EVOLUCIÓN DEL PRINCIPIO DE DEFENSA EN PROFUNDIDAD Y SU INTERNALIZACIÓN EN EL DISEÑO DEL CAREM-25

Giménez M., Zanocco P., Quiroga D.
Departamento de Seguridad Nuclear, Gerencia de Ingeniería Nuclear, CNEA, Bariloche
gimenez@cab.cnea.gov.ar; zanoccop@cab.cnea.gov.ar; quirogad@cab.cnea.gov.ar

Resumen

En este trabajo se discutirán avances en cuanto a nuevas propuestas sobre el alcance de cada nivel de Defensa en Profundidad, basándose en particular en las propuestas realizadas al respecto por WENRA (Western European Nuclear Regulators Association, 2013) [1] y por IAEA (TECDOC-1791, 2016) [2]. Esta nueva aproximación es la que ha tomado CAREM-25 para dar un encuadre a los distintos sistemas importantes para la seguridad como parte de estrategias de mitigación de eventos, y es la base para el desarrollo de criterios de Clasificación de Seguridad de estructuras, sistemas y componentes.

EVOLUTION OF THE DEFENSE IN DEPTH PRINCIPLE AND ITS INTERNALIZATION IN CAREM-25 DESIGN

Abstract

This paper will discuss progress in terms of new proposals on the scope of each level of defense in depth, based in particular on the proposals made in this regard by WENRA (Western European Nuclear Regulators Association, 2013) [1] and IAEA (TECDOC-1791, 2016) [2]. This new approach is the one that has taken CAREM-25 to give a frame to different systems important for safety as part of mitigation strategies of events, and is the basis for the development of criteria for the safety classification of structures, systems and components.

1. Introducción

El Principio de Defensa en Profundidad (DenP) establece una serie de medidas consecutivas, encuadradas en la prevención y detección temprana de desviaciones o fallas de sistemas para reducir la probabilidad ocurrencia de fallos, y en el control y la mitigación de las consecuencias de los mismos si falla la prevención. Esta serie de medidas se concretan mediante múltiples barreras físicas y niveles de protección, teniendo como objetivo cumplir las Funciones Fundamentales de Seguridad en el reactor y pileta de Elementos combustibles: control de la reactividad, remoción del calor y el confinamiento y/o la limitación de liberación accidentales del material radioactivo.

Las barreras físicas, cuyo objetivo es confinar los productos de fisión, son intrínsecas a la tecnología adoptada, como ser el combustible -material cerámico-, la vaina que lo contiene, la envuelta de presión y la contención. La integridad de estas barreras, se deberá lograr mediante una adecuada protección al establecer amplios márgenes de seguridad tanto en operación normal como ante los eventos postulados.

Con respecto a los niveles de protección, la prevención (Nivel 1) es la primera prioridad seguida de acciones de control de eventos (Niveles 2 y 3) y de mitigación (Niveles 4 y 5) tendientes a proveer protección adicional al público. Cada uno de estos niveles, independientes entre sí tanto como sea razonablemente posible, comprenden soluciones tecnológicas que se aplican utilizando combinación de soluciones relativas a la seguridad intrínseca y uso de sistemas activos y/o pasivos.

2. Nueva aproximación a DenP para nuevos pantas nucleares

La manera básica de que una planta se diseñada y operada de manera de prevenir accidentes y mitigar sus consecuencias es la aplicación del concepto de DenP. Este concepto o principio debe ser aplicado a todas las actividades relacionadas con la seguridad, desde el, diseño lo organizacional hasta el comportamiento en cuanto a cultura de la seguridad, tanto para la planta operando a plena potencia como en todos los otros estados operativos. Con el objetivo de asegurar que todas las actividades relacionadas con la seguridad estén sujetas a capas o niveles independientes de provisiones, de manera tal que si una fallase, será compensada o corregida por otras medidas. La aplicación de DenP a través del diseño y la operación provee protección contra eventos operacionales previstos (EOP), eventos y accidentes severos, originados por fallas de sistemas o humanas dentro de la planta y contra las consecuencias de eventos que se originan fuera de ella.

Por lo tanto DenP es un concepto clave para establecer los objetivos de seguridad de las nuevas plantas nucleares. En particular para ampliar la clásica aproximación de accidentes base de diseño, restringida al nivel 3, incorporando requerimientos que extiende dicha base para incluir eventos de fallas múltiples y a la mitigación de accidentes severos postulados. Es decir, que se incluyan ciertas protecciones que son consideradas como “más allá de la base de diseño” de las centrales actuales. Esta serie de niveles de protección debe ser reforzada, buscando independencia entre ellos y aplicada a cada fuente significativa de material radioactivo.

2.1 Desarrollo histórico de DenP y nueva propuesta

El concepto de DenP fue introducido en el área de seguridad nuclear en los comienzos de los años 70. Este concepto fue gradualmente refinado para constituirse en una aproximación efectiva que combina la prevención de un rango amplio de eventos y la mitigación de accidentes y sus consecuencias. Éstos fueron postulados en la base de eventos iniciantes únicos seleccionados de acuerdo al orden de magnitud de su frecuencia estimada de la experiencia general de la industria.

La definición de diferentes niveles de DenP son fijados según una escalada de gravedad desde la operación normal hasta accidentes severos y acciones fuera de la central, de manera tal que si uno falla el siguiente nivel entra en acción. Puede ser que ciertos eventos surjan de una falla inicial y la falla de un nivel precedente o algunos directamente eventos directamente requieran por su gravedad la acción directa de un nivel superior dado. Este concepto apunta desde la prevención y el control de eventos hasta la mitigación a proveer medios robustos que aseguren el cumplimiento de cada una de las funciones fundamentales de seguridad:

1. Control de la reactividad en el reactor y pileta de elementos combustibles irradiados
2. Remoción del calor generado en el núcleo del reactor y en pileta de elementos combustibles irradiados
3. Confinamiento del material radiactivo y control de las emisiones radiactivos previstas, así como limitación de las liberaciones radiactivas accidentales

En sus comienzos el concepto incluía tres niveles, como se muestra en la siguiente tabla extraída del reporte WENRA (2013) [1]:

Levels of defence in depth	Objective	Essential means	Associated plant condition categories (for explanation - not part of original table)
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation	Normal operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features	Anticipated operational occurrences
Level 3	Control of accident within the design basis	Engineered safety features and accident procedures	Design basis accidents (postulated single initiating events)

Luego el concepto de DenP que aplica a los reactores operando en la actualidad fue ampliado para tomar en cuenta las denominadas condiciones de daño grave de la planta

que no fueran explícitamente abordadas originalmente y que surgieron de las lecciones aprendidas del desarrollo de la metodología del Análisis Probabilista de Seguridad y de los accidentes de las Tres millas (USA 1979) y de Chernobyl (República Ucraniana de URSS 1986). Éstas llevaron al agregado de dos niveles más (INSAG-10, 1996) [4], como se muestra en la figura siguiente extraída directamente del documento WENRA (2013) [1]

Levels of defence in depth	Objective	Essential means	Associated plant condition categories (for explanation - not part of original table)
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation	Normal operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features	Anticipated operational occurrences
Level 3	Control of accident within the design basis	Engineered safety features and accident procedures	Design basis accidents (postulated single initiating events)
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management	Multiple failures Severe accidents
Level 5	Mitigation of radiological consequences of significant releases of radioactive material	Off-site emergency response	

Como se desprende de un análisis de la tabla anterior, el nivel 3 estaba dedicado sólo a los denominados accidentes base de diseño, en tanto que el nivel 4 agrupaba a todos los eventos denominados “más allá de la base de diseño” o bien “condiciones extendidas del diseño (IAEA SSR-2/1, 2016) [3], incluyendo tanto a eventos de fallas múltiples como a accidentes severos.

Se considera, sin embargo que dichas definiciones no encuadran en el nuevo enfoque, dado por la evolución en conceptos de seguridad nuclear y en requerimientos al diseño de reactores avanzados. En efecto, sistemas de control de Eventos de Fallas Múltiples y de mitigación de accidentes severos ahora forman parte de la base de diseño de los reactores avanzados, entrando por lo tanto en colisión con el alcance clásico de los llamados eventos o accidentes base de diseño, restringidos al nivel 3. Considerando además que los objetivos

de los diferentes niveles de DenP están definidos como sucesivos escalones en la protección contra la escalada a situaciones accidentales se evalúa priorizar un agrupamiento en cada nivel por un objetivo común para el control y gestión de eventos. Dado que los sistemas diseñados para controlar eventos de fallas múltiples comparten el mismo objetivo que los denominados en INSAG 10 [4] como accidentes base de diseño, que es precisamente prevenir su escalada a condiciones de núcleo fundido, se considera que sean tratados en un mismo nivel de DenP. Por otro lado, los fenómenos involucrados en accidentes con fusión de núcleo/combustibles difieren radicalmente de aquellos en los cuales no hay fusión. Por lo tanto, se considera que los accidentes severos deben ser tratados en un nivel específico de DenP.

Así es que WENRA, ha propuesto dividir al nivel 3 en el subnivel 3.a para tratar eventos iniciantes postulados únicos (EIPU, ex accidentes base de diseño) y el 3.b para eventos postulados de fallas múltiples (EPFM) y reservar el nivel 4 exclusivamente para accidentes severos postulados. Conformándose así una nueva base de diseño o envolvente de diseño que incluye a todos estos eventos. Esta propuesta es a la que han adherido los autores de este documento y el Proyecto CAREM. En la tabla siguiente, extraída del reporte WENRA (2013) [1], se muestra tal propuesta.

Levels of DiD	Associated plant condition categories	Objective
Level 1	Normal operation	Prevention of abnormal operation and failures
Level 2	Anticipated operational occurrences	Control of abnormal operation and failures
Level 3	DiD Level 3.a Postulated single initiating events	Control of accident to limit radiological releases and prevent escalation to core melt conditions
	DiD Level 3.b Postulated multiple failure events	
Level 4	Postulated core melt accidents	Control of accidents with core melt to limit off-site releases
Level 5	-	Mitigation of radiological consequences of significant releases of radioactive material

23 October 2013 WENRA views on DiD for new reactors Western European WENRA RHWG Nuclear Regulators Association

De esta manera se considera que se refleja una adecuada evolución y racionalidad en cuanto a la evolución de concepto de DenP, considerando ahora tales eventos de fallas múltiples y accidentes severos dentro de la base de diseño de los nuevos reactores. Es por ellos que los denominados eventos más allá de la base de diseño en la generación actual de reactores no es la misma que para los nuevos reactores y que éstos sean incluidos desde comienzo del diseño.

Por otro lado se puede observar que se mantiene para nivel 2 la denominación de Eventos Operacionales Previstos (EOP), que se ha eliminado la denominación de Accidentes Base de Diseño (Nivel 3), y ha sido reemplazada por Eventos Iniciantes Postulados Únicos (EIPU) (N3.a), que se agrega la denominación de Eventos Postulados de Fallas Múltiples (EPFM) y que se reserva para el Nivel 4 los denominados Accidentes con fusión de núcleo postulados. Todos ellos ahora constituyen la nueva base de diseño o envolvente de diseño de los nuevos reactores.

Es importante agregar que para demostrar el cumplimiento de cada nivel de DenP, con el diseño propuesto de la planta, se establecen criterios de aceptación deterministas relacionados con límites a aplicar a parámetros relevantes de la seguridad y que se recomienda la aplicación de metodologías de evaluación conservativas para demostrar dicho cumplimiento para el Nivel 3.a y del tipo mejor estimación para los otros niveles.

Finalmente se quiere mencionar que en IAEA (TECDOC 1791, 2016) [2] se plantea, además de reflejar la propuesta de WENRA, dejar en el Nivel 3 solo los denominados accidentes severos y dividir el nivel 4 en dos, 4.a para EPFM y 4.b para accidentes severos postulados. Los autores entienden que esta última propuesta surge de evitar un cambio de terminología para el nivel 3 respecto de lo usando hasta la fecha, pero que confunde a la hora de entender qué es base de diseño, y mantiene la terminología de “base de diseño extendida” que también puede confundir dado que la base de diseño es única y no una “clásica” y otra “adicional”. Pero sobre todo comparte el hecho de que la compartimentación de niveles se tiene que hacer por objetivos comunes, tal como se describió anteriormente, y no por solamente mantener una tradición. Entendemos por lo tanto que la propuesta de WENRA refleja de una manera más clara la evolución de este principio ante los nuevos requerimientos de seguridad incremental.

2.2 Consideraciones sobre independencia entre los Niveles de DenP

Respecto de la independencia requerida entre las distintas estructuras, sistemas y componentes (ESCs) que se utilizan en cada nivel, las siguientes consideraciones generales deberán ser tenidas en cuenta:

1- ESCs que cumplen funciones de seguridad ante EIPU (Nivel 3.a) o ante EPFM (Nivel 3.b) deben ser independientes en la medida de lo razonablemente practicable de ESCs utilizadas en operación normal (Nivel 1) o ante EOP (Nivel 2). Esta independencia se plantea de manera tal que fallas de ESCs usadas en operación normal o ante EOP no impidan la función de seguridad requeridas ante EIPU o EPFM.

2- ESCs cumpliendo funciones ante EIPU, deben ser independientes dentro de lo razonablemente practicables de las ESCs usadas en caso de EPFM. Para los análisis de seguridad se puede dar crédito de aquellas ESC de otros niveles no afectadas por la falla múltiple considerada. Pero para EIPU no se puede dar crédito de aquellas asignadas para controlar EPFM.

3- ESCs específicamente diseñadas para cumplir funciones de seguridad en accidentes severos postulados (Nivel 4) deben ser independientes dentro de lo razonablemente practicable de las ESC asignadas a otros niveles de DenP.

Como casos ESC relevantes se pueden establecer las siguientes consideraciones:

a) sistema de suministro alterno de potencia de emergencia perteneciente al Nivel 3.a: se permite el uso en el Nivel 2. Pero un suministro diverso debe ser asignado al 3.b debido a fallas de causa común que puedan postularse.
b) Sistema de protección del reactor (SPR): deber ser adecuadamente independiente de otros sistemas de I&C y debe estar funcionalmente aislado de ellos. El SPR puede tener funciones en otros niveles distintos al 3, ya que el sistema de SCRAM puede ser actuado por el SPR para eventos específicos del Nivel 2. Un sistema diverso al SPR debe plantearse para el nivel 3.b en caso de postularse fallas de causa común del SPR. Sistemas de Limitación y control (no el SPR) usados para la actuación de sistemas del nivel 2 pueden estar combinados con I&C de operación normal
c) Contención: dadp que en cada nivel de DenP hay una necesidad de confinamiento como función de seguridad, se considera que dicha función puede ser cumplida por ejemplo por la contención en combinación con otras ESCs, así es que la contención es un ejemplo de una estructura que es usada en diferentes niveles y para la cual no es razonablemente practicable requerirle independencia para los distintos niveles

3. Conclusiones

En este trabajo se ha descripto el concepto de Defensa en Profundidad, su evolución histórica y nuevas propuestas como la planeada por WENRA (2013) [1] y la que refleja el TECDOC 1791 (2016) [2]. La propuesta de WENRA es la que los autores han preferido y es la que ha sido adoptada en el Proyecto CAREM, cuya forma de internalizarla en el diseño es descripta en otro trabajo en este congreso de la AATN.

4. Referencias

[1] WENRA Report: “Safety of new NPP designs” – Study by Reactor Harmonization Working Group, March 2013.
[2] IAEA TECDOC-1791: “Considerations on the Application of the IAEA Safety Requirements for the Design of Nuclear Power Plants” – Vienna, 2016.
[3] IAEA SSR-2/1 (Rev. 1): “Safety of Nuclear Power Plants: Design” – Specific Safety Requirements – Vienna, 2016.
[4] INSAG-10: “Defence in Depth in Nuclear Safety” – International Nuclear Safety Advisory Group, June 1996.