UTILIZACION DE LOS ESTADOS SOPORTES EN LOS ANALISIS PROBABILISTAS DE SEGURIDAD

J. COBIAN-N. J. LIPARULO

José COBIAN es Ingeniero Industrial, Master of Science and Doctor of Philosophy en Ingeniería Nuclear (Northwestern University, USA). Actualmente ocupa el puesto de Nuclear Safety Manager, en Westinghouse Sistemas Energéticos, España.

Nicholas J. LIPARULO es Bachelor and Master of Science en Ingeniería Química (Pittsburgh University). Actualmente ocupa el puesto de Risk Assessment Technology Manager, Nuclear Advanced Technology Division.

INTRODUCCION

La Nuclear Regulatory Commission describe en el NUREG/CR-2815 dos grandes metodologías para realizar estudios de análisis probabilistas de Seguridad, la de árboles pequeños de sucesos / árboles grandes de fallos, y la de árboles grandes de sucesos / árboles pequeños de fallos.

La metodología de Westinghouse es una variante de la segunda, en la que el análisis de los árboles de sucesos se realiza en dos etapas al objeto de simplificar su manejo.

En la metodología de Westinghouse, los sistemas soporte, sistemas de seguridad de primera línea y acciones del operador se incluyen directamente en los árboles de sucesos. Los sistemas de primera línea se cuantifican para cada conjunto de condiciones, que tienen un único efecto en la probabilidad de fallo de cada sistema. Para cada árbol de sucesos se determinan los "vectores de impacto", que describen el fallo del sistema de primera línea, debido a fallos de los sistemas soporte. Los árboles de fallo, utilizados para modelar los sistemas de primera línea son sencillos de manejar al no incluir en ellos las dependencias de sistemas soporte.

La sencillez de la lógica de los árboles de sucesos y el reducido tamaño de los árboles de fallo permite la estimación de la frecuencia de daño al núcleo en un tiempo mínimo, y con reducidos medios informáticos. El modelo, fácilmente modificable, permite ir reflejando los cambios que tengan lugar a lo largo de la vida de la central. Estos cambios se pueden introducir mediante herramientas gráficas interactivas, facilitándose en forma muy rápida la evaluación del impacto que tienen en la Seguridad de la Central, tal como ha podido constatarse en las numerosas aplicaciones realizadas con esta metodología.

SUCESOS INICIADORES

La identificación de sucesos iniciadores se realiza en tres etapas conducentes la primera a la identificación propiamente dicha de dichos sucesos, la segunda

a su categorización de acuerdo a la respuesta de la Central y de sus sistemas, y la tercera a la determinación de su frecuencia de ocurrencia.

La identificación y categorización se realiza mediante la conjunción de un proceso inductivo consistente en la elaboración de una lista de sucesos iniciadores basada en la experiencia existente aplicable a la central objeto del estudio, y otro proceso, deductivo, basado en el análisis lógico de los diferentes niveles de causas que originan daño al núcleo llegando hasta el nivel último de causalidad.

Los transitorios aplicables identificados en el proceso inductivo, se categorizan mediante el diagrama lógico deductivo para reducir el número de árboles de sucesos a desarrollar al mínimo necesario. Los transitorios se agrupan según las funciones de seguridad o respuesta de la central requeridas. Todos los sucesos iniciadores agrupados en una determinada categoría requieren las mismas funciones de seguridad (es decir, sistemas para mitigar el suceso), y producen respuestas similares en planta.

Las frecuencias de sucesos iniciadores se determinan mediante el análisis estadístico de la experiencia histórica de centrales del mismo tipo, información que se encuentra recogida en bases de datos. Cada suceso así definido da lugar a la construcción de un árbol de sucesos.

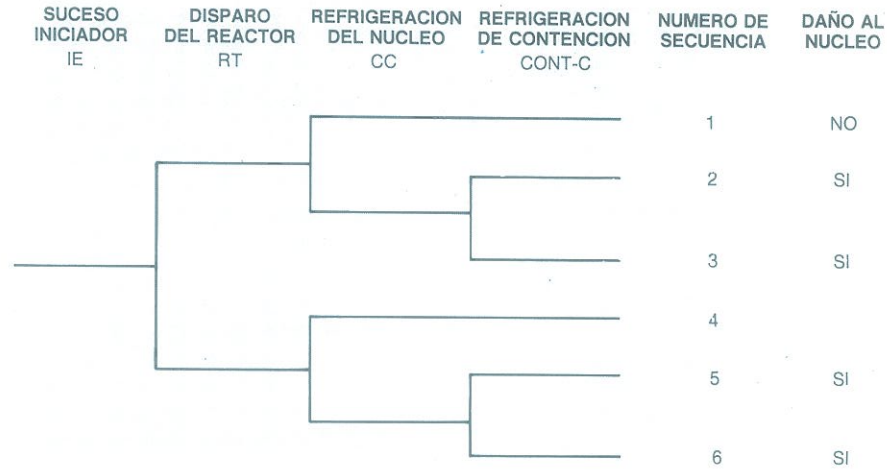
ARBOLES DE SUCESOS

Los árboles de sucesos son estructuras lógicas inductivas, que se desarrollan para determinar los resultados posibles que se derivan de un determinado suceso iniciador.

El primer paso en la construcción de un árbol de sucesos consiste en el desarrollo de estructuras funcionales de sucesos que ordenen e identifiquen las diversas funciones de seguridad que se precisan para cada un determinado suceso iniciador. Este tipo de estructuras se denominan "árboles de sucesos funcionales". Los cabeceros de este tipo de árbol de sucesos son funciones de seguridad que se utilizan posteriormente para determinar los sistemas de la central que deben llevar a cabo dicha función. Una vez que se hayan desarrollado estos modelos, las funciones de seguridad se traducen en sistemas reales específicos de la central.

En el árbol de sucesos se modelan en orden cronológico los sistemas identificados. Cada árbol de sucesos cubre todas las secuencias de accidente posibles que pueden derivarse del suceso iniciador.

En el proceso de construcción de árboles de sucesos se requiere el estudio



F I *Arbol de sucesos de LOCA de tamaño medio*

de las dependencias entre sistemas. Las dependencias pueden ser de los siguientes tipos: fallos de causa común, dependencia funcional, de equipos compartidos, de interacción física y de interacción humana. Los sucesos iniciadores de causa común, tal como la pérdida de la potencia exterior, requieren cabeceros independientes en el árbol de sucesos (por ejemplo recuperación de la potencia), y la modificación de criterios de éxito. Las dependencias funcionales, físicas y de interacción humana se reflejan en la estructura del árbol de sucesos. Por ejemplo, una dependencia funcional entre la inyección de alta presión y la recirculación puede originar el fallo de la recirculación, si la inyección ha fallado anteriormente. Las dependencias de equipo compartido (como el tanque de recarga) pueden incorporarse utilizando criterios de éxitos estrictos. Las dependencias entre sistemas de seguridad se identifican mediante revisión minuciosa de las secuencias de accidente.

Los árboles de sucesos así determinados se refinan por medio de la incorporación de los análisis que se describen a continuación. En la figura I se ilustra un árbol de sucesos para un LOCA de tamaño medio.

Dependiendo del tipo de acción y de la secuencia del accidente, la acción del operador bien se introduce directamente en el árbol de sucesos como un cabecero independiente o se incorpora indirectamente, por medio de su inclusión en el árbol de fallos de un sistema de primera línea. La acción del operador se acopla en el árbol de sucesos, cuando se requiere su actuación en la progresión de un accidente, modelándose todas las secuencias de accidente que surgen de dicha acción.

Una de las características de la metodología de Westinghouse es contemplar la posibilidad de fallos en cascada, es decir, aquellos fallos activos que pueden ocurrir durante la progresión de un accidente que podrían conducir a una situación de consecuencias más graves que las del suceso iniciador que los causó. La importancia de los fallos en cascada radica en la posibilidad que tienen para cambiar la respuesta de la planta y para requerir otros sistemas de primera línea diferentes. Un caso de fallos en cascada fue el accidente de Three Mile Island, donde un transitorio del agua de alimentación evolucionó en un pequeño LOCA. Los fallos en cascada se introducen en el modelo de árboles de sucesos como cabeceros adicionales de los mismos. En caso de un fallo en cascada, la secuencia se transfiere al árbol de sucesos asociado con dicho fallo.

CRITERIOS DE EXITO Y ESTADOS DE DAÑO

Una vez identificados los sistemas de primera línea específicos de la central, hay que definir los criterios de éxito para cada uno de ellos. Se utilizan entonces los criterios de éxito de sistemas para definir los sucesos no deseados para el análisis por árboles de fallos. Los análisis de árboles de fallos determinan las indisponibilidades de sistemas, que se utilizan directamente en la cuantificación de los árboles de sucesos. Se definen entonces, los criterios de éxito de sistemas para cada una de las secuencias de accidente y suceso iniciador. La definición de criterios de éxito para mantener el enfriamiento adecuado del núcleo, se basa en análisis neutrónicos y termohidráulicos de la respuesta de la central ante las condiciones postuladas del accidente. Tales análisis determinan los requisitos de caudal, bombas necesarias, necesidades y dependencias de sistemas o de equipos tales como refrigeración a los motores de

bombas. Estos criterios de éxito se basarán, siempre que sea posible, en análisis de "mejor estimación", en lugar de los análisis conservadores del informe de seguridad.

El definir los criterios de éxito es el paso más importante de los análisis de secuencias de accidente. La utilización de criterios de éxito realistas y documentables son las claves de un buen estudio de evaluación probabilista de seguridad.

Las secuencias de accidente que resultan en daño al núcleo se clasifican en grupos de estados de daño a la central. Cada estado de daño representa un conjunto de secuencias de accidente con características similares. Las secuencias de accidente se agrupan de acuerdo al tipo de accidente (LOCA/Transitorio), tiempo que tarda en producirse la fusión del núcleo (pronto/tarde) y estado de las salvaguardias de la contención (ventiladores/rociado).

ESTADOS SOPORTE

Se define un sistema soporte como un sistema del cual depende el correcto funcionamiento de los sistemas de primera línea o de otros sistemas soporte. En la metodología de Westinghouse, se modelan los sistemas soporte más importantes fuera de la estructura de los árboles de sucesos, con lo que se reduce el tamaño de los mismos, pudiéndose seguir con mayor claridad las secuencias del accidente.

La disponibilidad de sistemas de primera línea tales como inyección de seguridad o rociado de contención, dependen de determinados sistemas soporte como el sistema de eléctrico, agua de servicios o agua de refrigeración de componentes. El hecho de que los sistemas soporte puedan operar en modalidad de semi-fallo, crea un problema especial, pues si se tratan con un modelo de fallo binario (éxito/fallo), se obtendrán unos resultados conservadores y poco realistas.

El problema se soluciona identificando la combinación total o parcial, de los modos de fallo de los sistemas soporte y analizando los árboles de sucesos, para cada una de dichas combinaciones, reduciéndose así los árboles de sucesos a un tamaño manejable para su cuantificación.

El primer paso para la realización de este análisis consiste en la identificación de los sistemas soportes dominantes de la central. El segundo paso es la identificación de las dependencias existentes de los sistemas de primera línea y/o sistemas soporte con otros sistemas.

Como resultado de este análisis se identifican los "sistemas soporte dominantes" en la operación de la central. El sistema soporte dominante por excelencia es el sistema de suministro eléctrico, exterior e interior, de la central. Otros sistemas soporte dominantes importantes son el de actuación de salvaguardias, el de agua de servicios y el de agua de componentes. Estos se incluyen como cabeceros de los árboles de sucesos. El resto de los sistemas soporte pueden incorporarse bien en la fase de análisis de árboles de fallos o en la de árboles de sucesos. Seguidamente se determinan los estados de operación posibles para cada uno de ellos al objeto de integrarlos en un modelo específico de "estados soporte". Esto se realiza analizando cada sistema soporte e identificando los fallos principales en el sistema que pudieran limitar la operación del sistema.

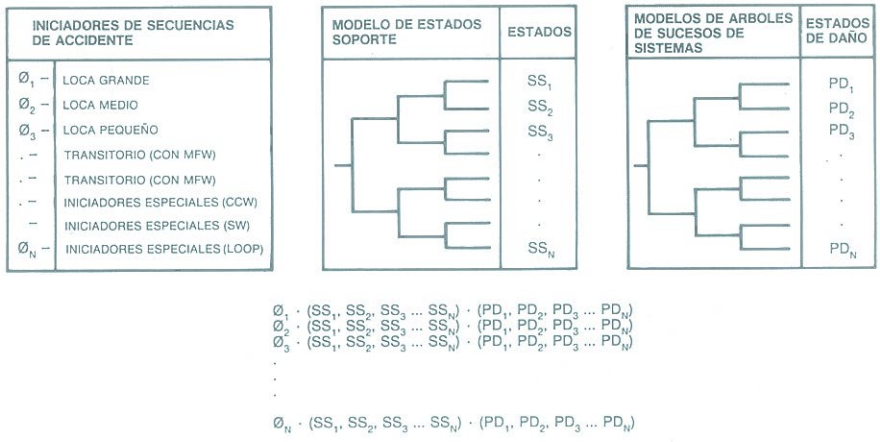
Cada sistema soporte dominante se considera como un sistema de primera línea (o cabecero) de un árbol de sucesos y los estados operativos asociados a ellos se interpretan como los posibles puntos de ramificación. Como primer sistema de primera línea se toma el sistema soporte eléctrico, como ya se dijo anteriormente. Si un sistema de actuación, tal como el sistema de actuación de salvaguardias, se incluye como un sistema soporte dominante, se colocan en segundo lugar en el árbol de sucesos. Los siguientes sistemas soporte que se modelan en el árbol de sucesos son los de refrigeración de fluidos de los equipos auxiliares de la central.

Una vez construido el modelo, se puede proceder a definir los "estados soporte" específicos. Al analizar en detalle los estados soporte específicos, es decir, las diferentes secuencias del árbol de estados soporte, se puede concluir que muchas de ellas son idénticas debido a las simetrías de la central. Además, muchas de las combinaciones que en un principio parecen únicas podrían, de hecho, tener unos efectos idénticos en los sistemas de primera línea de la central. Para determinar estos efectos y, en esta forma, conseguir reducir el número de combinaciones de estados operativos de sistemas de soporte, se procede al agrupamiento de combinaciones similares. Las combinaciones que quedan, una vez tenidas en cuenta las simetrías de la central y los efectos similares en sistemas de primera línea, definirán los estados soporte finales.

El modelo de estados soporte se cuantifica como cualquier modelo de árbol de sucesos. Para cada secuencia lógica del modelo se calcula la probabilidad de que los sistemas soporte de la central se encuentren en los estados operativos asociados a dicha secuencia. La probabilidad de la secuencia se calcula simplemente multiplicando las probabilidades de éxito o fallo de los correspondientes estados operativos de los sistemas soporte.

Una vez que las secuencias de accidente han sido modeladas, y las indisponibilidades de sistemas determinadas, las secuencias de accidente pueden ser cuantificadas. Antes de cuantificar las secuencias de accidente individuales, los sistemas de primera línea y los sistemas soporte se modelan y cuantifican utilizando técnicas de árboles de fallos. La frecuencia de cada secuencia de accidente es el producto de la frecuencia asociada al suceso iniciador, la probabilidad del estado soporte, y las probabilidades de éxito o fallo de los sistemas de primera línea modelados por el árbol de sucesos. En la figura II se representa el diagrama de flujo de la cuantificación de las secuencias de accidente.

La metodología de Westinghouse permite cuantificar las secuencias de accidente, identificar las secuencias dominantes, y la importancia de los sistemas con sencillos recursos informáticos.



F II *Diagrama de flujo de la cuantificación de una secuencia de accidente*

ARBOLES DE FALLOS

En el análisis mediante árboles de fallos, las causas que pueden provocar un funcionamiento insuficiente del sistema se organizan de forma deductiva.

Los fallos considerados comprenden: fallos aleatorios de componentes, indisponibilidades por pruebas y mantenimiento, errores humanos debidos a pruebas, mantenimiento y operación, fallos de interacción de sistemas y fallos de causa común. Se construyen árboles de fallos utilizando una simbología estándar de sucesos y puertas, y los sucesos básicos se identifican mediante la utilización de un sistema de codificación estándar.

Los árboles de fallo se desarrollan descendiendo hasta el nivel de fallos de componentes básicos por fallos aleatorios, parada de pruebas, mantenimiento y errores humanos. Los fallos de causa común se modelan cerca de la parte superior del árbol, debido a su efecto común sobre las partes redundantes del sistema.

El desarrollo de los árboles de fallos de componentes incluye, para componentes pasivos tales como válvulas de retención, únicamente el fallo mecánico a realizar la función requerida. Para componentes activos tales como bombas o válvulas motorizadas que hayan de cambiar de posición, el árbol de fallos muestra fallos independientes para los fallos mecánicos de circuitos eléctricos locales, de control, de enclavamiento, y de la parte local del sistema de actuación de salvaguardias u otras señales de actuación automática.

La cuantificación de los árboles de fallos de sistemas de primera línea y sistemas soporte requiere la estimación de la indisponibilidad debida a fallos de componentes, paradas de pruebas y mantenimiento, errores humanos y fallos de causa común.

Los árboles de fallos se cuantifican para diferentes estados soporte. La indisponibilidad de estos sistemas soporte se determina mediante el análisis por árboles de fallos, y se utiliza en la cuantificación de las frecuencias correspondientes a un determinado estado soporte. El análisis por árboles de fallos permite la cuantificación del conjunto de fallos mínimo de componentes que conduce a la indisponibilidad de un sistema ("conjuntos mínimos de corte").

ANALISIS DE IMPORTANCIA Y SENSIBILIDAD

Para determinar la contribución de los diferentes sucesos iniciadores y fallos de sistemas al daño del núcleo se evalúan todas las secuencias de accidente. Cada una de estas contribuciones se analizan para evaluar su peso en la secuencia del accidente. Este proceso se repite para cada secuencia y los mayores contribuyentes a las secuencias del accidente se suman, para obtener una lista de sistemas y sucesos iniciadores con su contribución porcentual al daño del núcleo.

Se analizan también los fallos de los componentes que contribuyen al fallo del sistema de seguridad o sistema soporte, mediante una revisión de los árboles de fallo de cada sistema, sus condiciones de contorno y los conjuntos mínimos de corte, para delimitar los fallos más importantes de los componentes.

Se realizan estudios de sensibilidad para investigar variaciones de la frecuencia de daño al núcleo, debido a cambio de parámetros de entrada como acciones del operador, frecuencias de sucesos iniciadores y cualquier otra alternativa de diseño en planta que modifique la indisponibilidad de importantes sistemas clave.

Cuando hay cambios en las frecuencias de los sucesos iniciadores dominantes, se revisan las configuraciones de los sistemas, y se estudian otras posibles alternativas que disminuyan la ocurrencia de los sucesos iniciadores. Los análisis de sensibilidad de modelos de sistemas incluyen modificaciones de los criterios de éxito, revisión de los análisis y de cualquier otro criterio de modelado que introduzca cambios en los sistemas, cuyos fallos contribuyen en forma importante a la frecuencia de daño al núcleo.

Las incertidumbres asociadas a las estimaciones puntuales de riesgo se contemplan en cada una de las fases del análisis. Se consideran tres tipos de incertidumbres en los estudios probabilísticos de seguridad. Incertidumbres en el modelado, limitaciones de los análisis e incertidumbres de los parámetros de entrada. Los dos primeros se consideran en forma cualitativa durante el desarrollo de los modelos, y si es necesario se completan con análisis de sensibilidad.

Las incertidumbres de los parámetros de entrada, se analizan utilizando técnicas cuantitativas estadísticas aplicadas a los datos obtenidos, para expandir las tasas de fallos de componentes de estimaciones puntuales a distribuciones de probabilidad. Dichas incertidumbres se propagarán a lo largo del estudio mediante el uso del método de los momentos y el método de los diagramas de probabilidad discretos.

TRATAMIENTO DE ERRORES HUMANOS

En la metodología se consideran los errores humanos por actuación y omisión, considerados importantes durante la operación normal de la planta y en condiciones de accidente. La contribución al riesgo, debida a la interacción hombre-máquina, se puede diferenciar en dos áreas principales, pruebas, mantenimiento y operación. La influencia de los factores humanos en el mantenimiento y pruebas de componentes se integra en el análisis de los árboles de fallos.

La influencia de los factores humanos en operación y en condiciones de accidente se refleja generalmente en el análisis de los árboles de sucesos.

El estudio de los errores humanos se lleva a cabo en tres etapas: identificación de las acciones importantes del operador, identificación de acciones importantes para la operación segura de la central, y análisis en profundidad de las acciones identificadas en el punto anterior, lo cual incluye evaluación de las acciones del operador, identificación de opciones alternativas y sus efectos en los árboles de sucesos y de fallos, cuantificación y documentación.

El método principal utilizado para la cuantificación detallada de la fiabilidad humana es el de Metodología de Indice de Probabilidad de Exito de Slim. Esta técnica ha sido desarrollada con el apoyo de la "Nuclear Regulatory Comission". Esta técnica permite también la cuantificación independiente de la probabilidad de diagnóstico correcto, por parte del operador, las acciones requeridas para lograr los objetivos deseados, y la probabilidad de recuperación del error. A partir de esta información obtenida con esta técnica se puede llevar a cabo análisis de sensibilidad para investigar los efectos que tiene sobre la fiabilidad humana el modificar el tiempo disponible para la respuesta, la calidad de información utilizada por el operador, etc.

ESTADO DE LA METODOLOGIA

La Metodología de Westinghouse se encuentra totalmente informatizada, pudiendo realizarse estos análisis en ordenadores personales, que permiten actualizar con facilidad los cambios que pueden originarse a lo largo de la vida de la Central. La amplia difusión de la metodología ha permitido la continua puesta al día de los códigos, que han incorporado los últimos desarrollos de la Tecnología. Esta metodología ha sido utilizada en conjunción con los modelos termohidráulicos de Westinghouse, habiéndose llegado a adquirir una gran experiencia en la determinación de criterios de éxito "de mejor estimación". Conviene resaltar la vertiente que hoy en día está teniendo la metodología en sus usos para la racionalización y relajación de especificaciones técnicas, y en la reducción de riesgo de los diseños avanzados.