

Tercer Ejercicio. Seguridad Nuclear

Tema 3.A.1

La Seguridad Nuclear. Fundamentos. Métodos de análisis. Aplicación a centrales nucleares e instalaciones del ciclo de combustible.

Resumen

Una instalación nuclear, como cualquier instalación industrial, incluye un conjunto de sistemas que realizan ciertas funciones operativas para la obtención de un determinado beneficio. Sin embargo, la operación de dichas instalaciones conlleva también riesgos, es decir la posibilidad de generar efectos no deseados o daños, que deben ser previstos y analizados para su prevención y/o mitigación mediante sistemas, adicionales a los de control de la operación, denominados sistemas de protección.

Para considerar que una planta es segura se debe garantizar que en condiciones normales o situaciones frecuentes no se superan determinados límites de daño y que aquellas situaciones susceptibles de generar daños importantes son extremadamente infrecuentes.

Por tanto, para mejorar la seguridad se deben introducir en el diseño distintos tipos de elementos: unos orientados a dificultar la ocurrencia de fenómenos generadores de daño (seguridad intrínseca), otros orientados a limitar la magnitud de los daños generados (seguridad mediante sistemas y procedimientos) y otros orientados a disminuir la frecuencia con la que dichos daños se pueden generar (redundancia, diversidad, separación, etc.)

La valoración del nivel de seguridad de la instalación no puede estar basada en medidas experimentales. En esta tarea sólo cabe el recurso a técnicas analíticas. Los análisis de seguridad son la herramienta fundamental de valoración de la seguridad de una planta. Existen dos tipos principales de técnicas de análisis: los análisis de transitorios base de diseño y los análisis de riesgo residual.

El análisis de transitorios base de diseño (comúnmente llamado análisis determinista) se basa en seleccionar situaciones especialmente exigentes para la protección con el fin de demostrar que, si la protección es eficaz en esos casos, también será eficaz en otros muchos casos que se ajustan a las hipótesis de diseño.

El análisis probabilista de seguridad (o análisis del riesgo residual) tiene por objetivo evaluar la eficacia de la protección diseñada mediante la estimación de la frecuencia con la que se pueden superar determinados límites de seguridad.

CONTENIDO

1. Introducción	3
2. Seguridad nuclear	3
3. Fundamentos	5
3.1. Defensa en profundidad	5
3.2. Principios de mitigación del daño: Seguridad intrínseca, mediante sistemas y mediante procedimientos	10
3.2.1. Seguridad intrínseca	11
3.2.2. Seguridad mediante sistemas	11
3.2.3. Seguridad mediante procedimientos	13
3.3. Principios para la reducción de la frecuencia del daño: Redundancia, Diversidad y Separación	14
3.3.1. Redundancia	15
3.3.2. Diversidad	15
3.3.3. Separación	15
4. Métodos de evaluación y análisis de seguridad	16
4.1. Análisis de transitorios base de diseño	17
4.2. Análisis del riesgo residual	19
5. Aplicación a las instalaciones del ciclo de combustible	21
5.1. Análisis Integrado de Seguridad (ISA)	24
6. Referencias	27
Relación con otros temas	28

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 pueden 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.

Los daños que la instalación genere en condiciones de operación normal o en situaciones que, siendo anormales, se pueden producir con cierta frecuencia, deben ser lógicamente pequeños. En caso de que la instalación pueda producir daños importantes en determinadas condiciones, se debe asegurar que la posibilidad de que esto ocurra es tanto más remota cuanto mayor es el daño potencial.

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 y la aplicación de otros principios de defensa en profundidad reducen la posibilidad de ocurrencia de daños, sin que por ello puedan ser ignorados ya que también pueden ser 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.).

En las secciones 2 a 4 que siguen se describen brevemente los fundamentos, principios y conceptos más importantes utilizados en Seguridad Nuclear, así como los principales métodos de análisis utilizados, principalmente en su aplicación al caso de las centrales nucleares en los casos que sea inevitable la particularización. En la sección 5 se añaden además los aspectos más singulares correspondientes a las instalaciones de ciclo de combustible.

2. Seguridad nuclear.

De lo dicho en el apartado anterior se deduce que la calificación de una instalación desde el punto de vista de la seguridad debe tener en cuenta dos variables: el **daño** que se puede producir y la **verosimilitud** de que ese daño efectivamente se produzca. El daño nuclear se puede medir, como se ha apuntado antes, en términos de dosis o en términos de liberación de materiales radiactivos al exterior de la instalación. Este daño se puede producir como

consecuencia del funcionamiento, normal o anormal, de los sistemas de la instalación; por tanto, el daño se genera cuando ocurren determinados sucesos o fenómenos en la instalación y su magnitud depende de la naturaleza de los fenómenos o sucesos que lo generan.

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 riesgo** 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 riesgo de la instalación.

Para que se pueda considerar que el nivel de riesgo de la instalación es aceptable, su curva característica de riesgo no puede cruzar en ningún punto a la curva límite. El objeto de la seguridad nuclear es por tanto obtener la característica de riesgo de la instalación, compararla con la curva límite de riesgo y obtener las conclusiones pertinentes sobre su aceptabilidad. Debe tenerse en cuenta, no obstante, que la elevada complejidad de los procesos que intervienen en una instalación nuclear no permite la determinación precisa de la curva característica de la instalación. Por ello, y para asegurar que no se superan los límites establecidos, se emplean metodologías acotantes (envolventes, en la terminología usual) y se complementan con un estudio de las incertidumbres presentes en los cálculos.

La bi-dimensionalidad del concepto de riesgo permite justificar el planteamiento de dos tipos de medidas compensatorias del riesgo, según que la componente que se pretenda optimizar sea el daño o la frecuencia. En el primer caso aparecen conceptos relativos a defensa en profundidad, protección por barreras, seguridad intrínseca y mediante sistemas y procedimientos, y en el segundo caso de redundancia, diversidad y separación, que son descritos en los apartados siguientes.

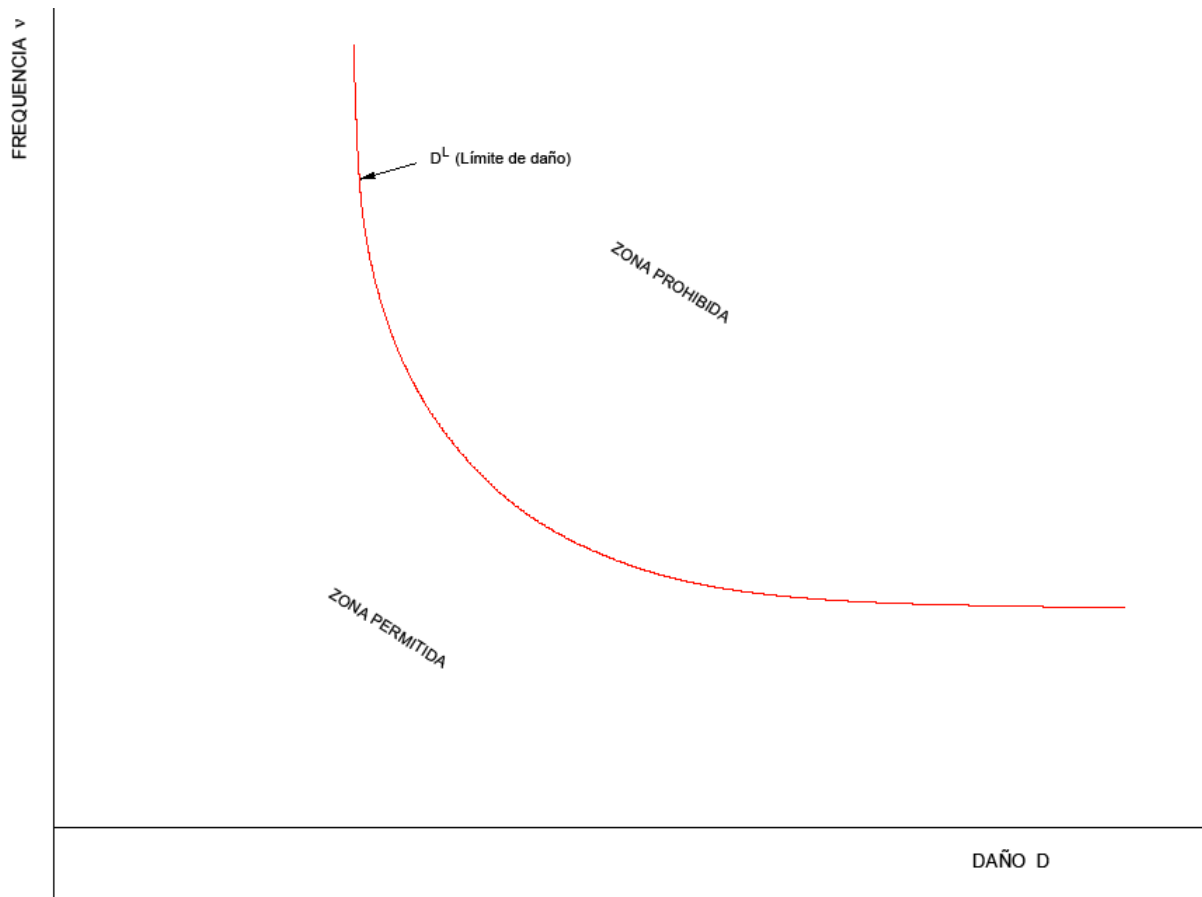


Figura 1: Representación del límite de daño.

3. Fundamentos.

La base fundamental de la seguridad nuclear recae en la aplicación del **principio de defensa en profundidad**, en el cual se enmarcan otros conceptos y elementos: **protección por barreras**, **seguridad intrínseca**, **mediante sistemas** y **mediante procedimientos**, **redundancia**, **diversidad**, **separación**, etc. Todos ellos se pueden estructurar y justificar según la dirección de la componente del riesgo (daño o frecuencia) que se pretenda optimizar (secciones 3.2 y 3.3).

3.1. Defensa en profundidad.

La defensa en profundidad consiste en la utilización de diversos niveles de equipos y procedimientos que permitan mantener la eficacia de las diversas barreras físicas dispuestas entre el material radiactivo y los trabajadores, público y medio ambiente, tanto en operación normal como ante sucesos operacionales previstos o accidentes en la instalación. El principio se implanta a través del diseño y la operación de una serie de protecciones graduales contra las consecuencias de un conjunto amplio de transitorios, incidentes y accidentes que incluyen fallos de equipos, errores humanos, y sucesos

externos a la planta. Esto es, lo que se pretende es dotar a la instalación con diversos niveles de protección que incluyen barreras sucesivas, para impedir la liberación de radiactividad al exterior. Sus objetivos son:

- compensar los eventuales fallos humanos y de equipos;
- mantener la eficacia de las barreras evitando el daño a la planta y las propias barreras; y
- protección del público y el ambiente en los casos de que estas barreras no sean totalmente eficaces.

En primera instancia, el público y el ambiente resultan protegidos a través de estas barreras sucesivas, que pueden desempeñar funciones tanto operativas como de seguridad. En el caso de los reactores de agua estas barreras que confinan los productos de fisión son típicamente:

1. la propia matriz de material combustible,
2. la vaina del elemento combustible,
3. el sistema de refrigeración del reactor, y
4. el edificio de la contención.

El concepto de defensa en profundidad intenta preservar la integridad de estas barreras contra la ocurrencia de sucesos (internos y externos) que pueden degradar su funcionalidad. Las estrategias utilizadas para su implantación son de dos tipos:

1. la **prevención de accidentes**, y
2. si la prevención fallase, **mitigación de accidentes**, esto es limitar las posibles consecuencias previniendo posibles deterioros en la evolución de éstos.

La prevención de ocurrencia de accidentes queda plasmada a través de:

- Una alta calidad durante el diseño, construcción y operación de la planta, que permite asegurar que las desviaciones con respecto al funcionamiento normal serán infrecuentes.
- La disponibilidad de las funciones de seguridad fundamentales (control de la potencia nuclear, refrigeración adecuada del núcleo y confinamiento del material radiactivo), mediante actuaciones automáticas y/o manuales de control y de seguridad.
- Programas de pruebas de vigilancia, tales como ensayos no destructivos o pruebas periódicas.

Estas estrategias se estructuran a su vez en cinco niveles secuenciales (i.e., de tal manera que si un nivel fallase se dispondría del siguiente nivel para atajar la situación):

1. Nivel 1: Prevención de operación anormal y fallos de sistemas.
2. Nivel 2: Control de la operación anormal, detección de fallos en los sistemas de control, limitación y protección, y otras características de supervisión.

3. Nivel 3: Control de accidentes dentro de la base de diseño.
4. Nivel 4: Control de accidentes severos, incluyendo la prevención y mitigación de consecuencias.
5. Nivel 5: Mitigación de consecuencias radiológicas de los escapes significativos.

Los cuatro primeros niveles se orientan a la protección de las barreras y mitigación de liberaciones, mientras que el último hacia las medidas de emergencia en el exterior.

Se debe asegurar además la independencia de cada uno de estos niveles, esto es, que cualquier fallo simple (en los equipos o en acciones humanas) en cualquiera de los niveles no se propaga deteriorando la capacidad de defensa en profundidad en niveles subsiguientes. Esto a su vez, se debe traducir en que la existencia de determinados niveles superiores de defensa en profundidad no justifica la operación continuada con niveles inferiores reducidos en su capacidad de defensa en profundidad.

Medidas asociadas a cada uno de estos niveles son las siguientes:

1. Nivel 1: Prevención de operación anormal y fallos de sistemas, a través de la adopción de medidas conservadoras, fundamentalmente durante el diseño, que aseguren el confinamiento del material radiactivo y minimicen desviaciones respecto a las condiciones normales de operación. Éstas, que deben ser consideradas desde la selección del emplazamiento, procesos de diseño, fabricación, construcción, operación, mantenimiento y clausura, incluyen:
 - definición clara de lo que son condiciones normales y anormales de operación;
 - diseño de sistemas y componentes con márgenes adecuados y suficientes para minimizar la necesidad de tomar acciones de los niveles 2 y 3.
 - selección cuidadosa de materiales así como utilización de adecuados procesos de fabricación, tecnología y pruebas;
 - diseño de adecuadas interfaces hombre-máquina que facilite disponer de tiempo suficiente para las acciones humanas;
 - personal de operación cualificado y adecuadamente entrenado;
 - instrucciones de operación adecuadas;
 - instrumentación fiable del estado y condiciones operativas de la instalación;
 - registro, evaluación y utilización de la experiencia operativa (propia y ajena);
 - mantenimiento preventivo priorizado según la importancia para la seguridad y requisitos de fiabilidad de los sistemas.

2. Nivel 2: Control de la operación anormal, detección de fallos en los sistemas de control, limitación y protección, y otras características de supervisión. Con el objetivo de asegurar que la instalación retorna rápidamente al funcionamiento normal en su caso, se debe asegurar que se dota a la instalación con:
- Características intrínsecas de la propia instalación (p.e., estabilidad e inercia térmica del núcleo del reactor) así como sistemas de control de la operación anormal (i.e., sucesos operacionales previstos), considerando además posibles fenómenos y circunstancias adicionales que puedan deteriorar la situación, y diseñados con criterios específicos de fiabilidad (p.e., cualificación, disposición, redundancia, ...);
 - Dispositivos y equipos de diagnóstico (p.e., sistemas automáticos de control) que tomen acciones correctoras antes de alcanzar los límites de actuación de las protecciones;
 - Programas de inspección en servicio y de pruebas periódicas para la vigilancia de la calidad y cumplimiento de requisitos de diseño, y la detección de cualquier funcionamiento degradado de equipos y componentes con anterioridad a que la seguridad de la instalación se vea afectada.
3. Nivel 3: Control de accidentes dentro de la base de diseño, mediante el diseño de sistemas de protección y de salvaguardias tecnológicas, para prevenir una evolución de la situación anormal hacia situaciones más degradadas (i.e., de accidente severo), y para asegurar el confinamiento del material radiactivo en el interior del sistema de contención. En esencia, estas medidas se encaminan a prevenir el daño en los elementos combustibles. Estos sistemas de protección y salvaguardias son diseñados sobre la base de unos accidentes postulados (i.e., accidentes base de diseño) representando conjuntos envolventes de sucesos similares, y haciendo uso de unos principios que aseguren una alta fiabilidad (p.e., *redundancia, separación física, diversidad o redundancia funcional, suficiente grado de automatismo, capacidad de pruebas, cualificación ambiental*; ver apartado 3.3).
- En el rango de tiempo corto (i.e., en el inicio del accidente) la actuaciones dominantes son las de los sistemas de seguridad automáticos, que pueden ser de actuación activa o pasiva, según que para su funcionamiento requiera o no de una alimentación externa de energía. Sin embargo, para la operación posterior se requiere también de unos procedimientos de operación con el propósito de asegurar y mantener en el largo plazo la integridad de las barreras, muy en especial del sistema de contención.
4. Nivel 4: Control de accidentes severos, incluyendo la prevención y mitigación de consecuencias. A pesar de que el cumplimiento de las medidas correspondientes a los tres niveles anteriores asegurarían el mantenimiento de la integridad estructural de los elementos combustibles y la limitación de potenciales riesgos radiológicos, se consideran medidas

de protección adicionales, con el objetivo de asegurar que la verosimilitud de un accidente con daño severo en los elementos combustibles, y la magnitud de los escapes en esas circunstancias, se mantienen tan bajos como sea razonablemente realizable (i.e., **criterio ALARP**).

En estos casos se contemplan circunstancias y condiciones severas que no fueron explícitamente consideradas en el diseño original (i.e., niveles 1 a 3) debido a su muy baja probabilidad de ocurrencia (p.e., tras fallos múltiples), y que originarían potencialmente escapes significativos de material radiactivos al exterior. Si bien algunas de las medidas de defensa correspondientes a los niveles previos pueden ayudar a paliar dichas condiciones degradadas, se diseñan sistemas adicionales específicos, así como los sistemas de soporte de éstos. Esto no debe servir para justificar o excusar deficiencias en niveles previos (y en cualquiera de sus etapas diseño, fabricación, construcción, operación, mantenimiento o desmantelamiento).

Adicionalmente, se dota con medidas de gestión de accidente preventivas y mitigadoras, para controlar el curso del accidente severo y de mitigar sus consecuencias. Objetivos esenciales de la gestión de accidentes son:

- seguimiento del estado de la instalación;
- control de subcriticidad;
- recuperación de un sumidero de calor para el combustible, y mantenimiento de la refrigeración en el largo plazo;
- asegurar la integridad de la contención, previniendo la aparición de cargas (térmicas o de presión);
- recuperación del control de la planta, o ralentización de la degradación en caso de que ésta no pueda ser finalizada, e implantación de medidas de emergencia interior y exterior.

El objetivo fundamental de las acciones de mitigación de la gestión de accidentes es la protección del confinamiento. En el caso de las plantas nucleares normalmente existe una estructura de contención resistente a la presión, y con estrictos límites de fugas ante determinadas condiciones de presión. Los sistemas que preservan la capacidad de la contención (p.e., refrigeración, control de penetraciones, etc.) se diseñan también con criterios y principios similares a los utilizados en el diseño de sistemas y protecciones asociados a niveles previos (p.e., conservadurismos, redundancia, etc.).

En este nivel resulta esencial el papel del equipo de operación, para actuación de equipos y sistemas en algunos casos desempeñando funciones más allá de las inicialmente previstas, o sistemas ad-hoc o temporales. Todo ello requiere por tanto un adecuado entrenamiento y preparación de éstos, así como una implicación amplia de otras instancias de la organización (p.e., centro de apoyo técnico de emergencias).

5. Nivel 5: Mitigación de consecuencias de radiológicas de los escapes significativos.

Incluso suponiendo plenamente eficaces las medidas del nivel 4, sería inconsistente con el concepto de defensa en profundidad no considerar unos planes de emergencia exterior, para recopilar y evaluar toda la información sobre la amplitud de las exposiciones a productos radiactivos que se originarían en las circunstancias improbables de que fallase todos los niveles previos, así como las medidas protectoras de corto y largo plazo que constituirían la intervención. Las autoridades responsables de las emergencias adoptarían las medidas correspondientes a instancias de la operadora de la instalación y del organismo regulador.

Estos planes de emergencia exterior son preparados por la operadora de la instalación aprobados por las autoridades correspondientes, y están sujetos a ciertos requisitos derivados de acuerdos internacionales, que por ejemplo demandan su ejercicio periódico junto con el de los planes de emergencia interior.

3.2. Principios de mitigación del daño: Seguridad intrínseca, mediante sistemas y mediante procedimientos.

La ocurrencia de desviaciones respecto de la operación prevista en las instalaciones industriales en general y en las instalaciones nucleares en particular puede ser de diversa naturaleza (p.e., aleatoria), dependiente de problemas en los equipos, condiciones ambientales o roturas en las conducciones de fluidos de la planta. Estas desviaciones hacen necesaria la implantación de medidas adecuadas en el diseño de la instalación que pretendan garantizar la operación segura de la misma limitando la ocurrencia de daños a las personas, al patrimonio o al medio ambiente. Esto requiere en primer lugar un profundo estudio de los procesos fisicoquímicos que ocurren en la instalación en el curso de la operación normal y de las desviaciones de esa operación normal.

La capacidad de respuesta ante fallos se implanta estableciendo sucesivas barreras para el confinamiento de los productos radiactivos y asegurando la integridad de estas barreras, lo que se hace en tres niveles. En el primer nivel, se aborda la estabilidad de la operación, eligiendo los puntos de trabajo de la misma de tal manera que las desviaciones respecto de la operación estacionaria tiendan a autocontrolarse. En segundo lugar, se disponen sistemas de control de la operación que devuelven los parámetros de la planta a valores controlados y sistemas de protección para detener la operación de la planta ante desviaciones más acusadas. También se instalan sistemas de accionamiento automático, considerados como salvaguardias, activadas mediante el sistema de protección, que mitigan las consecuencias de los accidentes. En tercer lugar, el personal que opera la central, además de su formación específica, dispone de procedimientos detallados para la realización de sus tareas. Estos procedimientos contemplan tanto la operación normal de la planta como la gestión de los accidentes que pudieran producirse. Se desarrollan estos tres conceptos en las secciones que siguen.

3.2.1. Seguridad intrínseca.

El primer nivel corresponde al diseño de la instalación para que su régimen de trabajo se sitúe en regiones donde los procesos físicos presenten características intrínsecamente estables, de forma que la evolución del sistema tienda a auto-amortiguar las desviaciones respecto de los puntos de equilibrio de funcionamiento. Se presenta a continuación un ejemplo ilustrativo.

En el apéndice A del 10CFR50 se establecen los criterios generales que deben regir el diseño de instalaciones nucleares para la producción de potencia. Son criterios muy generales que pretenden ser una referencia de alto nivel para garantizar la seguridad de las instalaciones a lo largo de su vida. La naturaleza general de estos principios surge de la necesidad de regular los muy distintos diseños posibles de centrales nucleares, por lo que no se hace referencia a diseños concretos.

En la segunda sección de los criterios generales de diseño (apéndice A del 10CFR50; ref. [1]), titulada *Protección por barreras múltiples*, el criterio general de diseño número 11 requiere que el diseño del núcleo del reactor y los sistemas de refrigeración asociados sea tal que en el rango de operación a potencia el efecto de las características de realimentación intrínseca tienda a compensar un incremento rápido en la reactividad.

Éste es un criterio que persigue que, de producirse un aumento indeseado de reactividad, la evolución del sistema modifique las condiciones físicas de los materiales de manera que se limite ese aumento, deteniendo el aumento de reactividad y estabilizando así la potencia. Esto se consigue con un diseño de los parámetros nucleares del combustible que aseguren que el coeficiente global de reactividad (coeficiente de potencia) sea negativo. Un comportamiento opuesto a éste implicaría la inestabilidad del proceso físico, en el sentido de que un aumento de la potencia resultaría autoalimentado.

Las características intrínsecas de estabilidad del sistema físico que constituye la instalación, la protegen de los transitorios accidentales que se desarrollan en tiempos muy cortos, tales que no pueden diseñarse sistemas de protección que los controlen.

3.2.2. Seguridad mediante sistemas.

Los mecanismos intrínsecos no son en general suficientes para controlar la evolución de las posibles secuencias accidentales. Por ello, se instalan sistemas automáticos de protección que atajan la evolución del accidente y conducen la planta a una situación segura. Estos sistemas se diseñan de forma que su intervención sea conmensurada con la magnitud del accidente que protegen. Para ello, se agrupan y clasifican las posibles secuencias accidentales en función de su frecuencia esperada; la tabla 1 ilustra los grupos de frecuencias considerados en la normativa americana, que se aplican también en la regulación española, diseñándose protecciones para cada grupo. Dependiendo de la severidad del accidente, las acciones de protección pueden incluir medidas como el bloqueo de determinadas acciones manuales o

automáticas, la parada automática del reactor o la activación de sistemas de salvaguardias tecnológicas.

Aunque las protecciones se diseñan por grupos de transitorios, en cada grupo se da crédito a las protecciones ya diseñadas para otros grupos. Los transitorios estudiados en cada grupo de frecuencias se han elegido de manera que cubran todas las situaciones que pueden ocurrir con esa frecuencia esperada. Con ello se asegura que ningún transitorio que pueda ocurrir superará los límites de daño especificados para cada grupo. Este objetivo hace necesaria la consideración de condiciones iniciales y de contorno que abarquen las condiciones creíbles de la planta y que sean las más penalizantes en términos del posible daño producido. Además, se imponen condiciones penalizantes en cuanto a la configuración de la planta, por ejemplo en cuanto a distribución de potencia o momento de la vida del núcleo. De esta manera, al limitar el daño máximo en esos transitorios se está limitando el daño de un gran número de posibles transitorios, garantizando que puede mantenerse la seguridad de la planta en todos ellos.

La simulación y el análisis de esos accidentes permiten diseñar la actuación de las distintas protecciones. El límite del daño impone criterios tanto para la intensidad de la protección como para el tiempo esperado de respuesta en la mitigación del accidente. En cuanto a la primera, se debe garantizar que la protección es capaz de controlar el accidente, conduciendo a la planta a una condición segura o, al menos, a una condición en la que los operadores sean capaces de tomar medidas adicionales que detengan la evolución del accidente. En cuanto al tiempo de respuesta, el estudio detallado de los transitorios proporciona los puntos de tarado que activan las protecciones para que la mitigación sea efectiva, permitiendo a la vez una banda de maniobra para acomodar las fluctuaciones normales de la operación sin que ocurra una actuación. El punto de tarado se calcula teniendo en cuenta los retrasos en las señales de actuación y las inercias mecánicas y termohidráulicas del sistema de protección. Además, una vez diseñada una protección, ésta pasa a formar parte de la instalación, por lo que deben contemplarse posibles incidencias en su actuación y se modifican las secuencias accidentales inicialmente previstas. Esto permite considerar, entre otras cosas, el efecto de la actuación indeseada de una protección, que puede alterar de manera notable el comportamiento de la instalación.

El diseño de las protecciones automáticas sigue, por tanto, un esquema iterativo, en el que la nueva instalación, que incluye las protecciones ya diseñadas, pasa a ser el objeto de estudio, considerándose la evolución conjunta de todo el sistema.

Las protecciones automáticas se diseñan para controlar la evolución de los transitorios accidentales que ocurren en una escala de tiempos tal que los operadores no tendrían ocasión de analizar y tomar acciones oportunas. Un criterio común en los diseños americanos es que los sistemas automáticos deben ser capaces de mitigar los accidentes sin necesidad de intervención humana al menos durante los primeros 10 minutos. En el diseño alemán el sistema de limitación está diseñado para proporcionar un margen para la actuación de los operadores, que como mínimo es de 30 minutos.

El **capítulo XV del Estudio de Seguridad** de cada planta contiene las conclusiones de los análisis del diseño de las protecciones. Los límites que se imponen como condiciones iniciales y de contorno en los análisis pasan a formar parte de las **Especificaciones Técnicas de Funcionamiento** de la instalación.

3.2.3. Seguridad mediante procedimientos.

El correcto diseño de las protecciones automáticas puede no garantizar la seguridad de la instalación de forma total. Pueden ocurrir fallos múltiples, incluyendo fallos en los sistemas de protección o situaciones anormales que requieran maniobras de recuperación de la planta más complejas y que tengan que ser realizadas por los operadores. Además, como se ha visto, los sistemas automáticos se diseñan para controlar los posibles transitorios accidentales durante los primeros instantes; son los operadores los que deben llevar finalmente la planta a condición segura.

La complejidad de las operaciones que se llevan a cabo en una central nuclear, incluso para las operaciones normales, y la necesidad de garantizar que se lleven a cabo con una muy baja probabilidad de error ha llevado a implantar un sistema muy amplio de procedimientos. Todas las actividades de operación de sistemas, de calibración, pruebas y mantenimiento, de recuperación de fallos y de operación en emergencias se realizan siguiendo procedimientos detallados que guían al personal de la planta en estas actuaciones.

El accidente de Three Mile Island (TMI), ocurrido en 1979, puso de manifiesto entre otras cosas la necesidad de disponer de instrucciones detalladas para la recuperación de un transitorio accidental. Se rediseñaron entonces los Procedimientos de Operación en Emergencia (POE) existentes, de forma que fueran capaces de cubrir las situaciones accidentales posibles, apoyándose en la actuación de los sistemas automáticos de protección, pero teniendo en cuenta también sus posibles fallos y circunstancias agravantes del accidente. Los nuevos POEs se han diseñado en casi todos los países y tecnologías siguiendo el modelo americano post-TMI de **procedimientos basados en síntomas**. Esto significa que no es necesario hacer previamente un diagnóstico detallado del accidente para ejecutar las acciones previstas. Cuando es necesario hacer algún tipo de diagnóstico, éste está también guiado por el procedimiento en función de los síntomas observados. Los procedimientos guían a los operadores para realizar una recuperación óptima teniendo en cuenta las posibles situaciones operativas de la planta.

El análisis y optimización de los procedimientos de operación ha de hacerse con herramientas adicionales a las que se usan para el diseño de las protecciones automáticas. En concreto, los denominados Análisis Probabilistas de Seguridad (ver sección 4.2) son un marco adecuado para la verificación de los POE.

3.3. Principios para la reducción de la frecuencia del daño: Redundancia, Diversidad y Separación.

Puesto que los sistemas y características de seguridad pueden fallar también cuando son demandados, su efectividad depende de su fiabilidad, es decir, de la probabilidad de que actúen cuando son demandados y de que cumplan con su función durante el tiempo requerido. Por tanto, un elemento esencial para conseguir un nivel de seguridad adecuado es que la indisponibilidad de las protecciones, entendida como probabilidad de no realizar su función, sea lo suficientemente baja para garantizar el cumplimiento de los criterios de aceptación del daño en cada zona de la curva del riesgo.

Para desacoplar el proceso de diseño de un estudio detallado de la fiabilidad de los sistemas, que lo haría demasiado complicado, se aplican principios generales de diseño que aseguran la alta disponibilidad de las protecciones diseñadas.

Con el propósito de mantener ciertas características de fiabilidad del diseño (i.e., minimizar la frecuencia de los daños) los siguientes criterios y principios están recogidos en los criterios generales de diseño del apéndice A al 10CFR50:

- **Criterio de fallo único**, según el cual ninguna función de seguridad debe quedar impedida por un único fallo de un componente dentro del sistema, o por ninguna acción de mantenimiento ni acción humana sobre componentes del sistema.
- **Criterio de redundancia**, por el cual cada función de seguridad se debe asegurar con sistemas redundantes. Se puede considerar como una consecuencia del criterio anterior.
- **Criterio de diversidad** o redundancia funcional, que consiste en la utilización, en la medida de lo posible, de métodos independientes, basados en principios físicos diferentes, para lograr análogos resultados. La aplicación de este criterio minimiza la posibilidad de fallos en modo común.
- **Criterio de separación**, también tendente a minimizar los fallos en modo común, mediante la separación física adecuada entre componentes o subsistemas redundantes.
- **Criterio de fallo seguro**, por el cual y cuando sea factible, el fallo de cada componente del sistema (caso de producirse) debe llevar a dicho sistema al estado más seguro posible.

Estos principios garantizan por tanto que un fallo simple en un componente de un sistema, en las fuentes de energía que le proporcionan la fuerza motriz o en las conducciones que necesita para su actuación no impedirá esa actuación, de forma que serían necesarios fallos múltiples para que el sistema no cumpla su función. Adicionalmente, estos principios deben aplicarse tanto al diseño del propio sistema, como de las señales y equipos adicionales que se necesitan para su correcta actuación (p.e., sensores primarios que detectan la necesidad de actuación, canales de instrumentación y control, etc.).

3.3.1. Redundancia.

La garantía de fiabilidad de los sistemas ante fallos simples en los componentes necesarios para su actuación mejora si se instalan componentes redundantes en el sistema, es decir, varios componentes que son capaces cada uno de cumplir la función protectora. Como es bien sabido, la probabilidad de fallo simultáneo en dos o más componentes es menor que la de fallo de uno cualquiera de ellos.

El principio de redundancia se aplica instalando dos o más trenes con la capacidad protectora requerida al sistema. A cada uno de los trenes redundantes se le suele denominar *redundancia*. La actuación final de un sistema con trenes redundantes se decide según distintas estrategias. Por ejemplo, en sistemas de salvaguardia como la inyección de seguridad, entran en funcionamiento todos los subsistemas redundantes, aunque dicha actuación esté sobredimensionada. En cambio, en sistemas de decisión, los canales redundantes se combinan según distintos esquemas lógicos (1 de 2, 1 de 2 dos veces, 2 de 3, 2 de 4, etc.), que también tienden a evitar las actuaciones espurias de las protecciones.

3.3.2. Diversidad.

El diseño debe asegurar, cuando sea factible, que una misma función de seguridad se pueda conseguir mediante distintos métodos y/o principios de funcionamiento de equipos. Ello impediría que una misma causa de fallo pueda afectar a todos los equipos necesarios para la correcta ejecución de la función de seguridad.

El ejemplo más extendido es el de la diversidad de fuentes de energía, puesto que la actuación de un sistema de protección necesita de energía primaria, que debe ser suministrada por sistemas auxiliares. Para prevenir contra un fallo de las fuentes de energía, que impediría la función protectora, se diseñan sistemas de actuación diversos. Para prevenir contra un fallo en la alimentación eléctrica proveniente de la red exterior a la central (que constituye la fuente usual de energía de los sistemas de protección), se instalan generadores eléctricos movidos por motores diesel, que proporcionan la energía suficiente para accionar los sistemas críticos de la central. Además, pueden existir sistemas de accionamiento que no dependan de la alimentación eléctrica. Un ejemplo de ello es el accionamiento de bombas por medio de turbinas de vapor. Otros ejemplos de aplicación del concepto de diversidad son el control de reactividad mediante las barras de control y sistemas de control de boro (requerido por el criterio general de diseño número 26 del apéndice A al 10CFR50) o la utilización de métodos de medida de una cierta variable basados en principios físicos diferentes.

3.3.3. Separación.

Para garantizar la efectividad de la actuación de los sistemas de protección deben evitarse interacciones indeseadas entre sus partes constituyentes. Por

ejemplo, se debe evitar que el fallo en una de sus partes se propague a otras impidiendo la función protectora.

La utilización de trenes redundantes para asegurar la fiabilidad de un sistema exige que en el momento de actuar estén físicamente separados entre sí. Esta separación se consigue por ejemplo, en el caso de sistemas de aporte de refrigerante, independizando los tramos de tubería que constituyen cada uno de los trenes por medio de válvulas. La separación de trenes redundantes debe evitar también que una misma causa externa (por ejemplo fuego o inundación) pueda afectar simultáneamente a más de un tren del sistema.

4. Métodos de evaluación y análisis de seguridad.

Tal como se ha explicado, la seguridad de una instalación nuclear se fundamenta en el principio de defensa en profundidad, en forma de protección por barreras sucesivas para controlar los materiales radiactivos, y en forma de niveles múltiples de protección contra el daño a estas barreras. La evaluación de la seguridad de una instalación pretende por tanto demostrar dichas características y confirmar que su funcionamiento no origina riesgos indebidos, es decir, que su curva característica de riesgo no supera la curva límite de daños (figura 1) aplicable. El concepto, en su expresión más amplia, incluye la revisión y confirmación de que se satisfacen otros requisitos relevantes para la seguridad, entre ellos:

- requisitos generales (p.e., suficiente defensa en profundidad, consideración de la experiencia operativa y del estado del arte del conocimiento e investigación),
- requisitos a equipos de la planta (p.e., cualificación, consideración de efectos de envejecimiento y fiabilidad), y
- requisitos de diseño de sistemas (p.e., requisitos específicos del núcleo del reactor, sistema de refrigeración, contención y salvaguardias tecnológicas),

considerando además todos estos aspectos para cualquier fase de la vida de la instalación (selección de emplazamiento, diseño, construcción, operación y desmantelamiento).

El mayor problema de la evaluación y verificación de la seguridad es que no se puede hacer mediante medidas experimentales ya que no se trata de evaluar lo que ocurre sino lo que *podría ocurrir*. Por tanto es inevitable el recurso a técnicas analíticas.

La evaluación de la seguridad incluye como componentes esenciales (aunque no únicos) los denominados análisis de seguridad. Con éstos se analiza y confirma, mediante herramientas analíticas adecuadas (normalmente herramientas computacionales de cálculo), cómo se satisfacen los requisitos de seguridad (p.e., la integridad de las barreras) para sucesos tanto internos como externos a la instalación que pueden ocurrir en un amplio espectro de condiciones operativas. Esencial a los análisis de seguridad es por tanto la

comprobación y confirmación cuantitativa de que el riesgo asociado al funcionamiento en operación normal y en accidente es menor que el riesgo tolerable aceptado.

Ya se ha indicado que el concepto de riesgo tiene dos ingredientes esenciales (frecuencia y daño), y por tanto los dos deben ser considerados en los estudios de riesgo. De esta bi-dimensionalidad del concepto se deriva el planteamiento de dos tipos de métodos de evaluación y análisis de seguridad complementarios (y necesarios), según el énfasis y detalle que se hace en la consideración y cuantificación de cada una de estas componentes. Son los denominados métodos de **análisis de transitorios** (también conocido como método determinista) y de **análisis probabilista de seguridad** (APS, o análisis del riesgo residual).

Además de diferencias en los planteamientos y técnicas, cada uno de ellos debe introducir sus propios criterios de aceptación, que normalmente reflejan los criterios utilizados por los diseñadores, consistentes con los requisitos impuestos por la regulación.

4.1. Análisis de transitorios base de diseño.

En esta metodología, cuyos resultados para las centrales nucleares en el modelo regulador americano se recogen en el capítulo XV de los Estudios de Seguridad, se selecciona un conjunto de **sucesos base de diseño** (DBE, Design Basis Events) agrupados en clases (condiciones) según su severidad y su frecuencia¹ (ver tabla 1). Estos DBE son sucesos en los que se someten las protecciones a las condiciones más difíciles de satisfacer y toman su nombre del hecho de que son usados para diseñar las capacidades y criterios de actuación de las protecciones, incluyendo la contención y los sistemas automáticos de protección.

Los criterios de aceptación están definidos de manera explícita tal como se muestra en la tabla 1. Además, se definen criterios de aceptación tanto en términos de integridad de barreras como en términos de daño radiológico lo cual es una expresión más del principio de defensa en profundidad.

Los criterios de daño radiológico constituyen una curva de límite de daño del tipo de la figura 1, aunque su aspecto no sería el de una curva continua sino el de una escalera ya que cada criterio es aplicable a todo un rango de frecuencias.

Los criterios de integridad de barreras se eligen de manera que no se pueda violar el límite de daño radiológico sin violar previamente el criterio de integridad de barreras correspondiente. Estos, a su vez, se suelen redefinir en términos de las denominadas **variables de seguridad**, tales como el DNBR (que mide la proximidad a condiciones termohidráulicas adversas en un PWR) o la temperatura de vaina.

¹ La consideración explícita de grupos de frecuencia demuestra que el análisis de transitorios no es puramente determinista.

Puesto que los sucesos base de diseño son los más limitantes dentro de su categoría, si en éstos no se sobrepasa el límite de riesgo, se puede asegurar que ningún otro transitorio real de dicha categoría, que se ajuste a las hipótesis del diseño, sobrepasaría tampoco dicho límite.

Categoría	Definición	Integridad barreras	Límite radiológico
Condición I	Operación normal y maniobras frecuentes.	No definidas explícitamente. Se suponen las mismas de condición II	No definidos explícitamente. Se suponen los mismos de condición II
Condición II	Incidentes, cualquiera de los cuales puede ocurrir durante un año natural en una planta dada.	Ninguna barrera a los productos radiactivos debe sufrir pérdida consecencial de su función.	10CFR20
Condición III	Incidentes, cualquiera de los cuales puede ocurrir durante el tiempo de vida de una planta dada.	Solo una pequeña fracción de elementos combustibles pueden resultar dañados. Las barreras del RCS y contención no deben sufrir pérdidas consecuenciales de su función.	Se pueden superar los límites de 10CFR20 pero sin limitar o interrumpir el uso público de áreas más allá del radio de exclusión.
Condición IV	Fallos no esperados pero que se postulan porque sus consecuencias potenciales incluirían la liberación de cantidades significativas de radiactividad.	Sin límite explícito para las vainas. No roturas consecuenciales significativas de la barrera de presión del RCS. No rotura consecencial de la contención.	10CFR100

Tabla 1. Intervalos de frecuencia y criterios de aceptación considerados en el análisis de transitorios accidentales.

Otra cuestión que se debe asegurar es la de la completitud del conjunto de DBEs, que debe representar una envolvente completa del conjunto de todos los posibles transitorios incluidos en el alcance del diseño. Normalmente, es la metodología de cada uno de los suministradores principales la que responde a esta cuestión, por lo que no hay un conjunto de DBEs único y universal, sino que éste es dependiente de los detalles metodológicos (normalmente cargados de sutilezas y de información restringida) de los fabricantes.

Dando por hecho que los anteriores criterios son satisfechos y que el conjunto de DBE es completo, la planta será segura únicamente si la fiabilidad de la protección es suficientemente alta. Este problema no se aborda explícitamente en el análisis de transitorios pero aquí juega un papel fundamental el criterio de fallo único comentado anteriormente. También contribuye a garantizar la fiabilidad el establecimiento de especificaciones técnicas sobre **requisitos de vigilancia** de los sistemas de protección.

En el análisis de los DBE se deben calcular con la adecuada precisión las variables de seguridad (y eventualmente las variables de daño de las que proceden). Si la selección de los DBE ha sido adecuada, los valores obtenidos formarán una envolvente de los valores que se obtendrían en cualquier transitorio real de la misma categoría. Esta envolvente de daño (o de su correspondiente variable de seguridad) puede ser calculada con modelos de simulación de mayor o menor detalle. El uso de modelos o hipótesis conservadoras para el cálculo de dicha envolvente de daño es una técnica habitual que, a cambio de simplificar los cálculos, añade márgenes extra respecto al comportamiento real de la planta y por tanto introduce requisitos más exigentes sobre la protección.

4.2. Análisis del riesgo residual.

El accidente de Three Mile Island, ocurrido en 1979, puso de manifiesto también que debido a que las plantas reales no se ajustaban en todos los casos a las hipótesis utilizadas en el diseño, algunos transitorios podían llevar a la planta **más allá de la envuelta de diseño**. Razones que podían llevar a dicha situación son:

- El suceso iniciador puede ocurrir a partir de unas condiciones iniciales no consideradas en la selección del conjunto de DBE.
- Pueden ocurrir varios sucesos iniciadores de manera simultánea o consecuentemente.
- La existencia de más de un fallo adicional al propio suceso iniciador, que hace que no funcionen correctamente las protecciones.
- La existencia de intervenciones humanas que hacen que la evolución del transitorio se aparte de las condiciones postuladas en el diseño.

Esto significa que, aunque se cuente con una protección correctamente diseñada, ésta puede no ser suficiente ya que hay una parte del riesgo que no está cubierta por ella. Podemos definir el riesgo residual como la frecuencia estimada de superación (frecuencia de excedencia) de los límites de seguridad que la protección automática trata de prevenir, contando con la existencia de dicha protección.

Los análisis probabilistas de seguridad (APS) se desarrollaron para ayudar a estimar la frecuencia de daño severo al núcleo, es decir, la frecuencia de excedencia de los límites de seguridad aplicables a los transitorios de condición IV. En este tipo de análisis no se garantiza el correcto funcionamiento de las funciones de protección sino que se cuantifica su indisponibilidad por fallo o por estar en mantenimiento, pruebas, etc. Las posibles evoluciones de esa

situación se determinan según la actuación de otras funciones de protección que intervendrían bien automática o manualmente como forma de recuperar el fallo de la protección previa. La nueva función de protección puede a su vez funcionar correctamente o fallar con una cierta probabilidad, con lo que el proceso continúa recurrentemente hasta que se pueda asegurar que se alcanza una situación estable y segura en la planta, o bien hasta que se llega a condiciones de daño severo al núcleo. El número de posibles combinaciones de condiciones iniciales, sucesos iniciadores, fallos o éxitos y tiempos de actuación de las funciones de protección es prácticamente infinito, por lo que también se hace necesaria una simplificación para llevar a cabo el análisis.

A tal objeto se definen **sucesos iniciadores** como las transiciones que sacan a la planta de su operación estable desde regiones determinadas de condiciones iniciales. Surge entonces el concepto de **secuencia** como el conjunto de transitorios desencadenados por un suceso iniciador, que partiendo desde una región de condiciones iniciales, presentan una historia similar de intervención de las protecciones. Todas las secuencias originadas por un mismo suceso iniciador, a partir de unas determinadas condiciones iniciales, y considerando las posibles actuaciones o fallos de las protecciones, forman lo que se denomina **árbol de sucesos**. Las funciones de protección que intervienen en las secuencias se denominan **cabeceros del árbol de sucesos**. En el estudio de su fiabilidad se tiene en cuenta no sólo la actuación de los componentes sino también la del personal de la planta, por lo que un ingrediente importante del APS es el estudio detallado de la fiabilidad humana, que no estaba presente en los análisis deterministas.

Una aportación esencial de los APS es la del cálculo de frecuencia con que puede ocurrir cada una de las secuencias del árbol de sucesos así delineado. Ello se traduce a su vez en dos tipos de elementos que deben ser calculados:

- la frecuencia de ocurrencia de cada uno de los sucesos iniciadores que se consideran (teniendo en cuenta que representa a un grupo de posibles sucesos iniciadores), y
- para cada uno de los sucesos iniciadores, la probabilidad de intervención efectiva (o la de fallo) de cada una de las protecciones que se demandan en las secuencias identificadas en la delineación del árbol de sucesos.

La probabilidad de fallo de cada una de las protecciones se calcula a partir de una estructura lógica, denominada **árbol de fallos** que relaciona dicho fallo con la indisponibilidad de los componentes del sistema. Tanto la frecuencia de los iniciadores como las probabilidades de fallo de los componentes son estimadas a partir de experiencia operativa previa en la industria nuclear y en la planta bajo estudio. El uso de árboles de fallo permite tener en cuenta las interacciones entre los sistemas debido a componentes comunes.

Así como en los análisis de transitorios no se calculaba con rigor la componente de frecuencia del riesgo, en los APS no se calcula con rigor el daño. Tan sólo se discute cualitativamente si se alcanzan condiciones de **daño severo en el núcleo**, considerando en caso contrario la **secuencia de éxito**. Por tanto el énfasis de los APS es la identificación de secuencias que originan el daño severo al núcleo y la frecuencia de excedencia de tal daño.

5. Aplicación a las instalaciones del ciclo de combustible.

Los análisis de seguridad de las instalaciones del ciclo de combustible añaden con respecto al caso de las centrales nucleares, la necesidad de considerar otros tipos de riesgos más propios de industrias convencionales no nucleares, p.e., explosiones, toxicidad química, etc.

En el caso de las fábricas de elementos combustibles, los documentos básicos adoptados en la aplicación de los principios fundamentales de seguridad nuclear son también las normas ANSI N18.2 ([2]) y ANSI N212 ([3]). A partir de éstas se desarrollan los criterios generales de seguridad, detallados a su vez en forma de criterios de diseño particulares de cada sistema, y se clasifican las diferentes estructuras, sistemas y equipos de por clases de seguridad y por categoría sísmica.

Estos criterios generales de seguridad incluyen una clasificación de las diferentes situaciones en que puede encontrarse la instalación en un momento dado durante su funcionamiento:

1. Las derivadas del proceso de fabricación del combustible, que pueden producirse durante el funcionamiento normal o en caso de accidente.
2. Las ocasionadas por fenómenos naturales (p.e., terremotos, inundaciones, huracanes, nieve, hielos, etc.).
3. Las derivadas de las condiciones ambientales de la zona (p.e., meteorológicas, geológicas, ecológicas, de disponibilidad de agua, etc.).
4. Las derivadas del uso de la tierra (distribución de la población, tipos de trabajo, recreo, transporte, etc.).
5. Las motivadas por la combinación de condiciones de proceso con fenómenos naturales.

En la tabla 2 se recogen ejemplos de situaciones según la clasificación anterior, asignando también a cada uno de ellos la condición correspondiente, debiéndose evaluar, como en el caso de las centrales nucleares, los efectos originados para cada una de ellas.

Estas situaciones se estructuran a su vez en orden creciente de severidad también en cuatro niveles (similares a los correspondientes para centrales nucleares; ver tabla 2), a los que se les asocia también criterios de aceptación utilizados en la valoración de los efectos que podrían producirse:

- **Condición I: Operación normal**, que incluye aquellos incidentes que tienen mayor probabilidad de suceder durante la vida de la instalación. Los efectos sobre el medio ambiente próximo, caso de existir, no excederían la décima parte de los valores máximos anuales debidos a las descargas de efluentes en operación normal.

CONDICIONES ESTUDIADAS	CONDICIÓN DE DISEÑO
1. CONDICIONES DE PROCESO	
1.1. Funcionamiento normal	I
1.2. Accidentes:	
Derrame de polvo de UO ₂	I
Pérdida de suministro de agua	I
Pérdida de suministro de electricidad	I
Fallo del Sistema de Ventilación y Aire Acondicionado	I
Fuga de una laguna	I
Rotura de una barra de combustible	I
Derrame de residuos radiactivos sólidos y líquidos	I
Explosión o fuego localizado	
Fallo de un filtro HEPA	I
Fallo total de una laguna	I
Explosión de un horno de sinterizado	
Fallo total de un contenedor de UO ₂	I
Accidente de criticidad	III/IV
2. FENÓMENOS NATURALES	
2.1. Sismo base de diseño (SBD)	IV
2.2. Máxima inundación previsible	III
2.3. Huracanes	II
2.4. Nieve y hielos	II
3. CONDICIONES AMBIENTALES	I
4. USO DE LA TIERRA	I
5. COMBINACIÓN DE LAS CONDICIONES DE PROCESO CON FENÓMENOS NATURALES (sólo se estudia la combinación del SBD con condiciones normales de funcionamiento y condiciones accidentales)	
SBD: Funcionamiento normal	IV
SBD: Accidente de criticidad	IV

Tabla 2: Clasificación de las condiciones de diseño.

- **Condición II: Incidentes de frecuencia moderada**, que incluye aquellos accidentes que es improbable que sucedan durante la vida de la instalación, pero que de ocurrir podrían dar lugar a la emisión de materiales radiactivos al medio ambiente próximo, que podrían superar las cantidades liberadas diariamente en operación normal no superando los límites máximos anuales. También se consideran aquellos accidentes que sin superar estos niveles pueden tener graves consecuencias, no necesariamente radiológicas, sobre la instalación.
- **Condición III: Incidentes infrecuentes**. Incidentes que se espera no ocurran durante la vida de la instalación y caso de ocurrir darían lugar a emisiones radiactivas, que producirían dosis probablemente inferiores a 5 mSv (500 mrem) a todo el cuerpo para una persona situada en los límites del emplazamiento.
- **Condición IV: Accidente base de diseño**. Accidentes que no se espera que se produzcan durante la vida de la instalación, pero que se toman en consideración porque sus consecuencias podrían incluir un riesgo potencial de liberación de cantidades significativas de material radiactivo. Las emisiones derivadas no producirían daños que excedan los límites fijados por el 10CFR100.

Las estructuras, componentes y sistemas de la instalación del ciclo se clasifican, de acuerdo con la importancia de su función para la seguridad nuclear de la planta, en

- **Clase A o de seguridad nuclear**, aplicada a aquellas estructuras, componentes y sistemas, cuyo fallo podría producir una condición III ó IV.
- **Clase B o de diseño convencional**, aplicable a aquellas estructuras, componentes y sistemas, cuyo fallo produciría una condición I ó II, y a los que no tienen asignada ninguna función relacionada con la seguridad nuclear de la instalación.

En el diseño, construcción y operación de la instalación se debe considerar la posibilidad de emisión y dispersión de materiales radiactivos, como consecuencia de los efectos que producirían los fenómenos naturales, en especial los terremotos. Para asegurar un alto grado de confinamiento, se adopta también el principio de protección por barreras:

- Diseño, construcción y mantenimiento adecuado de edificios (barrera final de confinamiento).
- Diseño, construcción y mantenimiento idóneo, de las barreras de confinamiento primarias (cabinas de mezcla, manipulación y máquinas, contenedores de almacenamiento, etc.) cuyo fallo podría liberar cantidades apreciables de uranio en el interior de los edificios.
- Diseño, instalación y mantenimiento de los sistemas previstos para proteger o vigilar la integridad de las barreras anteriores, o para mitigar las consecuencias de un accidente.

De acuerdo a ello, se elabora la siguiente clasificación de diseño sísmico:

- Categoría sísmica I, aplicable a la estructura de la barrera final de confinamiento (edificios), cuya función es esencial para asegurar el confinamiento del material radiactivo, la cual se ha diseñado y construido para resistir los efectos del sismo base de diseño, manteniendo las funciones de seguridad asignadas. También se aplica a las perchas de sujeción de los elementos de los almacenes de elementos combustibles PWR y BWR. Las estructuras y componentes de categoría sísmica I justificarán su integridad estructural para una carga sísmica estática equivalente de valor 0.15 g en dirección horizontal.
- Categoría sísmica II, aplicable para las demás estructuras, sistemas y componentes de la instalación del ciclo. El diseño de estas instalaciones se realiza de acuerdo con los requisitos convencionales que se consideren de aplicación.

5.1. Análisis Integrado de Seguridad (ISA).

El denominado Análisis Integrado de Seguridad (ISA) (ref. [8]) propuesto por la USNRC específicamente para las instalaciones del ciclo (fundamentalmente fábricas de combustible)², es una metodología de revisión sistemática de todos los procesos, equipos, estructuras, actividades y personal de la instalación para asegurar que todos los riesgos relevantes que pueden resultar en consecuencias inaceptables han sido adecuadamente evaluadas y se han identificado medidas protectoras adecuadas.

Aunque las técnicas de ISA se establecieron inicialmente como herramientas de análisis de riesgos en plantas químicas (p.e., con materiales tóxicos y/o explosivos), donde se les conoce como Análisis de Riesgo de Procesos (PHA), pueden ser extendidas con facilidad al tratamiento de riesgos radiológicos o de criticidad nuclear.

El 10 CFR 70 ([9]) define los análisis tipo ISA como un

"... análisis sistemático que identifica los riesgos internos y externos de la instalación y los posibles iniciadores, secuencias de accidentes, frecuencia de ocurrencia y consecuencias, y cualquier otro aspecto relacionado con la seguridad. El término *Integrado* se debe referir a la consideración conjunta de todo tipo de riesgos relevantes de la instalación, sean radiológicos, de criticidad nuclear, químicos o de incendios, así como de la protección asociada a cada uno de éstos."

De manera general, cada ISA debe suministrar:

- Descripción de las estructuras, equipos, actividades y procesos de la instalación.
- Identificación y análisis sistemático de los riesgos existentes en la instalación.

²

Pese a su idéntica denominación, el Análisis Integrado de Seguridad descrito aquí no se refiere a la consideración conjunta de métodos y técnicas de análisis de transitorios y de APS, sino a la consideración conjunta de cualquier tipo de daño, sea específico nuclear (p.e., radiológico, criticidad) o convencional (p.e., explosiones, toxicidad).

- Identificación completa de accidentes y secuencias de sucesos que podrían resultar en consecuencias inaceptables, así como la frecuencia esperada en la ocurrencia de estas secuencias.
- Identificación y descripción de controles (i.e., estructuras, sistemas, equipos y componentes) que están relacionados con prevención de posibles accidentes o en la mitigación de sus consecuencias.
- Identificación de las medidas llevadas a cabo para asegurar la disponibilidad y fiabilidad de los sistemas de seguridad identificados.

Como consecuencias inaceptables a considerar en este tipo de instalaciones hay que incluir las que dan origen a una exposición a niveles excesivos de radiación de los trabajadores o personas del público por una liberación o, por una criticidad inadvertida, pero también a niveles altos en la concentración de ciertos productos químicos que dar origen a toxicidad y/o a explosiones. Normalmente las liberaciones de productos químicos consideradas en la evaluación de seguridad de estas instalaciones, y por tanto dentro del ámbito de competencias del organismo regulador, se refieren tan solo a aquellas originadas por la manipulación o procesamiento del material nuclear o que tenga impacto sobre la protección radiológica. Otro tipo de liberaciones serían competencia de otras instancias de la administración.

En general, los análisis de ISA se plantean en términos de aproximaciones inductivas o deductivas. Mediante planteamientos inductivos (de abajo a arriba, bottom-up) se intenta identificar posibles secuencias accidentales examinando en detalle las posibles desviaciones de las condiciones de operación normal. A excepción del método de árboles de sucesos (usado en los APS de las CC NN), la mayor parte de estos métodos resultan más adecuados para el análisis de sucesos con un fallo simple (p.e., aquellos sucesos originados por el fallo de un único sistema).

Por contra, los planteamientos deductivos (de arriba a abajo, top-down) resultan más adecuados para la identificación de combinaciones de fallos de equipos o de errores humanos, que desencadenan un accidente particular (i.e., fallo múltiple). Normalmente estos métodos identifican de manera precisa un denominado *top-event* (p.e., la consecuencia no deseada a que lleva el riesgo que se analiza), e identifican las diferentes vías de que éste ocurra (incluyendo fallos simples y múltiples). En los APS, esta metodología se implanta con los árboles de fallos.

Por tanto, los planteamientos inductivos permitirían identificar el espectro más amplio de posibles accidentes, mientras que con los métodos deductivos se obtendrían las posibles causas por las cuales un accidente podría ocurrir (i.e., las combinaciones de fallos y causa raíz por las cuales se podría originar un determinado accidente). Por ello, una implantación más eficaz de un ISA sería el resultado de la combinación de técnicas de ambos tipos, aprovechando las buenas capacidades de los métodos inductivos para la identificación del espectro accidentes más amplio posible, y las buenas características de los métodos deductivos (p.e., árboles de fallo cualitativos) para el estudio de detalle de los más significativos (u otros que se postulen). Por ejemplo, el método inductivo HAZOP (*HAZard and OPerability Studies*) permite determinar si existe

la posibilidad de que ocurra una explosión que pueda originar una liberación radiológica y posterior exposición al público, y con un árbol de fallos se determinarían las combinaciones de fallos que pueden originar dicha explosión, y como consecuencia los medios de control que se pueden plantear para prevenirla o mitigar sus consecuencias.

Otro tipo de resultados de un ISA es la identificación de mecanismos de control, técnicos y/o administrativos, que son necesarios para limitar o prevenir accidentes o para mitigar sus efectos. La mera identificación, sin embargo, no es condición suficiente que garantice niveles adecuados de seguridad, puesto que se requieren además mecanismos eficaces mediante los cuales estos controles se activen y operen adecuadamente cuando sean necesarios, denominados de *gestión de la seguridad* entre los que se deben incluir:

- Procedimientos (desarrollo, revisión, aprobación e implantación);
- Entrenamiento y cualificación;
- Mantenimiento, calibración y vigilancia;
- Gestión de cambios de diseño;
- Garantía de calidad;
- Procesos de auditoría (internas y externas);
- Análisis de experiencia operativa;
- Registro documental.

La USNRC plantea ([8]) la aplicación y/o extensión de técnicas y métodos posibles para la realización de un ISA tomados de la industria química (p.e., [10]), mencionando como posibles los siguientes:

1. Revisión de seguridad
2. Análisis por listas de chequeo
3. Priorización y clasificación relativa
4. Análisis preliminar de riesgos
5. Análisis *What-If*
6. Análisis *What-If* con lista de chequeos
7. Análisis de operabilidad y riesgos (HAZOP)
8. Análisis de modos de fallo y efectos (FMEA)
9. Árboles de fallos
10. Árboles de sucesos
11. Análisis de causa-efecto
12. Análisis de fiabilidad humana

Los primeros cinco tipos (Revisión de seguridad, listas de chequeo, priorización y clasificación relativa, análisis preliminar de riesgos y *What-If*) se demuestran útiles para la identificación amplia de riesgos y accidentes, resultando los tres

siguientes (What-If con lista de chequeos, HAZOP y FMEA) más adecuados para la identificación de secuencias accidentales, y los últimos cuatro métodos (árboles de fallos, árboles de sucesos, análisis causa-efecto, y fiabilidad humana) para el análisis en profundidad de accidentes específicos previamente identificados mediante otros tipo de métodos.

Los métodos reseñados son esencialmente cualitativos, dado que permiten determinar características importantes que permitirían plantear reducciones de los riesgos sin necesidad de determinar ninguna estimación cuantitativa del mismo.

Además de estas técnicas y métodos mencionados, se plantea también la conveniencia de aplicar otras técnicas desarrolladas en otros ámbitos alejados de la industria química o nuclear. Ejemplos de ello son el MORT (Management Oversight and Risk Tree) empleado en el estudio del impacto de aspectos organizativos de los análisis de incidentes, o las técnicas de grafos dirigidos.

6. Referencias.

- [1] Code of Federal Regulation Title 10 (NRC Regulations) Part 50 (10CFR50). Domestic Licensing of Production and Utilization Facilities
- [2] American National Standards Institute. Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants. ANSI N-18.2-1973.
- [3] American National Standards Institute. Nuclear Safety Criteria for the Design of Stationary Boiling Water Reactor Plants. ANSI N-212, 1974.
- [4] USNRC. Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants (NUREG-0800), Chapter 15.1.1 - 15.1.4, Draft Revision 2, April 1996.
- [5] American Nuclear Society. American National Standard Criteria for Technical Specifications for Nuclear Power Stations. ANSI/ANS-58.4-1979.
- [6] The American Nuclear Society, The Institute of Electrical, and Electronics Engineers. PRA Procedures Guide. Technical Report NUREG/CR-2300, US NRC, 1983.
- [7] OIEA, Basic Principle for Nuclear Plants, IAEA-INSAG-12, Vienna (December 1999).
- [8] Integrated Safety Analysis Guidance Document, Technical Report NUREG-1513, US NRC, May 2001.
- [9] U.S. Nuclear Regulatory Commission, 10 CFR 70, Domestic Licensing of Special Nuclear Material; Possession of a Critical Mass of Special Nuclear Material, Federal Register Vol. 65, No. 181, page 56211, September 18, 2000.
- [10] Centre for Chemical Process Safety, AIChE, Guidelines for Hazard Evaluation Procedures. Second Edition with Worked Examples, New York, 1992.

Relación con otros temas

- C-2** Riesgo y Seguridad Nuclear. Principios de mitigación del daño: Seguridad intrínseca, mediante sistemas y mediante procedimientos. Principios de reducción de la frecuencia del daño: Redundancia, Diversidad y Separación. Métodos de evaluación y análisis.
- C-8** Importancia del análisis de transitorios en el proceso de licenciamiento de reactores de agua ligera. Clasificación de sucesos. Concepto de suceso base de diseño.
- C-9** Evaluación de seguridad de instalaciones nucleares. Régimen de autorizaciones. Documentación.
- C-11** Sistemas de salvaguardia en centrales nucleares.
- C-14** Análisis probabilista de seguridad.
- SN-1** La Seguridad Nuclear. Fundamentos. Métodos de análisis. Aplicación a centrales nucleares e instalaciones del ciclo de combustible.
- SN-2** Criterios básicos de diseño aplicables a centrales nucleares. Normas, comparación entre ellas.
- SN-3** La seguridad mediante sistemas. Sistemas de salvaguardia en centrales nucleares.
- SN-5** El sistema de refrigeración del reactor en centrales nucleares de agua ligera. Análisis de seguridad.
- SN-6** Sistemas de refrigeración de emergencia en centrales nucleares de agua ligera.
- SN-9** El sistema de protección del reactor en centrales nucleares.
- SN-13** Análisis de transitorios en reactores de agua ligera.
- SN-14** Ejemplos significativos de accidentes base de diseño: Accidentes con pérdida de refrigerante. Accidentes con inserción de reactividad en el núcleo.
- SN-15** Accidentes fuera de la base de diseño: Transitorios previstos sin parada rápida. Pérdida total de corriente alterna.
- SN-16** Procedimientos de operación normal y de emergencia en centrales nucleares. Criterios de elaboración.
- SN-17** Guías de gestión de accidentes severos.