TERCER EJERCICIO

GRUPO A - SEGURIDAD NUCLEAR

TEMA 28

Análisis probabilista de seguridad (APS). Secuencias de accidente: árboles de sucesos. Criterios de éxito. Análisis de sistemas mediante árboles de fallo. Resultados de los APS y sus aplicaciones. Análisis probabilistas de seguridad (APS) de Nivel 2.

Contenido

Resumen

El análisis del riesgo de una instalación exige estudiar los daños que pueden producirse y la frecuencia con que pueden ocurrir, siendo el objetivo de la regulación que no se supere una curva daño-frecuencia aceptada. Para el análisis se usan distintas metodologías en función de la región de daño y frecuencia bajo estudio. Los APS estudian la región de alto daño, en la que el núcleo del reactor puede sufrir una degradación importante, liberándose productos radiactivos al medio ambiente de forma masiva.

Para su realización, los APS se dividen en tareas. La delineación de secuencias en un APS de nivel 1 describe la evolución posible de un accidente como secuencias que ocurren a partir de un suceso iniciador y tienen en cuenta la actuación de los sistemas automáticos de protección y las acciones de los operadores en su mitigación. El resultado será un conjunto de árboles de sucesos en los que se proporciona una clasificación de las secuencias en función de la ocurrencia o no del daño al núcleo.

La actuación de los sistemas está contemplada en los árboles de sucesos según su criterio de éxito, es decir, la capacidad del sistema para cumplir su misión en la mitigación del accidente. Se representa el fallo en el cumplimiento de la misión a través de un árbol de fallos, que descompone ese fallo en función de sucesos elementales, llamados sucesos básicos.

El APS de nivel 2 estudia la evolución de los accidentes que, habiendo provocado la fusión del núcleo del reactor, progresan hasta el fallo de la contención, bien por fallo de su estructura, por fallo de sus sistemas de aislamiento o porque el accidente resulta en su derivación (baipás). El APS de Nivel 2 se estructura en varias fases, ampliando el análisis de Nivel 1 mediante la consideración de la actuación de los sistemas de la contención, el estudio de la evolución del accidente en la contención, prestando atención a la fenomenología específica que ocurre en condiciones de accidente severo, y el cálculo de medidas de riesgo que proporcionen la frecuencia de fallo de la contención y la frecuencia de liberación de productos de fisión, generalmente agrupados por familias radioquímicas. De importancia reguladora es la determinación de la Frecuencia de Grandes Liberaciones Tempranas (FGLT, Large Early Release Frequency (LERF)), una medida de riesgo usada en las aplicaciones de los APS para caracterizar la aceptabilidad del riesgo de la instalación.

1. INTRODUCCIÓN

En toda actividad industrial, además de obtenerse un producto que es el objetivo de la instalación, se generan también efectos indeseados o daños, que además tienen la particularidad de que suelen afectar a seres vivos (incluyendo personas), entornos u objetos distintos de los que resultan beneficiados por el producto de la instalación. Esto hace difícil estimar la aceptabilidad del daño en función del beneficio obtenido. Aunque el recurso a estudios coste/beneficio es frecuente aún en estos casos, es inevitable definir otros criterios de aceptabilidad del daño y utilizar dichos estudios solamente como criterio complementario.

En una instalación nuclear, el daño último que se trata de evitar es la dosis radiológica a las personas (trabajadores y público), al medio ambiente o al patrimonio. Ello justifica que la industria nuclear sea regulada con rigor en el principio fundamental de la Seguridad Nuclear de proteger a individuos, sociedad y ambiente de los daños radiológicos estableciendo las adecuadas defensas que los previenen o mitigan. Los mecanismos que pueden llevar a la generación de un daño radiológico son de una complejidad considerable y su ocurrencia se ha limitado interponiendo sucesivas barreras a la dispersión de elementos contaminantes. Esta filosofía de protección por barreras o defensa en profundidad reduce la posibilidad de ocurrencia de daños, sin que por ello puedan ser ignorados ya que también son de una magnitud importante. Esto hace que la seguridad nuclear sea una disciplina de particular dificultad y que sea necesario aplicarla en todos los niveles (diseño, regulación, verificación, operación, etc.).

La magnitud adecuada para medir la verosimilitud de la ocurrencia de un fenómeno a lo largo del tiempo es la frecuencia esperada de dicho fenómeno. En particular, el estudio de la seguridad de la instalación se enfoca a determinar la frecuencia con la que se puede producir un daño mayor que uno dado, lo que se denomina frecuencia de excedencia del daño. Ésta es la magnitud que debe estar limitada en una instalación para asegurar que tiene un nivel de riesgo aceptable. Solamente cuando se determina un periodo de observación se puede hablar de probabilidad de ocurrencia y su valor se puede obtener a partir de la frecuencia esperada con mayor o menor dificultad. Sin embargo, en los estudios de riesgo de las instalaciones no existe normalmente un periodo temporal de referencia por lo que es mucho más adecuado trabajar con frecuencias que con probabilidades.

Definimos como **riesgo** de una instalación la relación entre la magnitud del daño y su frecuencia de excedencia. El riesgo es, por tanto, un concepto bidimensional, es decir, una relación entre dos variables, que se puede representar mediante una curva, pero difícilmente mediante un número. No es sencillo encontrar cuál es la curva que caracteriza el riesgo de una determinada instalación, pero sí se puede definir con no mucha dificultad una curva límite que no puede ser superada por la curva característica de la instalación. A esta curva la llamamos curva límite de daño. La Figura 1 muestra una hipotética curva de límite de daño y se identifican las zonas permitida y prohibida para la curva característica de la instalación.

El riesgo de la instalación se analiza en las distintas zonas de daño con metodologías distintas. La zona de alto daño es materia de estudio de los Análisis Probabilistas de Seguridad (APS). Históricamente, los APS en la industria nuclear nacieron con el NUREG-075, [1], también llamado WASH 1400 e Informe Rasmussen. Tras la ocurrencia del

accidente con fusión del núcleo en la central de Three Mile Island II (TMI), en 1979 se promovieron desde la NRC este tipo de análisis, editándose el NUREG-1150 [2] en 1987.

Los APS se estructuran en varios niveles, clasificados según la barrera de protección estudiada en cada caso. Surgen así los tres niveles característicos de todo APS:

- Nivel 1, que se ocupa de aquellas secuencias que conducen al daño severo al núcleo.
- Nivel 2, que se ocupa de las secuencias que implican fallo del recinto de contención y por tanto escape de productos radiactivos.
- Nivel 3, que finalmente trata de estimar la frecuencia de daños producidos al público, el medio ambiente y el patrimonio como consecuencia de los escapes radiactivos.

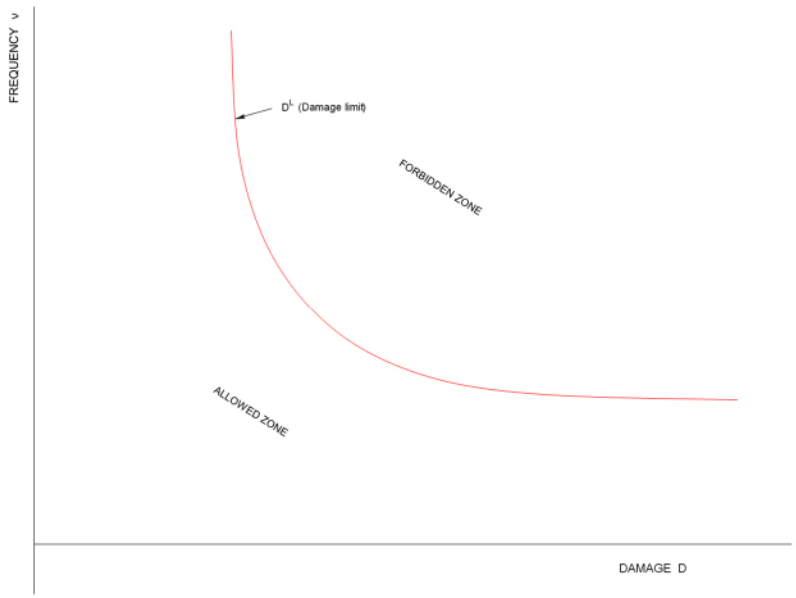

Figura 1 Representación del límite de daño

El Nivel 1 del APS tiene dos aspectos básicos: la modelación lógica de los accidentes y la cuantificación de los elementos de esa lógica. La modelación lógica se realiza en la práctica en tres etapas, o tareas, del APS: la determinación de cuáles son los sucesos iniciadores a considerar y su agrupamiento, la delineación de secuencias en los árboles de sucesos y el análisis de sistemas mediante los árboles de fallos. La cuantificación de los elementos de esa lógica, es decir, la obtención de las probabilidades de fallo de los sucesos elementales y la frecuencia de los sucesos iniciadores, se realiza en la tarea de análisis de datos. Una tarea adicional contempla el análisis de la fiabilidad humana.

El estudio de la evolución de los posibles accidentes que provocan el daño al núcleo se describe en la tarea de delineación de secuencias de un APS de nivel 1, en la que se analiza cómo se desarrolla un accidente, qué funciones de seguridad son necesarias para su mitigación y cómo intervienen los operadores en el seguimiento de los Procedimientos de Operación en Emergencia. La actuación de las funciones de seguridad se lleva a cabo mediante los sistemas de la instalación. El análisis de la forma en la que estos sistemas pueden dejar de cumplir su misión de seguridad se realiza en la tarea de análisis de

sistemas. Allí debe definirse el criterio de éxito de cada función de seguridad, cómo se consigue y qué combinaciones de fallos implican que no se cumpla este criterio de éxito.

Para verificar la calidad de los Análisis Probabilistas de Seguridad, la industria americana, con el apoyo y la participación de la NRC promovió la edición del estándar ASME/ANS-RA-S-2002 *Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications*, que se ha actualizado en varias ocasiones desde esa fecha y del cual la versión más reciente está dada por el ASME/ANS RA-S-1.1–2022, que constituye una revisión de la actualización de 2008. La NRC ha editado la Regulatory Guide 1.200 *An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities* que contiene la posición reguladora sobre la forma aceptable de demostrar la calidad de los APS para aplicaciones reguladoras que hagan uso de los resultados de los APS. El estándar de ASME establece tres Categorías de calidad de los APS en función del cumplimiento de ciertos requisitos. En cada aplicación debe determinarse qué Categoría debe cumplir el APS para poderse usar en esa aplicación, pudiendo llegar a especificar distintas Categorías aplicables para distintas partes del Análisis de Riesgo (distintos modelos de APS) asociados con la aplicación.

Con el fin de plantear la forma más conveniente de abordar las distintas aplicaciones de los APS en nuestro país en la Guía de Seguridad GS-1.14 *Criterios básicos para la realización de aplicaciones de los APS* se señalaba, de forma genérica, la necesidad de disponer de un APS actualizado como requisito para la realización de aplicaciones de APS y se definían los requisitos mínimos que dicha actualización debía requerir para ser aceptable como soporte de una aplicación. Para desarrollar detalladamente el proceso aceptable para dar cumplimiento a este requisito genérico de mantenimiento de un APS actualizado, el CSN ha editado la Guía de Seguridad GS-1.15 *Actualización y Mantenimiento de los Análisis Probabilistas de Seguridad*, usada por los titulares en sus procesos de elaboración de los APS. Además, dentro del Plan Base de Inspección del CSN se mantienen inspecciones periódicas (bienales) a los procesos de realización de los APS de las centrales nucleares (CC NN) españolas.

2. SECUENCIAS DE ACCIDENTE: ÁRBOLES DE SUCESOS

2.1 Árboles de sucesos

2.1.1 Sucesos iniciadores

Llamamos *iniciador* a un cambio de un cierto tipo y una cierta magnitud en equipos o en condiciones de contorno, que ocurre en condiciones de estado estacionario, y que saca a la instalación de dicho estado estacionario. En la situación estable a potencia, los iniciadores son aquellas circunstancias que desembocan en un disparo del reactor. Como consecuencia del suceso iniciador, la planta experimentará una evolución en la que deben actuar sistemas de seguridad y tener lugar acciones de los operadores para controlar la instalación y alcanzar un estado seguro.

Si se pretende considerar todos los tipos de iniciadores, de todas las magnitudes, ocurriendo desde todas las condiciones iniciales, tenemos que calcular un número infinito de transitorios. La forma de solucionar este problema es recurrir al agrupamiento y

clasificación de sucesos iniciadores, condiciones iniciales y evolución de los transitorios para hacer el problema abordable.

El espacio de todas las posibles condiciones iniciales se divide en regiones que cumplen las siguientes condiciones:

- Las frecuencias de los iniciadores son aproximadamente uniformes en toda la región.
- Un mismo iniciador que ocurra desde cualquier punto de la región daría lugar al mismo conjunto secuencias de transiciones.

La primera condición permite obtener un valor único para la frecuencia que va a ser usada en la cuantificación; la segunda permite representar las evoluciones de los transitorios que ocurren a partir de cada iniciador.

De la misma forma se clasifican las magnitudes de cada tipo de iniciador. Por ejemplo, las roturas se clasifican por tamaño y se incluyen en un mismo grupo todas las roturas que dan lugar a un mismo conjunto de posibles secuencias de transiciones. A veces incluso se pueden agrupar iniciadores de distinto tipo si dan lugar a consecuencias similares.

Una vez hechos los agrupamientos se elige como representante de cada grupo la combinación de condiciones iniciales, tipo y tamaño de iniciador que da lugar a consecuencias más severas para calcular con ellos una envolvente superior del gráfico de seguridad.

La identificación de sucesos iniciadores tiene lugar de varias formas.

- Exploración sistemática de la experiencia operativa en la central y de otras centrales de similar tecnología, determinándose qué sucesos han provocado el disparo del reactor y son aplicables a la planta bajo estudio.
- Análisis de las posibles causas de disparo mediante un estudio de los diagramas lógicos del sistema de protección del reactor.
- Análisis de modos y efectos de fallos (Failure Mode and Effect Analysis, FMEA)

En el APS en otros modos (es decir, el APS específico que evalúa el riesgo causado por sucesos iniciadores que se pueden producir durante modos de operación distintos de la operación a potencia), los iniciadores son de nuevo desviaciones respecto de las actividades que se llevan a cabo en la planta y que pueden poner en peligro la refrigeración de los elementos de combustible. La búsqueda de estos iniciadores se basa en el análisis de las funciones de seguridad que se mantienen en las actividades de parada, y se refieren a pérdidas de inventario (roturas del primario), pérdida de sistemas frontales (sistema de extracción de calor residual) y pérdidas de los sistemas soportes (agua de refrigeración de componentes o de servicios, potencia eléctrica exterior).

2.1.2 Secuencias de transiciones

Una vez definido el representante de cada iniciador, deben explorarse todas las evoluciones posibles de la dinámica de la planta. Para ello se consideran las actuaciones de las funciones de seguridad de que se dispone para conducir la planta a una situación segura. En los primeros instantes de la evolución del transitorio se activarán de forma automática el sistema de protección, que, en función de puntos de tarado definidos,, hace intervenir el sistema de disparo del reactor y los sistemas automáticos de aporte de

refrigerante, de despresurización de la vasija, de evacuación de calor, etc. La intervención de cada función protectora depende de su disponibilidad, y tendrá una cierta probabilidad de actuar, calculada mediante técnicas discutidas más adelante.

Para gestionar la parada segura de la central cuando ocurre una situación que requiera el disparo del reactor, se han diseñado procedimientos de operación en emergencia (POE). Estos son un conjunto detallado de instrucciones que guían a los operadores en la realización de las tareas necesarias para conducir la planta a condición segura. Los POE se han diseñado, además, considerando las distintas situaciones que pueden ocurrir en la central cuando no actúan las protecciones automáticas en la forma prevista, en cuyo caso conducen a la gestión del transitorio mediante la actuación de otros sistemas disponibles. Estos sistemas no tienen por qué ser de los clasificados como de seguridad en los documentos oficiales de explotación de la central.

La evolución de la planta es por tanto completamente dependiente de las acciones de los operadores en la activación de funciones de protección, por lo que la delineación de secuencias no puede hacerse sin considerar esas acciones.

2.1.3 Funciones de seguridad

Como se ha dicho, los sistemas automáticos de la planta, y posteriormente los operadores activarán distintos sistemas para gestionar un accidente y conducir la planta a condición segura. Cada uno de estos sistemas implanta una función de protección de la planta, que pueden dividirse en los siguientes grandes grupos:

- Control de la reactividad
- Refrigeración del reactor
- Integridad de la envuelta a presión del reactor
- Integridad de la contención

En función del tipo de diseño, estas funciones de seguridad vendrán implantadas por distintos sistemas, y su actuación será automática o activada por los operadores en el curso del seguimiento de los POE. Los sistemas que intervienen directamente en la mitigación de los accidentes se denominan *sistemas frontales*, y dependen para su funcionamiento de otros sistemas auxiliares, denominados *sistemas soporte.* Ejemplos de sistemas frontales son el sistema de inyección de seguridad o el de agua de alimentación auxiliar. Sistemas soporte son por ejemplo los sistemas de alimentación eléctrica de corriente alterna y continua, o los sistemas de refrigeración de componentes y de agua de servicios esenciales de la planta.

La actuación de cada uno de los sistemas en su función de seguridad tendrá lugar si se produce la demanda y el sistema no está fallado. La ocurrencia o no de la demanda dependerá de la evolución de las variables de estado de la planta, y deberá determinarse con ayuda de herramientas de simulación termohidráulica. La actuación de cada función de seguridad tendrá lugar según su diseño y según lo indicado en los POE.

Se deberá determinar para cada una de las actuaciones posibles cuál es la capacidad necesaria de la protección y en qué ventana temporal debe producirse la actuación para que sea capaz de mitigar el accidente. El conjunto de estas condiciones en las cuales se

cumple la función de seguridad se denomina el criterio de éxito de la función, que se traslada a los sistemas con los que se consigue esa función de seguridad.

Estos criterios deben determinarse también por medio de simulaciones de las posibles evoluciones de la planta.

2.1.4 Simulación de transitorios

El estudio de la evolución de la planta para determinar tanto los criterios de éxito en términos de la capacidad de los sistemas para mitigar el accidente, como para obtener el tiempo disponible para que los operadores realicen las acciones recogidas en los POE se realiza mediante simulaciones con códigos de cálculo. Estos son grandes programas de computación que calculan el comportamiento termohidráulico del reactor nuclear y de los sistemas de la planta. Códigos usados en la industria nuclear y en particular por las CC NN españolas en la delineación de secuencias de un APS son MAAP [3], RELAP [4] o MELCOR [5].

2.1.5 Representación del árbol de sucesos

Las secuencias que tienen lugar tras producirse un iniciador se representan de forma gráfica de la manera mostrada en la Figura 2.

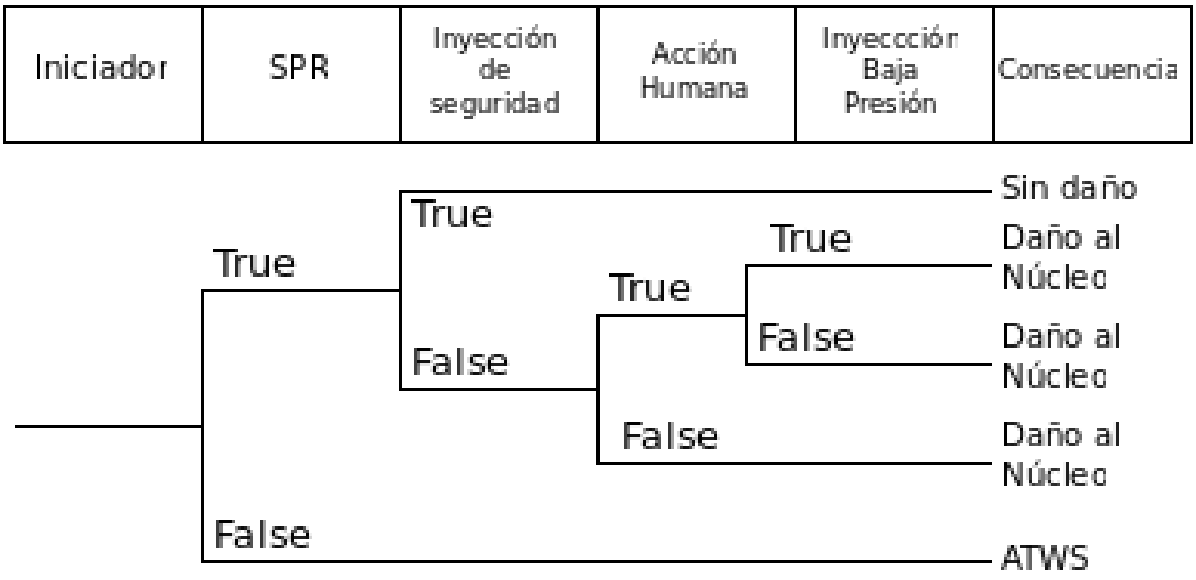

Figura 2 Ejemplo de representación de un árbol de sucesos

El primer nodo del árbol corresponde al suceso iniciador. Cada función de seguridad que interviene (es decir, es demandada para controlarlo) en el curso del accidente figura en la parte superior de la representación, en lo que se denomina cabeceros del árbol de sucesos. Al llegar a cada demanda se presentan (al menos) dos posibilidades, que la función de seguridad cumpla la misión de protección que tiene asignada o que no la cumpla y por tanto falle. El caso de fallo se representa por medio de la rama descendente; el de actuación correcta, por medio de la otra rama.

Los cabeceros del árbol de sucesos son, como se ha dicho, funciones de protección previstas en el diseño o en los procedimientos para mitigar los accidentes. Estas funciones

de protección se representan por medio de árboles funcionales que contemplan el fallo de la función de protección modelado mediante árboles de fallos. Los sistemas de seguridad, y otros no cualificados pero disponibles en la planta y contemplados en los procedimientos, son en general los encargados de ejercer la función de seguridad. Para alguna de las funciones de protección es necesaria la intervención directa de los operadores para iniciarla, por lo que los árboles funcionales contendrán los sucesos básicos que modelan el fallo en la actuación humana. Ocasionalmente, si así lo aconseja la modelación, puede haber sucesos básicos que modelan acciones humanas directamente como cabeceros en el árbol de sucesos.

Sin ser estrictamente sucesos que representan el éxito o fallo de las funciones de protección, para la modelación del accidente contenida en el árbol de sucesos puede necesitarse incluir en los cabeceros sucesos dinámicos. Éstos corresponden a la ocurrencia o no de fenómenos físicos o a la probabilidad de que ciertas variables tengan valores tales que modifiquen la evolución del accidente y hagan necesaria la intervención de distintas funciones de seguridad en caso de que ocurran. Ejemplos son la presurización del sistema primario hasta la presión de apertura de las válvulas de alivio o seguridad, la ocurrencia del fallo de los sellos de las bombas de refrigerante primario (que provoca la pérdida de refrigerante) o el valor de ciertos coeficientes de reactividad, que implican una evolución distinta del accidente en función del comportamiento del sistema de protección del reactor.

2.1.6 Criterios de éxito de las secuencias

Se continúa la descripción del accidente hasta llegar a dos tipos de estados:

- Estado seguro de la central, en el que se puede asegurar la refrigeración del núcleo a largo plazo y que no se han superado los límites de integridad del núcleo durante el transitorio. Los límites usados corresponden a los límites de integridad usados en el Estudio de Seguridad de la central para los accidentes limitativos. El criterio directo de daño al núcleo es alcanzar los 1204ºC en las vainas. Deben analizarse otras variables de proceso para asegurar que se mantiene la integridad de la envuelta a presión, limitando la presión a la presión de diseño.
- Daño al núcleo, en el que no se pueden asegurar estas condiciones. La situación de daño al núcleo puede cualificarse según las características de las secuencias para el análisis del nivel 2, dando lugar a distintos estados de daño a planta.

Es necesario establecer un límite temporal a la simulación del accidente. Este límite se toma como 24 horas tras la ocurrencia del iniciador. Es decir, se examina el estado de la central en las 24 horas de secuencia accidental, determinándose para ese instante las consecuencias de cada secuencia. La motivación para imponer ese límite temporal viene de la hipótesis de que será posible aportar ayuda externa a la central en caso de que la evolución del accidente no haya llevado a daño al núcleo en 24 horas pero no se haya alcanzado un estado estable y controlado de la instalación. En este caso, debe estar asegurado, mediante la existencia de procedimientos adecuados, el aporte de ayuda exterior.

2.2 Requisitos de alto nivel requeridos en el ASME/ANS-RA-Sa 2009

El estándar ASME/ANS-RA-Sa 2009 establece requisitos de alto nivel referidos a los siguientes aspectos de las tareas de análisis de sucesos iniciadores y desarrollo de los árboles de sucesos.

En lo que se refiere a la determinación de los sucesos iniciadores, se tienen los siguientes requisitos

HLR-AE-A El análisis de sucesos iniciadores debe proporcionar una identificación razonablemente completa de los sucesos iniciadores

HLR-BE-B El análisis de sucesos iniciadores debe agrupar los sucesos iniciadores de manera que los sucesos en el mismo grupo tengan requisitos de mitigación similares (es decir, los requisitos para la mayor parte de sucesos del grupo son menos restrictivos que los requisitos de mitigación limitantes para el grupo), para facilitar una estimación eficiente paro realista de la frecuencia de daño al núcleo.

HLR-CE-C El análisis de sucesos iniciadores debe estimar la frecuencia anual de ocurrencia de cada iniciador o grupo de iniciadores.

HLR-DE-D La documentación del análisis de sucesos iniciadores debe ser consistente con los requisitos soporte aplicables.

La delineación de secuencias se verifica mediante los siguientes requisitos de alto nivel,

HLR-AS-A El análisis de secuencias de accidente debe describir los escenarios específicos de planta que pueden alcanzar el daño al núcleo como consecuencia de cada iniciador modelado. Estos escenarios deben tener en cuenta la respuesta de los sistemas y las acciones de los operadores, incluyendo acciones de recuperación en apoyo de las funciones de seguridad clave necesarias para impedir el daño al núcleo.

HLR-BS-B Deben tenerse en cuenta las dependencias que pueden tener impacto en la capacidad de los sistemas para operar y proporcionar la función de seguridad.

HLR-CS-C La documentación del análisis de secuencias debe ser consistente con los requisitos soporte aplicables.

3. CRITERIOS DE ÉXITO. ÁRBOLES DE FALLO

Las funciones de seguridad representadas en los cabeceros de los árboles de sucesos corresponden a sistemas o acciones humanas requeridas por los POE. En los APS se hace un estudio de la fiabilidad de cada una de las funciones de seguridad que intervienen en la mitigación de accidentes.

En el caso de sistemas, se comienza por definir cuál es el funcionamiento necesario del sistema para cumplir su misión, lo que se denomina criterio de éxito del sistema. Se generan entonces dos tipos de requisitos:

1. La intensidad de la actuación, entendiendo como tal la capacidad necesaria del sistema. Por ejemplo, en el caso de sistemas de fluidos será necesario un caudal determinado para mitigar el accidente, que será proporcionado por uno o más trenes del sistema. Si el sistema dispone de *N* trenes redundantes y son necesarios *m* para

proporcionar la capacidad de protección, se habla de un criterio de éxito *m de N*, entendiéndose que con el funcionamiento de al menos *m* cualesquiera de los trenes se cumple el criterio, y que, con un número inferior, no.

2. El instante último en el que el sistema puede intervenir para cumplir su misión y el tiempo de actuación. El tiempo límite de actuación corresponde al momento a partir del cual, aunque el sistema intervenga, no será efectivo a la hora de evitar las consecuencias del accidente. El tiempo de actuación incide sobre la probabilidad de fallo en operación y sobre la probabilidad de fallo de las acciones humanas asociadas al sistema.

Una vez encontrado el criterio de éxito para un cabecero, se usa un procedimiento deductivo para descomponer el fallo en su cumplimiento en función de fallos más simples de los que se dispone de datos. Se buscan entonces las causas del llamado suceso indeseado (*top event*), esto es, el fallo del sistema a cumplir su criterio de éxito y se procede de forma recursiva descomponiendo las causas hasta el punto donde no es posible o practicable continuar la descomposición. Los fallos se concatenan usando puertas lógicas de fundamentalmente dos tipos, *AND* y *OR*. Se usan las primeras cuando es necesario el fallo concurrente de varios elementos para fallar otro, y las segundas cuando el fallo de un solo componente provoca el fallo de otro.

En los árboles de fallos se pueden encontrar los siguientes tipos de sucesos:

Top event. Es el suceso en el que culmina un árbol de fallos, y representa éxito o fallo de un cabecero. Será de forma habitual una puerta.

Puertas (gate events.) Son las salidas de las puertas lógicas, y que por tanto pueden expresarse como combinación de otras puertas y sucesos básicos.

Sucesos básicos (basic events.) Son aquellos que ya no pueden desarrollarse mediante un subárbol. Es decir, no son la salida de ninguna puerta lógica. Pueden referirse a componentes o a acciones del personal de la planta. En el primer caso están caracterizados por una *indisponibilidad*, es decir, por la probabilidad de que el componente no realice su función. Ésta debe suministrarse como un dato de entrada, y su obtención constituye una de las actividades propias de la tarea de análisis de datos de un APS. Atendiendo al origen de la indisponibilidad, se distinguen:

- Fallos a la demanda, en operación o en espera
- Indisponibilidades por pruebas o mantenimiento

Los sucesos básicos de fiabilidad humana generalmente corresponden a errores humanos que se producen antes de la ocurrencia del suceso iniciador (errores tipo 1 en la clasificación de EPRI) y a errores humanos de apoyo a los automatismos, que generalmente son requeridos por los procedimientos de operación y se clasifican como de tipo 3 en el caso de que los procedimientos sean basados en síntomas y de tipo 4, si no lo son.

Sucesos casa (house events). Son aquellos que resultan de las condiciones de contorno impuestas a la operación del sistema por el accidente considerado. Sirven además para seleccionar modos de operación de los sistemas. Su valor es sólo lógico, no probabilista.

Sucesos especiales. Dependen de la evolución dinámica de la planta o de la necesidad de considerar configuraciones especiales.

La estructura con que se construyen los árboles de fallos, usando puertas lógicas, permite construir la función de estructura que representa el fallo del sistema. Esta función es una ecuación booleana en la que aparecen los sucesos básicos en forma de suma de productos. Cada producto es una combinación de sucesos básicos que provoca el fallo del sistema.

En la cuantificación de un APS se usan las funciones de estructura de los sistemas que intervienen en cada secuencia para obtener la ecuación booleana que describe todas las combinaciones de fallos y sucesos iniciadores que conducen al daño al núcleo y a partir de la cual se puede estimar su frecuencia estimada de ocurrencia.

3.1 Requisitos de alto nivel requeridos en el ASME/ANS RA-S-1.1–2022

Se describen los siguientes requisitos de alto nivel para la determinación de los criterios de éxito:

HLR-SC-A Los criterios de éxito globales para el APS y los criterios de éxito para estructuras, sistemas, componentes (ESC) y acciones humanas usados en el APS deben definirse y referenciarse, y deben ser consistentes con las características, procedimientos y filosofía de operación de la planta.

HLR-SC-B Las bases ingenieriles termohidráulicas, estructurales y otras bases de apoyo deben ser capaces de proporcionar criterios de éxito y secuencia temporal de ocurrencia de sucesos suficiente para la cuantificación de la frecuencia de daño al núcleo y la de grandes liberaciones tempranas (LERF), para la determinación del impacto relativo de los criterios de éxito en las ESC y acciones humanas, y el impacto de la incertidumbre en esta determinación.

HLR-SC-C La documentación del análisis de criterios de éxito debe ser consistente con los requisitos soporte aplicables.

En lo que se refiere al análisis de sistemas, el ASME/ANS-RA-Sa 2009 establece los siguientes requisitos de alto nivel:

HLR-SY-A El análisis de sistemas debe proporcionar un tratamiento razonablemente completo de los modos de fallos o indisponibilidad de los sistemas representados en la definición de los sucesos iniciadores y en las definiciones de secuencia.

HLR-SY-B El análisis de sistemas debe proporcionar un tratamiento razonablemente completo de los fallos de causa común y de las dependencias en cada sistema y entre los sistemas entre sí.

4. RESULTADOS CUANTITATIVOS Y CUALITATIVOS

La cuantificación de un APS de nivel 1 consiste en la obtención de resultados del APS en términos de la frecuencia de daño al núcleo correspondiente a cada secuencia definida en la tarea de delineación de secuencias, la frecuencia de cada árbol de secuencias y la frecuencia global de daño al núcleo de la central, sumando todas las contribuciones de las secuencias. El cálculo de la frecuencia de daño al núcleo pasa por la obtención de la

ecuación de daño al núcleo, en la que aparecen las combinaciones de un suceso iniciador y fallos o indisponibilidades de componentes y errores humanos que llevan al daño al núcleo. Adicionalmente se obtienen las llamadas medidas de importancia de sucesos, componentes y sistemas, útiles en las aplicaciones directas de los resultados del APS (por ejemplo, al mantenimiento).

Esta tarea se alimenta de todas las anteriores, en cuanto que usa los árboles de sucesos como definición de las secuencias accidentales y los árboles de fallos que forman parte de los árboles funcionales, que a su vez son los cabeceros de los árboles de sucesos. Las frecuencias de los sucesos iniciadores y las probabilidades de fallo obtenidas en la tarea de datos, junto con los datos de fiabilidad humana de la correspondiente tarea constituyen los elementos básicos del cálculo.

4.1 Frecuencia de daño al núcleo

4.1.1 Álgebra de Boole

La representación de la fiabilidad de un sistema en función de los componentes mediante árboles de fallos se hace por medio de combinaciones de puertas de tipo AND y OR. Las secuencias de los árboles de sucesos vienen representadas por el estado de los cabeceros. El daño al núcleo se producirá entonces con ciertas combinaciones de cabeceros fallados, lo que puede representarse por una puerta AND. Las combinaciones de puertas AND y OR se tratan mediante el Álgebra de Boole. Las operaciones AND y OR en el álgebra de Boole tienen las propiedades asociativa y distributiva; como consecuencia de la tabla de verdad de las operaciones, se verifican las reglas de Idempotencia, Absorción, Aniquilación y De Morgan.

4.1.2 Conjuntos mínimos de fallo. Truncación

Cualquier ecuación booleana puede reducirse a una suma irreducible de productos de sucesos básicos. En el caso de los APS, usando a las propiedades del Álgebra de Boole, la ecuación en conjuntos mínimos de fallo que representa el daño al núcleo derivado de una secuencia se obtiene mediante la composición de las ecuaciones de los árboles funcionales asociados a los cabeceros que la definen. La composición se realiza multiplicando las ecuaciones booleanas de los cabeceros que están en estado fallado. El resultado se expresa como suma de productos de sucesos básicos que reciben el nombre de *conjunto mínimo de fallos* (CMF) o minimal *cut-set*. Cada uno de los cut-sets está formado por un suceso iniciador y una combinación de indisponibilidades de componentes o de errores humanos, cuya ocurrencia lleva a la fusión del núcleo. Los sucesos que representan fallos de componentes o errores humanos están caracterizados por su probabilidad mientras que el suceso iniciador está caracterizado por su frecuencia anual esperada.

Debido al gran número de conjuntos mínimos de fallo que pueden aparecer en la ecuación de daño al núcleo, en el proceso de obtención se truncan los conjuntos mínimos de fallo cuya probabilidad se encuentra por debajo de un cierto valor. Los valores usados normalmente en APS de CC NN españolas están en el rango de 10^{-11}.

4.1.3 Cálculo de la frecuencia de daño al núcleo

De acuerdo a la teoría de la probabilidad, la probabilidad de la unión de dos conjuntos viene dada por,

$$P(A \cup B) = P(A) + P(B) - P(A \cap B).$$

Esta relación puede extenderse para sumas de un número arbitrario de sucesos, apareciendo con signos alternados los productos de dos, tres, etc. hasta el número total de sumandos. En general,

$$P(A_1 \cup A_2 \cup \cdots \cup A_n) = \sum_{i=1}^{N} P(A_i) - \sum_{i<j} P(A_i)P(A_j) + \ldots + (-1)^N \prod_{i=1}^{N} P(A_i) \qquad (1)$$

Esta fórmula exacta para el cálculo de la probabilidad (o frecuencia) de una ecuación booleana no puede aplicarse en el caso de los resultados de los APS debido al gran número de términos que origina. Se recurre, por tanto, a aproximaciones reteniendo solo los primeros términos de la suma. Una expresión más compacta se obtiene por medio de la aproximación *Min Cut upper Bound*.

4.1.4 Medidas de importancia

La ecuación de daño al núcleo proporciona una información muy valiosa sobre el diseño de la planta, ya que identifica cuáles son las combinaciones de iniciador y fallos de sistemas o errores de los operadores que llevan a fusión del núcleo. Cada una de estas combinaciones tiene una probabilidad de ocurrencia, pero un mismo componente puede intervenir en muchas de esas combinaciones. Por ello, se definen distintas medidas de importancia para clasificar los sucesos básicos. Las medidas de importancia usuales son el incremento del riesgo, reducción del riesgo y la medida de Fussell-Vessely.

El incremento del riesgo (*risk increase*, RI) debido a un componente se define como el valor de la frecuencia de daño al núcleo cuando ese componente está fallado relativo a la frecuencia original de daño al núcleo. Da una idea de la importancia del fallo del componente en la planta.

La reducción del riesgo se define como la relación entre la frecuencia de daño al núcleo y la que se obtendría si el componente funcionase perfectamente. Da una idea de la importancia del funcionamiento correcto del componente.

La medida de Fussell-Vessely de un componente se define como el cociente de la frecuencia dada por todos los CMF que contienen fallos de ese componente y la frecuencia global del daño al núcleo.

4.2 Cálculo de incertidumbres

En los apartados anteriores se ha citado en varios puntos la necesidad de hacer un análisis de incertidumbres. Sin embargo, es importante separar conceptualmente dicho análisis de lo que significa la caracterización del riesgo. Por eso, aunque en la práctica ambas cosas se realizan de manera conjunta y por tanto aparecen como íntimamente relacionadas, se ha preferido en esta exposición poner de manifiesto la diferencia.

Resulta útil identificar tres tipos de incertidumbre que se deben valorar y que tienen impacto en los resultados de loa APS: incertidumbre paramétrica, incertidumbre en el modelo, e incertidumbre en la completitud del análisis.

Incertidumbre paramétrica. Las incertidumbres proceden de los modelos que representan la fenomenología de los accidentes. En estos modelos hay parámetros cuyo valor no se puede determinar, bien porque son difíciles de medir, o bien porque en realidad representan implícitamente un conjunto de fenómenos desconocidos.

Los valores de probabilidad asignados a los sucesos básicos no pueden considerarse como valores únicos. Son valores obtenidos mediante técnicas estadísticas, usando bases de datos de fallos de componentes. Estos valores de probabilidad de fallo están por tanto dados en realidad por medio de una distribución. Además, la consideración de la experiencia operativa propia de la planta, a través del análisis bayesiano de los datos también tiene como resultado una función de distribución de la probabilidad de fallo de los sucesos básicos. El valor puntual usado en el APS cuando se hace una cuantificación simple es el valor medio de la distribución.

Los resultados obtenidos deben complementarse por medio del cálculo de la incertidumbre asociada al resultado, que se obtiene propagando las distribuciones de incertidumbre de la probabilidad de los sucesos básicos. Esta propagación se hace mediante técnicas de Monte Carlo con muestreo estratificado, como es la técnica de hipercubo latino, para un número grande de historias (del orden de 10^6).

Como resultado final se obtiene una distribución estadística (tabulada) de la frecuencia de daño al núcleo, de la que se proporciona el valor medio y los percentiles 5, 50 y 95.

Incertidumbre en los modelos. El grado de conocimiento sobre los modelos que representan los sucesos y fenomenología que puede darse en un accidente analizado en los APS puede muy bien ser incompleto o admitir distintos enfoques respecto del modelo que debe usarse. Normalmente se elige un determinado modelo que sirve como estándar, si bien debe reconocerse que pueden existir modelos alternativos igualmente válidos; para algunos se desarrollan análisis de sensibilidad

Incertidumbre en la completitud. La falta de completitud no es en sí una medida de incertidumbre, sino un reflejo de la limitación en el alcance del modelo.

5. APLICACIONES DE LOS APS

La realización de los APS proporciona un análisis del diseño y operación de la central, enfocado al riesgo de accidentes que impliquen daño al núcleo del reactor y la posibilidad de escape radiactivo al exterior. El detalle con que se estudia la instalación y la capacidad de modificar los modelos para incorporar aspectos específicos de la central proporcionan un medio para analizar modificaciones de la instalación o de los procesos que en ella se realizan. El uso de los modelos de APS para obtener una estimación del riesgo en condiciones distintas del modelo base con un objetivo de análisis de estas nuevas condiciones se denomina aplicaciones de los APS.

5.1 Aplicaciones de los titulares

Atendiendo a su objetivo, pueden distinguirse dos tipos de aplicaciones de los APS. Las primeras se refieren al análisis de situaciones particulares que requieren estudios específicos de la instalación y que, en general, se deben a cambios fortuitos o inesperados de la planta, esto es, incidentes que alteran la configuración de los sistemas de seguridad o de la operación de la planta. Incorporando esta circunstancia en el modelo de APS puede deducirse la importancia que tiene ese estado concreto de la instalación en comparación con el estado sin alterar. Puesto que se trata de valorar una situación concreta, es posible contemplar las condiciones particulares observadas, en general menos restrictivas que las empleadas en los análisis genéricos. El análisis también recoge las medidas compensatorias implantadas para atenuar el riesgo, y permite valorar su impacto, modificarla o proponer nuevas medidas compensatorias en función de los resultados del análisis.

Un segundo tipo corresponde al análisis de actuaciones voluntarias de los titulares que alteran o pueden alterar las condiciones de su Autorización. En efecto, puede ser necesario o conveniente para el titular efectuar modificaciones en la instalación o en los procesos o procedimientos usados para mejorar la explotación, sea en aspectos de seguridad o económicos. Estas modificaciones requieren la apreciación favorable del CSN en los casos contemplados por la IS-21 y la GS-1.11. Esta normativa establece como criterio básico la necesidad de analizar si la alteración modifica de manera sustancial la frecuencia de ocurrencia de iniciadores o la magnitud de las consecuencias de los posibles accidentes. Para apoyar su solicitud, los titulares pueden hacer uso del cálculo de la alteración en el resultado de los APS, verificando que no constituye un incremento inaceptable del riesgo de la instalación. La valoración de estas circunstancias conlleva la estimación de las modificaciones de los modelos de APS para tenerlas en cuenta y el recálculo de los resultados de APS en esas nuevas condiciones. Cada tipo de aplicación tiene una metodología de uso que trata de asegurar que los resultados obtenidos cubren las condiciones más desfavorables para la instalación. En la sección 5.4 se identifican las reglas que concretan, en la normativa actual, cuándo el incremento de riesgo derivado de una solicitud resulta aceptable.

A continuación, se indican algunos tipos de aplicaciones de los APS propuestas por los titulares, a iniciativa propia o derivadas de requisitos de la normativa, realizados en España.

- El uso de los APS se ha extendido al análisis desde el punto de vista del riesgo de daño al núcleo de las actividades rutinarias de la instalación. Ejemplos son la valoración de la periodicidad o la planificación de las pruebas de los equipos o las tareas de mantenimiento. En este caso, este análisis deriva del requisito normativo de acotar el riesgo de las tareas de mantenimiento de la instalación contenido en la IS-15 emitida por el CSN, desarrollada por la GS-1.18.
- Las centrales han hecho uso de los APS también para la clasificación de los equipos en función de la influencia que tiene su indisponibilidad en el resultado de frecuencia de daño al núcleo o de liberación de material radiactivo. Esta clasificación, que hace uso de las medidas de importancia definidas más arriba, se ha empleado para la estructuración de los procesos de inspección y pruebas en servicio.

- Un caso significativo de aplicación de los análisis probabilistas de seguridad es la modificación de especificaciones técnicas de funcionamiento (ETF). El marco de uso de los APS se centra en los cambios de los intervalos de vigilancia y de los tiempos máximos de inoperabilidad contenidos en las ETF, que no tienen un soporte claro en los análisis de transitorios. Estos elementos solamente se pueden evaluar de manera sistemática con criterios probabilistas. Ambos parámetros tienen una traslación directa a parámetros de los APS que permite la valoración directa del cambio en su magnitud y por tanto permite establecer un juicio sobre la aceptabilidad del cambio propuesto.
- Transición de la norma que rige los sistemas y procedimientos de protección contra incendios para adoptar la normativa NFPA-805. Esta modificación requiere un análisis probabilista de incendios, centrado en el daño al núcleo (nivel) 1 y de Frecuencia de Grandes Liberaciones Tempranas (parte del análisis de nivel 2) que justifique que el riesgo calculado, derivado de los incendios con el conjunto de medidas y equipos existentes en la instalación (programa de protección contra incendios) se mantiene en valores aceptables.
- Adicionalmente, resultado de los análisis de APS se han propuesto varias modificaciones de diseño en CC NN españolas que han supuesto mejoras en la operación de las centrales, reduciendo la frecuencia de daño al núcleo.

5.2 Aplicaciones impulsadas por el CSN

El organismo regulador, en su misión de garantizar que la operación de las CC NN transcurre de forma segura, hace uso también de los APS como herramientas de valoración de ese nivel de seguridad. Existen varias actividades en este sentido, que se describen de forma resumida a continuación.

- El uso más significativo de los APS en la actualidad es el apoyo en la valoración de las desviaciones encontradas en las inspecciones del SISC (Sistema Integrado de Supervisión de Centrales). Los procedimientos del SISC demandan la valoración de la variación en el riesgo de daño al núcleo y de grandes liberaciones tempranas provocada por las deficiencias en los procesos de los titulares que se descubren en las inspecciones que realiza el CSN. Esta valoración permite dar criterios para establecer la gravedad de las deficiencias encontradas usando criterios numéricos derivados de los resultados de los APS y tienen incidencia directa en el proceso supervisor por cuanto la superación de determinados niveles preestablecidos desencadena acciones adicionales por parte del CSN.
- A la hora de analizar una solicitud de los titulares, aún en el caso de que no se haya remitido aportando información del impacto en los APS, por parte del CSN puede usarse esa información en apoyo en las evaluaciones, proporcionando un elemento más de juicio para valorar la solicitud.
- El análisis de incidentes ocurridos en CC NN constituye también una aplicación habitual en los organismos reguladores en la que se valora la importancia de un suceso ocurrido en las centrales por medio del impacto que tiene en el riesgo de daño al núcleo de la instalación. Este análisis se emplea también para determinar la conveniencia de realizar una inspección reactiva tras un incidente ocurrido en una central nuclear.

5.3 Concepto de Regulación Informada por el Riesgo (RIR)

5.3.1 Integración de los métodos de análisis en la RIR

Se conoce como *Regulación Informada por el Riesgo* (RIR) la utilización de métodos de licenciamiento y regulación de la actividad de las instalaciones que tienen en cuenta la información proporcionada por los APS en la toma de decisiones. Este concepto se ha desarrollado en la NRC y está plasmado en varias guías reguladoras que se comentarán más adelante. Solamente destacaremos aquí dos puntos relacionados con estas guías:

1. La información proporcionada por los análisis de APS se denomina en estas guías *información sobre el riesgo*.
2. Según se indica en las propias guías, el uso de la tecnología de APS debe incrementarse en todas las disciplinas de licenciamiento de forma que *complemente* el enfoque determinista y soporte la filosofía tradicional de defensa en profundidad.

Por tanto, no se trata de reemplazar los análisis de seguridad tradicionales con análisis basados en el APS sino de complementar los primeros con la visión adicional que puede obtenerse de los segundos. Incluso en aquellos temas que son difícilmente abordables con los métodos de análisis de transitorios, se debe hacer algún tipo de estimación sobre si se mantienen o no los márgenes de seguridad demostrados por dichos análisis.

El mayor problema que se encuentra la aplicación práctica de la RIR es conseguir la consistencia de los distintos tipos de análisis, debido a que se han desarrollado de forma bastante independiente y con objetivos distintos. Mientras los análisis de transitorios están centrados en la verificación del diseño de las protecciones automáticas, que afecta a la zona de menor daño y mayor frecuencia de las curvas de límite de daño y de riesgo de la instalación, los APS nacieron con una cierta vocación de verificación global de la seguridad de la planta, aunque solamente se centran en las zonas de alto daño y baja frecuencia de las curvas aludidas. Puesto que el objetivo es distinto, son distintas las hipótesis subyacentes en ambos casos y, en general, los análisis de transitorios suelen contener hipótesis más conservadoras que los APS, lo que dificulta la consistencia entre ambos métodos. Por otra parte, los APS, en su concepción actual, dependen fuertemente de la validez del diseño de los sistemas automáticos, aunque esta dependencia no aparece explícitamente, sino que está recogida en los criterios de éxito y en la delineación de secuencias. Todo esto hace que existan relaciones difíciles de identificar entre ambos métodos de análisis y que las conclusiones obtenidas con cualquiera de ellos deban ser analizadas también a la luz del otro para evitar degradaciones inadvertidas de la seguridad.

5.4 Normativa para la aplicación de la RIR

5.4.1 Normativa de la US NRC

La Nuclear Regulatory Commission (US NRC) ha emitido normativas de distinto nivel para incorporar los métodos basados en los APS para la regulación de las actividades de las CC NN. En las secciones siguientes se describe la normativa generada y se hace mención a los desarrollos en curso.

Normativa reglamentaria. Se está en la actualidad estudiando cambios en la regulación americana de nivel reglamentario, es decir, en el *Code of Federal Regulations* 10CFR50 en varios puntos, para incluir requisitos basados en los APS. El estudio de estos cambios se concreta en dos posibles caminos, que la NRC ha denominado opciones 2 y 3 para introducir elementos basados en los APS en la regulación.

En el año 1998 [6], la US NRC propuso tres opciones para aplicar los resultados de los APS en la regulación.

La primera opción consiste en usar las guías reguladoras que establecen métodos aceptables para problemas concretos, manteniendo las limitaciones actuales, es decir, sin hacer modificaciones en el 10CFR50 y sin modificar la consideración de los sistemas.

La opción 2 consiste en el cambio de los requisitos operacionales y de cualificación de las Estructuras, Sistemas y Componentes (ESC) de las CC NN de forma que reflejen además su relevancia para el daño al núcleo. Esta información adicional introduce un nuevo elemento para la toma de decisiones que afecten a la seguridad de las CC NN. Estos cambios afectarían a temas como la garantía de calidad, especificaciones técnicas, cualificación ambiental y evaluaciones de cambios de diseño basadas en el 10CFR50.59 *Cambios, pruebas y experimentos*.

La tercera opción corresponde a modificar los requisitos contenidos en el 10CFR50, incluso en su apéndice A donde se establecen los criterios generales de diseño, de forma que se incluyan consideraciones basadas en los APS.

Regulatory Guide 1.174 y siguientes El marco de aplicación actual de la RIR en la US NRC está gobernado por la guía reguladora RG 1.174 [7], *Un enfoque para usar Análisis Probabilistas de Riesgo en decisiones informadas por el riesgo sobre cambios específicos de planta a la base de licencia*, editada en 1998 conjuntamente con el capítulo 19 del *Standard Review Plan [8]*, y revisada en 2002. Al hilo de esta guía reguladora se editaron también en 1998 las siguientes:

RG 1.175. *An Approach for Plant-Specific, Risk-Informed Decisionmaking: Inservice Testing*. Establece un marco para las decisiones informadas por el riesgo en pruebas en servicio [9], editada conjuntamente con el capítulo 3.9.7 del *Standard Review Plan*.

RG 1.177. *An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications [10]*. Trata específicamente de los cambios en especificaciones técnicas de funcionamiento.

RG 1.178 *An approach for plant-specific risk-informed decisionmaking for inservice inspection of piping [11]*.Se ocupa de la inspección en servicio de tuberías

La guía reguladora 1.174 proporciona los métodos aceptables para usar las conclusiones de los APS y consideraciones sobre el riesgo para apoyar solicitudes de cambio en las bases de licencia aplicables a una CC NN, en el caso de que se requiera explícitamente la evaluación y aceptación de la NRC. La guía es de aplicación cuando el licenciatario incluye argumentos basados en los resultados de los APS-IPE (Individual Plant Examinations) en apoyo de su solicitud de cambio en las bases de licencia. Se indica, además, que el método puede ser aceptable en otras solicitudes que usen argumentos basados en el APS, aunque

no se refieran específicamente a cambios en la base de licencia. Se describe a continuación el contenido de la RG 1.174.

Cualquier cambio que el licenciatario proponga para cambiar la base de licencia que le es aplicable debe mantener un conjunto de principios básicos. Estos son:

1. El cambio propuesto es acorde con la regulación actual, a menos que se refiera explícitamente a un cambio de regulación, es decir un cambio específico o una solicitud de reglamentación.
2. El cambio propuesto es consistente con la filosofía de defensa en profundidad.
3. El cambio propuesto mantiene márgenes de seguridad suficientes.
4. Cuando el cambio tenga como resultado un incremento en la frecuencia de daño al núcleo o en el riesgo, los cambios deben ser pequeños y consistentes con la declaración del objetivo de seguridad de la US NRC.
5. El impacto de los cambios propuestos se vigilará usando estrategias de comprobación del funcionamiento.

Cada uno de los principios debe considerarse en el proceso de toma de decisiones integrado informado por el riesgo. La guía reguladora descansa en cuatro elementos, que se muestran en la Figura 3 y se describen a continuación.

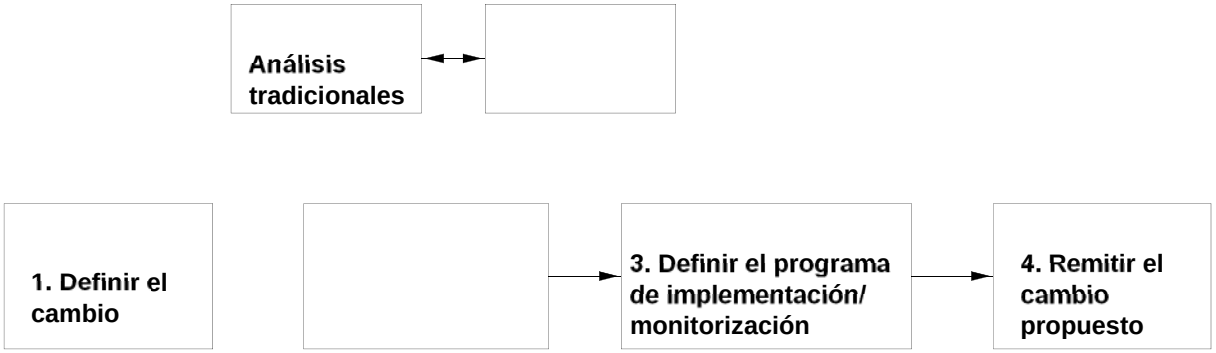

Figura 3 Elementos principales del proceso de toma de decisiones específico de planta e informado por el riesgo

Elemento 1: Definición de la propuesta de cambio. Se compone de tres actividades primarias. En primer lugar, deben identificarse los aspectos de la base de licencia que pueden verse afectados por el cambio, incluyendo aunque no limitándose a la regulación, Estudio de Seguridad, Especificaciones Técnicas de Funcionamiento y condiciones de licencia. En segundo lugar, se deben identificar todas las estructuras, sistemas y componentes, procedimientos y actividades que están cubiertas por el cambio en la base de licencia y deben considerarse las razones originales de cada requisito. En tercer lugar, se deben identificar estudios de ingeniería, métodos, datos aplicables de la planta y de la industria, conclusiones de los APS y resultados de programas de investigación disponibles y que son relevantes para el cambio.

Elemento 2: Realización de análisis de ingeniería. Dentro de este elemento se debe evaluar el mantenimiento del principio de defensa en profundidad y de márgenes de seguridad. En cuanto al primero, se debe asegurar que

- se mantiene el equilibrio entre la prevención del daño al núcleo, la prevención del fallo de la contención y la mitigación de consecuencias,
- se evita la excesiva confianza en procedimientos para compensar debilidades en el diseño, se preserva la redundancia, independencia y diversidad, se mantienen las defensas contra modos comunes de fallo, no se degrada la independencia de barreras se mantienen defensas contra los errores humanos, y
- se mantiene el espíritu de los Criterios Generales de Diseño del apéndice A del 10CFR50.

El mantenimiento de los márgenes de seguridad se garantiza usando códigos y estándares aceptados por la NRC, y se mantienen los criterios de aceptación contenidos en la base de licencia.

Los análisis cubren también elementos probabilistas. En ellos, el licenciatario debe demostrar que los incrementos en la frecuencia de daño al núcleo (CDF) y de las grandes liberaciones tempranas (LERF) son pequeños y están de acuerdo con el objetivo global de seguridad. Para ello, el modelo de APS usado debe tener un grado de detalle y una calidad adecuados para el análisis realizado. La RG 1.174 establece algunas indicaciones para determinar si el modelo de APS usado es aceptable para cada análisis propuesto.

Los incrementos en el riesgo en términos de CDF y LERF deben estar dentro de las bandas toleradas de la Figura 4, y debe realizarse el pertinente análisis de incertidumbre.

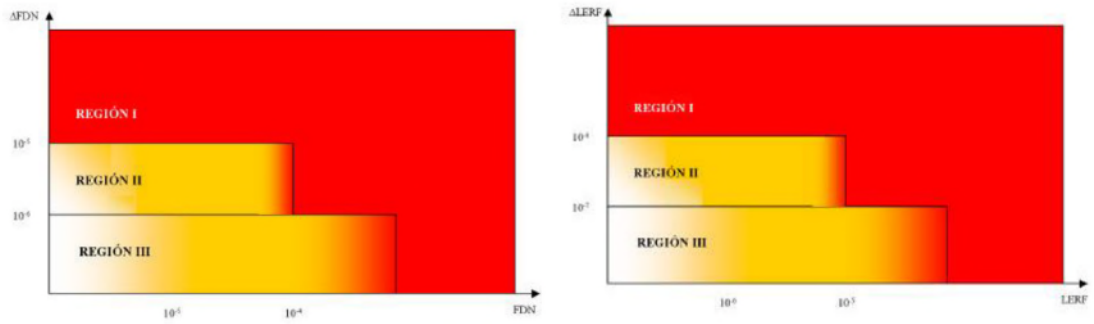

Figura 4 Criterios de aceptación para incrementos de CDF y LERF

Ambos criterios de aceptación de la Figura 4 deben usarse en la consideración de evaluaciones basadas en el APS, con las siguientes indicaciones (las unidades usadas son año^{-1}):

- Si la modificación presenta una disminución en CDF o LERF, se considerará aceptable desde el punto de vista de cada magnitud.
- Cuando el incremento en CDF es menor que 10^{-6} (incremento en LERF menor que 10^{-7}) se considera como muy pequeño y sería aceptable, salvo en el caso de que la CDF total sea mayor que 10^{-4} (LERF total mayor que 10^{-5}).

- Si el incremento en CDF es mayor de 10^{-6} pero menor de 10^{-5} ($10^{-7} < \Delta LERF < 10^{-6}$) se acepta el cambio si se puede demostrar razonablemente que la CDF total es menos de 10^{-4} (LERF menos de 10^{-5}).
- No se aceptarán cambios que resulten en incrementos de más de 10^{-5} (LERF mayor de 10^{-6}).

Se solicita explícitamente un estudio de las incertidumbres en los parámetros que pueden afectar al resultado, así como de las incertidumbres en la estructura del modelo y en su completitud.

Elemento 3: Definición del programa de implantación y vigilancia del cambio. El objetivo primario de estos elementos es asegurar que no hay degradación de la seguridad causada por cambios en las bases de licencia; para aplicaciones específicas se hace referencia a las restantes guías reguladoras 1.175 a 1.178. Este programa debe tener en cuenta las incertidumbres asociadas a los cálculos de ingeniería realizados, debe considerar el fallo de equipos que puedan afectar a las conclusiones del análisis y debe estar integrado en las actividades de la planta, en particular de acuerdo a la Regla de Mantenimiento 10CFR50.65. Son de aplicación también los requisitos del apéndice B del 10CFR50 de garantía de calidad.

Elemento 4: Remisión de la solicitud. Se menciona explícitamente la forma de remitir la solicitud para consideración de la US NRC.

Regulatory Guide 1.200 y ASME/ANS-RA-Sa 2009 Para verificar la calidad de los Análisis Probabilistas de Seguridad, la industria americana, con el apoyo y la participación de la US NRC promovió la edición del estándar ASME/ANS-RA-S-2002 *Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications*. La NRC ha editado la Regulatory Guide 1.200 *An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities* que contiene la posición reguladora sobre la forma aceptable de demostrar la calidad de los APS para aplicaciones reguladoras que hagan uso de los resultados de los APS. El estándar de ASME establece tres Categorías de calidad de los APS en función del cumplimiento de ciertos requisitos. En cada aplicación debe determinarse qué Categoría debe cumplir el APS para poderse usar en esa aplicación, pudiendo llegar a especificar distintas Categorías aplicables para distintas partes del Análisis de Riesgo (distintos modelos de APS) asociados con la aplicación.

5.4.2 Normativa del CSN. IS-25, GS 1.14 y GS 1.15

La Instrucción del Consejo IS-25 [12] establece los criterios y requisitos sobre la realización de los análisis probabilistas de seguridad y sus aplicaciones a las centrales nucleares, indicando el alcance de los modelos de APS que deben realizar las CC NN españolas y los criterios de calidad y actualización que deben mantener. Establece también condiciones sobre el uso de los APS como herramientas de apoyo en las solicitudes de los titulares.

Es CSN ha hecho una adaptación de la RG 1.174 que ha editado como Guía de Seguridad (GS) 1.14 [13], que establece los principios básicos para la realización de aplicaciones de los APS, en relación con el impacto en la seguridad de los cambios que se pide en la GS 1.11 del CSN. La GS 1.14 hace especial énfasis en los requisitos de los APS para adecuarse a las solicitudes presentadas, teniendo en cuenta las particularidades de los

estudios de APS realizados por las CC NN españolas, y sus criterios de mantenimiento y actualización.

La GS 1.15 [14] desarrolla los criterios de actualización de los modelos de APS en función de las novedades (modificaciones de diseño o procedimentales) que haya habido en la instalación, distinguiendo distintos tipos de procesos de mantenimiento de los modelos de APS en función del impacto de los cambios habidos.

6. VISIÓN GENERAL DEL APS DE NIVEL 2

El Nivel 2 de APS parte del análisis realizado en el APS de nivel 1, y extiende el análisis considerando el comportamiento de los sistemas de la contención y las acciones humanas contenidas en los Procedimientos de Operación de Emergencia o en las Guías de Gestión de Accidente Severo. Para el análisis debe recogerse información de la fenomenología de accidente severo y la forma en que esta fenomenología contribuye al fallo de la contención y a la liberación de productos de fisión al medio ambiente. Los resultados del APS de nivel 2 expresan la frecuencia de ocurrencia de los modos de fallo de la contención y la frecuencia de excedencia de liberación al medio ambiente de los grupos radiológicos definidos. La Figura 5 presenta un esquema simplificado de la realización de un APS de nivel 2. En este esquema, se parte de las secuencias que han llevado a daño al núcleo, ampliando primero los árboles de sucesos con los sistemas de mitigación de accidentes en la contención. Esta ampliación no altera el estado final de las secuencias, pero proporciona los elementos necesarios para el cálculo de la frecuencia posterior. Estas secuencias se agrupan en conjuntos que se denominan *Estados de Daño a Planta* (EDP, PDS en sus siglas en inglés), que constituyen el punto de partida inicial del análisis de la liberación de productos de fisión al exterior de la central. La agrupación recoge distintas características de las secuencias que permiten analizar la progresión del accidente de una manera eficaz. La primera distinción que puede hacerse corresponde al estado de la contención en el momento del accidente severo. La contención puede no ser estanca en ese momento, porque haya ocurrido un fallo de los sistemas de aislamiento o porque las características del accidente resulten en una vía de escape de los productos de fisión al exterior de la contención, como son los casos de LOCA de interfase o rotura de tubos de los generadores de vapor. Si no es ése el caso, debe analizarse la progresión del accidente dentro de la contención y la probabilidad de su fallo condicionada a la condición inicial (es decir, al EDP considerado en cada caso). Cada uno de los fenómenos que pueden ocurrir durante la evolución del accidente severo en la contención contribuye a la probabilidad de que falle la contención. Este cálculo se realiza mediante un árbol de sucesos de progresión del accidente (APET), que guarda cierta semejanza con los árboles de sucesos de nivel 1, pero que incorpora las probabilidades de ocurrencia de los fenómenos que pueden poner en peligro la integridad de la contención. Para calcular la frecuencia esperada de escape de productos de fisión al exterior, se combinan las secuencias de ambos grupos de EDP, clasificándolas en categorías de liberación (*bines*), a partir de las cuales se calcula la frecuencia de excedencia de liberaciones de material radiactivo.

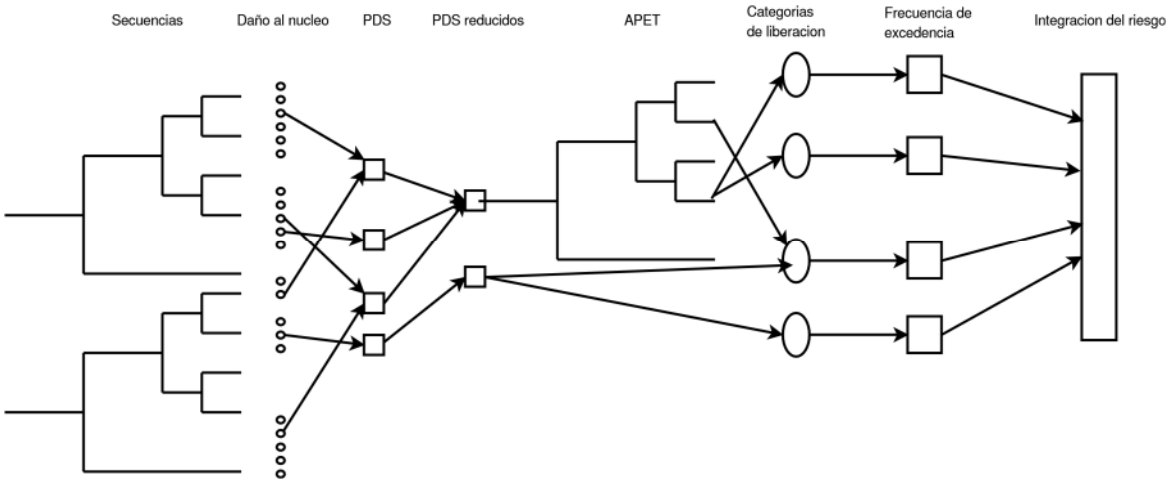

Figura 5 Esquema simplificado de realización del APS de nivel 2

Se define además la Frecuencia de Grandes Liberaciones Tempranas (FGLT, *Large Early Release Frequency (LERF)*), una medida de riesgo usada en las aplicaciones de los APS para caracterizar la aceptabilidad del riesgo de la instalación, como las liberaciones rápidas y no mitigadas desde la contención al exterior de productos de fisión, que ocurren antes de la implantación de medidas efectivas de gestión de la emergencia exterior, en magnitud tal que hay potencialidad de efectos tempranos para la salud.

7. BIBLIOGRAFÍA

[1] N.Rasmussen et al . Reactor safety study. Technical Report NUREG-75/014, USNRC, 1975.

[2] US NRC. Reactor risk reference document. Technical Report NUREG-1150, US Nuclear Regulatory Commision, 1987.

[3] Fauske & Associates Inc. *MAAP 3.0B, User's Manual*, 1995.

[4] The RELAP5 Code Development Team. RELAP5/MOD3 code manual, volume I: Code structure, system models and solution methods. Technical Report NUREG/CR-5535, INEL-95/0174, Idaho National Engineering Laboratory, June 1995.

[5] D. I. Chanin et al. Melcor computer code manuals. Technical Report NUREG/CR6119, US NRC, 1994.

[6] USNRC. *SECY 98-300. Options for Risk-Informed Revision to 10 CFR Part 50. Domestic Licensing of Production and Utilization Facilities*, dic 1998.

[7] USNRC. *Regulatory Guide 1.174. An approach for using probabilistic risk assessment in risk-informed decisions on plant-specific changes to the licensing basis*. US NRC, 2002. Rev. 1.

[8] USNRC. *Use of probabilistic risk assessment in plant-specific, risk-informed decisionmaking: general guidance*, chapter 19. Number NUREG-0800. USNRC, 2002.

[9] USNRC. *Regulatory Guide 1-175. An Approach for Plant-Specific, Risk-Informed Decisionmaking: Inservice Testing*. US NRC, 2002. Rev. 1.

[10]USNRC. *Regulatory Guide 1-177. An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications*. US NRC, 2002. Rev. 1.

[11]USNRC. *Regulatory Guide 1-178. An approach for plant-specific risk-informed decisionmaking for inservice inspection of piping*. US NRC, 2002. Rev. 1.

[12]Instrucción IS-25, de 9 de junio de 2010, del Consejo de Seguridad Nuclear, sobre criterios y requisitos sobre la realización de los análisis probabilistas de seguridad y sus aplicaciones a las centrales nucleares.

[13]Guía de Seguridad 1.14 (Rev. 1) "Criterios básicos para la realización de aplicaciones de los Análisis Probabilistas de Seguridad"

[14]Guía de Seguridad 1.15 (Rev. 1) "Actualización y mantenimiento de los Análisis Probabilistas de Seguridad"