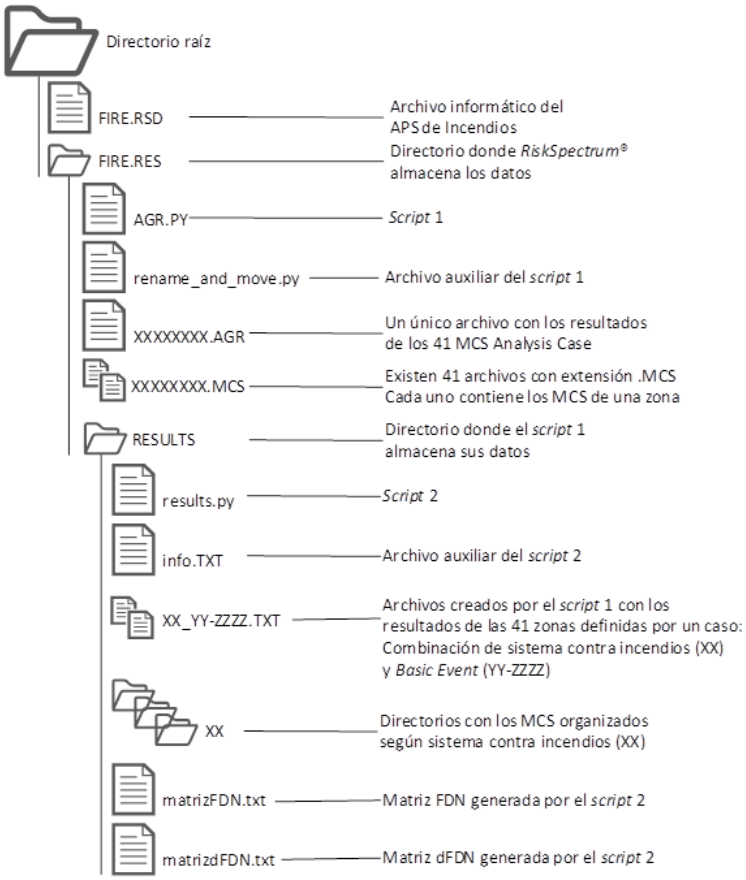


Figura Q.1: Jerarquía de carpetas y archivos implementada.

Q.3. Script 1: organización de los datos

El script 1 se encarga de preparar, a lo largo de las iteraciones, los archivos de texto que posteriormente se utilizarán en el cálculo de los elementos de la matriz MCI. El script necesita recibir instrucciones por parte del usuario y que se cumplan unas condiciones específicas. Primero es necesario tener instalado correctamente *Python™*. Todas las ejecuciones se han realizado en entorno Windows con la versión 2.7.6 de *Python™*. Los scripts no son compatibles con la versión 3.X de Python™. La versión de *RiskSpectrum®* usada es *PSA Professional 2.10.4* con el módulo *Analysis Tools 2.00.11*. Usar una versión distinta que extraiga los resultados en formato de texto de forma distinta podría inhabilitar completamente la función del script 1 y dar resultados inesperados.

Q.3.1. Preparativos en RiskSpectrum®

Para proceder a realizar las iteraciones de la metodología optimizada de cuantificación es necesario preparar a *RiskSpectrum® PSA* para:

- Agrupar resultados.
- Extraer los resultados deseados en forma de texto.

El modelo APS de incendios utilizado está diseñado de tal manera que la FDN inducida por incendios de la central es el resultado de sumar las FDN asociadas a cada zona de incendio. Tal y como se expresa en la memoria, la FDN asociada a una zona de incendio se cuantifica mediante un *MCS Analysis Case* después de haber sido cuantificados sus respectivos *Consequence Analysis Cases*. Es necesario ejecutar 384 + 41 simulaciones (todos los *Consequence Analysis Cases* más un *MCS Analysis Case* por zona) para obtener la FDN de incendios de cada zona de incendio en una situación particular. Para no tener que ejecutar las 384 + 41 simulaciones seleccionándolas manualmente, se procede usando los *Analysis Case Groups* (ACG). Los ACGs permiten ejecutar *Consequence Analysis Cases* y *MCS Analysis Cases* e incluso otros *Analysis Case Groups*, tantos como se quieran y en el orden que se quiera.

El único que se ejecuta por orden directa del usuario en una iteración normal es el *Analysis Case Group* llamado "ALL". Este primer ACG ejecuta a su vez dos ACGs más. El primero se llama "CONSEQ INC-D", y se encarga de ejecutar primero los 384 *Consequence Analysis Cases*. Seguidamente se ejecuta el segundo ACG, llamado "MCS XINC". "MCS XINC" se encarga de ejecutar los 41 *MCS Analysis Cases*. Se muestra en la figura Q.2 la jerarquía descrita. Es muy importante que primero se ejecuten los 384 *Consequence Analysis Cases* y luego los 41 *MCS Analysis Cases*, ya que los segundos dependen directamente de la correcta ejecución de los primeros. Además, el ACG "MCS XINC" se debe configurar para que saque el resultado en forma de texto. Como muestra se presenta en la figura Q.3 una captura del programa con la configuración del ACG "ALL" y de la confirmación de que "MCS XINC" extrae los resultados de los 41 *MCS Analysis Cases* en un archivo de texto. En la figura Q.3 también se muestran los mismos ACGs descritos pero con el sufijo "SPE". Ejecutar "ALL_SPE" es necesario para hacer los casos especiales de la zona CXXX6. La jerarquía es análoga.

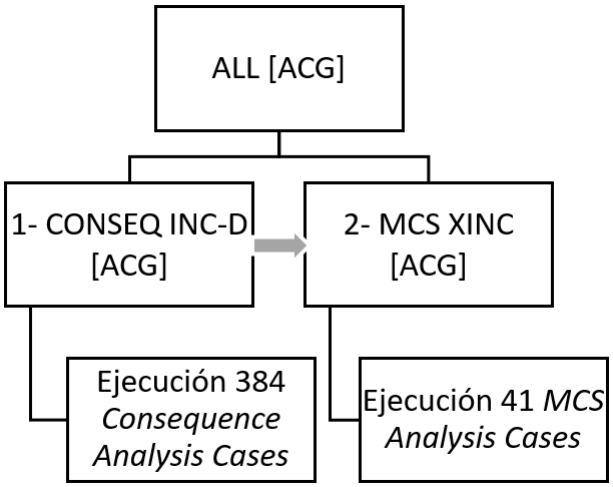


Figura Q.2: Jerarquía de ejecución de casos para cada iteración de la metodología optimizada.

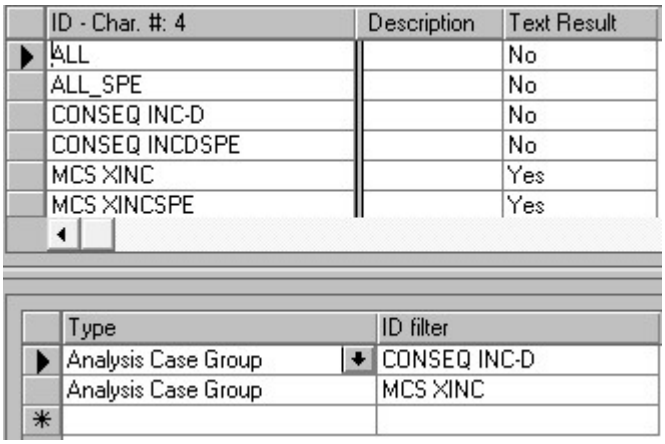


Figura Q.3: Captura de RiskSpectrum® que muestra los ACG.

Cuando un ACG está configurado para dar una salida en formato de texto, se genera en el directorio de resultados un fichero con un número igual al código interno con el que *RiskSpectrum® PSA* identifica al ACG más la extensión .AGR. A priori y sin abrir el archivo no es posible identificar qué ACG se encuentra dentro de un archivo .AGR, a no ser que se conozca de antemano qué código usa *RiskSpectrum® PSA* internamente para identificarlo.

Q.3.2. Ejecución del script 1

El script 1 trabaja desde el directorio de resultados de *RiskSpectrum® PSA*. Este directorio es creado automáticamente por *RiskSpectrum® PSA* y su nombre está formado por el nombre del archivo del APS ("FIRE" en el caso actual) y con el sufijo ".RES". El script 1 se llama "AGR.py".

Para ejecutar AGR.py es necesario abrir una ventana de comandos (se recomienda ir al directorio "FIRE.RES" y una vez dentro hacer click con el botón derecho del ratón dentro de la carpeta mientras la tecla "SHIFT" (o mayus) del teclado se encuentra pulsada, en el menú que aparece seguidamente se selecciona la opción "Abrir ventana de comandos aquí"). Dependiendo de la configuración del ordenador se puede prescindir de la palabra clave "python" en las siguientes figuras, aunque se recomienda su uso.

El uso correcto de AGR.py se muestra en la figura Q.4. Para ejecutar AGR.py es necesario pasar al script dos parámetros, CI y BE. CI significa sistema contra incendios y BE *Basic Event*. Los *Basic Events* se escriben con el siguiente formato: XX-YYYYYYYY; las XX representan el código numérico del *Basic Event*, asignado al seleccionar los *Basic Events* relevantes de las Funciones de Seguridad, e YYYYYYYY es el propio nombre del *Basic Event* en la base de datos del APS. Es decir, la información para representar al *Basic Event* es redundante, pero facilita el trabajo y la ordenación a posteriori. CI puede tomar los valores OK, PDA, PS PEA y PFB; BE en su lugar puede tomar además del sistema de *Basic Events* descrito el valor 00-OK u OK directamente.

```
D:\F2\FIRE.RES>python AGR.py CI BE
```

Figura Q.4: Correcta ejecución de AGR.py.

En la figura Q.5 se muestra un ejemplo completo de una ejecución típica:

```
D:\F2\FIRE.RES>python AGR.py PFC 01-1BMW6789
D:\F2\FIRE.RES>
```

Figura Q.5: Ejemplo de ejecución de AGR.py.

Si la ejecución termina sin errores no se muestra nada, y ya se puede ejecutar la siguiente iteración, preparando primero el programa *RiskSpectrum® PSA*, a continuación ejecutando el análisis completo y terminar con la ejecución del script 1 con los nuevos parámetros (CI y BE).

AGR.py realiza la conversión mostrada en la figura Q.6. Lee el único archivo con extensión .AGR que se encuentra dentro del directorio de resultados de *RiskSpectrum® PSA* y extrae en el archivo de resultados la información relevante, es decir, zona y su contribución para el caso estudiado.

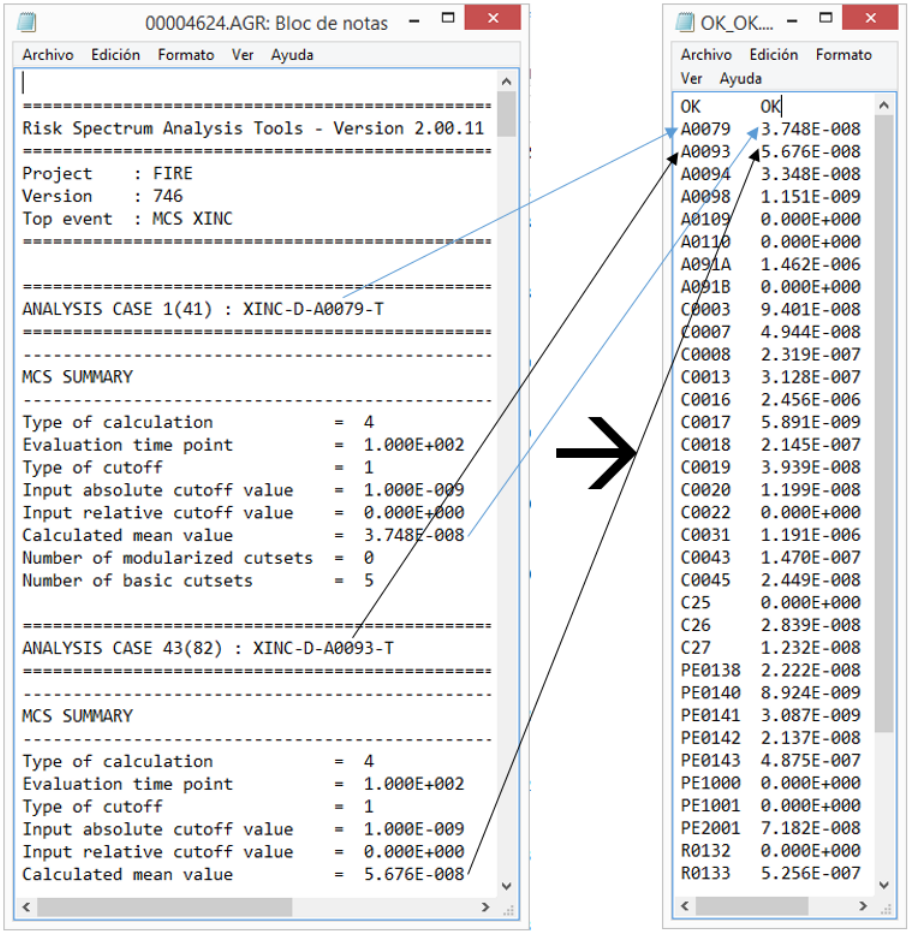
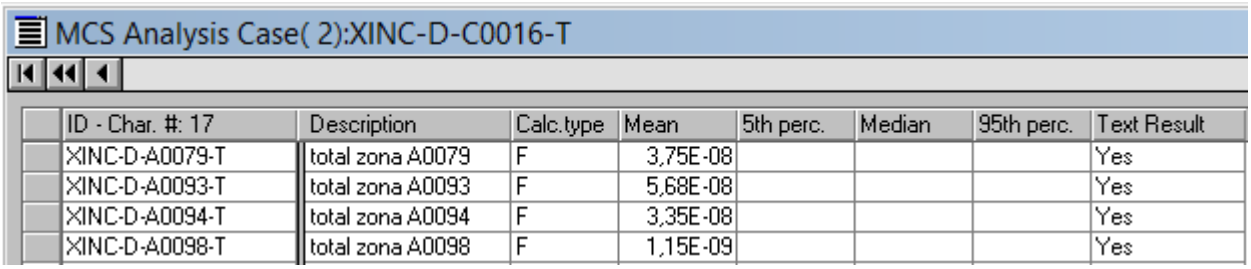


Figura Q.6: Trabajo de conversión realizado por AGR.py.

Q.3.3. Almacenamiento de conjuntos mínimos de fallo

Si se desea tener la lista de los conjuntos mínimos de fallos de cada zona y situación (conjunto de indisponibilidad de sistema contra incendios y función clave de seguridad), es necesario dar la instrucción de

extraer los resultados en modo texto a *RiskSpectrum® PSA*. Esta función se habilita dentro del apartado de gestión de los *MCS Analysis Cases*. Se muestran en la figura Q.7 cuatro *MCS Analysis Cases* configurados para extraer el listado de los conjuntos mínimos de fallos en modo de texto. Modificar la columna *Text Result* en *RiskSpectrum® PSA* es trivial ya que al hacer clic en la pertinente casilla se abre un desplegable con las opciones *Yes* y *No*.


MCS Analysis Case(2):XINC-D-C0016-T

ID - Char. #: 17	Description	Calc.type	Mean	5th perc.	Median	95th perc.	Text Result
XINC-D-A0079-T	total zona A0079	F	3,75E-08				Yes
XINC-D-A0093-T	total zona A0093	F	5,68E-08				Yes
XINC-D-A0094-T	total zona A0094	F	3,35E-08				Yes
XINC-D-A0098-T	total zona A0098	F	1,15E-09				Yes

Figura Q.7: Modo texto en RiskSpectrum®.

Si se decide extraer los resultados en forma de texto, *RiskSpectrum® PSA* genera un archivo de la forma "XXXXXXX.MCS", dentro del directorio de resultados, tal y como se aprecia en la figura Q.1 anterior. El nombre es a priori irreconocible, ya que *RiskSpectrum® PSA* usa un código interno con el que identifica cada *MCS Analysis Case* para poner el nombre. Estos archivos se pueden abrir con cualquier editor de texto, o modificar la extensión de ".MCS" a ".TXT" para abrirlos normalmente.

Es cuando existen estos resultados que el archivo auxiliar *rename_and_move.py* entra en acción. Este script auxiliar es llamado por AGR.py directamente para almacenar los conjuntos mínimos de fallos de forma que sean correctamente organizados y almacenados. Su funcionamiento consiste en leer cada archivo con extensión MCS, reconocerlo (reconoce la zona a la que pertenece) y moverlo a otro directorio con un nombre que permita su fácil identificación. Se muestra un ejemplo gráfico en la figura Q.8. La gran cantidad de archivos generados se organiza en distintas carpetas. Se ha decidido que el script auxiliar los almacene dentro de subcarpetas según el estado del sistema contra incendios en cada iteración, así las carpetas que existen tomarán los valores estándar OK, PDA, PEA, PFB y PS y los valores adicionales generados por los casos especiales HUM, AGUA, TERM, CO2, ASP y PEA2. Estos directorios deben ser creados manualmente.

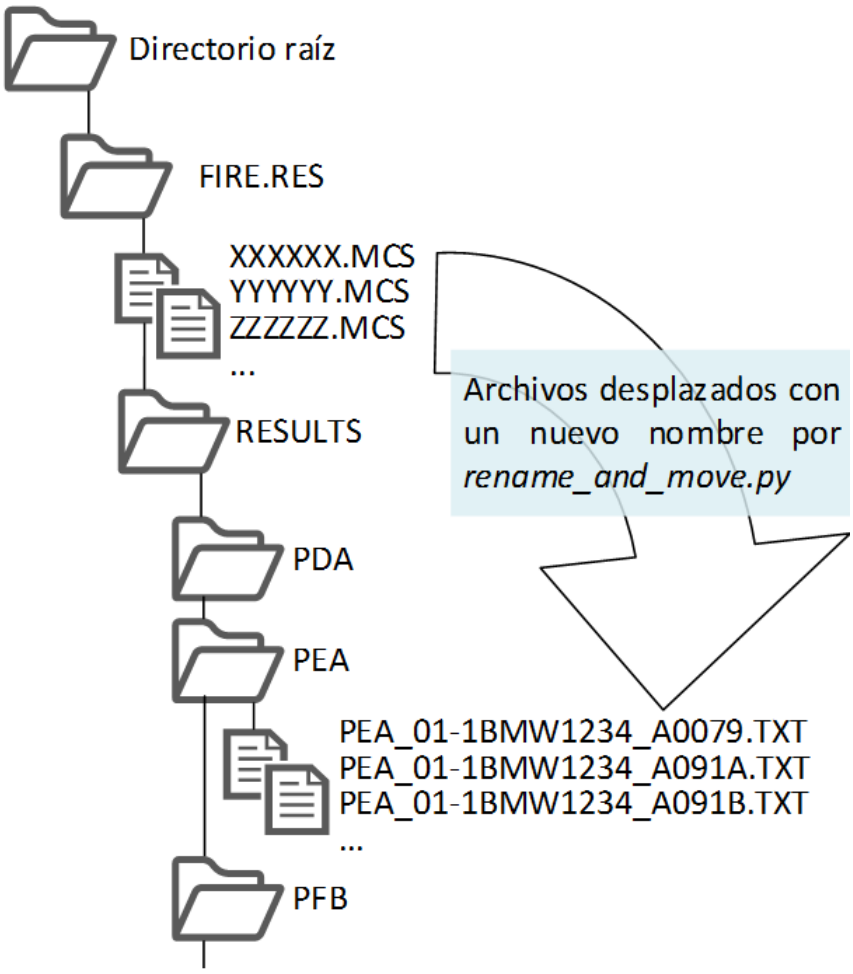


Figura Q.8: Trabajo realizado por rename_and_move.py cuando CI=PEA y BE=01-1BMW1234.

Q.4. Script 2: Cálculo de la matriz MCI

Q.4.1. Preparación del script 2

El script 2 es el fichero *results.py*, que se encuentra dentro de la carpeta /RESULTS/ tal y como se muestra en la figura Q.1 anterior. Este script usa un archivo de información auxiliar de donde lee:

1. Las zonas que conforman el análisis.
2. El listado de sistemas de detección y extinción generalistas (OK, PDA, PS, PEA y PFB).
3. El listado de *Basic Events* del análisis, los representantes de las Funciones de Seguridad.
4. Las zonas especiales con los sistemas de detección y extinción que las caracterizan.

Este archivo se llama *info.txt* y se encuentra en el mismo directorio que *results.py*. Los 4 ítems listados anteriormente no tienen por qué estar en este mismo orden, el orden es indiferente, pero es importante que existan todos los ítems, ya que en caso contrario los resultados son inesperados.

Dentro de *info.txt*, cada vez que se cambia de categoría se hace empezando una línea con un asterisco (*), y a continuación la primera palabra, en mayúsculas, es la clave para identificar a qué grupo pertenece la información que se está leyendo en el archivo. Los grupos son:

- *ZONES_LIST
- *DETECTION_EXTINCTION_LIST
- *BASIC_EVENTS_LIST
- *SPECIAL_ZONES_AND_FIRE_DETECTION_AND_EXCTINCTION_SYSTEMS_DIRECT_TO_CDF

Pero con solo contener el asterisco y la primera palabra, el script 2 ya puede funcionar:

- *ZONES
- *DETECTION
- *BASIC
- *SPECIAL

Debajo de cada grupo es dónde mediante saltos de línea se van entrando los elementos que conforman cada lista, ya sean zonas, sistemas, sucesos básicos, u otros.

La lista *SPECIAL tiene un comportamiento distinto, su funcionamiento es el siguiente:

código_de_zona:Sistemas,contra,incendios,separados,por,comas,sin,espacios

Ejemplo:

CXXX6:OK,HUM,AGUA,TERM,CO2,ASP,PFB,PS,PEA2

Puntos importantes a destacar para una correcta creación del fichero *info.txt*:

- Las zonas especiales también tienen que existir en el listado "*ZONES", ya que si no serían omitidas.
- Tanto las zonas, como las zonas especiales, se deben ordenar por orden alfabético (0-9, A-Z).
- El sistema contra incendios "OK" siempre debe existir, tanto en el listado *DETECTION como en el listado de los sistemas contra incendios de las zonas especiales, y se debe situar en la primera posición.

Q.4.2. Funcionamiento del script 2

Una vez se han realizado las 146 iteraciones ya se puede proceder a la ejecución del segundo script. Dependiendo de la configuración del ordenador, sólo es necesario hacer doble clic en el archivo *results.py* o se puede usar el mismo método que con el script 1, mediante una ventana de comandos. *results.py* se encuentra en el mismo directorio que los resultados procesados por el script 1 (AGR.py). Si no se produce ningún error grave aparecerán en el mismo directorio los archivos *matrizFDN.txt* y *matrizdFDN.txt* con los resultados.

Es importante destacar que este script realiza una cantidad enorme de cálculos, que sólo serán correctos si los datos aportados por el usuario lo son. Por ejemplo, escribir mal el nombre del *Basic Event* durante

la ejecución del script 1 generaría un fichero que *results.py* no leería (ya que no reconocería el nombre por no encontrarse dentro de *info.txt*), pero seguiría ejecutándose sin avisar al usuario y se obtendrían igualmente las dos matrices en los dos ficheros.

Primero de todo se recomienda observar detenidamente el contenido del fichero *matrizdFDN.txt* para comprobar que se encuentra correctamente rellenado. La información contenida ahí es una organización sistemática de todas las iteraciones que se han realizado. Es decir, los números no han sufrido ningún cambio. El error más destacable es cuando no se ha leído uno de los ficheros, y eso es fácil de ver, ya que la matriz muestra el patrón de ceros en la misma posición dentro de cada zona mostrado en la figura Q.9.

Basic_events:	OK	[illegible]BE01	[illegible]BE02
A0079			
OK:	3.748e-08	3.748e-08	3.748e-08
PDA:	0.0	4.519e-08	4.519e-08
PS:	4.559e-08	0.0	4.559e-08
PEA:	3.748e-08	3.748e-08	3.748e-08
PFB:	4.965e-08	4.965e-08	4.965e-08
A0093			
OK:	5.676e-08	5.676e-08	5.676e-08
PDA:	0.0	2.27e-07	2.27e-07
PS:	5.676e-08	0.0	5.676e-08
PEA:	5.676e-08	5.676e-08	5.676e-08
PFB:	2.27e-07	2.27e-07	2.27e-07
A0094			
OK:	3.348e-08	3.348e-08	3.348e-08
PDA:	0.0	7.198e-08	7.198e-08
PS:	3.348e-08	0.0	3.348e-08
PEA:	3.348e-08	3.348e-08	3.348e-08
PFB:	7.198e-08	7.198e-08	7.198e-08
A0098			
OK:	1.151e-09	1.151e-09	1.151e-09
PDA:	0.0	1.151e-09	1.151e-09
PS:	1.669e-09	0.0	1.669e-09
PEA:	1.151e-09	1.151e-09	1.151e-09
PFB:	1.588e-09	1.588e-09	1.588e-09
A0109			
OK:	0.0	0.0	0.0
PDA:	0.0	0.0	0.0
PS:	0.0	0.0	0.0
PEA:	0.0	0.0	0.0
PFB:	0.0	0.0	0.0

Figura Q.9: Patrón de ceros causado por la omisión de un archivo de información.

En la figura Q.9 se observa la consecuencia de una matriz dFDN con dos errores. Cada error está resaltado con un color distinto. El resaltado amarillo hace referencia a la ausencia del archivo de resultados PDA_OK.TXT, y el resaltado verde al PS_01-BE01.TXT. O bien el usuario se ha olvidado de ejecutar el script 1 (AGR.py) durante esas iteraciones, o bien ha escrito mal alguno de los parámetros que se deben adjuntar al script 2 (PDA OK sería lo correcto en el caso amarillo y PS 01-BE01 para el caso verde). Ejemplos de errores en los parámetros a la hora de ejecutar el script 1 podrían ser haber escrito "PSA OK" para el error amarillo y "PS 01-BEE01" para el error verde.

Que una zona tenga todo ceros no es un error, es más bien una zona con una contribución al riesgo muy

baja que no ha generado conjuntos mínimos de fallos por encima del valor de truncamiento.

Q.4.3. Zonas especiales

El diseño de zonas especiales en el script 2 está enfocado a tratar las habitaciones CXXX6 y CXXX1. Las zonas especiales son aquellas con una configuración de sistemas contra incendios distintos a la configuración por defecto. Las tres funciones que permite el script *results.py* respecto a las zonas especiales son:

1. Adición de nuevos sistemas contra incendios.
2. Supresión de sistemas contra incendios.
3. Alteración del orden por defecto de los sistemas contra incendios.

Si se desea añadir nuevos sistemas contra incendios, es necesario que:

1. El código que reciba como nombre sea distinto a cualquier otro.
2. Forme parte de un árbol CI con consecuencia directa a daño al núcleo. El motivo es que debe ser una sistema contra incendios que sea independiente de las Funciones de Seguridad (*Basic Events* / columnas de la Matriz), no debe pasar por lo tanto por un árbol SI. Cuando se calcule b. dicho valor dFDN, los parámetros deberán ser "COD OK"; entendiendo por COD el código del nuevo sistema contra incendios. Al ser independiente de las funciones clave de seguridad, el segundo parámetro debe ser OK. Por ejemplo: >python AGR.py COD1 OK.
3. Modificar *info.txt*. Se debe escribir la zona seguido de dos puntos, OK y los nuevos códigos separados por comas y sin espacios. Se pueden usar en conjunción con los sistemas contra incendios habituales. Ejemplo del apartado *SPECIAL de *info.txt*: A1234:OK,COD1,COD2,PDA,COD3. En este caso los sistemas PS, PEA y PFB ya no se tendrán en cuenta para esta zona.

Si se desea alterar el orden, y/o suprimir algún sistema contra incendios, es necesario que se escriba la zona, seguido de dos puntos, y el nuevo orden de los sistemas contra incendios, omitiendo los indeseados, separados por comas y sin espacios. Por ejemplo si se quieren eliminar PDA y PFB, y cambiar PS y PEA de orden: A5678:OK,PEA,PS.

Q.4.3.1. Zona CXXX6

Para la zona CXXX6 se han añadido sistemas contra incendios especiales independientes de las funciones de seguridad, y a la vez también se han usado PFB y PS. Se usan por lo tanto las tres funciones disponibles.

*SPECIAL

CXXX6:OK,HUM,AGUA,TERM,CO2,ASP,PFB,PS,PEA2

Q.4.3.2. Zona CXXX1

Para la zona CXXX1 es necesario añadir tres nuevos sistemas contra incendios, pero en este caso la FDN de la zona CXXX1 sí depende de las funciones de seguridad. Para sortear la limitación se usan tres sistemas contra incendios de los comunes. Por lo tanto se usa la segunda y tercera función de las disponibles para las zonas especiales:

*SPECIAL

CXXX1:OK,PEA,PDA,PS

La sistemática consiste en usar las iteraciones "normales" para calcular también HUM ASP y EXT de la zona CXXX1. Para ello, cuando se fuerza la indisponibilidad de PEA, PDA y PS, se añaden como indisponibles los *Basic Events* representantes de HUM, ASP y EXT respectivamente. Al ejecutar el script 2 el resultado NO tendrá HUM, ASP y EXT, en su lugar se obtendrán los sistemas contra incendios PEA, PDA y PS respectivamente. Es tarea del usuario reemplazar manualmente los códigos de los sistemas contra incendios por los correctos.

Apéndice R

Scripts utilizados en el análisis de incertidumbre de la matriz MCI

R.1. Introducción

El presente anexo contiene la descripción de los diferentes *scripts* desarrollados para aplicar el análisis de incertidumbre mediante simulación Monte Carlo a los elementos de la matriz MCI. Se hace referencia a este anexo desde el capítulo 15 de la tercera parte de la tesis.

R.2. *Script* de la metodología base

Las figuras R.1 a muestran las diferentes partes del *script* de aplicación de la metodología base. En la figura R.1 se muestra la declaración de las variables, línea *syms*, la declaración del número de simulaciones *ns*, en este caso 1000, aunque finalmente se ha fijado en 10000, y la creación de una matriz R que contiene todos los valores aleatorios a usar en las simulaciones del *script*, cada simulación es una fila de esta matriz.

```
syms d f c fd s ns

ns = 1000; %número de simulaciones

%el 4 se ha de cambiar por el número de zonas a analizar (para automatizar
%debería estar ligado al número de columnas de data entre 2)
R = rand(ns,4); %generación de números aleatorios. Cada fila es una simulación
```

Figura R.1: Declaración del número de simulaciones *ns* y generación de una matriz de valores aleatorios.

La figura R.2 muestra la parte del *script* que contiene la adquisición del input. El *script* lee los archivos .UNC que estén en la carpeta donde se ejecuta y crea una matriz *data* con las CDFs de cada archivo .UNC. Cada CDF ocupa dos columnas de la matriz *data*.

```
fitxers=dir('*.UNC');
data=[];
for i=1:length(fitxers)
    data = [data,dlmread(fitxers(i).name,'',[230 0 330 0])];
    data = [data,dlmread(fitxers(i).name,'',[230 1 330 1])/100];
%Lectura de datos de archivos RiskSpectrum
end
```

Figura R.2: Adquisición del input.

En la figura R.3 se muestra el cuerpo del *script*, que contiene las órdenes necesarias para llevar a cabo las *ns* simulaciones especificadas. Esta parte del *script* está específicamente preparada para la suma de cuatro elementos, cuatro sFDNs. El vector E almacena el resultado de cada simulación. Las variables *prc95*, *prc5*, y *prc50* guardan la progresión de los percentiles a lo largo de las simulaciones.

```
for f = 1:ns %1000 simulaciones correspondientes a las filas de R
    E(f) = 0;
    %el rango de la c se ha de cambiar por el número de zonas (núm cols de
    %R)
     for c = 1:4 %En este caso se analizan solo 4 FDNs
         d = 2*c; %d es el índice de las columnas que contienen la y de las cdfs
         for fd=1:101 %la matriz data tiene 101 filas

               if R(f,c) <= data(fd,d) %búsca en qué punto cae el número aleatorio
                      if R(f,c)<0.01
                       a(f,c)=data(fd,d-1);
                       break
                      end
                       if R(f,c) > 0.99
                       a(f,c) = data(fd-1,d-1);
                       break
                       end
                  x1 = data(fd-1,d-1);%límite inferior x del intervalo en el que cae el número aleatorio
                  x2 = data(fd,d-1);%límite superior x del intervalo en el que cae el número aleatorio
                  y1 = data(fd-1,d);%límite inferior y del intervalo en el que cae el número aleatorio
                  y2 = data(fd,d);%límite superior y del intervalo en el que cae el número aleatorio
                  y= R(f,c);
                  A = [1 x1 ;1 x2];
                  B = [y1 y2]';
                  X= linsolve(A,B); %obtiene los coeficientes de la recta que une los límites
                  a(f,c) = (y-X(1))/X(2); %proporciona la x del número aleatorio y, y la coloca en una matriz 1000x4
                  break
                   end

         end
        E(f) = E(f) + a(f,c);%Realiza el cálculo final. Ecuación final.
     end


  %Cálculo progresión percentiles
     prc95(f)=prctile(E,95);
    prc5(f)=prctile(E,5);
    prc50(f)=prctile(E,50);
end
```

Figura R.3: Simulación Monte Carlo. Obtención de valor puntual de dFDN y cálculo de la suma de dFDNs.

La figura muestra la parte del *script* en la que se calculan los parámetros estadísticos resultado (media, mediana, percentil 5, percentil 95, y la desviación estándar). También se muestra la parte del *script* en la que se obtiene la progresión de la media y la desviación estándar a lo largo de las simulaciones para llevar a cabo el análisis de sensibilidad.

```
%Resultados y estadísticos

average = mean(E)
median = median(E)
p5 = prctile(E,5)
p95 = prctile(E,95)
stdE = std(E)

%Análisis de sensibilidad. Progresión de la media y std con las simulaciones
%cálculo media y std
s = 0;
for z = 1:ns
    s = s + E(z);
    avg(z) = s/z;
    summ = 0;
    for i = 1:z
      summ = summ + (E(i)-avg(z))^2;
    end
    std(z) = (summ/z)^(1/2);
end
```

Figura R.4: Parte del *script* que proporciona los resultados finales y la progresión de la media y la desviación estándar.

R.3. Modificación del *script* de la metodología base para la validación

La adquisición del input del *script* generado para la validación de la metodología base es diferente a la del *script* de aplicación de la metodología base. En el caso de la validación, las distribuciones de probabilidad de los inputs, las *failure rates* obtenidas en el modelo APS de incendios creado en *RiskSpectrum® PSA*, son conocidas. Matlab® permite obtener parejas de valores de *cummulative distribution functions* cuya distribución de probabilidad es conocida. En consecuencia, se modifica la adquisición del input del *script* de aplicación de la metodología base para que proporcione parejas de valores de la CDF de distribuciones de probabilidad conocidas, las asociadas a las *failure rates*. Estas parejas de valores cubren el total del rango de probabilidad acumulada (de 0 a 1) en intervalos de 0,1. La figura R.5 presenta la parte de adquisición del input del *script* de validación.

```
n=100;
pEmp = (0:100)'/n;
%Lectura de datos de archivos RiskSpectrum
y1data = pEmp;
x1data = icdf('gamma',y1data,3.01,4.48E-8);
y2data = pEmp;
x2data = icdf('gamma',y2data,8.67E-01,9.62E-08);
y3data = pEmp;
x3data = icdf('gamma',y3data,2.08,8.62E-08);
y4data = pEmp;
x4data = icdf('gamma',y4data,2,1.27E-06);
%integración de los datos en una única matriz
data = [x1data,y1data,x2data,y2data,x3data,y3data,x4data,y4data];
```

Figura R.5: Adquisición de inputs del *script* de validación.

R.4. Script de aplicación de la metodología base a la matriz MCI

```
syms d f c fd s ns
ns = 10000; %número de simulaciones
Mavg = zeros(168,30);
Mmed = zeros(168,30);
Mp5 = zeros(168,30);
Mp95 = zeros(168,30);
Mcavg = zeros(168,30);
Mcp95 = zeros(168,30);
cols = dir;%lee las carpetas asignadas a las columnas de la matriz
for ci = 3:length(cols)
     cd('D:\MonteCarlo_Matriu\');
    cii(ci)=ci;
    if isdir(cols(ci).name) == 1
         if (length(cols(ci).name)<4)&&(length(cols(ci).name) > 5)
            continue
        end
         if length(cols(ci).name) == 4%proporciona el índice de la columna
            nums = cols(ci).name(end:end);
            ncol=str2num(nums);
         elseif length(cols(ci).name) == 5
             nums = cols(ci).name(end-1:end);
            ncol=str2num(nums);
         end

         cd(strcat('D:\MonteCarlo_Matriu\',cols(ci).name));%entra en la carpeta
         %columna para calcular sus elementos



folders = dir;%lee los archivos y carpetas de la carpeta columna
```

Figura R.6: Declaración de variables y lectura de carpetas columna.

La figura R.6 muestra la parte del *script* en la que se declaran variables y la parte del *script* que lee (reconoce) las carpetas columna y entra en ellas.

```
for fi = 3:length(folders)
    if fi > 3
    cd(strcat('D:\MonteCarlo_Matriu\',cols(ci).name));
    end
    fii(fi)=fi;
    if isdir(folders(fi).name)==1%dice si lo seleccionado es una carpeta
    cd(strcat('D:\MonteCarlo_Matriu\',cols(ci).name, '\',folders(fi).name));%entra en la carpeta elemento
fitxers=dir('*.TXT');%lee los archivos de incerteza
```

Figura R.7: Entrada en las carpetas elementos de la matriz y lectura de ficheros.

La entrada del *script* en las carpetas elementos de la matriz se muestra en la figura R.7. También se muestra la orden de lectura de los archivos .TXT existentes en las carpetas elemento de la matriz.

```
data=[];
for i=1:length(fitxers)
    data = [data,dlmread(fitxers(i).name,'',[230 0 330 0])];
    data = [data,dlmread(fitxers(i).name,'',[230 1 330 1])/100];
%Lectura de datos de archivos RiskSpectrum
end
datacol = size(data,2);%Da las columnas de data.
```

Figura R.8: Creación de la matriz input de las simulaciones Monte Carlo.

La figura R.8 muestra la parte del *script* que lee los datos de incertidumbre de los archivos .TXT de la carpeta elemento de la matriz objetivo y los escribe en una matriz *data*. La matriz *data* es el input de las simulaciones Monte Carlo. Cada pareja de columnas de la matriz *data* contiene los datos de una zona de incendio de la planta.

```
R = rand(ns,(datacol/2)); %generación de números aleatorios. Cada fila es una simulación. Cada columna es una zona
%Simulación MonteCarlo
for f = 1:ns %ns simulaciones correspondientes a las filas de R
   E(f) = 0;

    for c = 1:(datacol/2) %Para toda zona
        d = 2*c; %d es el íncide de las columnas que contienen la y de las cdfs
        for fd=1:101 %la matriz data tiene 101 filas

              if R(f,c) <= data(fd,d) %búsca en qué punto cae el número aleatorio
                    if R(f,c)<0.01
                     a(f,c)=data(fd,d-1);
                     break
                    elseif R(f,c) > 0.99
                     a(f,c) = data(fd-1,d-1);
                     break
                    elseif (R(f,c)>=0.01)&&(R(f,c)<=0.99)
                        if data(fd,d-1)==data(fd-1,d-1)
                            a(f,c)=data(fd,d-1);
                            break
                        elseif data(fd,d-1)> data(fd-1,d-1)
                            x1 = data(fd-1,d-1);%límite inferior x del intervalo en el que cae el número aleatorio
                           x2 = data(fd,d-1);%límite superior x del intervalo en el que cae el número aleatorio
                            y1 = data(fd-1,d);%límite inferior y del intervalo en el que cae el número aleatorio
                            y2 = data(fd,d);%límite superior y del intervalo en el que cae el número aleatorio
                           y= R(f,c);
                               A = [1 x1 ;1 x2];
                           B = [y1 y2]';
                            X= linsolve(A,B); %obtiene los coeficientes de la recta que une los límites
                            a(f,c) = (y-X(1))/X(2); %proporciona la x del número aleatorio y, y la coloca en una matriz
                   break
                            end
                        end
              end

        end
       E(f) = E(f) + a(f,c);%Realiza el cálculo final. Ecuación final.
    end
```

Figura R.9: Simulación Monte Carlo.

La parte del *script* que ejecuta la simulación Monte Carlo se presenta en la figura R.9. Este *script* es prácticamente idéntico al de la metodología base de la figura R.3. Se ha introducido una corrección para casos en los que haya parejas consecutivas de valores de la CDF cuya componente x sea la misma.

```
%Resultados y estadísticos

average = mean(E);
mediana = median(E);
p5 = prctile(E,5);
p95 = prctile(E,95);
```

Figura R.10: Estadísticos resultados para un elemento de la matriz.

La figura R.10 muestra la extracción de resultados para un elemento de la matriz.

```
Mavg(folder-168*(ncol-1),ncol)=average;%matriz de medias
Mmed(folder-168*(ncol-1),ncol)=mediana;%matriz de medianas
Mp5(folder-168*(ncol-1),ncol)=p5;%matriz de p5
Mp95(folder-168*(ncol-1),ncol)=p95;%matriz de p95
```

Figura R.11: Escritura de resultados en formato matriz.

Finalmente, la figura R.11 muestra las órdenes utilizadas para guardar los resultados de un elemento de la matriz en matrices de resultados. Estas matrices tienen la misma estructura que la matriz de compatibilidades de indisponibilidades de sistemas contra incendio y funciones clave de seguridad.

Apéndice S

Figuras

S.1. Tabla 6-1 del NUREG/CR-6850

La Tabla 6-1 del NUREG/CR-6850 contiene la estimación de las frecuencias genéricas de incendio para diferentes combinaciones de localización en planta y de fuentes de incendio según tipo de componente.

Fire Ignition Frequencies (Task 6)

Table 6-1
Fire Frequency Bins and Generic Frequencies

ID	Location	Ignition Source (Equipment Type)	Mode	Generic Freq (per rx yr)	Split Fractions for Fire Type					
					Electrical	Oil	Transient	Hotwork	Hydrogen	HEAF[1]
1	Battery Room	Batteries	All	7.5E-04	1.0	0	0	0	0	0
2	Containment (PWR)	Reactor Coolant Pump	Power	6.1E-03	0.14	0.86	0	0	0	0
3	Containment (PWR)	Transients and Hotwork	Power	2.0E-03	0	0	0.44	0.56	0	0
4	Control Room	Main Control Board	All	2.5E-03	1.0	0	0	0	0	0
5	Control/Aux/Reactor Building	Cable fires caused by welding and cutting	Power	1.6E-03	0	0	0	1.0	0	0
6	Control/Aux/Reactor Building	Transient fires caused by welding and cutting	Power	9.7E-03	0	0	0	1.0	0	0
7	Control/Aux/Reactor Building	Transients	Power	3.9E-03	0	0	1.0	0	0	0
8	Diesel Generator Room	Diesel Generators	All	2.1E-02	0.16	0.84	0	0	0	0
9	Plant-Wide Components	Air Compressors	All	2.4E-03	0.83	0.17	0	0	0	0
10	Plant-Wide Components	Battery Chargers	All	1.8E-03	1.0	0	0	0	0	0
11	Plant-Wide Components	Cable fires caused by welding and cutting	Power	2.0E-03	0	0	0	1.0	0	0
12	Plant-Wide Components	Cable Run (Self-ignited cable fires)	All	4.4E-03	1.0	0	0	0	0	0
13	Plant-Wide Components	Dryers	All	2.6E-03	0	0	1.0	0	0	0
14	Plant-Wide Components	Electric Motors	All	4.6E-03	1.0	0	0	0	0	0

6-3

Figura S.1: Tabla 6-1 del NUREG/CR-6850 (1).

Table 6-1
Fire Frequency Bins and Generic Frequencies (Continued)

ID	Location	Ignition Source (Equipment Type)	Mode	Generic Freq (per rx yr)	Split Fractions for Fire Type					
					Electrical	Oil	Transient	Hotwork	Hydrogen	HEAF[1]
15	Plant-Wide Components	Electrical Cabinets	All	4.5E-02	1.0	0	0	0	0	0
16	Plant-Wide Components	High Energy Arcing Faults[1]	All	1.5E-03	0	0	0	0	0	1.0
17	Plant-Wide Components	Hydrogen Tanks	All	1.7E-03	0	0	0	0	1.0	0
18	Plant-Wide Components	Junction Boxes	All	1.9E-03	1.0	0	0	0	0	0
19	Plant-Wide Components	Misc. Hydrogen Fires	All	2.5E-03	0	0	0	0	1.0	0
20	Plant-Wide Components	Off-gas/H2 Recombiner (BWR)	Power	4.4E-02	0	0	0	0	1.0	0
21	Plant-Wide Components	Pumps	All	2.1E-02	0.54	0.46	0	0	0	0
22	Plant-Wide Components	RPS MG Sets	Power	1.6E-03	1.0	0	0	0	0	0
23a	Plant-Wide Components	Transformers (Oil filled)	All	9.9E-03	0	1.0	0	0	0	0
23b	Plant-Wide Components	Transformers (Dry)			1.0	0	0	0	0	0
24	Plant-Wide Components	Transient fires caused by welding and cutting	Power	4.9E-03	0	0	0	1.0	0	0

Figura S.2: Tabla 6-1 del NUREG/CR-6850 (2).

Table 6-1
Fire Frequency Bins and Generic Frequencies (Continued)

ID	Location	Ignition Source (Equipment Type)	Mode	Generic Freq (per rx yr)	Split Fractions for Fire Type					
					Electrical	Oil	Transient	Hotwork	Hydrogen	HEAF[1]
25	Plant-Wide Components	Transients	Power	9.9E-03	0	0	1.0	0	0	0
26	Plant-Wide Components	Ventilation Subsystems	All	7.4E-03	0.95	0.05	0	0	0	0
27	Transformer Yard	Transformer – Catastrophic[2]	Power	6.0E-03	1.0[3]		0	0	0	0
28	Transformer Yard	Transformer - Non Catastrophic[2]	Power	1.2E-02	1.0[3]		0	0	0	0
29	Transformer Yard	Yard transformers (Others)	Power	2.2E-03	1.0	0	0	0	0	0
30	Turbine Building	Boiler	All	1.1E-03	0	1.0	0	0	0	0
31	Turbine Building	Cable fires caused by welding and cutting	Power	1.6E-03	0	0	0	1.0	0	0
32	Turbine Building	Main Feedwater Pumps	Power	1.3E-02	0.11	0.89	0	0	0	0
33	Turbine Building	Turbine Generator Excitor	Power	3.9E-03	1.0	0	0	0	0	0
34	Turbine Building	Turbine Generator Hydrogen	Power	6.5E-03	0	0	0	0	1.0	0
35	Turbine Building	Turbine Generator Oil	Power	9.5E-03	0	1.0	0	0	0	0
36	Turbine Building	Transient fires caused by welding and cutting	Power	8.2E-03	0	0	0	1.0	0	0
37	Turbine Building	Transients	Power	8.5E-03	0	0	1.0	0	0	0

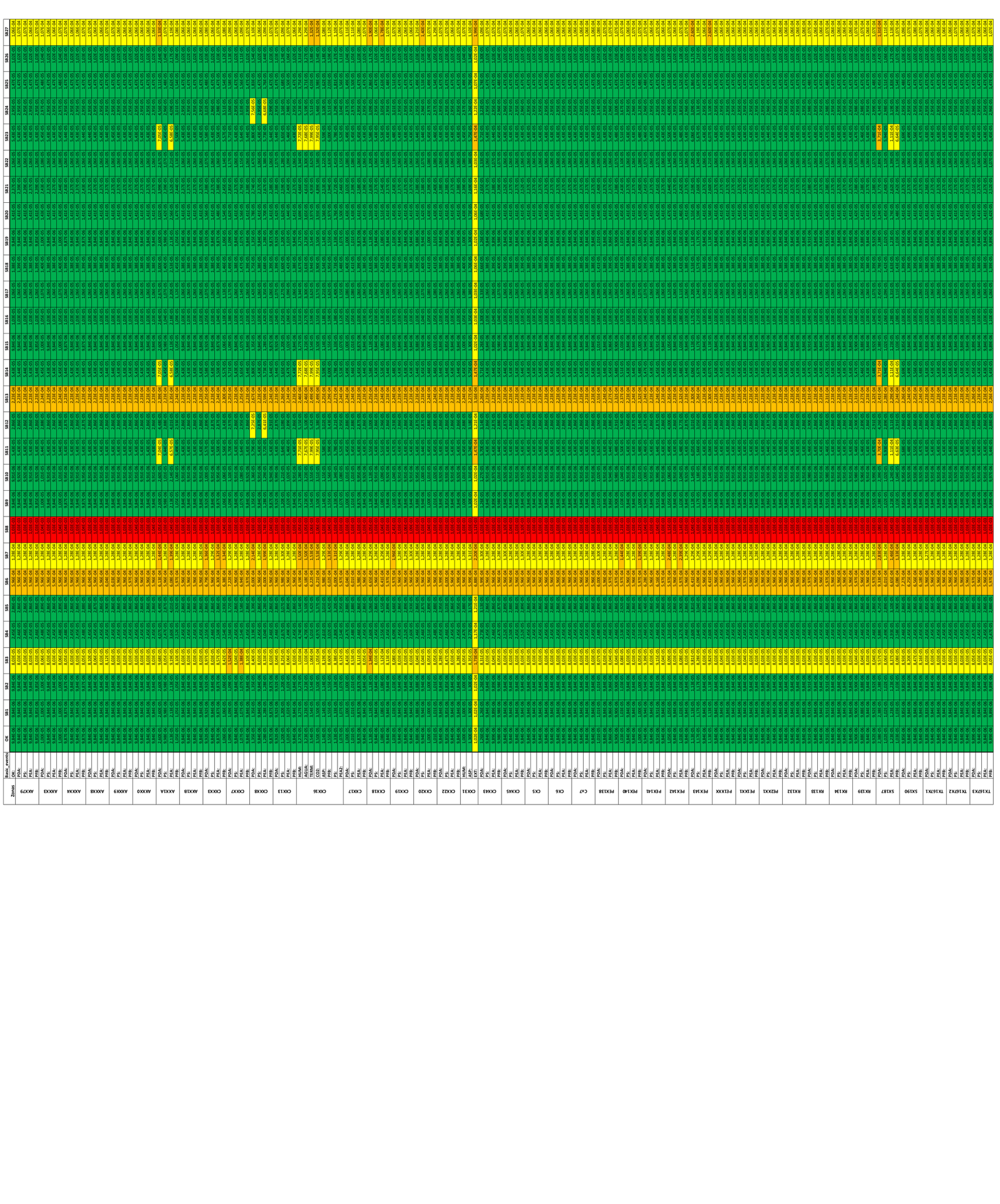
1. See Appendix M for a description of high-energy arcing fault (HEAF) fires.

2. See Section 6.5.6 below for a definition.

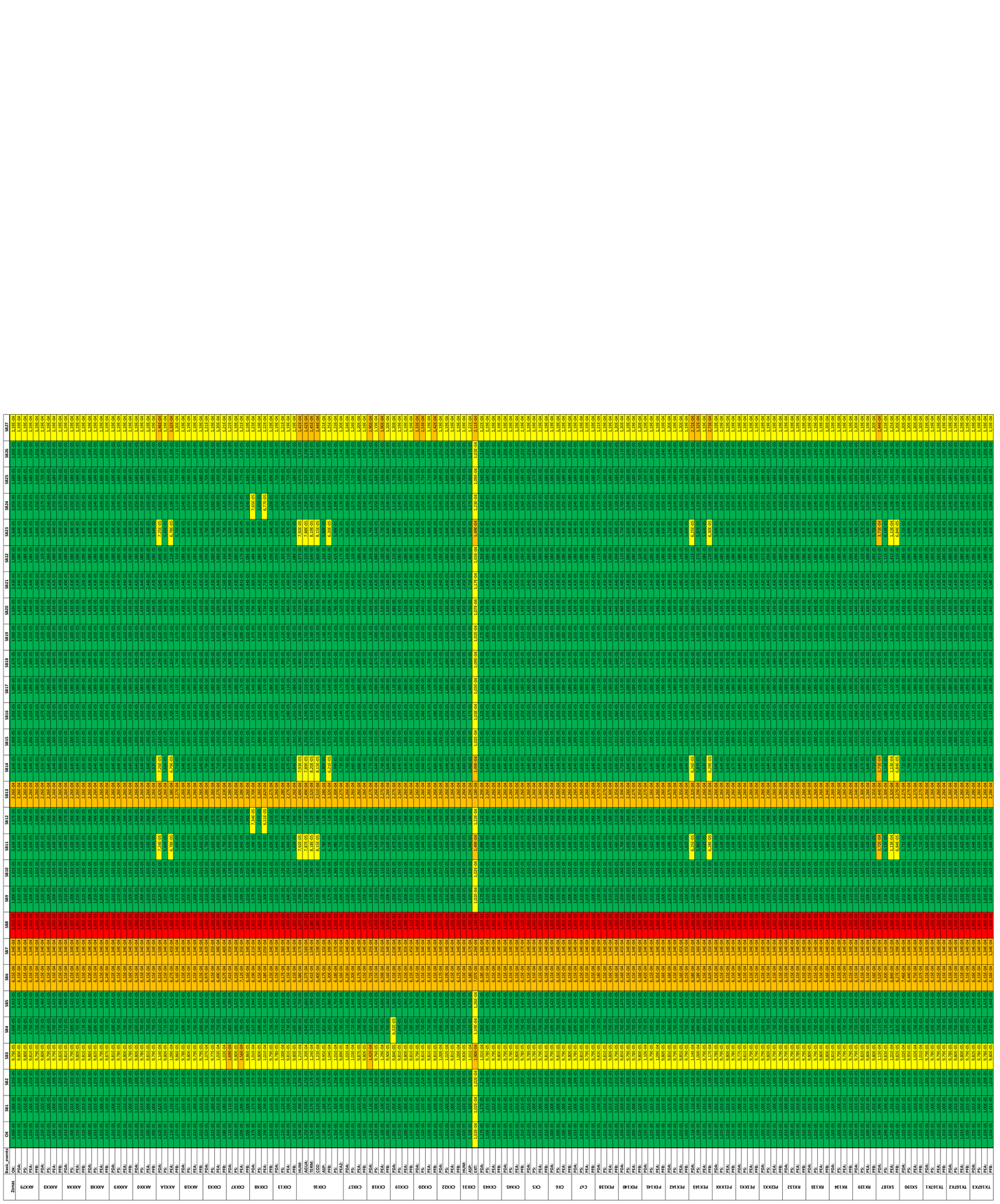
3. The event should be considered either as an electrical or oil fire, whichever yields the worst consequences.

Figura S.3: Tabla 6-1 del NUREG/CR-6850 (3).

S.2. Matriz MCI de valores puntuales



S.3. Matriz MCI de valores medios



S.4. Matriz MCI de valores percentil 95

	Basic_events	OK	SB1	SB2	SB3	SB4	SB5	SB6	SB7	SB8	SB9	SB10	SB11	SB12	SB13	SB14	SB15	SB16	SB17	SB18	SB19	SB20	SB21	SB22	SB23	SB24	SB25	SB26	SB27
Zonas	OK:	1,28E-05	1,28E-05	1,29E-05	1,17E-04	3,12E-05	3,91E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,15E-05	3,38E-05	2,31E-04	6,17E-05	1,29E-05	1,34E-05	1,37E-05	3,15E-05	1,29E-05	1,74E-05	3,34E-05	1,35E-05	6,16E-05	3,47E-05	2,32E-05	1,34E-05	1,41E-04
AXX79	PDA:	1,29E-05	1,29E-05	1,29E-05	1,17E-04	3,12E-05	3,93E-05	6,32E-04	1,44E-04	1,07E-03	1,30E-05	1,30E-05	6,16E-05	3,38E-05	2,31E-04	6,17E-05	1,28E-05	1,34E-05	1,37E-05	3,14E-05	1,29E-05	1,75E-05	3,37E-05	1,37E-05	6,15E-05	3,47E-05	2,29E-05	1,34E-05	1,41E-04
	PS:	1,29E-05	1,30E-05	1,29E-05	1,16E-04	3,12E-05	3,94E-05	6,32E-04	1,44E-04	1,07E-03	1,30E-05	1,30E-05	6,14E-05	3,37E-05	2,31E-04	6,16E-05	1,30E-05	1,33E-05	1,37E-05	3,12E-05	1,30E-05	1,75E-05	3,40E-05	1,36E-05	6,15E-05	3,48E-05	2,29E-05	1,34E-05	1,41E-04
	PEA:	1,29E-05	1,29E-05	1,29E-05	1,17E-04	3,13E-05	3,92E-05	6,32E-04	1,44E-04	1,07E-03	1,28E-05	1,30E-05	6,16E-05	3,37E-05	2,31E-04	6,16E-05	1,28E-05	1,35E-05	1,36E-05	3,15E-05	1,29E-05	1,75E-05	3,34E-05	1,36E-05	6,16E-05	3,48E-05	2,30E-05	1,34E-05	1,41E-04
	PFB:	1,29E-05	1,29E-05	1,29E-05	1,16E-04	3,13E-05	3,94E-05	6,32E-04	1,44E-04	1,07E-03	1,30E-05	1,29E-05	6,16E-05	3,36E-05	2,31E-04	6,15E-05	1,30E-05	1,34E-05	1,38E-05	3,23E-05	1,29E-05	1,75E-05	3,43E-05	1,35E-05	6,16E-05	3,47E-05	2,31E-05	1,33E-05	1,41E-04
AXXX3	PDA:	1,32E-05	1,31E-05	1,30E-05	1,16E-04	3,17E-05	3,96E-05	6,32E-04	1,44E-04	1,08E-03	1,31E-05	1,32E-05	6,17E-05	3,39E-05	2,31E-04	6,18E-05	1,31E-05	1,36E-05	1,38E-05	3,17E-05	1,31E-05	1,76E-05	3,42E-05	1,37E-05	6,18E-05	3,48E-05	2,34E-05	1,35E-05	1,41E-04
	PS:	1,29E-05	1,29E-05	1,29E-05	1,16E-04	3,12E-05	3,93E-05	6,31E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,14E-05	3,38E-05	2,31E-04	6,16E-05	1,28E-05	1,33E-05	1,37E-05	3,22E-05	1,29E-05	1,74E-05	3,29E-05	1,35E-05	6,14E-05	3,46E-05	2,31E-05	1,34E-05	1,41E-04
	PEA:	1,29E-05	1,28E-05	1,28E-05	1,16E-04	3,12E-05	3,93E-05	6,31E-04	1,44E-04	1,07E-03	1,28E-05	1,30E-05	6,15E-05	3,37E-05	2,31E-04	6,16E-05	1,29E-05	1,34E-05	1,37E-05	3,15E-05	1,29E-05	1,75E-05	3,31E-05	1,36E-05	6,16E-05	3,48E-05	2,31E-05	1,34E-05	1,41E-04
	PFB:	1,30E-05	1,31E-05	1,30E-05	1,17E-04	3,16E-05	3,97E-05	6,32E-04	1,44E-04	1,08E-03	1,31E-05	1,31E-05	6,17E-05	3,39E-05	2,31E-04	6,19E-05	1,30E-05	1,36E-05	1,39E-05	3,23E-05	1,30E-05	1,76E-05	3,40E-05	1,37E-05	6,17E-05	3,49E-05	2,31E-05	1,36E-05	1,41E-04
AXXX4	PDA:	1,29E-05	1,29E-05	1,29E-05	1,17E-04	3,14E-05	3,94E-05	6,32E-04	1,44E-04	1,08E-03	1,29E-05	1,29E-05	6,16E-05	3,38E-05	2,31E-04	6,18E-05	1,29E-05	1,34E-05	1,37E-05	3,20E-05	1,29E-05	1,76E-05	3,46E-05	1,36E-05	6,17E-05	3,48E-05	2,30E-05	1,34E-05	1,41E-04
	PS:	1,29E-05	1,30E-05	1,30E-05	1,16E-04	3,11E-05	3,92E-05	6,31E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,16E-05	3,37E-05	2,31E-04	6,16E-05	1,29E-05	1,34E-05	1,38E-05	3,20E-05	1,30E-05	1,75E-05	3,31E-05	1,36E-05	6,16E-05	3,48E-05	2,30E-05	1,33E-05	1,41E-04
	PEA:	1,29E-05	1,29E-05	1,28E-05	1,17E-04	3,12E-05	3,93E-05	6,31E-04	1,44E-04	1,07E-03	1,30E-05	1,30E-05	6,14E-05	3,37E-05	2,31E-04	6,16E-05	1,31E-05	1,34E-05	1,36E-05	3,21E-05	1,30E-05	1,75E-05	3,36E-05	1,36E-05	6,16E-05	3,48E-05	2,28E-05	1,34E-05	1,41E-04
	PFB:	1,29E-05	1,29E-05	1,28E-05	1,17E-04	3,15E-05	3,95E-05	6,32E-04	1,44E-04	1,08E-03	1,29E-05	1,30E-05	6,16E-05	3,37E-05	2,31E-04	6,18E-05	1,29E-05	1,34E-05	1,36E-05	3,16E-05	1,30E-05	1,75E-05	3,50E-05	1,37E-05	6,16E-05	3,47E-05	2,31E-05	1,35E-05	1,41E-04
AXXX8	PDA:	1,29E-05	1,30E-05	1,29E-05	1,17E-04	3,13E-05	3,95E-05	6,39E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,15E-05	3,39E-05	2,31E-04	6,17E-05	1,29E-05	1,34E-05	1,37E-05	3,23E-05	1,30E-05	1,74E-05	3,33E-05	1,36E-05	6,17E-05	3,46E-05	2,31E-05	1,33E-05	1,41E-04
	PS:	1,30E-05	1,29E-05	1,30E-05	1,17E-04	3,12E-05	3,96E-05	6,31E-04	1,44E-04	1,07E-03	1,29E-05	1,29E-05	6,13E-05	3,37E-05	2,31E-04	6,17E-05	1,28E-05	1,34E-05	1,37E-05	3,18E-05	1,29E-05	1,75E-05	3,33E-05	1,37E-05	6,16E-05	3,48E-05	2,30E-05	1,34E-05	1,41E-04
	PEA:	1,29E-05	1,28E-05	1,29E-05	1,17E-04	3,13E-05	3,92E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,31E-05	6,15E-05	3,38E-05	2,31E-04	6,15E-05	1,29E-05	1,34E-05	1,38E-05	3,18E-05	1,30E-05	1,74E-05	3,32E-05	1,36E-05	6,15E-05	3,47E-05	2,29E-05	1,34E-05	1,41E-04
	PFB:	1,29E-05	1,30E-05	1,29E-05	1,18E-04	3,13E-05	3,97E-05	6,41E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,16E-05	3,37E-05	2,31E-04	6,19E-05	1,29E-05	1,34E-05	1,37E-05	3,19E-05	1,30E-05	1,75E-05	3,36E-05	1,36E-05	6,15E-05	3,47E-05	2,31E-05	1,33E-05	1,41E-04
AXXX9	PDA:	1,30E-05	1,29E-05	1,29E-05	1,17E-04	3,13E-05	3,92E-05	6,47E-04	1,44E-04	1,07E-03	1,29E-05	1,32E-05	6,16E-05	3,35E-05	2,31E-04	6,17E-05	1,29E-05	1,34E-05	1,37E-05	3,15E-05	1,29E-05	1,75E-05	3,31E-05	1,37E-05	6,17E-05	3,47E-05	2,31E-05	1,34E-05	1,41E-04
	PS:	1,29E-05	1,30E-05	1,29E-05	1,16E-04	3,12E-05	3,92E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,14E-05	3,37E-05	2,31E-04	6,16E-05	1,28E-05	1,34E-05	1,37E-05	3,14E-05	1,29E-05	1,74E-05	3,38E-05	1,36E-05	6,16E-05	3,48E-05	2,32E-05	1,33E-05	1,41E-04
	PEA:	1,29E-05	1,29E-05	1,29E-05	1,17E-04	3,13E-05	3,93E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,17E-05	3,37E-05	2,31E-04	6,17E-05	1,28E-05	1,34E-05	1,37E-05	3,10E-05	1,29E-05	1,74E-05	3,33E-05	1,36E-05	6,13E-05	3,47E-05	2,31E-05	1,34E-05	1,41E-04
	PFB:	1,29E-05	1,28E-05	1,29E-05	1,16E-04	3,14E-05	3,91E-05	6,33E-04	1,44E-04	1,07E-03	1,29E-05	1,31E-05	6,15E-05	3,37E-05	2,31E-04	6,16E-05	1,29E-05	1,33E-05	1,37E-05	3,14E-05	1,29E-05	1,74E-05	3,36E-05	1,36E-05	6,15E-05	3,47E-05	2,31E-05	1,33E-05	1,41E-04
AXXX0	PDA:	1,30E-05	1,29E-05	1,28E-05	1,17E-04	3,12E-05	3,94E-05	6,31E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,16E-05	3,37E-05	2,31E-04	6,17E-05	1,28E-05	1,35E-05	1,37E-05	3,22E-05	1,30E-05	1,75E-05	3,31E-05	1,36E-05	6,15E-05	3,47E-05	2,29E-05	1,34E-05	1,41E-04
	PS:	1,30E-05	1,29E-05	1,28E-05	1,16E-04	3,12E-05	3,93E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,15E-05	3,36E-05	2,31E-04	6,17E-05	1,29E-05	1,34E-05	1,36E-05	3,19E-05	1,29E-05	1,74E-05	3,36E-05	1,36E-05	6,15E-05	3,47E-05	2,31E-05	1,34E-05	1,40E-04
	PEA:	1,29E-05	1,29E-05	1,29E-05	1,17E-04	3,12E-05	3,93E-05	6,32E-04	1,44E-04	1,07E-03	1,30E-05	1,30E-05	6,15E-05	3,37E-05	2,31E-04	6,16E-05	1,29E-05	1,33E-05	1,38E-05	3,16E-05	1,29E-05	1,75E-05	3,37E-05	1,37E-05	6,15E-05	3,48E-05	2,29E-05	1,33E-05	1,41E-04
	PFB:	1,28E-05	1,29E-05	1,30E-05	1,17E-04	3,12E-05	3,92E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,16E-05	3,36E-05	2,31E-04	6,17E-05	1,29E-05	1,33E-05	1,37E-05	3,12E-05	1,31E-05	1,76E-05	3,33E-05	1,35E-05	6,14E-05	3,46E-05	2,27E-05	1,34E-05	1,41E-04
AXX1A	PDA:	2,91E-05	2,91E-05	2,91E-05	1,33E-04	4,75E-05	5,56E-05	6,48E-04	1,60E-04	1,08E-03	2,90E-05	2,91E-05	7,76E-05	4,98E-05	2,47E-04	7,78E-05	2,91E-05	2,95E-05	2,98E-05	4,77E-05	2,90E-05	3,36E-05	4,93E-05	2,97E-05	7,77E-05	5,08E-05	3,97E-05	2,95E-05	1,68E-04
	PS:	1,29E-05	1,30E-05	1,31E-05	1,17E-04	3,14E-05	3,95E-05	6,32E-04	1,44E-04	1,07E-03	1,30E-05	1,31E-05	6,17E-05	3,38E-05	2,31E-04	6,18E-05	1,30E-05	1,35E-05	1,38E-05	3,14E-05	1,30E-05	1,75E-05	3,33E-05	1,37E-05	6,16E-05	3,50E-05	2,31E-05	1,37E-05	1,41E-04
	PEA:	2,45E-05	2,44E-05	2,44E-05	1,28E-04	4,28E-05	5,08E-05	6,43E-04	1,55E-04	1,08E-03	2,44E-05	2,44E-05	7,30E-05	4,51E-05	2,42E-04	7,33E-05	2,43E-05	2,50E-05	2,52E-05	4,35E-05	2,44E-05	2,89E-05	4,48E-05	2,51E-05	7,29E-05	4,62E-05	3,47E-05	2,49E-05	1,54E-04
	PFB:	1,35E-05	1,36E-05	1,36E-05	1,17E-04	3,19E-05	3,99E-05	6,32E-04	1,45E-04	1,07E-03	1,36E-05	1,36E-05	6,21E-05	3,43E-05	2,31E-04	6,23E-05	1,37E-05	1,39E-05	1,43E-05	3,21E-05	1,34E-05	1,82E-05	3,41E-05	1,42E-05	6,23E-05	3,53E-05	2,35E-05	1,41E-05	1,42E-04
AXX1B	PDA:	1,29E-05	1,30E-05	1,29E-05	1,17E-04	3,12E-05	3,92E-05	6,31E-04	1,44E-04	1,07E-03	1,30E-05	1,30E-05	6,13E-05	3,37E-05	2,31E-04	6,16E-05	1,30E-05	1,34E-05	1,37E-05	3,26E-05	1,29E-05	1,75E-05	3,34E-05	1,36E-05	6,15E-05	3,46E-05	2,31E-05	1,34E-05	1,41E-04
	PS:	1,29E-05	1,30E-05	1,29E-05	1,17E-04	3,12E-05	3,93E-05	6,32E-04	1,44E-04	1,07E-03	1,28E-05	1,30E-05	6,17E-05	3,36E-05	2,31E-04	6,16E-05	1,29E-05	1,34E-05	1,37E-05	3,13E-05	1,30E-05	1,74E-05	3,33E-05	1,35E-05	6,17E-05	3,47E-05	2,30E-05	1,35E-05	1,42E-04
	PEA:	1,30E-05	1,28E-05	1,29E-05	1,17E-04	3,13E-05	3,92E-05	6,31E-04	1,44E-04	1,07E-03	1,28E-05	1,30E-05	6,16E-05	3,39E-05	2,31E-04	6,16E-05	1,29E-05	1,34E-05	1,38E-05	3,09E-05	1,29E-05	1,75E-05	3,32E-05	1,36E-05	6,16E-05	3,46E-05	2,32E-05	1,33E-05	1,41E-04
	PFB:	1,30E-05	1,29E-05	1,28E-05	1,16E-04	3,11E-05	3,92E-05	6,31E-04	1,44E-04	1,07E-03	1,30E-05	1,30E-05	6,15E-05	3,38E-05	2,31E-04	6,17E-05	1,29E-05	1,35E-05	1,35E-05	3,15E-05	1,30E-05	1,75E-05	3,30E-05	1,36E-05	6,16E-05	3,48E-05	2,30E-05	1,33E-05	1,41E-04
CXXX3	PDA:	1,31E-05	1,30E-05	1,29E-05	1,27E-04	3,22E-05	3,93E-05	7,14E-04	1,52E-04	1,08E-03	1,29E-05	1,31E-05	6,32E-05	3,40E-05	2,33E-04	6,33E-05	1,29E-05	1,35E-05	1,39E-05	3,18E-05	1,30E-05	1,93E-05	3,31E-05	1,37E-05	6,31E-05	3,55E-05	2,32E-05	1,34E-05	1,43E-04
	PS:	1,29E-05	1,29E-05	1,29E-05	1,16E-04	3,12E-05	3,92E-05	6,31E-04	1,45E-04	1,07E-03	1,30E-05	1,30E-05	6,14E-05	3,38E-05	2,31E-04	6,15E-05	1,30E-05	1,33E-05	1,37E-05	3,22E-05	1,29E-05	1,74E-05	3,31E-05	1,35E-05	6,15E-05	3,49E-05	2,30E-05	1,34E-05	1,41E-04
	PEA:	1,30E-05	1,30E-05	1,30E-05	1,24E-04	3,18E-05	3,93E-05	6,66E-04	1,48E-04	1,07E-03	1,29E-05	1,30E-05	6,22E-05	3,38E-05	2,32E-04	6,24E-05	1,29E-05	1,35E-05	1,36E-05	3,22E-05	1,30E-05	1,83E-05	3,35E-05	1,36E-05	6,24E-05	3,51E-05	2,32E-05	1,35E-05	1,42E-04
	PFB:	1,37E-05	1,36E-05	1,36E-05	1,22E-04	3,23E-05	4,00E-05	6,74E-04	1,50E-04	1,08E-03	1,37E-05	1,37E-05	6,33E-05	3,94E-05	2,38E-04	6,32E-05	1,36E-05	1,42E-05	1,44E-05	3,24E-05	1,36E-05	1,93E-05	3,35E-05	1,44E-05	6,31E-05	4,05E-05	2,37E-05	1,44E-05	1,42E-04
CXXX7	PDA:	1,39E-05	1,41E-05	1,40E-05	1,89E-04	3,24E-05	4,89E-05	7,61E-04	1,45E-04	1,07E-03	1,39E-05	1,42E-05	6,44E-05	3,48E-05	2,33E-04	6,44E-05	1,41E-05	1,78E-05	1,49E-05	3,34E-05	1,41E-05	1,96E-05	3,86E-05	1,48E-05	6,45E-05	3,58E-05	2,42E-05	1,45E-05	1,44E-04
	PS:	1,30E-05	1,29E-05	1,29E-05	1,17E-04	3,13E-05	3,92E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,31E-05	6,15E-05	3,37E-05	2,31E-04	6,17E-05	1,30E-05	1,33E-05	1,37E-05	3,16E-05	1,29E-05	1,75E-05	3,36E-05	1,36E-05	6,16E-05	3,47E-05	2,29E-05	1,34E-05	1,41E-04
	PEA:	1,38E-05	1,38E-05	1,38E-05	1,76E-04	3,22E-05	4,73E-05	7,33E-04	1,45E-04	1,07E-03	1,37E-05	1,37E-05	6,36E-05	3,47E-05	2,32E-04	6,39E-05	1,37E-05	1,69E-05	1,45E-05	3,27E-05	1,38E-05	1,91E-05	3,73E-05	1,45E-05	6,37E-05	3,57E-05	2,37E-05	1,42E-05	1,43E-04
	PFB:	1,29E-05	1,29E-05	1,29E-05	1,17E-04	3,12E-05	3,95E-05	6,33E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,15E-05	3,36E-05	2,31E-04	6,16E-05	1,28E-05	1,34E-05	1,38E-05	3,21E-05	1,30E-05	1,75E-05	3,36E-05	1,35E-05	6,16E-05	3,45E-05	2,29E-05	1,33E-05	1,41E-04
CXXX8	PDA:	1,78E-05	1,75E-05	1,75E-05	1,20E-04	4,03E-05	4,55E-05	6,37E-04	2,38E-04	1,97E-03	1,75E-05	1,78E-05	6,57E-05	7,76E-05	2,75E-04	6,59E-05	1,78E-05	1,93E-05	1,84E-05	3,54E-05	1,76E-05	2,21E-05	3,75E-05	1,88E-05	6,59E-05	8,15E-05	2,73E-05	2,09E-05	1,45E-04
	PS:	1,29E-05	1,29E-05	1,29E-05	1,17E-04	3,12E-05	3,93E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,15E-05	3,39E-05	2,31E-04	6,17E-05	1,29E-05	1,34E-05	1,37E-05	3,16E-05	1,29E-05	1,76E-05	3,31E-05	1,36E-05	6,17E-05	3,49E-05	2,27E-05	1,34E-05	1,41E-04
	PEA:	1,67E-05	1,66E-05	1,66E-05	1,19E-04	3,84E-05	4,38E-05	6,35E-04	2,21E-04	1,78E-03	1,67E-05	1,69E-05	6,48E-05	6,92E-05	2,66E-04	6,51E-05	1,65E-05	1,81E-05	1,73E-05	3,45E-05	1,65E-05	2,14E-05	3,61E-05	1,75E-05	6,50E-05	7,25E-05	2,62E-05	1,91E-05	1,44E-04
	PFB:	1,30E-05	1,29E-05	1,29E-05	1,16E-04	3,12E-05	3,93E-05	6,31E-04	1,45E-04	1,08E-03	1,29E-05	1,30E-05	6,15E-05	3,41E-05	2,31E-04	6,18E-05	1,29E-05	1,34E-05	1,38E-05	3,17E-05	1,29E-05	1,75E-05	3,31E-05	1,37E-05	6,15E-05	3,52E-05	2,30E-05	1,35E-05	1,42E-04
CXX13	PDA:	1,30E-05	1,30E-05	1,29E-05	1,16E-04	3,12E-05	3,93E-05	6,32E-04	1,44E-04	1,07E-03	1,31E-05	1,31E-05	6,17E-05	3,37E-05	2,31E-04	6,17E-05	1,30E-05	1,35E-05	1,38E-05	3,20E-05	1,30E-05	1,75E-05	3,34E-05	1,36E-05	6,17E-05	3,48E-05	2,32E-05	1,35E-05	1,41E-04
	PS:	1,51E-05	1,49E-05	1,50E-05	1,19E-04	3,33E-05	4,14E-05	6,34E-04	1,46E-04	1,07E-03	1,51E-05	1,51E-05	6,36E-05	3,59E-05	2,33E-04	6,38E-05	1,51E-05	1,56E-05	1,60E-05	3,37E-05	1,51E-05	1,96E-05	3,54E-05	1,58E-05	6,36E-05	3,69E-05	2,52E-05	1,55E-05	1,43E-04
	PEA:	1,33E-05	1,32E-05	1,33E-05	1,17E-04	3,15E-05	3,95E-05	6,33E-04	1,44E-04	1,07E-03	1,32E-05	1,33E-05	6,18E-05	3,40E-05	2,31E-04	6,20E-05	1,32E-05	1,36E-05	1,40E-05	3,24E-05	1,33E-05	1,77E-05	3,36E-05	1,39E-05	6,19E-05	3,50E-05	2,33E-05	1,37E-05	1,42E-04
	PFB:	1,30E-05	1,30E-05	1,30E-05	1,17E-04	3,11E-05	3,94E-05	6,31E-04	1,44E-04	1,07E-03	1,30E-05	1,30E-05	6,16E-05	3,38E-05	2,31E-04	6,17E-05	1,30E-05	1,34E-05	1,36E-05	3,21E-05	1,29E-05	1,75E-05	3,31E-05	1,35E-05	6,14E-05	3,47E-05	2,30E-05	1,34E-05	1,41E-04
CXX16	HUM:	3,57E-05	3,57E-05	3,58E-05	1,40E-04	5,40E-05	6,21E-05	6,55E-04	1,67E-04	1,09E-03	3,58E-05	3,59E-05	8,44E-05	5,66E-05	2,54E-04	8,46E-05	3,58E-05	3,62E-05	3,65E-05	5,45E-05	3,57E-05	4,03E-05	5,68E-05	3,65E-05	8,44E-05	5,75E-05	4,60E-05	3,63E-05	1,64E-04
	AGUA:	3,53E-05	3,54E-05	3,54E-05	1,39E-04	5,37E-05	6,18E-05	6,54E-04	1,66E-04	1,09E-03	3,54E-05	3,55E-05	8,39E-05	5,62E-05	2,53E-04	8,41E-05	3,54E-05	3,58E-05	3,60E-05	5,48E-05	3,54E-05	3,99E-05	5,58E-05	3,60E-05	8,40E-05	5,71E-05	4,55E-05	3,58E-05	1,64E-04
	TERM:	3,85E-05	3,86E-05	3,85E-05	1,42E-04	5,68E-05	6,48E-05	6,57E-04	1,69E-04	1,09E-03	3,86E-05	3,86E-05	8,70E-05	5,92E-05	2,56E-04	8,72E-05	3,86E-05	3,90E-05	3,93E-05	5,72E-05	3,84E-05	4,31E-05	5,87E-05	3,92E-05	8,70E-05	6,03E-05	4,86E-05	3,90E-05	1,67E-04
	CO2:	3,81E-05	3,81E-05	3,82E-05	1,41E-04	5,64E-05	6,44E-05	6,57E-04	1,69E-04	1,09E-03	3,81E-05	3,82E-05	8,67E-05	5,89E-05	2,56E-04	8,68E-05	3,82E-05	3,85E-05	3,89E-05	5,78E-05	3,81E-05	4,26E-05	5,84E-05	3,87E-05	8,67E-05	5,98E-05	4,79E-05	3,86E-05	1,66E-04
	ASP:	1,45E-05	1,45E-05	1,46E-05	1,18E-04	3,28E-05	4,07E-05	6,33E-04	1,45E-04	1,07E-03	1,45E-05	1,46E-05	6,29E-05	3,53E-05	2,32E-04	6,33E-05	1,45E-05	1,49E-05	1,52E-05	3,36E-05	1,44E-05	1,90E-05	3,49E-05	1,51E-05	6,30E-05	3,62E-05	2,47E-05	1,50E-05	1,42E-04
	PFB:	1,86E-05	1,86E-05	1,86E-05	1,22E-04	3,68E-05	4,50E-05	6,37E-04	1,49E-04	1,07E-03	1,87E-05	1,85E-05	6,73E-05	3,93E-05	2,36E-04	6,74E-05	1,85E-05	1,91E-05	1,93E-05	3,79E-05	1,85E-05	2,32E-05	3,89E-05	1,92E-05	6,72E-05	4,04E-05	2,88E-05	1,91E-05	1,47E-04
	PS:	1,63E-05	1,65E-05	1,65E-05	1,20E-04	3,48E-05	4,27E-05	6,35E-04	1,47E-04	1,07E-03	1,63E-05	1,66E-05	6,51E-05	3,72E-05	2,34E-04	6,51E-05	1,63E-05	1,69E-05	1,72E-05	3,49E-05	1,64E-05	2,09E-05	3,68E-05	1,70E-05	6,51E-05	3,82E-05	2,66E-05	1,69E-05	1,44E-04
	PEA2:	1,40E-05	1,39E-05	1,38E-05	1,17E-04	3,21E-05	4,01E-05	6,32E-04	1,45E-04	1,07E-03	1,37E-05	1,40E-05	6,25E-05	3,45E-05	2,32E-04	6,25E-05	1,39E-05	1,43E-05	1,46E-05	3,27E-05	1,38E-05	1,83E-05	3,48E-05	1,45E-05	6,25E-05	3,56E-05	2,37E-05	1,44E-05	1,42E-04
CXX17	PDA:	1,31E-05	1,32E-05	1,31E-05	1,21E-04	3,15E-05	3,97E-05	6,40E-04	1,44E-04	1,07E-03	1,32E-05	1,32E-05	6,17E-05	3,40E-05	2,31E-04	6,23E-05	1,32E-05	1,37E-05	1,39E-05	3,16E-05	1,32E-05	1,77E-05	4,16E-05	1,37E-05	6,22E-05	3,48E-05	2,32E-05	1,35E-05	1,45E-04
	PS:	1,30E-05	1,30E-05	1,32E-05	1,22E-04	3,15E-05	3,94E-05	6,37E-04	1,44E-04	1,07E-03	1,32E-05	1,33E-05	6,18E-05	3,38E-05	2,31E-04	6,20E-05	1,32E-05	1,37E-05	1,40E-05	3,20E-05	1,30E-05	1,77E-05	3,38E-05	1,37E-05	6,19E-05	3,51E-05	2,35E-05	1,36E-05	1,47E-04
	PEA:	1,29E-05	1,29E-05	1,31E-05	1,17E-04	3,12E-05	3,91E-05	6,34E-04	1,44E-04	1,07E-03	1,30E-05	1,30E-05	6,15E-05	3,38E-05	2,31E-04	6,18E-05	1,29E-05	1,33E-05	1,37E-05	3,16E-05	1,29E-05	1,75E-05	3,55E-05	1,36E-05	6,18E-05	3,47E-05	2,30E-05	1,35E-05	1,42E-04
	PFB:	1,29E-05	1,29E-05	1,30E-05	1,16E-04	3,12E-05	3,91E-05	6,31E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,14E-05	3,36E-05	2,31E-04	6,17E-05	1,29E-05	1,35E-05	1,38E-05	3,21E-05	1,29E-05	1,75E-05	3,33E-05	1,35E-05	6,16E-05	3,48E-05	2,32E-05	1,34E-05	1,41E-04
CXX18	PDA:	1,42E-05	1,42E-05	1,42E-05	1,69E-04	3,27E-05	6,34E-05	7,11E-04	1,45E-04	1,09E-03	1,42E-05	1,43E-05	6,27E-05	3,52E-05	2,32E-04	6,29E-05	1,42E-05	1,47E-05	1,51E-05	6,03E-05	1,42E-05	1,88E-05	3,64E-05	1,49E-05	6,28E-05	3,60E-05	4,66E-05	1,48E-05	2,62E-04
	PS:	1,29E-05	1,29E-05	1,29E-05	1,16E-04	3,12E-05	3,92E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,31E-05	6,15E-05	3,37E-05	2,31E-04	6,16E-05	1,29E-05	1,34E-05	1,37E-05	3,22E-05	1,29E-05	1,75E-05	3,30E-05	1,36E-05	6,15E-05	3,46E-05	2,30E-05	1,34E-05	1,40E-04
	PEA:	1,40E-05	1,40E-05	1,40E-05	1,52E-04	3,23E-05	5,60E-05	6,97E-04	1,45E-04	1,08E-03	1,41E-05	1,41E-05	6,23E-05	3,48E-05	2,32E-04	6,26E-05	1,40E-05	1,45E-05	1,49E-05	6,25E-05	1,39E-05	1,85E-05	3,57E-05	1,47E-05	6,27E-05	3,58E-05	4,61E-05	1,45E-05	2,66E-04
	PFB:	1,29E-05	1,29E-05	1,29E-05	1,18E-04	3,12E-05	3,98E-05	6,33E-04	1,44E-04	1,07E-03	1,28E-05	1,30E-05	6,18E-05	3,37E-05	2,31E-04	6,17E-05	1,30E-05	1,34E-05	1,37E-05	3,21E-05	1,29E-05	1,75E-05	3,35E-05	1,36E-05	6,16E-05	3,48E-05	2,32E-05	1,33E-05	1,42E-04
CXX19	PDA:	1,33E-05	1,33E-05	1,34E-05	1,17E-04	7,76E-05	6,14E-05	6,32E-04	2,31E-04	2,49E-03	1,34E-05	1,34E-05	6,20E-05	3,45E-05	2,32E-04	6,21E-05	1,34E-05	1,39E-05	1,42E-05	3,18E-05	1,34E-05	1,80E-05	3,44E-05	1,42E-05	6,19E-05	3,54E-05	2,36E-05	1,38E-05	1,42E-04
	PS:	1,30E-05	1,29E-05	1,29E-05	1,17E-04	3,11E-05	3,92E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,29E-05	6,15E-05	3,38E-05	2,31E-04	6,16E-05	1,29E-05	1,34E-05	1,37E-05	3,12E-05	1,28E-05	1,74E-05	3,30E-05	1,35E-05	6,14E-05	3,48E-05	2,32E-05	1,34E-05	1,41E-04
	PEA:	1,28E-05	1,29E-05	1,29E-05	1,17E-04	3,20E-05	3,98E-05	6,32E-04	1,45E-04	1,10E-03	1,28E-05	1,30E-05	6,15E-05	3,36E-05	2,31E-04	6,17E-05	1,29E-05	1,34E-05	1,37E-05	3,20E-05	1,29E-05	1,75E-05	3,32E-05	1,36E-05	6,17E-05	3,47E-05	2,32E-05	1,34E-05	1,41E-04
	PFB:	1,29E-05	1,29E-05	1,29E-05	1,16E-04	3,95E-05	4,32E-05	6,31E-04	1,57E-04	1,12E-03	1,30E-05	1,30E-05	6,15E-05	3,39E-05	2,31E-04	6,15E-05	1,30E-05	1,34E-05	1,38E-05	3,16E-05	1,29E-05	1,75E-05	3,33E-05	1,36E-05	6,16E-05	3,47E-05	2,31E-05	1,34E-05	1,42E-04
CXX20	PDA:	1,30E-05	1,29E-05	1,30E-05	1,16E-04	3,14E-05	3,94E-05	6,31E-04	1,44E-04	1,07E-03	1,28E-05	1,31E-05	6,15E-05	3,39E-05	2,31E-04	6,17E-05	1,29E-05	1,34E-05	1,37E-05	3,23E-05	1,31E-05	1,75E-05	3,33E-05	1,36E-05	6,16E-05	3,46E-05	2,31E-05	1,34E-05	1,56E-04
	PS:	1,30E-05	1,30E-05	1,31E-05	1,17E-04	3,14E-05	3,94E-05	6,32E-04	1,44E-04	1,07E-03	1,31E-05	1,31E-05	6,18E-05	3,38E-05	2,31E-04	6,18E-05	1,30E-05	1,36E-05	1,39E-05	3,22E-05	1,30E-05	1,76E-05	3,35E-05	1,38E-05	6,18E-05	3,48E-05	2,39E-05	1,35E-05	1,74E-04
	PEA:	1,30E-05	1,32E-05	1,31E-05	1,17E-04	3,17E-05	3,96E-05	6,32E-04	1,44E-04	1,08E-03	1,31E-05	1,33E-05	6,16E-05	3,39E-05	2,31E-04	6,19E-05	1,33E-05	1,36E-05	1,38E-05	3,27E-05	1,31E-05	1,77E-05	3,38E-05	1,37E-05	6,18E-05	3,49E-05	2,35E-05	1,35E-05	1,41E-04
	PFB:	1,32E-05	1,31E-05	1,30E-05	1,16E-04	3,14E-05	3,94E-05	6,32E-04	1,44E-04	1,07E-03	1,31E-05	1,33E-05	6,17E-05	3,39E-05	2,31E-04	6,19E-05	1,31E-05	1,37E-05	1,39E-05	3,23E-05	1,32E-05	1,77E-05	3,33E-05	1,39E-05	6,19E-05	3,49E-05	2,41E-05	1,36E-05	1,63E-04
CXX22	PDA:	1,29E-05	1,29E-05	1,30E-05	1,20E-04	3,12E-05	4,04E-05	6,34E-04	1,44E-04	1,07E-03	1,30E-05	1,30E-05	6,13E-05	3,37E-05	2,31E-04	6,17E-05	1,28E-05	1,35E-05	1,37E-05	3,11E-05	1,29E-05	1,74E-05	3,35E-05	1,35E-05	6,15E-05	3,47E-05	2,32E-05	1,33E-05	1,41E-04
	PS:	1,29E-05	1,29E-05	1,29E-05	1,21E-04	3,13E-05	4,10E-05	6,36E-04	1,44E-04	1,07E-03	1,29E-05	1,31E-05	6,15E-05	3,36E-05	2,31E-04	6,15E-05	1,30E-05	1,35E-05	1,37E-05	3,15E-05	1,28E-05	1,74E-05	3,36E-05	1,36E-05	6,15E-05	3,47E-05	2,33E-05	1,35E-05	1,41E-04
	PEA:	1,29E-05	1,29E-05	1,29E-05	1,17E-04	3,11E-05	3,92E-05	6,32E-04	1,44E-04	1,07E-03	1,30E-05	1,31E-05	6,15E-05	3,36E-05	2,31E-04	6,18E-05	1,29E-05	1,34E-05	1,37E-05	3,15E-05	1,29E-05	1,73E-05	3,38E-05	1,35E-05	6,16E-05	3,46E-05	2,30E-05	1,33E-05	1,41E-04
	PFB:	1,29E-05	1,30E-05	1,28E-05	1,19E-04	3,12E-05	4,03E-05	6,34E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,15E-05	3,38E-05	2,31E-04	6,16E-05	1,29E-05	1,34E-05	1,38E-05	3,19E-05	1,29E-05	1,75E-05	3,35E-05	1,36E-05	6,17E-05	3,47E-05	2,30E-05	1,34E-05	1,41E-04
CXX31	HUM:	1,31E-05	1,30E-05	1,31E-05	1,17E-04	3,15E-05	3,94E-05	6,32E-04	1,44E-04	1,07E-03	1,31E-05	1,33E-05	6,18E-05	3,38E-05	2,31E-04	6,18E-05	1,30E-05	1,35E-05	1,38E-05	3,26E-05	1,31E-05	1,77E-05	3,33E-05	1,38E-05	6,17E-05	3,50E-05	2,33E-05	1,35E-05	1,41E-04
	ASP:	1,60E-05	1,61E-05	1,61E-05	1,20E-04	3,44E-05	4,23E-05	6,35E-04	1,47E-04	1,07E-03	1,61E-05	1,61E-05	6,46E-05	3,69E-05	2,34E-04	6,48E-05	1,62E-05	1,65E-05	1,69E-05	3,54E-05	1,60E-05	2,06E-05	3,65E-05	1,66E-05	6,48E-05	3,79E-05	2,63E-05	1,66E-05	1,44E-04
	EXT:	1,05E-04	1,05E-04	1,05E-04	2,09E-04	1,24E-04	1,32E-04	7,24E-04	2,36E-04	1,16E-03	1,05E-04	1,05E-04	1,54E-04	1,26E-04	3,23E-04	1,54E-04	1,05E-04	1,06E-04	1,06E-04	1,24E-04	1,05E-04	1,10E-04	1,25E-04	1,06E-04	1,54E-04	1,27E-04	1,15E-04	1,06E-04	2,33E-04
CXX43	PDA:	1,93E-05	1,95E-05	1,92E-05	1,20E-04	3,66E-05	4,47E-05	6,35E-04	1,48E-04	1,07E-03	1,94E-05	1,99E-05	6,67E-05	3,92E-05	2,36E-04	6,72E-05	1,92E-05	1,98E-05	2,03E-05	3,56E-05	1,94E-05	2,41E-05	3,80E-05	1,98E-05	6,69E-05	4,05E-05	2,79E-05	1,94E-05	1,45E-04
	PS:	1,29E-05	1,30E-05	1,28E-05	1,16E-04	3,12E-05	3,93E-05	6,32E-04	1,44E-04	1,07E-03	1,30E-05	1,30E-05	6,15E-05	3,37E-05	2,31E-04	6,17E-05	1,29E-05	1,34E-05	1,37E-05	3,11E-05	1,29E-05	1,75E-05	3,36E-05	1,37E-05	6,16E-05	3,47E-05	2,31E-05	1,34E-05	1,41E-04
	PEA:	1,30E-05	1,30E-05	1,30E-05	1,17E-04	3,14E-05	3,93E-05	6,32E-04	1,44E-04	1,07E-03	1,30E-05	1,30E-05	6,15E-05	3,38E-05	2,31E-04	6,17E-05	1,29E-05	1,35E-05	1,38E-05	3,15E-05	1,31E-05	1,75E-05	3,34E-05	1,37E-05	6,17E-05	3,46E-05	2,32E-05	1,35E-05	1,41E-04
	PFB:	1,30E-05	1,31E-05	1,31E-05	1,16E-04	3,13E-05	3,95E-05	6,32E-04	1,44E-04	1,07E-03	1,31E-05	1,31E-05	6,17E-05	3,39E-05	2,31E-04	6,19E-05	1,31E-05	1,35E-05	1,38E-05	3,17E-05	1,30E-05	1,75E-05	3,32E-05	1,37E-05	6,18E-05	3,48E-05	2,35E-05	1,35E-05	1,41E-04
CXX45	PDA:	1,28E-05	1,30E-05	1,30E-05	1,17E-04	3,20E-05	3,97E-05	6,32E-04	1,47E-04	1,14E-03	1,29E-05	1,30E-05	6,14E-05	3,37E-05	2,31E-04	6,16E-05	1,29E-05	1,34E-05	1,35E-05	3,12E-05	1,29E-05	1,75E-05	3,59E-05	1,35E-05	6,16E-05	3,48E-05	2,29E-05	1,34E-05	1,41E-04
	PS:	1,29E-05	1,30E-05	1,29E-05	1,16E-04	3,17E-05	3,95E-05	6,32E-04	1,44E-04	1,08E-03	1,28E-05	1,29E-05	6,14E-05	3,37E-05	2,31E-04	6,16E-05	1,29E-05	1,33E-05	1,38E-05	3,16E-05	1,29E-05	1,75E-05	3,30E-05	1,36E-05	6,16E-05	3,47E-05	2,32E-05	1,34E-05	1,41E-04
	PEA:	1,30E-05	1,30E-05	1,30E-05	1,17E-04	3,13E-05	3,92E-05	6,32E-04	1,44E-04	1,07E-03	1,30E-05	1,30E-05	6,15E-05	3,36E-05	2,31E-04	6,17E-05	1,29E-05	1,34E-05	1,37E-05	3,20E-05	1,29E-05	1,76E-05	3,31E-05	1,36E-05	6,15E-05	3,46E-05	2,29E-05	1,33E-05	1,41E-04
	PFB:	1,29E-05	1,30E-05	1,28E-05	1,16E-04	3,20E-05	3,95E-05	6,32E-04	1,48E-04	1,14E-03	1,29E-05	1,30E-05	6,15E-05	3,38E-05	2,31E-04	6,17E-05	1,30E-05	1,34E-05	1,37E-05	3,15E-05	1,29E-05	1,74E-05	3,70E-05	1,36E-05	6,16E-05	3,49E-05	2,30E-05	1,34E-05	1,41E-04
CX5	PDA:	1,29E-05	1,29E-05	1,30E-05	1,16E-04	3,13E-05	3,93E-05	6,32E-04	1,44E-04	1,07E-03	1,31E-05	1,30E-05	6,15E-05	3,38E-05	2,31E-04	6,16E-05	1,30E-05	1,34E-05	1,37E-05	3,08E-05	1,29E-05	1,75E-05	3,36E-05	1,36E-05	6,16E-05	3,48E-05	2,31E-05	1,34E-05	1,41E-04
	PS:	1,30E-05	1,29E-05	1,29E-05	1,17E-04	3,12E-05	3,93E-05	6,31E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,16E-05	3,35E-05	2,31E-04	6,18E-05	1,30E-05	1,33E-05	1,37E-05	3,16E-05	1,29E-05	1,74E-05	3,32E-05	1,36E-05	6,16E-05	3,47E-05	2,32E-05	1,33E-05	1,41E-04
	PEA:	1,29E-05	1,28E-05	1,29E-05	1,16E-04	3,11E-05	3,93E-05	6,31E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,15E-05	3,36E-05	2,31E-04	6,16E-05	1,30E-05	1,34E-05	1,36E-05	3,25E-05	1,29E-05	1,75E-05	3,29E-05	1,37E-05	6,16E-05	3,47E-05	2,33E-05	1,34E-05	1,42E-04
	PFB:	1,29E-05	1,29E-05	1,30E-05	1,16E-04	3,13E-05	3,92E-05	6,32E-04	1,44E-04	1,07E-03	1,30E-05	1,31E-05	6,15E-05	3,38E-05	2,31E-04	6,17E-05	1,29E-05	1,34E-05	1,37E-05	3,17E-05	1,29E-05	1,74E-05	3,33E-05	1,36E-05	6,17E-05	3,47E-05	2,30E-05	1,34E-05	1,41E-04
CX6	PDA:	1,28E-05	1,29E-05	1,30E-05	1,16E-04	3,11E-05	3,93E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,15E-05	3,37E-05	2,31E-04	6,16E-05	1,29E-05	1,34E-05	1,37E-05	3,17E-05	1,28E-05	1,75E-05	3,30E-05	1,35E-05	6,17E-05	3,47E-05	2,29E-05	1,34E-05	1,40E-04
	PS:	1,29E-05	1,29E-05	1,30E-05	1,17E-04	3,12E-05	3,93E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,14E-05	3,37E-05	2,31E-04	6,16E-05	1,28E-05	1,35E-05	1,36E-05	3,15E-05	1,28E-05	1,76E-05	3,32E-05	1,36E-05	6,16E-05	3,47E-05	2,30E-05	1,34E-05	1,41E-04
	PEA:	1,30E-05	1,28E-05	1,29E-05	1,16E-04	3,12E-05	3,93E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,16E-05	3,36E-05	2,31E-04	6,17E-05	1,30E-05	1,34E-05	1,37E-05	3,16E-05	1,29E-05	1,74E-05	3,33E-05	1,36E-05	6,16E-05	3,48E-05	2,30E-05	1,33E-05	1,41E-04
	PFB:	1,29E-05	1,30E-05	1,30E-05	1,16E-04	3,12E-05	3,91E-05	6,32E-04	1,44E-04	1,07E-03	1,28E-05	1,30E-05	6,15E-05	3,37E-05	2,31E-04	6,17E-05	1,29E-05	1,33E-05	1,37E-05	3,16E-05	1,30E-05	1,75E-05	3,32E-05	1,37E-05	6,17E-05	3,48E-05	2,29E-05	1,33E-05	1,41E-04
Cx7	PDA:	1,29E-05	1,29E-05	1,29E-05	1,17E-04	3,12E-05	3,91E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,29E-05	6,15E-05	3,36E-05	2,31E-04	6,17E-05	1,29E-05	1,34E-05	1,37E-05	3,17E-05	1,29E-05	1,74E-05	3,33E-05	1,36E-05	6,16E-05	3,47E-05	2,31E-05	1,34E-05	1,42E-04
	PS:	1,30E-05	1,29E-05	1,29E-05	1,17E-04	3,12E-05	3,94E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,15E-05	3,38E-05	2,31E-04	6,17E-05	1,29E-05	1,34E-05	1,36E-05	3,13E-05	1,29E-05	1,74E-05	3,35E-05	1,37E-05	6,16E-05	3,47E-05	2,32E-05	1,34E-05	1,41E-04
	PEA:	1,29E-05	1,28E-05	1,29E-05	1,16E-04	3,11E-05	3,94E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,14E-05	3,38E-05	2,31E-04	6,16E-05	1,29E-05	1,34E-05	1,36E-05	3,21E-05	1,29E-05	1,74E-05	3,29E-05	1,35E-05	6,16E-05	3,48E-05	2,31E-05	1,33E-05	1,41E-04
	PFB:	1,29E-05	1,29E-05	1,29E-05	1,17E-04	3,13E-05	3,93E-05	6,31E-04	1,44E-04	1,07E-03	1,29E-05	1,29E-05	6,14E-05	3,38E-05	2,31E-04	6,16E-05	1,29E-05	1,34E-05	1,37E-05	3,20E-05	1,27E-05	1,73E-05	3,29E-05	1,35E-05	6,16E-05	3,46E-05	2,30E-05	1,33E-05	1,41E-04
PEX138	PDA:	1,32E-05	1,32E-05	1,33E-05	1,17E-04	3,15E-05	3,97E-05	6,35E-04	1,47E-04	1,07E-03	1,32E-05	1,34E-05	6,36E-05	3,58E-05	2,62E-04	6,36E-05	1,33E-05	1,38E-05	1,40E-05	3,20E-05	1,33E-05	1,76E-05	3,39E-05	1,40E-05	6,35E-05	3,66E-05	2,34E-05	1,38E-05	1,43E-04
	PS:	1,29E-05	1,30E-05	1,30E-05	1,17E-04	3,12E-05	3,91E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,15E-05	3,36E-05	2,31E-04	6,17E-05	1,29E-05	1,35E-05	1,37E-05	3,21E-05	1,30E-05	1,75E-05	3,35E-05	1,35E-05	6,17E-05	3,47E-05	2,30E-05	1,34E-05	1,42E-04
	PEA:	1,30E-05	1,30E-05	1,30E-05	1,16E-04	3,12E-05	3,93E-05	6,32E-04	1,44E-04	1,07E-03	1,30E-05	1,30E-05	6,17E-05	3,38E-05	2,34E-04	6,17E-05	1,29E-05	1,34E-05	1,38E-05	3,20E-05	1,30E-05	1,75E-05	3,34E-05	1,35E-05	6,16E-05	3,48E-05	2,29E-05	1,35E-05	1,41E-04
	PFB:	1,31E-05	1,29E-05	1,29E-05	1,17E-04	3,13E-05	3,94E-05	6,32E-04	1,44E-04	1,07E-03	1,30E-05	1,31E-05	6,21E-05	3,42E-05	2,39E-04	6,20E-05	1,30E-05	1,34E-05	1,38E-05	3,15E-05	1,29E-05	1,76E-05	3,32E-05	1,36E-05	6,20E-05	3,52E-05	2,29E-05	1,34E-05	1,41E-04
PEX140	PDA:	1,35E-05	1,34E-05	1,32E-05	1,18E-04	3,19E-05	3,98E-05	6,33E-04	1,55E-04	1,27E-03	1,34E-05	1,34E-05	6,22E-05	4,08E-05	2,44E-04	6,24E-05	1,34E-05	1,38E-05	1,42E-05	3,18E-05	1,34E-05	1,79E-05	3,42E-05	1,40E-05	6,25E-05	4,18E-05	2,37E-05	1,41E-05	1,42E-04
	PS:	1,30E-05	1,29E-05	1,29E-05	1,17E-04	3,12E-05	3,94E-05	6,32E-04	1,44E-04	1,07E-03	1,31E-05	1,30E-05	6,16E-05	3,37E-05	2,31E-04	6,15E-05	1,30E-05	1,33E-05	1,37E-05	3,15E-05	1,29E-05	1,74E-05	3,36E-05	1,36E-05	6,17E-05	3,48E-05	2,31E-05	1,33E-05	1,41E-04
	PEA:	1,28E-05	1,28E-05	1,30E-05	1,16E-04	3,11E-05	3,92E-05	6,31E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,15E-05	3,36E-05	2,31E-04	6,17E-05	1,29E-05	1,34E-05	1,37E-05	3,15E-05	1,30E-05	1,75E-05	3,32E-05	1,36E-05	6,17E-05	3,47E-05	2,31E-05	1,34E-05	1,41E-04
	PFB:	1,31E-05	1,31E-05	1,31E-05	1,16E-04	3,17E-05	3,97E-05	6,33E-04	1,58E-04	1,26E-03	1,31E-05	1,32E-05	6,20E-05	3,66E-05	2,39E-04	6,21E-05	1,31E-05	1,36E-05	1,40E-05	3,18E-05	1,32E-05	1,76E-05	3,34E-05	1,38E-05	6,21E-05	3,74E-05	2,32E-05	1,36E-05	1,42E-04
PEX141	PDA:	1,30E-05	1,30E-05	1,31E-05	1,30E-04	3,14E-05	4,49E-05	6,63E-04	1,44E-04	1,07E-03	1,30E-05	1,31E-05	6,18E-05	3,37E-05	2,31E-04	6,20E-05	1,30E-05	1,34E-05	1,38E-05	3,18E-05	1,29E-05	1,76E-05	3,36E-05	1,37E-05	6,19E-05	3,47E-05	2,32E-05	1,36E-05	1,41E-04
	PS:	1,30E-05	1,29E-05	1,30E-05	1,17E-04	3,13E-05	3,94E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,14E-05	3,38E-05	2,31E-04	6,16E-05	1,29E-05	1,34E-05	1,37E-05	3,18E-05	1,28E-05	1,74E-05	3,35E-05	1,36E-05	6,17E-05	3,48E-05	2,29E-05	1,33E-05	1,42E-04
	PEA:	1,29E-05	1,31E-05	1,29E-05	1,28E-04	3,12E-05	4,48E-05	6,54E-04	1,44E-04	1,07E-03	1,31E-05	1,31E-05	6,18E-05	3,38E-05	2,31E-04	6,19E-05	1,30E-05	1,35E-05	1,38E-05	3,16E-05	1,29E-05	1,76E-05	3,37E-05	1,36E-05	6,18E-05	3,48E-05	2,32E-05	1,33E-05	1,41E-04
	PFB:	1,29E-05	1,29E-05	1,28E-05	1,16E-04	3,12E-05	3,93E-05	6,33E-04	1,44E-04	1,07E-03	1,29E-05	1,29E-05	6,15E-05	3,36E-05	2,31E-04	6,18E-05	1,29E-05	1,34E-05	1,37E-05	3,08E-05	1,29E-05	1,74E-05	3,36E-05	1,36E-05	6,15E-05	3,47E-05	2,31E-05	1,34E-05	1,41E-04
PEX142	PDA:	1,35E-05	1,35E-05	1,36E-05	1,16E-04	4,06E-05	3,99E-05	6,33E-04	2,65E-04	1,19E-03	1,36E-05	1,37E-05	6,21E-05	4,47E-05	2,42E-04	6,22E-05	1,35E-05	1,40E-05	1,43E-05	3,26E-05	1,35E-05	1,81E-05	3,37E-05	1,44E-05	6,23E-05	4,56E-05	2,35E-05	1,44E-05	1,41E-04
	PS:	1,29E-05	1,29E-05	1,29E-05	1,17E-04	3,13E-05	3,93E-05	6,31E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,14E-05	3,38E-05	2,31E-04	6,17E-05	1,29E-05	1,34E-05	1,37E-05	3,21E-05	1,29E-05	1,74E-05	3,34E-05	1,34E-05	6,15E-05	3,47E-05	2,30E-05	1,33E-05	1,41E-04
	PEA:	1,34E-05	1,34E-05	1,34E-05	1,18E-04	4,23E-05	3,98E-05	6,32E-04	2,55E-04	1,18E-03	1,35E-05	1,34E-05	6,20E-05	4,28E-05	2,40E-04	6,21E-05	1,34E-05	1,39E-05	1,41E-05	3,23E-05	1,33E-05	1,79E-05	3,39E-05	1,42E-05	6,20E-05	4,39E-05	2,35E-05	1,41E-05	1,42E-04
	PFB:	1,28E-05	1,30E-05	1,29E-05	1,16E-04	3,12E-05	3,93E-05	6,32E-04	1,45E-04	1,07E-03	1,29E-05	1,31E-05	6,15E-05	3,39E-05	2,31E-04	6,16E-05	1,29E-05	1,34E-05	1,37E-05	3,15E-05	1,29E-05	1,74E-05	3,34E-05	1,36E-05	6,16E-05	3,48E-05	2,31E-05	1,34E-05	1,41E-04
PEX143	PDA:	1,43E-05	1,44E-05	1,44E-05	1,33E-04	3,28E-05	5,02E-05	6,81E-04	1,45E-04	1,08E-03	1,45E-05	1,44E-05	7,43E-05	3,52E-05	2,44E-04	7,40E-05	1,43E-05	1,49E-05	1,52E-05	3,30E-05	1,44E-05	1,90E-05	3,57E-05	1,50E-05	7,33E-05	3,62E-05	2,78E-05	1,49E-05	2,95E-04
	PS:	1,48E-05	1,48E-05	1,48E-05	1,19E-04	3,31E-05	4,12E-05	6,45E-04	1,46E-04	1,07E-03	1,47E-05	1,48E-05	6,41E-05	3,55E-05	2,34E-04	6,43E-05	1,49E-05	1,52E-05	1,55E-05	3,30E-05	1,47E-05	1,93E-05	3,57E-05	1,55E-05	6,42E-05	3,66E-05	2,49E-05	1,52E-05	1,54E-04
	PEA:	1,29E-05	1,29E-05	1,29E-05	1,16E-04	3,11E-05	3,92E-05	6,32E-04	1,44E-04	1,07E-03	1,30E-05	1,31E-05	6,15E-05	3,35E-05	2,31E-04	6,15E-05	1,30E-05	1,34E-05	1,36E-05	3,19E-05	1,29E-05	1,75E-05	3,33E-05	1,37E-05	6,15E-05	3,48E-05	2,32E-05	1,35E-05	1,41E-04
	PFB:	1,45E-05	1,44E-05	1,45E-05	1,36E-04	3,28E-05	5,15E-05	6,86E-04	1,45E-04	1,08E-03	1,45E-05	1,46E-05	7,48E-05	3,53E-05	2,44E-04	7,42E-05	1,45E-05	1,50E-05	1,53E-05	3,33E-05	1,45E-05	1,89E-05	3,60E-05	1,53E-05	7,49E-05	3,63E-05	2,84E-05	1,49E-05	2,94E-04
PE1XXX	PDA:	1,30E-05	1,29E-05	1,28E-05	1,17E-04	3,12E-05	3,91E-05	6,32E-04	1,44E-04	1,07E-03	1,30E-05	1,30E-05	6,15E-05	3,38E-05	2,31E-04	6,16E-05	1,30E-05	1,34E-05	1,36E-05	3,14E-05	1,30E-05	1,75E-05	3,32E-05	1,37E-05	6,16E-05	3,47E-05	2,32E-05	1,34E-05	1,41E-04
	PS:	1,30E-05	1,29E-05	1,29E-05	1,17E-04	3,12E-05	3,92E-05	6,33E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,15E-05	3,37E-05	2,31E-04	6,16E-05	1,28E-05	1,33E-05	1,38E-05	3,12E-05	1,29E-05	1,74E-05	3,32E-05	1,35E-05	6,16E-05	3,47E-05	2,29E-05	1,34E-05	1,41E-04
	PEA:	1,30E-05	1,29E-05	1,29E-05	1,17E-04	3,12E-05	3,94E-05	6,32E-04	1,43E-04	1,07E-03	1,29E-05	1,30E-05	6,15E-05	3,38E-05	2,31E-04	6,14E-05	1,28E-05	1,34E-05	1,38E-05	3,18E-05	1,29E-05	1,75E-05	3,35E-05	1,35E-05	6,14E-05	3,48E-05	2,31E-05	1,34E-05	1,41E-04
	PFB:	1,29E-05	1,30E-05	1,29E-05	1,16E-04	3,12E-05	3,91E-05	6,31E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,14E-05	3,37E-05	2,31E-04	6,19E-05	1,29E-05	1,34E-05	1,36E-05	3,19E-05	1,29E-05	1,75E-05	3,33E-05	1,36E-05	6,16E-05	3,47E-05	2,30E-05	1,34E-05	1,41E-04
PE1XX1	PDA:	1,30E-05	1,29E-05	1,30E-05	1,16E-04	3,10E-05	3,93E-05	6,31E-04	1,43E-04	1,06E-03	1,28E-05	1,30E-05	6,15E-05	3,38E-05	2,31E-04	6,16E-05	1,29E-05	1,34E-05	1,37E-05	3,17E-05	1,29E-05	1,75E-05	3,30E-05	1,35E-05	6,15E-05	3,46E-05	2,27E-05	1,34E-05	1,41E-04
	PS:	1,29E-05	1,30E-05	1,29E-05	1,17E-04	3,12E-05	3,93E-05	6,32E-04	1,44E-04	1,07E-03	1,28E-05	1,30E-05	6,16E-05	3,37E-05	2,31E-04	6,17E-05	1,29E-05	1,35E-05	1,37E-05	3,18E-05	1,29E-05	1,75E-05	3,32E-05	1,36E-05	6,16E-05	3,47E-05	2,29E-05	1,33E-05	1,42E-04
	PEA:	1,29E-05	1,29E-05	1,29E-05	1,17E-04	3,12E-05	3,92E-05	6,32E-04	1,44E-04	1,07E-03	1,30E-05	1,31E-05	6,15E-05	3,38E-05	2,31E-04	6,16E-05	1,30E-05	1,35E-05	1,38E-05	3,23E-05	1,29E-05	1,75E-05	3,28E-05	1,36E-05	6,15E-05	3,49E-05	2,30E-05	1,34E-05	1,41E-04
	PFB:	1,29E-05	1,28E-05	1,30E-05	1,17E-04	3,12E-05	3,92E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,15E-05	3,38E-05	2,31E-04	6,21E-05	1,30E-05	1,34E-05	1,38E-05	3,21E-05	1,29E-05	1,75E-05	3,38E-05	1,36E-05	6,16E-05	3,48E-05	2,29E-05	1,34E-05	1,40E-04
PE2XX1	PDA:	1,29E-05	1,29E-05	1,29E-05	1,17E-04	3,12E-05	3,92E-05	6,31E-04	1,44E-04	1,07E-03	1,28E-05	1,31E-05	6,15E-05	3,36E-05	2,31E-04	6,15E-05	1,28E-05	1,34E-05	1,36E-05	3,13E-05	1,29E-05	1,74E-05	3,32E-05	1,35E-05	6,16E-05	3,46E-05	2,29E-05	1,34E-05	1,41E-04
	PS:	1,30E-05	1,29E-05	1,29E-05	1,17E-04	3,13E-05	3,94E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,29E-05	6,16E-05	3,40E-05	2,32E-04	6,16E-05	1,29E-05	1,35E-05	1,37E-05	3,22E-05	1,29E-05	1,75E-05	3,31E-05	1,37E-05	6,16E-05	3,47E-05	2,32E-05	1,34E-05	1,41E-04
	PEA:	1,30E-05	1,29E-05	1,29E-05	1,16E-04	3,13E-05	3,92E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,29E-05	6,15E-05	3,37E-05	2,31E-04	6,17E-05	1,30E-05	1,34E-05	1,37E-05	3,21E-05	1,30E-05	1,75E-05	3,34E-05	1,36E-05	6,16E-05	3,47E-05	2,31E-05	1,34E-05	1,41E-04
	PFB:	1,29E-05	1,30E-05	1,29E-05	1,17E-04	3,12E-05	3,92E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,31E-05	6,14E-05	3,36E-05	2,31E-04	6,17E-05	1,29E-05	1,34E-05	1,37E-05	3,23E-05	1,30E-05	1,75E-05	3,32E-05	1,37E-05	6,15E-05	3,47E-05	2,30E-05	1,34E-05	1,41E-04
RX132	PDA:	1,30E-05	1,29E-05	1,29E-05	1,17E-04	3,12E-05	3,92E-05	6,31E-04	1,44E-04	1,07E-03	1,29E-05	1,29E-05	6,15E-05	3,38E-05	2,31E-04	6,16E-05	1,29E-05	1,35E-05	1,37E-05	3,17E-05	1,28E-05	1,75E-05	3,30E-05	1,36E-05	6,16E-05	3,47E-05	2,31E-05	1,34E-05	1,41E-04
	PS:	1,29E-05	1,30E-05	1,30E-05	1,17E-04	3,13E-05	3,93E-05	6,32E-04	1,44E-04	1,07E-03	1,30E-05	1,30E-05	6,15E-05	3,38E-05	2,31E-04	6,16E-05	1,29E-05	1,35E-05	1,38E-05	3,13E-05	1,29E-05	1,76E-05	3,33E-05	1,36E-05	6,16E-05	3,47E-05	2,27E-05	1,33E-05	1,41E-04
	PEA:	1,30E-05	1,30E-05	1,28E-05	1,16E-04	3,13E-05	3,92E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,29E-05	6,16E-05	3,38E-05	2,31E-04	6,16E-05	1,29E-05	1,36E-05	1,36E-05	3,21E-05	1,29E-05	1,75E-05	3,35E-05	1,36E-05	6,16E-05	3,47E-05	2,34E-05	1,34E-05	1,41E-04
	PFB:	1,29E-05	1,29E-05	1,29E-05	1,17E-04	3,11E-05	3,93E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,31E-05	6,15E-05	3,37E-05	2,31E-04	6,17E-05	1,29E-05	1,34E-05	1,38E-05	3,23E-05	1,29E-05	1,75E-05	3,34E-05	1,36E-05	6,15E-05	3,49E-05	2,30E-05	1,33E-05	1,41E-04
RX133	PDA:	1,31E-05	1,30E-05	1,31E-05	1,17E-04	3,13E-05	3,94E-05	6,32E-04	1,44E-04	1,07E-03	1,30E-05	1,32E-05	6,21E-05	3,44E-05	2,39E-04	6,20E-05	1,31E-05	1,36E-05	1,37E-05	3,16E-05	1,30E-05	1,76E-05	3,33E-05	1,38E-05	6,19E-05	3,50E-05	2,29E-05	1,37E-05	1,42E-04
	PS:	1,30E-05	1,29E-05	1,29E-05	1,17E-04	3,13E-05	3,93E-05	6,32E-04	1,44E-04	1,07E-03	1,30E-05	1,30E-05	6,16E-05	3,38E-05	2,31E-04	6,16E-05	1,28E-05	1,33E-05	1,37E-05	3,13E-05	1,30E-05	1,75E-05	3,35E-05	1,37E-05	6,16E-05	3,47E-05	2,31E-05	1,34E-05	1,41E-04
	PEA:	1,29E-05	1,29E-05	1,30E-05	1,17E-04	3,12E-05	3,93E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,14E-05	3,37E-05	2,31E-04	6,17E-05	1,30E-05	1,33E-05	1,37E-05	3,20E-05	1,29E-05	1,75E-05	3,34E-05	1,36E-05	6,15E-05	3,47E-05	2,34E-05	1,33E-05	1,41E-04
	PFB:	1,31E-05	1,31E-05	1,31E-05	1,17E-04	3,14E-05	3,94E-05	6,32E-04	1,45E-04	1,07E-03	1,31E-05	1,32E-05	6,20E-05	3,43E-05	2,38E-04	6,22E-05	1,31E-05	1,35E-05	1,39E-05	3,18E-05	1,31E-05	1,78E-05	3,33E-05	1,37E-05	6,22E-05	3,53E-05	2,31E-05	1,37E-05	1,42E-04
RX134	PDA:	1,29E-05	1,29E-05	1,29E-05	1,17E-04	3,12E-05	3,92E-05	6,32E-04	1,43E-04	1,07E-03	1,29E-05	1,29E-05	6,13E-05	3,34E-05	2,31E-04	6,13E-05	1,28E-05	1,34E-05	1,36E-05	3,09E-05	1,28E-05	1,74E-05	3,34E-05	1,36E-05	6,12E-05	3,44E-05	2,31E-05	1,33E-05	1,41E-04
	PS:	1,29E-05	1,28E-05	1,29E-05	1,16E-04	3,12E-05	3,93E-05	6,31E-04	1,44E-04	1,07E-03	1,29E-05	1,29E-05	6,16E-05	3,36E-05	2,31E-04	6,18E-05	1,30E-05	1,34E-05	1,38E-05	3,19E-05	1,29E-05	1,74E-05	3,29E-05	1,36E-05	6,15E-05	3,46E-05	2,30E-05	1,33E-05	1,41E-04
	PEA:	1,29E-05	1,30E-05	1,29E-05	1,16E-04	3,13E-05	3,93E-05	6,31E-04	1,44E-04	1,07E-03	1,29E-05	1,29E-05	6,15E-05	3,37E-05	2,31E-04	6,16E-05	1,28E-05	1,35E-05	1,37E-05	3,18E-05	1,30E-05	1,74E-05	3,33E-05	1,37E-05	6,15E-05	3,48E-05	2,29E-05	1,34E-05	1,41E-04
	PFB:	1,28E-05	1,29E-05	1,29E-05	1,16E-04	3,12E-05	3,93E-05	6,31E-04	1,44E-04	1,07E-03	1,30E-05	1,30E-05	6,14E-05	3,37E-05	2,31E-04	6,16E-05	1,29E-05	1,34E-05	1,37E-05	3,20E-05	1,29E-05	1,74E-05	3,29E-05	1,36E-05	6,17E-05	3,47E-05	2,31E-05	1,34E-05	1,42E-04
RX139	PDA:	1,30E-05	1,30E-05	1,30E-05	1,17E-04	3,13E-05	3,95E-05	6,33E-04	1,44E-04	1,07E-03	1,31E-05	1,31E-05	6,21E-05	3,44E-05	2,38E-04	6,23E-05	1,30E-05	1,36E-05	1,38E-05	3,22E-05	1,30E-05	1,76E-05	3,31E-05	1,38E-05	6,21E-05	3,53E-05	2,33E-05	1,37E-05	1,41E-04
	PS:	1,29E-05	1,30E-05	1,30E-05	1,17E-04	3,12E-05	3,92E-05	6,32E-04	1,44E-04	1,07E-03	1,30E-05	1,31E-05	6,19E-05	3,42E-05	2,34E-04	6,20E-05	1,29E-05	1,34E-05	1,36E-05	3,15E-05	1,30E-05	1,76E-05	3,33E-05	1,38E-05	6,19E-05	3,49E-05	2,30E-05	1,34E-05	1,41E-04
	PEA:	1,29E-05	1,30E-05	1,30E-05	1,16E-04	3,12E-05	3,93E-05	6,32E-04	1,44E-04	1,07E-03	1,28E-05	1,30E-05	6,15E-05	3,38E-05	2,31E-04	6,16E-05	1,29E-05	1,34E-05	1,37E-05	3,19E-05	1,29E-05	1,74E-05	3,36E-05	1,35E-05	6,16E-05	3,49E-05	2,32E-05	1,34E-05	1,41E-04
	PFB:	1,30E-05	1,30E-05	1,31E-05	1,17E-04	3,14E-05	3,92E-05	6,32E-04	1,44E-04	1,07E-03	1,31E-05	1,31E-05	6,23E-05	3,47E-05	2,40E-04	6,27E-05	1,31E-05	1,36E-05	1,40E-05	3,24E-05	1,31E-05	1,77E-05	3,36E-05	1,38E-05	6,25E-05	3,55E-05	2,34E-05	1,37E-05	1,42E-04
SX187	PDA:	3,27E-05	3,25E-05	3,29E-05	1,34E-04	7,85E-05	5,81E-05	9,69E-04	3,10E-04	1,14E-03	3,31E-05	3,39E-05	3,78E-04	5,24E-05	2,55E-04	3,78E-04	3,31E-05	3,36E-05	3,36E-05	4,88E-05	3,27E-05	4,31E-05	5,21E-05	3,99E-05	3,78E-04	5,33E-05	4,91E-05	3,31E-05	1,70E-04
	PS:	1,33E-05	1,32E-05	1,32E-05	1,17E-04	3,14E-05	3,95E-05	6,37E-04	1,44E-04	1,07E-03	1,32E-05	1,33E-05	6,64E-05	3,39E-05	2,35E-04	6,67E-05	1,32E-05	1,37E-05	1,41E-05	3,23E-05	1,32E-05	1,80E-05	3,37E-05	1,39E-05	6,66E-05	3,50E-05	2,36E-05	1,37E-05	1,45E-04
	PEA:	1,60E-05	1,59E-05	1,58E-05	1,20E-04	3,72E-05	4,19E-05	7,01E-04	1,64E-04	1,08E-03	1,60E-05	1,61E-05	1,18E-04	3,66E-05	2,37E-04	1,18E-04	1,59E-05	1,64E-05	1,66E-05	3,41E-05	1,59E-05	2,15E-05	3,59E-05	1,79E-05	1,19E-04	3,74E-05	2,72E-05	1,63E-05	1,47E-04
	PFB:	1,35E-05	1,34E-05	1,33E-05	1,17E-04	3,26E-05	3,98E-05	6,44E-04	1,49E-04	1,07E-03	1,34E-05	1,34E-05	7,36E-05	3,42E-05	2,31E-04	7,37E-05	1,35E-05	1,39E-05	1,42E-05	3,25E-05	1,34E-05	1,83E-05	3,38E-05	1,43E-05	7,35E-05	3,52E-05	2,38E-05	1,38E-05	1,42E-04
SX190	PDA:	1,30E-05	1,29E-05	1,30E-05	1,23E-04	3,13E-05	3,93E-05	7,63E-04	1,44E-04	1,07E-03	1,29E-05	1,31E-05	6,25E-05	3,37E-05	2,32E-04	6,28E-05	1,29E-05	1,35E-05	1,37E-05	3,17E-05	1,30E-05	1,75E-05	3,28E-05	1,35E-05	6,26E-05	3,46E-05	2,32E-05	1,34E-05	1,42E-04
	PS:	1,30E-05	1,29E-05	1,30E-05	1,19E-04	3,12E-05	3,91E-05	6,60E-04	1,44E-04	1,07E-03	1,28E-05	1,31E-05	6,21E-05	3,36E-05	2,31E-04	6,25E-05	1,30E-05	1,34E-05	1,38E-05	3,28E-05	1,30E-05	1,75E-05	3,31E-05	1,37E-05	6,23E-05	3,46E-05	2,33E-05	1,34E-05	1,42E-04
	PEA:	1,30E-05	1,29E-05	1,29E-05	1,22E-04	3,13E-05	3,91E-05	6,92E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,30E-05	3,38E-05	2,32E-04	6,32E-05	1,29E-05	1,34E-05	1,37E-05	3,18E-05	1,30E-05	1,75E-05	3,34E-05	1,37E-05	6,32E-05	3,47E-05	2,32E-05	1,34E-05	1,43E-04
	PFB:	1,29E-05	1,29E-05	1,29E-05	1,20E-04	3,12E-05	3,92E-05	6,53E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,25E-05	3,37E-05	2,32E-04	6,28E-05	1,30E-05	1,35E-05	1,37E-05	3,15E-05	1,29E-05	1,75E-05	3,35E-05	1,36E-05	6,28E-05	3,47E-05	2,30E-05	1,34E-05	1,42E-04
TX167X1	PDA:	1,29E-05	1,29E-05	1,28E-05	1,17E-04	3,12E-05	3,92E-05	6,32E-04	1,43E-04	1,06E-03	1,28E-05	1,31E-05	6,14E-05	3,37E-05	2,30E-04	6,15E-05	1,30E-05	1,33E-05	1,33E-05	3,15E-05	1,29E-05	1,74E-05	3,29E-05	1,36E-05	6,16E-05	3,48E-05	2,31E-05	1,34E-05	1,41E-04
	PS:	1,29E-05	1,29E-05	1,29E-05	1,16E-04	3,12E-05	3,93E-05	6,32E-04	1,44E-04	1,07E-03	1,30E-05	1,29E-05	6,15E-05	3,37E-05	2,31E-04	6,17E-05	1,30E-05	1,33E-05	1,37E-05	3,15E-05	1,28E-05	1,75E-05	3,31E-05	1,35E-05	6,16E-05	3,47E-05	2,28E-05	1,33E-05	1,41E-04
	PEA:	1,30E-05	1,28E-05	1,29E-05	1,16E-04	3,12E-05	3,94E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,31E-05	6,16E-05	3,37E-05	2,31E-04	6,17E-05	1,30E-05	1,34E-05	1,37E-05	3,13E-05	1,30E-05	1,75E-05	3,30E-05	1,36E-05	6,14E-05	3,47E-05	2,31E-05	1,33E-05	1,41E-04
	PFB:	1,29E-05	1,29E-05	1,29E-05	1,17E-04	3,13E-05	3,93E-05	6,32E-04	1,44E-04	1,07E-03	1,30E-05	1,31E-05	6,16E-05	3,37E-05	2,31E-04	6,14E-05	1,29E-05	1,35E-05	1,37E-05	3,13E-05	1,29E-05	1,75E-05	3,30E-05	1,36E-05	6,15E-05	3,46E-05	2,31E-05	1,34E-05	1,41E-04
TX167X2	PDA:	1,29E-05	1,29E-05	1,29E-05	1,16E-04	3,14E-05	3,92E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,15E-05	3,39E-05	2,31E-04	6,18E-05	1,28E-05	1,34E-05	1,37E-05	3,17E-05	1,30E-05	1,75E-05	3,32E-05	1,37E-05	6,14E-05	3,47E-05	2,31E-05	1,34E-05	1,41E-04
	PS:	1,29E-05	1,29E-05	1,29E-05	1,17E-04	3,12E-05	3,94E-05	6,32E-04	1,44E-04	1,07E-03	1,30E-05	1,30E-05	6,15E-05	3,38E-05	2,31E-04	6,17E-05	1,29E-05	1,33E-05	1,38E-05	3,18E-05	1,28E-05	1,75E-05	3,32E-05	1,36E-05	6,16E-05	3,47E-05	2,31E-05	1,34E-05	1,41E-04
	PEA:	1,29E-05	1,29E-05	1,29E-05	1,17E-04	3,12E-05	3,93E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,14E-05	3,37E-05	2,31E-04	6,15E-05	1,29E-05	1,34E-05	1,37E-05	3,14E-05	1,29E-05	1,75E-05	3,34E-05	1,36E-05	6,14E-05	3,46E-05	2,30E-05	1,34E-05	1,41E-04
	PFB:	1,29E-05	1,30E-05	1,29E-05	1,17E-04	3,12E-05	3,92E-05	6,32E-04	1,44E-04	1,07E-03	1,29E-05	1,30E-05	6,15E-05	3,38E-05	2,31E-04	6,16E-05	1,29E-05	1,34E-05	1,36E-05	3,14E-05	1,30E-05	1,76E-05	3,32E-05	1,35E-05	6,16E-05	3,46E-05	2,30E-05	1,34E-05	1,41E-04
TX167X3	PDA:	1,30E-05	1,29E-05	1,30E-05	1,17E-04	3,14E-05	3,95E-05	6,33E-04	1,45E-04	1,07E-03	1,29E-05	1,31E-05	6,17E-05	3,40E-05	2,35E-04	6,19E-05	1,29E-05	1,46E-05	1,38E-05	3,21E-05	1,29E-05	1,75E-05	3,58E-05	1,37E-05	6,16E-05	3,48E-05	2,28E-05	1,35E-05	1,42E-04
	PS:	1,29E-05	1,28E-05	1,29E-05	1,16E-04	3,12E-05	3,92E-05	6,32E-04	1,44E-04	1,07E-03	1,30E-05	1,31E-05	6,15E-05	3,37E-05	2,31E-04	6,17E-05	1,28E-05	1,33E-05	1,37E-05	3,20E-05	1,30E-05	1,75E-05	3,33E-05	1,36E-05	6,16E-05	3,47E-05	2,32E-05	1,34E-05	1,41E-04
	PEA:	1,30E-05	1,28E-05	1,29E-05	1,16E-04	3,14E-05	3,93E-05	6,32E-04	1,44E-04	1,07E-03	1,30E-05	1,30E-05	6,15E-05	3,37E-05	2,31E-04	6,16E-05	1,29E-05	1,34E-05	1,37E-05	3,18E-05	1,29E-05	1,74E-05	3,35E-05	1,36E-05	6,15E-05	3,48E-05	2,32E-05	1,34E-05	1,41E-04
	PFB:	1,30E-05	1,31E-05	1,30E-05	1,16E-04	3,14E-05	3,94E-05	6,32E-04	1,45E-04	1,07E-03	1,30E-05	1,31E-05	6,16E-05	3,38E-05	2,36E-04	6,18E-05	1,30E-05	1,46E-05	1,38E-05	3,19E-05	1,29E-05	1,76E-05	3,61E-05	1,38E-05	6,18E-05	3,50E-05	2,31E-05	1,33E-05	1,42E-04

S.5. Matriz MRI

Basic_events:	OK	SB1	SB2	SB3	SB4	SB5	SB6	SB7	SB8	SB9	SB10	SB11	SB12	SB13	SB14	SB15	SB16	SB17	SB18	SB19	SB20	SB21	SB22	SB23	SB24	SB25	SB26	SB27
FDN Total	9,61E-06	9,61E-06	9,61E-06	7,77E-05	2,41E-05	2,80E-05	5,94E-04	1,25E-04	1,02E-03	9,61E-06	9,69E-06	5,35E-05	2,23E-04	2,80E-05	5,36E-05	9,61E-06	1,00E-05	9,98E-06	1,36E-05	9,61E-06	1,37E-05	2,28E-05	1,04E-05	5,36E-05	2,87E-05	1,43E-05	1,00E-05	1,05E-04
Te /(días)	INF	INF	INF	5,36	25,26	19,83	0,62	3,16	0,36	INF	4762,53	8,32	1,71	19,80	8,30	INF	940,56	989,37	91,54	INF	89,62	27,71	488,22	8,30	19,17	77,18	952,99	3,81
AXXX9	3,75E-08	3,75E-08	3,75E-08	2,45E-07	2,39E-07	3,05E-07	2,45E-07	3,06E-07	1,15E-05	3,75E-08	3,75E-08	3,75E-08	3,75E-08	3,75E-08	3,75E-08	3,75E-08	3,75E-08	3,75E-08	3,75E-08	3,75E-08	3,75E-08	6,31E-07	3,75E-08	3,75E-08	3,75E-08	3,75E-08	3,75E-08	3,75E-08
AXXX3	5,68E-08	5,68E-08	5,68E-08	7,04E-08	6,83E-08	1,08E-07	7,04E-08	2,40E-07	1,12E-05	5,68E-08	5,68E-08	5,68E-08	8,29E-08	8,29E-08	5,68E-08	5,68E-08	5,68E-08	5,68E-08	5,68E-08	5,68E-08	5,68E-08	2,31E-07	5,68E-08	5,68E-08	8,29E-08	5,68E-08	5,68E-08	5,68E-08
AXXX4	3,35E-08	3,35E-08	3,35E-08	1,49E-07	1,48E-07	2,41E-07	1,49E-07	1,79E-07	1,05E-05	3,35E-08	3,35E-08	3,35E-08	3,35E-08	3,35E-08	3,35E-08	3,35E-08	3,35E-08	3,35E-08	3,35E-08	3,35E-08	3,35E-08	5,88E-07	3,35E-08	3,35E-08	3,35E-08	3,35E-08	3,35E-08	3,35E-08
AXXX8	1,15E-09	1,15E-09	1,15E-09	6,89E-07	1,15E-09	3,28E-07	1,20E-06	1,15E-09	3,28E-07	1,15E-09	1,15E-09	1,15E-09	1,15E-09	1,15E-09	1,15E-09	1,15E-09	1,15E-09	1,15E-09	1,15E-09	1,15E-09	1,15E-09	1,83E-08	1,15E-09	1,15E-09	1,15E-09	1,15E-09	1,15E-09	1,15E-09
AXXX9	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	1,16E-06	9,48E-09	0,00E+00	0,00E+00	0,00E+00	1,76E-09	0	0,00E+00	1,76E-09	0,00E+00	0,00E+00	1,97E-09	5,43E-09	0,00E+00	0,00E+00	0,00E+00	0,00E+00	1,63E-08	0,00E+00	0,00E+00	0,00E+00	0
AXXX0	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	3,28E-09	9,19E-07	0,00E+00	0,00E+00	0,00E+00	2,06E-09	2,06E-09	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	2,06E-09	0,00E+00	0,00E+00	0
AXX1A	1,46E-06	1,46E-06	1,46E-06	1,48E-06	1,46E-06	1,47E-06	1,49E-06	1,46E-06	1,47E-06	1,46E-06	1,46E-06	1,46E-06	1,46E-06	1,46E-06	1,46E-06	1,46E-06	1,46E-06	1,46E-06	1,46E-06	1,46E-06	1,46E-06	1,46E-06	1,46E-06	1,46E-06	1,46E-06	1,48E-06	1,46E-06	2,10E-06
AXX1B	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	6,13E-07	0,00E+00	0,00E+00	0,00E+00	0	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	3,53E-09	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0
CXXX3	9,40E-08	9,40E-08	9,40E-08	2,01E-05	1,85E-07	9,40E-08	1,94E-04	1,76E-06	2,61E-06	9,40E-08	1,25E-07	3,76E-06	4,71E-06	7,66E-07	3,78E-06	9,40E-08	1,04E-07	9,40E-08	9,40E-08	9,40E-08	3,76E-06	1,12E-07	9,64E-08	3,78E-06	7,94E-07	1,79E-07	1,15E-07	3,76E-06
CXXX7	4,94E-08	4,94E-08	4,94E-08	5,38E-06	4,94E-08	6,82E-07	1,05E-05	4,94E-08	4,94E-08	4,94E-08	4,94E-08	1,52E-07	1,01E-07	4,94E-08	1,52E-07	4,94E-08	2,40E-07	4,94E-08	4,94E-08	4,94E-08	1,00E-07	2,80E-07	4,94E-08	1,52E-07	4,94E-08	4,94E-08	4,94E-08	1,52E-07
CXXX8	2,32E-07	2,32E-07	2,32E-07	2,32E-07	3,43E-07	2,93E-07	2,76E-07	7,27E-06	7,86E-05	2,32E-07	2,32E-07	2,32E-07	3,76E-06	3,76E-06	2,32E-07	2,32E-07	3,23E-07	2,32E-07	2,32E-07	2,32E-07	2,32E-07	2,32E-07	2,33E-07	2,32E-07	3,76E-06	2,32E-07	3,51E-07	2,32E-07
CXX13	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07	3,13E-07
CXX16	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,43E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06	2,46E-06
CXX17	5,89E-09	5,89E-09	5,89E-09	2,68E-07	5,89E-09	5,89E-09	5,62E-07	5,89E-09	1,98E-08	5,89E-09	5,89E-09	5,89E-09	5,89E-09	5,89E-09	2,58E-08	5,89E-09	5,89E-09	5,89E-09	5,89E-09	5,89E-09	5,89E-09	3,96E-07	5,89E-09	2,58E-08	5,89E-09	8,20E-09	5,89E-09	3,15E-07
CXX18	2,15E-07	2,15E-07	2,15E-07	1,35E-05	2,15E-07	5,44E-06	1,86E-05	2,15E-07	5,44E-06	2,15E-07	2,15E-07	1,39E-07	1,39E-07	2,15E-07	2,15E-07	2,15E-07	2,15E-07	2,15E-07	4,19E-06	2,15E-07	2,15E-07	5,05E-07	2,15E-07	2,15E-07	2,15E-07	3,21E-06	2,15E-07	1,99E-05
CXX19	3,94E-08	3,94E-08	3,94E-08	3,94E-08	7,49E-06	3,67E-06	3,94E-08	1,24E-05	2,60E-04	3,94E-08	3,94E-08	3,94E-08	4,48E-08	4,48E-08	3,94E-08	3,94E-08	3,94E-08	3,94E-08	3,94E-08	3,94E-08	3,94E-08	7,10E-08	4,48E-08	3,94E-08	4,48E-08	3,94E-08	3,94E-08	3,94E-08
CXX20	1,20E-08	1,20E-08	1,20E-08	1,20E-08	2,24E-08	1,37E-08	2,02E-08	2,61E-08	4,67E-07	1,20E-08	1,20E-08	1,20E-08	1,20E-08	1,20E-08	1,20E-08	1,20E-08	1,20E-08	1,20E-08	1,20E-08	1,20E-08	1,20E-08	1,20E-08	1,20E-08	1,20E-08	1,20E-08	4,28E-08	1,20E-08	1,93E-06
CXX22	0,00E+00	0,00E+00	0,00E+00	2,26E-07	0,00E+00	6,84E-08	2,26E-07	0,00E+00	6,84E-08	0,00E+00	0,00E+00	0,00E+00	0	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	4,07E-09	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0
CXX31	1,19E-06	1,19E-06	1,19E-06	1,31E-06	1,36E-06	1,38E-06	3,78E-06	4,17E-06	1,75E-05	1,19E-06	1,19E-06	2,77E-06	3,21E-06	2,81E-06	2,80E-06	1,19E-06	1,19E-06	1,19E-06	1,19E-06	1,19E-06	1,19E-06	1,25E-06	1,19E-06	2,77E-06	2,81E-06	1,20E-06	1,20E-06	1,20E-06
CXX43	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07	1,47E-07
CXX45	2,45E-08	2,45E-08	2,45E-08	2,45E-08	2,33E-06	1,12E-06	1,42E-07	1,50E-05	3,11E-04	2,45E-08	2,45E-08	4,41E-08	1,88E-07	1,42E-07	4,41E-08	2,45E-08	2,45E-08	2,45E-08	2,45E-08	2,45E-08	9,13E-06	2,45E-08	4,41E-08	8,77E-07	2,45E-08	2,45E-08	4,41E-08
CX5	0,00E+00	0,00E+00	0,00E+00	5,87E-07	0,00E+00	2,94E-07	5,87E-07	0,00E+00	5,70E-07	0,00E+00	0,00E+00	0,00E+00	0	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	1,29E-08	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0
CX6	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	8,58E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,84E-08	2,25E-07	2,84E-08	1,23E-05
Cx7	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,38E-08	1,23E-08	1,23E-08	2,91E-07	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,23E-08	1,23E-08
PEX138	2,22E-08	2,22E-08	2,22E-08	2,22E-08	2,22E-08	2,22E-08	2,18E-07	2,15E-07	1,64E-07	2,22E-08	2,22E-08	1,35E-07	4,26E-06	1,32E-07	1,34E-07	2,22E-08	2,22E-08	2,22E-08	2,22E-08	2,22E-08	2,22E-08	2,22E-08	2,22E-08	1,34E-07	1,31E-07	2,22E-08	2,22E-08	1,36E-07
PEX140	8,92E-09	8,92E-09	8,92E-09	8,92E-09	2,55E-07	1,11E-07	2,10E-08	1,14E-05	2,26E-04	8,92E-09	8,92E-09	1,21E-08	1,22E-06	7,39E-07	1,21E-08	8,92E-09	8,92E-09	8,92E-09	8,92E-09	8,92E-09	8,92E-09	9,53E-08	8,92E-09	1,21E-08	7,39E-07	8,92E-09	2,92E-08	1,21E-08
PEX141	3,09E-09	3,09E-09	3,09E-09	2,97E-06	3,09E-09	1,31E-06	6,76E-06	3,09E-09	1,31E-06	3,09E-09	3,09E-09	8,32E-09	8,32E-09	3,09E-09	8,32E-09	3,09E-09	3,09E-09	3,09E-09	3,09E-09	3,09E-09	3,09E-09	7,52E-08	3,09E-09	8,32E-09	3,09E-09	3,09E-09	3,09E-09	8,32E-09
PEX142	2,14E-08	2,14E-08	2,14E-08	2,14E-08	2,63E-06	2,14E-08	3,31E-08	4,00E-05	4,00E-05	2,14E-08	2,14E-08	2,14E-08	1,50E-06	1,50E-06	2,14E-08	2,14E-08	2,14E-08	2,14E-08	2,14E-08	2,14E-08	2,14E-08	2,14E-08	2,39E-08	2,14E-08	1,50E-06	2,14E-08	5,08E-08	2,14E-08
PEX143	4,88E-07	4,88E-07	4,88E-07	7,23E-06	4,88E-07	5,39E-06	1,55E-05	5,77E-07	5,98E-06	4,88E-07	4,88E-07	5,04E-06	5,04E-06	4,88E-07	5,11E-06	4,88E-07	4,88E-07	4,88E-07	4,88E-07	4,88E-07	4,90E-07	1,73E-06	4,90E-07	5,11E-06	4,88E-07	1,22E-06	4,88E-07	4,09E-05
PE1XXX	0,00E+00	0,00E+00	0,00E+00	1,74E-07	0,00E+00	0,00E+00	1,15E-06	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	2,17E-07	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0
PE1XX1	0,00E+00	0,00E+00	0,00E+00	2,79E-07	2,61E-08	9,50E-09	1,77E-06	1,59E-07	6,94E-06	0,00E+00	0,00E+00	0,00E+00	3,84E-07	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0
PE2XX1	7,18E-08	7,18E-08	7,18E-08	7,18E-08	7,18E-08	7,18E-08	5,41E-07	6,60E-07	6,22E-07	7,18E-08	7,18E-08	3,54E-07	6,80E-06	4,93E-07	3,48E-07	7,18E-08	7,18E-08	7,18E-08	7,18E-08	7,18E-08	1,53E-07	7,72E-08	1,53E-07	3,48E-07	4,88E-07	7,18E-08	7,64E-08	3,59E-07
RX132	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	6,03E-09	3,40E-08	0,00E+00	3,01E-06	0,00E+00	0,00E+00	0,00E+00	1,60E-07	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	1,45E-08	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0
RX133	5,26E-07	5,26E-07	5,26E-07	5,26E-07	5,26E-07	5,26E-07	4,77E-06	4,70E-06	3,74E-06	5,26E-07	5,26E-07	3,28E-06	5,12E-05	3,28E-06	3,24E-06	5,26E-07	5,26E-07	5,26E-07	5,26E-07	5,26E-07	5,29E-07	5,26E-07	5,26E-07	3,24E-06	3,24E-06	5,77E-07	5,75E-07	3,33E-06
RX134	7,54E-07	7,54E-07	7,54E-07	7,54E-07	7,54E-07	7,54E-07	6,68E-06	6,58E-06	5,26E-06	7,54E-07	7,54E-07	4,61E-06	7,17E-05	4,61E-06	4,55E-06	7,54E-07	7,54E-07	7,54E-07	7,54E-07	7,54E-07	7,54E-07	7,54E-07	7,59E-07	4,55E-06	4,55E-06	8,46E-07	8,41E-07	4,67E-06
RX139	5,61E-07	5,61E-07	5,61E-07	5,61E-07	5,61E-07	5,61E-07	5,40E-06	5,27E-06	6,47E-06	5,61E-07	5,61E-07	3,68E-06	5,64E-05	3,67E-06	3,63E-06	5,61E-07	5,61E-07	5,61E-07	5,61E-07	5,61E-07	5,61E-07	6,04E-07	9,41E-07	3,63E-06	3,63E-06	6,02E-07	6,01E-07	3,73E-06
SX187	6,85E-07	6,85E-07	6,85E-07	7,65E-07	1,79E-06	6,85E-07	2,06E-05	8,74E-06	2,86E-06	6,85E-07	6,85E-07	1,90E-05	9,96E-07	6,85E-07	1,90E-05	6,85E-07	6,85E-07	6,85E-07	6,85E-07	6,85E-07	9,36E-07	6,85E-07	9,36E-07	1,90E-05	6,85E-07	1,03E-06	6,85E-07	1,34E-06
SX190	3,86E-08	3,86E-08	3,86E-08	1,71E-05	3,86E-08	3,86E-08	2,94E-04	7,75E-08	7,90E-08	3,86E-08	8,47E-08	5,66E-06	5,66E-06	3,86E-08	5,66E-06	3,86E-08	3,86E-08	3,86E-08	3,86E-08	3,86E-08	5,52E-08	3,86E-08	5,52E-08	5,66E-06	3,86E-08	1,66E-07	3,86E-08	5,66E-06
TX167X1	6,65E-09	6,65E-09	6,65E-09	6,65E-09	6,65E-09	1,75E-08	7,63E-08	4,20E-07	4,98E-06	6,65E-09	6,65E-09	6,65E-09	2,49E-07	6,65E-09	6,65E-09	6,65E-09	6,79E-08	3,74E-07	8,86E-09	6,65E-09	7,69E-09	1,47E-07	7,69E-09	6,65E-09	6,65E-09	6,65E-09	6,65E-09	6,65E-09
TX167X2	1,83E-08	1,83E-08	1,83E-08	1,83E-08	1,83E-08	1,83E-08	4,46E-08	1,83E-08	1,08E-07	1,83E-08	1,83E-08	1,83E-08	3,15E-08	1,83E-08	1,83E-08	1,83E-08	1,83E-08	1,83E-08	1,96E-08	1,83E-08	1,83E-08	2,14E-08	1,83E-08	1,83E-08	1,83E-08	1,83E-08	1,83E-08	1,98E-08
TX167X3	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	3,33E-09	7,81E-09	0,00E+00	2,46E-08	0,00E+00	0,00E+00	0,00E+00	1,43E-07	0,00E+00	0,00E+00	0,00E+00	3,53E-08	0,00E+00	0,00E+00	0,00E+00	0,00E+00	7,37E-08	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0,00E+00	0