Julio GONZALEZ FERNANDEZ es Ph. D. en Física por la Universidad de Manchester. Fue Profesor Titular del Departamento de Ingeniería Energética de la ETSII de Bilbao.
Cuenta con doce años de experiencia en la Ingeniería de Centrales Nucleares y es Jefe del Grupo de Sistemas del Departamento de Ingeniería y Proyectos de Nuclenor, S. A.

# APLICACIONES DEL ANALISIS PROBABILISTICO DE SEGURIDAD

J. GONZALEZ – G. GUTIERREZ

Gerardo GUTIERREZ SIMON es Ingeniero Industrial por la ETSII de Bilbao. Participó en el Análisis Probabilístico de Seguridad de Santa María de Garoña. Posee cinco años de experiencia en Ingeniería de Centrales Nucleares y es miembro del Departamento de Ingeniería y Proyectos de Nuclenor, S. A.

## OBJETIVOS Y UTILIDAD DEL APS

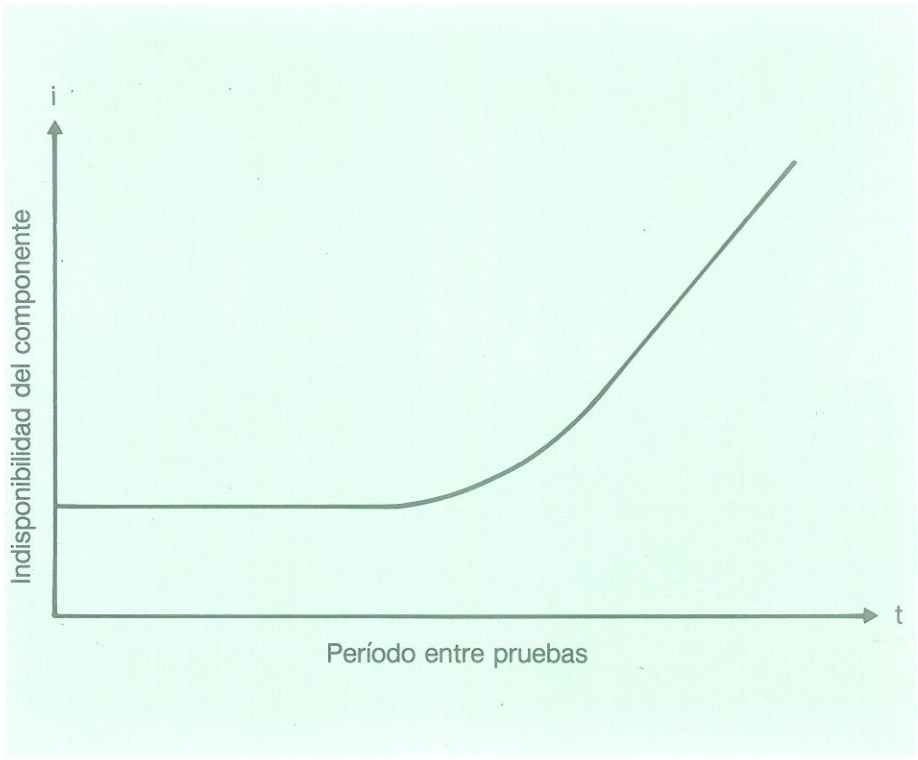
El APS es una técnica analítica para integrar diversos aspectos de diseño y operación de cara a reducir el riesgo de una central nuclear y en particular para conseguir una base de información que permita analizar aspectos genéricos y específicos de la planta. A la vez que se consiguen estos objetivos, el APS sirve a una variedad de propósitos.

La evaluación del riesgo específico de la planta de desembocar en una situación de deterioro del núcleo, proporciona una cierta medida del riesgo al público que causaría un potencial accidente, así como resultados en cuanto a la adecuación del diseño y la operación de la planta.

El análisis del diseño y de los procedimientos de operación de la planta se realiza identificando aquellas secuencias de posibles sucesos que dominan el riesgo, y estableciendo qué características de la planta contribuyen más a la frecuencia de tales secuencias. Estas características de la planta pueden consistir en posibles fallos de equipo, fallos en modo común de los mismos, errores humanos durante actividades de prueba o mantenimiento o procedimientos inadecuados que conducen a errores humanos. De esta forma, el Análisis Probabilístico puede revelar aspectos de la planta que merecen una atención especial, y de esta manera posibilita mejorar la seguridad de la instalación.

El otro objetivo conseguido por el APS es el desarrollo de una base de información que permita el análisis de temas genéricos o específicos de la central. Esta base de información identifica las secuencias de accidente dominantes y las características de la planta que contribuyen significativamente al riesgo, proporcionando así mismo los modelos de sistemas desarrollados durante el estudio. El conocimiento de los accidentes más probables ayuda a identificar las estrategias a seguir para controlar estos accidentes, muchas veces diferentes a los definidos en el diseño. Esta información puede, por tanto, enfocar así el entrenamiento de operadores a prevenir tales accidentes y se puede enfatizar la diagnosis de las secuencias de accidente más pro-

bables proporcionando información y consejo a los operadores sobre cómo actuar en tales ocasiones.
La información desarrollada en el análisis puede ayudar así mismo a tomar decisiones sobre la distribución de recursos en mejoras de seguridad, dirigiendo la atención a aquellos puntos que más disminuyen el riesgo total de la planta.
Los modelos de la planta desarrollados en el análisis sirven para diversas aplicaciones. Pueden ser usados para evaluar el impacto en seguridad de ciertas ocurrencias operacionales en la planta; pueden ser así mismo utilizados para evaluar la aplicabilidad y significancia de incidentes en otras plantas, y pueden así proporcionar un criterio de evaluación para optimizar diversos cambios de diseño posibles y mejorar la seguridad de la instalación.
En suma, el análisis proporciona de manera conjunta una visión de diversos aspectos de diseño de la planta y su operación, en un solo modelo, que puede proporcionar a operadores y a ingenieros de la empresa perspectivas adicionales a la hora de mejorar la seguridad y la disponibilidad de la central.
A continuación trataremos tres aspectos típicos de aplicación que la herramienta generada en el análisis probabilístico nos permite tratar.




**F I** *Modelo de fallo de un componente que combina el fallo en demanda y dependiente del tiempo*

## ESPECIFICACIONES TECNICAS

Las Especificaciones Técnicas son un documento voluminoso que regula la operación de las centrales nucleares y establece un cierto número de condiciones y limitaciones a la misma de obligado cumplimiento.
Las bases técnicas para estas limitaciones son lo suficientemente vagas como para que uno pueda hacer cambios sustanciales en los requerimientos específicos sin necesidad de cambiar las mencionadas bases técnicas. Por esta razón podría decirse que los requisitos de las Especificaciones Técnicas han sido definidos de una manera bastante arbitraria.
Las Especificaciones Técnicas tienen, sin embargo, un considerable número de implicaciones en la disponibilidad de la planta, por lo que hay un creciente interés hoy día en encontrar un equilibrio razonable entre disponibilidad de la planta y seguridad, revisando para ello estas Especificaciones Técnicas.
Parece claro que el método tradicional de regulación en seguridad nuclear no va a contribuir mucho más a la mejora de las Especificaciones Técnicas. Los métodos basados en técnicas de fiabilidad y evaluación del riesgo han tomado el relevo y son los que hoy en día están siendo estudiados y propuestos.
Las Especificaciones Técnicas afectan a la fiabilidad de los sistemas principalmente en el sentido de que establecen Condiciones Limitativas de Operación (LCO) y requisitos de vigilancia para pruebas "On-line" y reparaciones de componentes de sistemas de seguridad de la planta.
Las Condiciones Limitativas de Operación se refieren a límites máximos de tiempo que sistemas de seguridad pueden estar indisponibles; condición esta impuesta por el organismo regulador como parte de la licencia de operación del reactor. Generalmente, cuando un componente de un sistema de seguridad se pone fuera de servicio para repararlo o probarlo, por un período de tiempo, existe un incremento de la vulnerabilidad del sistema en el sentido de que disminuye la probabilidad de que dicho sistema esté disponible para mitigar un accidente. Este incremento de vulnerabilidad perdura hasta que el componente es vuelto a poner en servicio. Las restricciones a la duración de este período, el Tiempo Permitido Fuera de Servicio (AOT) es el aspecto de las LCO que aquí se comenta. Hay métodos para relacionar las medidas del riesgo con las AOT, y sólo relacionando explícitamente estos dos conceptos pueden definirse los tiempos máximos de fuera de servicio que limiten dicho riesgo.
Los Requisitos de Vigilancia se refieren a las frecuencias mínimas con las que han de probarse periódicamente, de manera activa, esto es, verificando su operabilidad, componentes de sistemas de seguridad en reserva. Estos requisitos se expresan normalmente como un límite superior del período entre pruebas. No hay razones por las cuales no definir de la misma forma un tiempo mínimo entre pruebas para estos componentes, puesto que también existen fallos y envejecimiento causados por las pruebas, que necesitan ser controlados. Los intervalos de prueba idóneos son aquellos que intentan equilibrar ambos tipos de riesgo para conseguir un riesgo total aceptablemente bajo.
En todos los casos, el análisis de los "tiempos de fuera de servicio" que contribuyen a la indisponibilidad de un sistema es fácil si los modelos de APS están ya disponibles. Sin embargo, el juzgar adecuadamente el incremento de indisponibilidad causada por las AOT's que puede considerarse aceptable es una tarea difícil, debido a la contribución relativamente pequeña que este concepto tiene en el riesgo total de la central.

Básicamente, hay dos posibles juicios:
- *Juicio relativo:* el incremento de la disponibilidad del sistema debe ser limitado por un factor F en compara-

ción con la indisponibilidad del sistema con la AOT previa.
- *Juicio absoluto:* el incremento del riesgo en la planta debe ser limitado en caso de cambiar la AOT.

El primer juicio es fácil de aplicar y suministra números bien definidos. Su inconveniente es que este método podría producir AOT's más cortas para sistemas de mayor fiabilidad que para aquellos de menor fiabilidad, y no tiene en cuenta la importancia del sistema en el contexto de la secuencia de accidente. Básicamente, el segundo tipo de evaluación suministra valores significativos del riesgo. En este caso hay que reconocer que la variación del riesgo producida por los cambios en las AOT's es pequeña en comparación con la incertidumbre del riesgo. Además este concepto es mucho más complicado de manejar, con propósito comparativo, puesto que el APS específico y completo de la planta ha de estar disponible.

## PRUEBAS DE SISTEMAS

Las pruebas de componentes de sistemas en espera se realizan con la frecuencia prescrita en las Especificaciones Técnicas de la planta. Se hacen pruebas de los equipos porque el modelo de fallos para los componentes lleva implícita la hipótesis de que la indisponibilidad del componente se incrementa con el tiempo que el mismo está en situación de espera, esto es, se supone que el mejor modelo para el componente es aquel con una tasa de fallo dependiente del tiempo. Si esto no fuese así, es decir, si la probabilidad de fallo del componente no dependiese del tiempo entre pruebas, éstas no serían necesarias. De hecho, las pruebas incrementarían la indisponibilidad del componente si el mismo fuese retirado de su posición de servicio durante la duración de la prueba. Así pues, y puesto que los componentes que se prueban tienen implícitamente asociada una tasa de fallos basada en el tiempo, la indisponibilidad del componente depende del período de prueba y este período debe, por tanto, ser determinado para cada uno de tales componentes.

En realidad, la mayor parte de los componentes tienen generalmente las dos contribuciones a su indisponibilidad: la debida al tiempo entre pruebas y la de demanda. La figura I representa la probabilidad de fallo en función del período de prueba para un componente con una combinación de ambas tasas de fallos, la de demanda y la dependiente del tiempo. Para tiempos de pruebas relativamente cortos, el modelo de fallos en demanda es razonablemente bueno para la mayoría de los componentes, pero, por el contrario, cuando el período de prueba se alarga, el modelo de fallo dependiente del tiempo representa probablemente mejor la situación.

Como se puede ver, no hay escalas en la figura, y éstas indudablemente dependerán del tipo de componente y de sus probabilidades de fallo.

Las pruebas de componentes de sistemas de seguridad tienen como resultado, normalmente pero no siempre, el retirar el componente de servicio durante la duración de la prueba. Cuando el componente se retira de servicio por una prueba está obviamente indisponible para mitigar un accidente y, por tanto, la prueba contribuye de esta forma a la indisponibilidad tanto del componente como del sistema de seguridad que lo incluye. Por otra parte, si el componente no fuera probado, la indisponibilidad del mismo crecería continuamente y se acercaría con el tiempo al valor unidad. Por esto, bajo la hipótesis de combinación de modelos de fallos en demanda y dependientes del tiempo, son necesarias las pruebas para evitar que las indisponibilidades individuales de los componentes crezcan aproximándose a uno. Es necesario, pues, estimar ambas contribuciones a la indisponibilidad global: la contribución del fallo del componente y la contribución de la prueba.

Los tiempos de prueba de los componentes no solamente están circunscritos a las pruebas formales de los mismos, sino también a pruebas ocasionales que se dan durante la operación normal de la planta al ocurrir ciertas incidencias. Por ejemplo, considérense las válvulas de un sistema de alimentación de agua de emergencia para el que mensualmente se hace una prueba de apertura de válvulas que verifica los actuadores de las mismas, esto es, que verifica el modo de fallo "No abre en demanda", pero que no comprueba el modo de fallo "válvula obstruida", modo este último que sólo resulta probado cuando se actúa el sistema en su conjunto.

Supóngase así mismo que este sistema de agua de alimentación es requerido siempre que ocurre un disparo de turbina, el cual puede darse con una frecuencia anual de 6 a 10; resulta que aunque no hubiera pruebas formales del sistema de agua de alimentación, éste quedaría probado el mismo número de veces que los disparos de turbina habidos.

Como un segundo ejemplo, considérese un sistema de extracción de calor para el que las pruebas de las bombas no verifican completamente el camino de flujo en accidente. Sin embargo, si el sistema se usa en la recarga, entonces sí que se comprueba el camino completo del fluido y el modo de fallo de cada uno de los componentes, por lo que esta prueba de recarga debería tenerse en cuenta junto al resto de pruebas formales para determinar el período óptimo de tiempo entre pruebas de los componentes del sistema.

### MEJORA DE PRUEBAS

La redundancia y diversidad en el diseño de sistemas de seguridad es requerida por la regulación nuclear actual como medio de asegurar dicha seguridad. Sin embargo, los requisitos de Especificaciones Técnicas en el área de pruebas no necesariamente garantizan que todos los componentes de un sistema están operables después de llevar a cabo una prueba con éxito.

Las pruebas hechas sobre los sistemas no siempre comprueban todos los componentes que están en una posición de espera. Las Especificaciones Técnicas de la planta requieren ciertas pruebas de cara a verificar que un sistema cumple su función (suministrar un cierto flujo, alcanzar una tensión prefijada, etc.), pero no requieren la verificación de cada uno de los caminos dentro del sistema que pueden satisfacer el mismo propósito.

El APS refleja la importancia de ciertos componentes que, debido a su alto valor de indisponibilidad, aparecen en los resultados dominantes de la cuantificación de secuencias de accidente. Como antes se dijo, la indisponibilidad del componente aumenta directamente con el tiempo que el mismo está en situación de espera y por tanto es obvio que reduciendo este tiempo, esto es, forzando a las pruebas a cubrir la mayor parte de los componentes del sistema, se consiguen probabilidades de fallo menores y, consiguientemente, menores frecuencias de accidente.

El APS y otros métodos de fiabilidad son herramientas claramente valiosas para identificar "lagunas" en las pruebas y mejorar posteriormente los procedimientos de prueba de sistemas de alta fiabilidad.

### ESTRATEGIAS DE PRUEBAS DE SISTEMAS

Hay dos estrategias básicas de pruebas: pruebas consecutivas y pruebas alternas.

Considérese un sistema de dos trenes; bajo la estrategia de prueba consecutiva el tren "A" sería probado y restablecido a su posición de servicio, e inmediatamente después de ello el tren "B" sería descargado de servicio, probado y repuesto a su posición previa. Esto constituiría una prueba del sistema, la cual volvería a repetirse al cabo, por ejemplo, de un mes.

*(Pasa a la pág. 59)*