TERMOHIDRAULICA

ESTUDIOS DE FIABILIDAD Y SU APLICACION EN PLANTAS NUCLEARES Y DE PROCESO

U. HAUPTMANNS y H. SEEL

Desde hace más de diez años se están realizando estudios probabilísticos para centrales nucleares en mayor escala. Por una parte, se trata de análisis de sistemas individuales, como, por ejemplo, el de refrigeración de emergencia, con objeto de establecer su probabilidad o frecuencia esperada de fallo. Por otra parte, se elaboran estudios de riesgo. En ellos se analiza una serie de sucesos iniciadores de accidentes, como, por ejemplo, rupturas de tuberías o el fallo del suministro eléctrico y las consecuencias que dichos sucesos pueden acarrear tanto dentro como fuera de la central. Cada suceso iniciador desencadena la activación de una serie de sistemas de protección, cuyo funcionamiento o fallo, respectivamente, determina si se produce un accidente o no. Con ayuda de métodos probabilísticos se calcula entonces la frecuencia esperada con la que ocurre un accidente. Además se emplean modelos adicionales para estimar el volumen de daños originados por dicho accidente. Un estudio de riesgo se diferencia, por tanto, de un análisis de fiabilidad de un sistema en que el primero evalua, además de la frecuencia de fallo, los daños que éste causa. Asimismo, es mayor el número de sistemas que se analizan y se tiene en cuenta la interacción de ellos en la tarea de controlar los diferentes sucesos iniciadores de accidentes. Por tanto, se trata de investigaciones que tienen un mayor alcance que un estudio de fiabilidad.

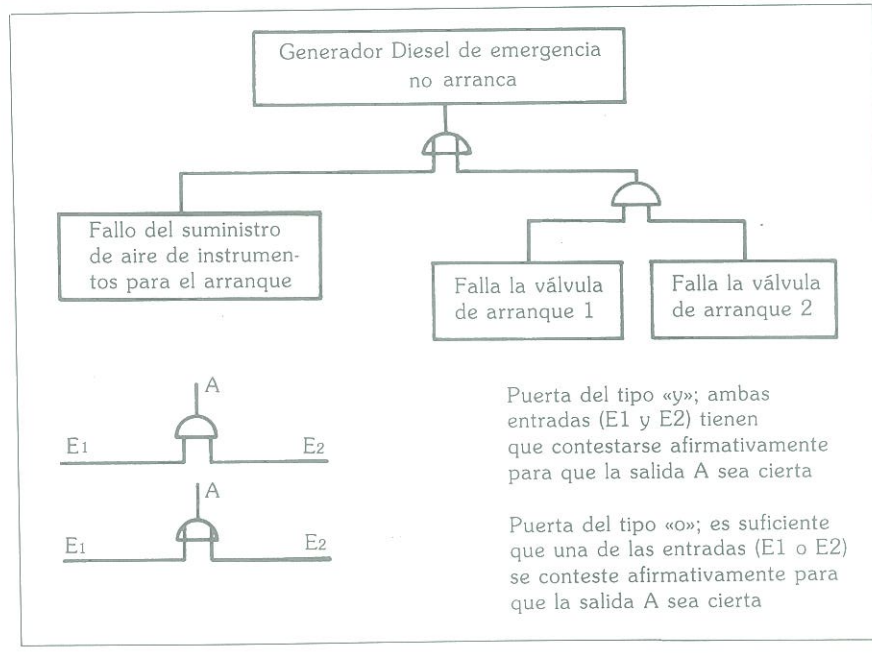
La herramienta principal para la determinación de la probabilidad o la frecuencia esperada de fallos o accidentes en ambos casos es el análisis de árboles de fallos. Se trata de un procedimiento en el que primero se define un suceso no deseado, por ejemplo, el fallo del sistema, y luego se buscan los fallos de los componentes que por sí sólos o conjuntamente con los fallos de otros componentes producen el suceso no deseado. En el análisis, que es de carácter deductivo, se suelen contemplar dos únicos estados, tanto para los componentes como para el sistema: el funcionamiento y el fallo, lo cual naturalmente conduce a un modelo simplificado del sistema analizado. La Fig. 1 muestra un ejemplo sencillo de un árbol de fallos.

Como se puede apreciar, las conexiones lógicas de las cuales se compone el árbol son de dos tipos:

- La puerta del tipo «o», la unión lógica, que significa que cada uno de los sucesos representados por las entradas puede producir el suceso simbolizado por su salida.
- La puerta del tipo «y», la intersección lógica, que significa que todos los sucesos representados por sus entradas tienen que producirse a la vez para que ocurra el suceso representado por su salida.

Todos los sistemas técnicos se componen de configuraciones que se pueden representar por las citadas puertas. Cabe mencionar que la puerta de tipo «y», es decir, todos los sucesos representados por sus entradas tienen que producirse a la vez para que ocurra el suceso de salida, es la representación lógica de una redundancia.

F 1 *Ejemplo de un árbol de fallos para el fallo de arranque de un generador diesel de emergencia.*



La parte del análisis de árboles de fallos que se ha esbozado hasta ahora y que corresponde a los dos primeros pasos que se indican en la Fig. II es la parte cualitativa del análisis. Su realización requiere un estudio profundo del sistema bajo investigación a partir de los diagramas de flujo y de una descripción del funcionamiento del sistema. Además se precisa el conocimiento del comportamiento dinámico del sistema como consecuencia del fallo de sus componentes, ya que la decisión de si un fallo desemboca en una situación peligrosa depende de él. Por ejemplo, si falla un sistema de refrigeración es preciso saber si como consecuencia se superan temperaturas límite o no.

F II

Esquema de flujo para la elaboración de un análisis de árboles de fallos.

- Adquisición de conocimientos sobre el sistema a partir de una descripción del proceso, diagramas de flujo, etc.
- Definición del suceso no deseado.
- Desarrollo del árbol de fallos.
- Adquisición de datos de fiabilidad para componentes, incluyendo fallos de causa común y el error humano. Elección de modelos para describir los componentes, teniendo en cuenta posibles revisiones y mantenimiento.
- Evaluación numérica del árbol de fallos.
- Valoración de los resultados y modificaciones del diseño original, si fueran necesarias, modificación y nueva evaluación del árbol.

Este conocimiento se deduce de cálculos dinámicos para el sistema o de experimentos. Cuando se carece de estas fuentes de información, el analista tiene que recurrir a hipótesis pesimistas sobre el comportamiento del sistema. En el estudio de riesgo para las centrales nucleares de la República Federal de Alemania se han utilizado, por ejemplo, los cálculos dinámicos presentados en el proceso de licenciamiento, que se pueden considerar como pesimistas, como base del desarrollo de los árboles de fallos. Dichos cálculos se diferencian de aquellos que se denominan «best estimate», y que conducen a hipótesis más realistas para el funcionamiento de un sistema. Un ejemplo para los dos conceptos mencionados lo facilita el análisis de las fugas pequeñas en el circuito primario de la central de referencia del citado estudio. Mientras que en el proceso de licenciamiento se parte de la base de que se necesitan por lo menos dos de los sistemas de inyección de alta presión para controlar este suceso iniciador, cálculos más recientes indican que bastaría con uno. Tal diferencia naturalmente repercute en el árbol de fallos correspondiente, como se puede apreciar en la Fig. III. Si se denomina con u la probabilidad de fallo de cada uno de los sistemas, se obtiene una probabilidad de fallo de $4 \cdot u^3$ en el primer caso frente a u^4 en el segundo, si se desprecia una posible aportación de fallos de causa común, es decir, fallos que conducen a una no disponibilidad simultánea de varios sistemas redundantes. Evidentemente $u^4 \leqq 4 \cdot u^3$, ya que $u \varepsilon [0,1]$.

La fase de elaboración del árbol de fallos, es decir la fase cualitativa del análisis, resulta útil en sí, ya que conlleva una revisión detallada del sistema bajo investigación. Esta se realiza además bajo la perspectiva de posibles fallos del sistema en lugar del punto de vista de las condiciones de su funcionamiento, siendo esta última la perspectiva del diseñador. Por tanto, el análisis implica una comprobación de la observación de las normas conocidas de diseño y conlleva normalmente algunas propuestas de mejora del sistema, sobre todo si se ve que existe la posibilidad de que el fallo de un solo componente ya puede acarrear el fallo del sistema.

Con la elaboración del árbol de fallos termina la fase cualitativa del análisis. La cuantificación del árbol de fallos requiere el conocimiento de las probabilidades de fallo de los componentes del sistema y de las probabilidades para los errores humanos que se pueden cometer en su manejo y mantenimiento y que se tratan igual que los componentes técnicos en el contexto del análisis. Con ayuda de las citadas probabilidades se puede calcular entonces la probabilidad de fallo del sistema.

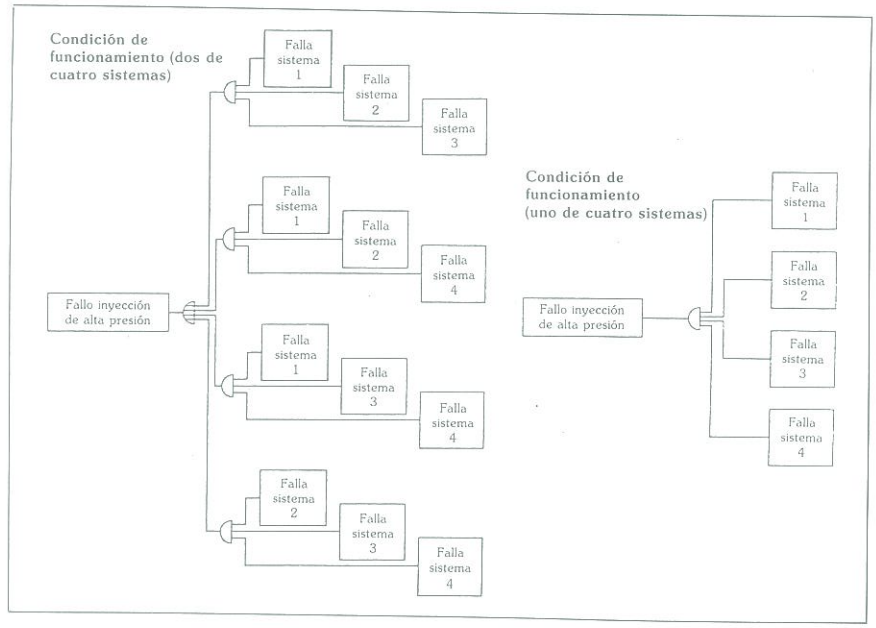
Los datos para los componentes se obtienen a partir de la observación de sus fallos en centrales que ya están en funcionamiento. Para la descripción correcta de los componentes del sistema bajo investigación con ayuda de los citados datos es preciso que se conozcan las dependencias de las probabilidades de fallo de los componentes de parámetros que posiblemente influyen en la duración de su vida. Estos pueden ser, por ejemplo, la temperatura, la presión, el medio de trabajo. Con esta información se puede utilizar en un análisis la probabilidad de fallo que mejor corresponde a las condiciones de trabajo del componente que se pretende describir. Debido a las observaciones que la GRS ha realizado tanto en centrales convencionales como nucleares se dispone de una colección de datos que reúne las citadas condiciones. Su campo de aplicación habitual naturalmente es la industria nuclear y únicamente se permiten extrapolaciones a otras industrias como, por ejemplo, la de procesos en casos específicos. En esta última, los análisis, por desgracia, siguen padeciendo de la escasez de datos adecuados para las probabilidades de fallo de los componentes.

Los datos para el error humano se evalúan sobre la base de un estudio de la situación en la que se deben realizar los actos humanos teniendo en cuenta factores como la complejidad del acto, el estress, el tiempo disponible para su realización, la preparación de la persona que lo lleva a cabo, etc. Aunque la calidad de los datos para describir el comportamiento humano difícilmente alcanza la de los datos para los componentes, el análisis ya muestra su utilidad indicando, por ejemplo, en qué contextos se exige demasiado del hombre y, por tanto, resultaría útil reemplazar su actuación por la de un sistema automático.

Una vez disponibles los citados datos se puede proceder a la evaluación del árbol de fallos obteniéndose la probabilidad o frecuencia esperada con la que se produce el suceso no deseado. Además se puede ver cuáles son los fallos o combinaciones de fallos que más aportan a la frecuencia del suceso no deseado. De este modo se conocen la importancia relativa de las diferentes combinaciones de fallos y las áreas donde posibles mejoras del sistema tedrían su mejor rendimiento. Las modificaciones del diseño naturalmente conducen a cambios en el árbol de fallos. La evaluación del árbol de fallos modificado permite entonces obtener la reducción de la frecuencia esperada del suceso no deseado. De este modo se llega a conocer la eficacia de la medida propuesta.

Después de haber esbozado el procedimiento de un análisis de fiabilidad para

F III *Arboles de fallos para dos casos diferentes de condiciones de funcionamiento de un sistema.*



sistemas técnicos, cabe preguntar, ¿cuáles son los beneficios que se pueden obtener de este tipo de análisis y en qué contexto ya se ha aplicado?

En contestación a la primera de las preguntas se pueden aducir los puntos que se indican en la Figura IV. Las ventajas citadas se obtienen en independencia de la clase de centrales que se analizan y han conducido en la República Federal de Alemania al empleo de estudios de fiabilidad para sistemas en el contexto del proceso de licenciamiento. A esto haré referencia a continuación.

Las centrales nucleares al igual que otras instalaciones técnicas se contruyen basándose en principios determinísticos. La causa para eso no es solamente histórica sino que obedece al hecho de que las dimensiones de los componentes y sistemas técnicos se pueden calcular únicamente a partir de las cargas físicas y químicas a las cuales están sometidos. Además de los requisitos que se deducen de la operación normal de la central se define una serie de accidentes, los llamados accidentes base de diseño. El más conocido indudablemente es la ruptura total del circuito primario. Dichos accidentes conducen generalmente a las cargas máximas para los componentes y sistemas y, por tanto, a los requisitos más severos para su dimensionamiento. En el análisis de accidente correspondiente se demuestra que tales accidentes se pueden controlar de forma segura. Además se observan en el diseño una serie de principios de comprobado valor como la redundancia, la diversidad, el criterio del fallo único, componentes que anuncian su propio fallo, el fallo sin riesgo, la elección de materiales idóneos y la garantía de calidad durante la fabricación y el montaje.

El concepto determinístico ha demostrado su valor y debido a las necesidades del diseño no se puede reeemplazar por un concepto probabilístico. Este último, sin embargo, permite calcular la eficacia de los principios de diseño mencionados que a pesar de su formulación determinística pueden ser objeto de una interpretación probabilística. Unicamente un análisis probabilístico puede mostrar, por ejemplo, la influencia de una redundancia o de componentes que anuncian su propio fallo calculando la reducción de la probabilidad de fallo del sistema originada por su utilización. En este sentido los estudios probabilísticos de riesgos se han empleado para facilitar información adicional y ampliar la base de decisión en el proceso de licenciamiento en la República Federal. Dicho proceso por lo demás desconoce valores de consigna para la probabilidad de fallo de determinados sistemas tal como se especifican, por ejemplo, en el Canadá o para reactores de agua ligera en el Reino Unido. Algunos de los sistemas y funciones que han sido objeto de análisis de fiabilidad en la República Federal de Alemania se enumeran en la Fig. V.

Además de las investigaciones citadas se ha elaborado un número elevado de estudios de fiabilidad para los reactores avanzados, el reproductor rápido y el reactor de alta temperatura, que se están contruyendo empleando una normativa desarrollada para reactores de agua ligera a pesar de sus diferencias conceptuales que naturalmente conducen, por lo menos en parte, a sistemas diferentes. En general los objetivos principales de los análisis probabilísticos empleados en los procesos de licenciamiento han sido los que se indican en la Fig. VI.

Los análisis muestran que las no disponibilidades de los sistemas que se precisan para controlar los sucesos iniciadores de accidentes normalmente son del orden de magnitud del 10^{-3} o menor. El límite superior se alcanza por aquellos sucesos cuyo control impone exigencias muy elevadas sobre el reactor como, por ejemplo, la fuga pequeña desde el circuito primario en el caso de los reactores de agua a presión o la ruptura de la tubería de alimentación dentro del sistema de supresión de presión en el caso de los reactores de agua en ebullición. Además se manifiesta una reducción de las no disponibilidades de los sistemas en reactores posteriores a la central de Biblis B, que ha sido la planta de referencia del Estudio Alemán del Riesgo de las Centrales Nucleares. Esto se debe a mejoras de los sistemas, que dicho de paso también se han realizado en la citada central, y que se refieren, por ejemplo, a la automatización de la parada con un gradiente de 100° k/h después de manifestarse una fuga pequeña en el circuito primario.

En resumen se puede decir que los estudios de fiabilidad tienen una cierta implantación en el proceso de autorización de centrales nucleares en la República Federal. En cambio, no se utilizan hasta ahora en el contexto del licenciamiento de plantas de proceso. Esto se explica por el hecho de que según los criterios del BMI estudios probabilísticos se deben emplear en el proceso de autorización de una central nuclear si el estado de la ciencia y tecnología permite alcanzar el nivel de exactitud requerido. La normativa correspondiente para plantas de proceso, en cambio, indica únicamente que tales estudios se pueden emplear para demostrar la seguridad de una instalación.

A pesar del hecho de que todavía quedan áreas que necesitan una mayor atención como la de los fallos de causa común, es decir la no disponibilidad simultánea de varios componentes de sistemas redundantes, o una modelación mejor del error humano, los análisis probabilísticos han mostrado ser un complemento sumamente útil de los procedimientos tradicionales de diseño. Sus ventajas les convierten en un instrumento para optimizar el diseño y la operación de instalaciones técnicas, lo cual les asegura un campo de empleo en plena independencia de posibles requisitos del proceso de autorización.

F IV

Ventajas de un análisis de árboles de fallos.

- Reducción de la probabilidad de fallo.
- Aumento de la disponibilidad del sistema.
- Diseño equilibrado en cuanto a la seguridad.
- Comparación de diseños alternativos.
- Optimización de las estrategias de revisión.
- Estimación del efecto de la duración del mantenimiento sobre la disponibilidad del sistema.
- Determinación de las duraciones máximas tolerables del mantenimiento.
- Estimación del efecto del error humano sobre la probabilidad de fallo del sistema.
- Mejor base para preparar al operario para sus intervenciones.

F V

Relación de algunos de los análisis probabilísticos realizados en la República Federal de Alemania.

Reactores de agua a presión

- Eliminación del calor residual en caso de fugas «grandes», «medianas» y «pequeñas» del circuito primario y fuga «pequeña» del presionador.
- Eliminación del calor residual en caso de fallo del suministro eléctrico.
- Fiabilidad del sistema de presurización.
- Fiabilidad del aislamiento del primario.
- Fiabilidad del sistema de protección del reactor en el caso de una fuga «grande» con fallo simultáneo del suministro eléctrico.
- Fiabilidad de los sistemas de protección de la turbina.
- Fiabilidad del suministro eléctrico.
- Fiabilidad de la refrigeración de la piscina de combustible gastado.

Reactores de agua en ebullición

- Fallo del sumidero principal de calor.
- Ruptura en la turbina de agua de alimentación.
- Accidentes de pérdida de refrigeración, «fuga en el fondo del recipiente a presión».
- Fallo del suministro eléctrico.

F VI

Objetivos de análisis probabilísticos utilizados en procesos de licenciamiento.

- Búsqueda de puntos débiles en los sistemas de protección; identificación de aquellos fallos de componentes que aportan sustancialmente al fallo del sistema.
- Comparaciones entre diseños alternativos con objeto de elegir la configuración mejor.
- Optimización de los intervalos de tiempo entre inspecciones recurrentes.
- Determinación de las duraciones máximas tolerables de las reparaciones.