Antonio B. SEGURA ROCHE es Licenciado en Química-Física por la Universidad Complutense de Madrid (1983). Diplomado en Ingeniería Nuclear por el Instituto de Estudios Nucleares (1984). Diplomado en Análisis Probabilístico de Seguridad, CIEMAT/DOE (1986).
Becario del INI en la División de Energía, Sección Nuclear, de INITEC (1984). En 1985 se incorpora a UITESA como Analista de Fiabilidad, donde participa en la Automatización de Especificaciones Técnicas de CN Cofrentes (1985). En 1987 dirige la implantación del sistema de control de Especificaciones Técnicas para CN Laguna Verde, México. En 1988 participa en la actividad de Garantía de Calidad Técnica del APS de CN Almaraz. En la actualidad desarrolla la coordinación técnica y la aplicación de sistemas de Inteligencia Artificial a la automatización y control de Especificaciones Técnicas.

CONSIDERACIONES PRACTICAS

METODOLOGIA DE UNION DE ARBOLES DE FALLOS PARA EL DESARROLLO DE UN ANALISIS PROBABILISTA DE SEGURIDAD.

A. B. SEGURA - A. J. FERNANDEZ - E. GUTIERREZ

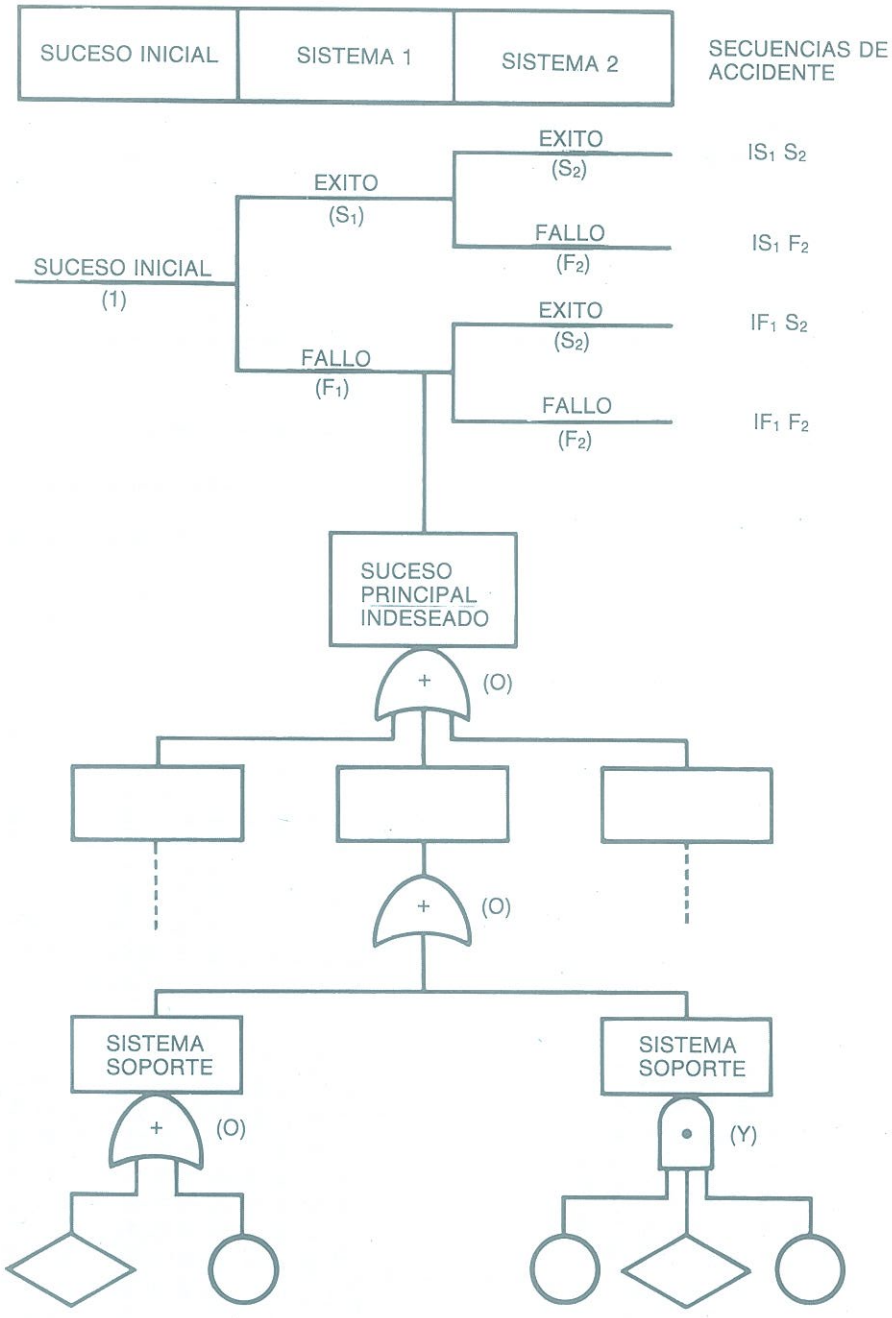
INTRODUCCION

El objetivo básico perseguido con la realización de un Análisis Probabilista de Seguridad de una central nuclear, que en adelante denominaremos APS, es el estudio de la evolución de posibles accidentes ocasionados por la aparición de un suceso no deseado y el comportamiento negativo de los sistemas diseñados para la anulación o mitigación de los efectos que pudieran derivarse.
El resultado cualitativo concreto será la identificación de las combinaciones más probables de sucesos que pueden conducir a un estado de daño considerado según un particular escenario definido por la aparición de un suceso no deseado (suceso iniciador). Estas combinaciones de sucesos (conjuntos mínimos de fallo), que pueden representar fallos o estados indisponibles de sistemas, equipos, aparatos o partes de aparatos de la central nuclear, serán el punto de partida para realizar cualquier tipo de aplicación o estudio posterior.
Dos son las metodologías de análisis que en la actualidad más se aplican en el desarrollo de los APS de centrales nucleares, a saber:

- Metodología de árboles de sucesos con condiciones de contorno (árboles de sucesos grandes/árboles de fallos pequeños).
- Metodología de unión de árboles de fallos (árboles de sucesos pequeños/árboles de fallos grandes).

Antonio José FERNANDEZ PEREZ es Ingeniero Industrial, especialidad Técnicas Energéticas, por la ETSII de Madrid. Profesor del Departamento Eléctrico de la ETSII (1981-1983), Colaborador del Instituto Tecnológico de Postgraduados en la sección de Fiabilidad (1982-1983) y Coordinador del área de Fiabilidad del Instituto de Investigación Tecnológica ICAI (1984). En 1985 se incorpora a UITESA, donde desempeña el puesto de Jefe del Departamento de Fiabilidad, Disponibilidad y Mantenibilidad. Diplomado en Análisis Probabilista de Seguridad (CIEMAT/DOE, 1986).

Eduardo GUTIERREZ FERNANDEZ es Ingeniero Aeronáutico por la ETSIA de Madrid. Profesor de Termodinámica y Técnica Atómica y Nuclear en el Centro de Estudios Aeronáuticos (1978), Colaborador del Departamento de Seguridad Nuclear de la Junta de Energía Nuclear (1980-1981). Ingeniero de Fiabilidad, Mantenibilidad y APS en la Dirección de Innovación y Desarrollo del Grupo CIAT (1982), Consultor en el Area de Seguridad, Fiabilidad y Mantenibilidad en OPTIPLANT (1983). En 1987 se incorpora a UITESA, donde es en la actualidad Jefe de Garantía de Calidad Técnica del APS de CN Almaraz.



F I *Esquema general del método de Unión de Arboles de Fallos*

Aunque existen notables diferencias entre ambas metodologías en cuanto a alcance, nivel de aplicación, recursos requeridos, etc., la diferencia básica entre ellas, a nivel técnico, es el proceso de construcción de los árboles de sucesos. Estos modelos son diagramas gráficos que representan la evolución de un accidente desde el suceso iniciador hasta el estado de daño o de no daño asociados al considerar el comportamiento positivo (éxito) o negativo (fallo) de los sistemas de seguridad. El proceso de elaboración de los árboles de sucesos influirá considerablemente en el resto de tareas a realizar en el APS y, fundamentalmente, en las correspondientes al análisis de sistemas (árboles de fallos) y a la cuantificación de la frecuencia del daño (Fig. I).

En el presente artículo, se describe la metodología de unión de árboles de fallos, señalando algunas consideraciones prácticas obtenidas por UITESA con su participación en el desarrollo de los Análisis Probabilistas de CN Almaraz, CN Ascó y CN Cofrentes.

ETAPAS DE DESARROLLO DE LA METODOLOGIA DE UNION DE ARBOLES DE FALLO

Esta metodología, conocida comúnmente como la metodología de árboles de sucesos pequeños/árboles de fallos grandes en referencia al tamaño de estos diagramas construidos durante el análisis, requiere la ejecución de las siguientes tareas:

TAREA I. DEFINICION DE LOS OBJETIVOS DEL ANALISIS

Esta actividad inicial es fundamental, ya que la identificación de los objetivos a cubrir con el estudio va a establecer las condiciones de contorno del mismo en cuanto a aspectos tales como el nivel de detalle o las actividades que es preciso desarrollar.

La selección de un nivel de detalle adecuado, acorde con los objetivos perseguidos, es una cuestión de máxima trascendencia por su impacto en el dimensionamiento de los recursos destinados al proyecto, al tratarse de un aspecto al que el APS resulta muy sensible en todas y cada una de sus tareas. El plantear cualquier análisis con el máximo nivel de detalle posible, independientemente de los objetivos a alcanzar, resulta una alternativa teóricamente aceptable, pero operativa y técnicamente ineficiente.

Por otra parte, los objetivos fijados para el estudio determinan las actividades que deberán llevarse a cabo y el grado de profundidad en su desarrollo.

TAREA II. FAMILIARIZACION CON LA PLANTA

El propósito de esta tarea es la recopilación y análisis de toda la información necesaria para la identificación, selección y agrupación de los sucesos iniciadores a considerar en el estudio, la identificación de los sistemas frontales y soportes implicados en la mitigación de los sucesos iniciadores seleccionados, así como el análisis de las dependencias funcionales entre ellos y, por último, el establecimiento de los criterios de éxito asociados a todos estos sistemas identificados.

Para el desarrollo adecuado de esta tarea resulta fundamental contar con personal experimentado en la operación de la planta.

La lista de sucesos iniciadores a considerar deberá ser lo más completa posible de acuerdo con los objetivos perseguidos en el proyecto y, para su elaboración, deberán analizarse los sucesos que hayan ocurrido en la propia

planta y en plantas similares, además de los considerados en la documentación técnica específica sobre este tema.
La identificación de los sistemas implicados en la mitigación de los sucesos iniciadores seleccionados se establecerá a partir de las funciones de seguridad requeridas para prevenir o mitigar la aparición de los estados de daño objeto de análisis, diferenciándose entre sistemas frontales y soportes.

Fijado un determinado suceso iniciador, cada función de seguridad tendrá un criterio de éxito asociado que definirá el conjunto de requerimientos operativos que deben cumplir los sistemas encargados de realizar dicha función de seguridad. La negación de este criterio de éxito, en lo que respecta a cada uno de esos sistemas constituirá el suceso indeseable cabecera del árbol de fallos que habrá que desarrollar en la tarea de modelización de sistemas.
Por último en esta tarea y a partir de la lista de sucesos iniciadores elaborada, se agruparán dichos sucesos en categorías de modo que cada grupo incluya aquellos sucesos iniciadores que exijan los mismos requerimientos operativos y criterios de éxito de los sistemas que intervengan en su mitigación. Este modo de proceder resulta aconsejable al objeto de reducir el número de árboles de sucesos que deberán desarrollarse en la siguiente tarea.

TAREA III. DELINEACION DE SECUENCIAS DE ACCIDENTE

Esta tarea consiste en la elaboración de los denominados árboles de sucesos y su desarrollo constituye la diferencia básica entre las dos metodologías generales de realización de un APS mencionadas con anterioridad.
La técnica de análisis mediante árboles de sucesos permite representar explícitamente las relaciones lógicas existentes entre los fallos y funcionamientos potenciales de los sistemas de mitigación considerados en la respuesta a un determinado grupo de sucesos iniciadores. Estas relaciones lógicas de fallos/funcionamientos constituyen las denominadas secuencias de accidente.
En la metodología de árboles de sucesos con condiciones de contorno es preciso desarrollar los árboles de sucesos con la restricción de que los sucesos cabecera considerados sean independientes estadísticamente, lo que requerirá, al menos, que se consideren explícitamente como cabeceras los criterios operativos de aquellos sistemas, subsistemas o componentes comunes necesarios para el cumplimiento de varios criterios de éxito simultáneamente. Este método exigirá considerar un mayor número de cabeceras en el árbol de sucesos a desarrollar (como mínimo, habría que considerar como cabeceras adicionales los criterios de éxito de los sistemas soporte) y un mayor número de secuencias accidentales generadas que en el caso de utilizar la metodología de unión de árboles de fallo en la que no existe esta restricción.
Una vez construido un árbol de sucesos, cada secuencia accidental tendrá asociado un determinado estado de daño tal que permita su agrupación en diferentes categorías.

TAREA IV. MODELIZACION DE SISTEMAS

El objetivo de esta tarea es el desarrollo, para cada uno de los sistemas considerados, de unos modelos lógicos, denominados árboles de fallos que describan, mediante operadores booleanos, la relación lógica existente entre un particular suceso que represente la negación del criterio de éxito del sistema (suceso principal) y otros sucesos asociados con el comportamiento de los componentes que lo integran (sucesos básicos).

La metodología de unión de árboles de fallos requiere que el desarrollo de los árboles de fallos de los sistemas soporte se encuentren integrados dentro de los árboles de fallos de los sistemas frontales a los que apoyan, mientras que en la metodología de árboles de sucesos con condiciones de contorno estos modelos resultan independientes, apareciendo su criterio de éxito como cabecera del árbol de sucesos.

La elaboración de un árbol de fallos está considerado tanto un arte como una técnica en el sentido de que la estructura desarrollada puede no ser única, aunque sí lo deberá ser la función booleana asociada a su suceso principal, sin embargo, resultará adecuado establecer una sistemática común de desarrollo de árboles de fallos para todos los analistas que intervengan en esta tarea.

En cuanto al nivel de detalle de los árboles de fallos, conviene señalar que deberá ser consistente con los objetivos del estudio, con los datos disponibles y suficiente para que todas las posibles dependencias queden identificadas, representadas y cuantificadas.
Además del propio modelo de árbol de fallos, en esta tarea se determinará la función booleana asociada al suceso principal considerado. Esta actividad se llevará a cabo de modo automático mediante la utilización del correspondiente código informático, fijando una determinada probabilidad de truncación que permita desechar aquellos conjuntos mínimos de fallo cuya probabilidad de aparición sea menor que dicha probabilidad de corte.

TAREA V. ANALISIS DE LA INTERACCION HUMANA

El análisis de fiabilidad humana, dentro de un APS, consiste en la identificación, incorporación y análisis de todas aquellas acciones humanas con un impacto potencialmente importante en el riesgo global de la central.
Este tema es uno de los más abiertos en el APS, habiéndose desarrollado diferentes alternativas y técnicas para el análisis y cuantificación de las acciones humanas.
En este trabajo mencionaremos únicamente a la alternativa SHARP ("Systematic Human Action Reliability Procedure"), que constituye un intento de estructurar el análisis de Fiabilidad Humana en los APS. Su aplicación práctica supondrá la ejecución de las siguientes tareas:

- Examen de los árboles de fallos y de sucesos elaborados para la identificación e inclusión de las acciones humanas en los mismos, según el tipo de acción que sea.
- Determinación de las acciones humanas «significativas» a las que se aplicará un análisis detallado.
- Cuantificación de las acciones humanas en términos de probabilidad de aparición.
- Realización de análisis de sensibilidad e incertidumbre de las hipótesis y estimaciones efectuadas para las acciones humanas que resultan más significativas.

TAREA VI. DESARROLLO DE LA BASE DE DATOS DEL PROYECTO

El objetivo de esta tarea es la determinación de la probabilidad de aparición asociada a todos y cada uno de los sucesos básicos considerados en el estudio y de las frecuencias de ocurrencia de los sucesos iniciadores seleccionados.
El cálculo de los valores mencionados requiere la estimación inicial, utilizando fuentes genéricas, de unos parámetros básicos de acuerdo con el modelo de indisponibilidad que aplique a cada suceso básico. Este proceso requerirá tanto la selección de unos valores medios como una medida de su incertidumbre y la caracterización de su distribución estadística asociada.
Obtenidas las frecuencias y probabilidades a partir de datos genéricos, resultará adecuado corregir estos valores con los datos específicos recogidos en la propia planta por aplicación de la teoría bayesiana.
Un criterio operativo a señalar sobre esta tarea es la necesidad de contar

con una estructura informática capaz de gestionar de forma eficiente todos los cálculos y procesos de obtención de información asociados a dicha tarea.

TAREA VII. CUANTIFICACION DE SECUENCIAS DE ACCIDENTE

El objetivo de esta tarea es obtener la ecuación booleana, unión de conjuntos mínimos de fallo, asociada a cada secuencia accidental con impacto en el deterioro del núcleo y su posterior cuantificación. El procedimiento de obtención de estas ecuaciones booleanas requerirá la integración lógica de las ecuaciones de fallo y de éxito correspondientes a los sistemas que constituyen dicha secuencias.

A diferencia de la metodología de árboles de sucesos con condiciones de contorno, en la metodología que comentamos, las dependencias por componentes compartidos entre sistemas no presentarán mayor problema en su tratamiento siempre y cuando la codificación de un mismo componente sea única para todos los sistemas.

Operativamente, el proceso de cuantificación suele llevarse a cabo en dos etapas: cuantificación preliminar y cuantificación final.

El objetivo principal de la cuantificación preliminar es obtener las secuencias de accidente candidatas o de mayor impacto para las cuales se realizará la cuantificación final afinando las probabilidades asignadas conservadoramente en el proceso anterior e incluyendo los factores de recuperación pertinentes.

Realizado este proceso para las secuencias de accidente, se operará análogamente para los estados de daño al núcleo considerados.

TAREA VIII. ANALISIS DE INCERTIDUMBRE, SENSIBILIDAD E IMPORTANCIA

El trabajar con variables aleatorias y modelos que constituyen una cierta aproximación de la realidad conlleva la existencia de una incertidumbre en los resultados que es preciso acotar. Para realizar de un modo sistemático esta acotación en un APS, se llevan a cabo los análisis de incertidumbre, sensibilidad e importancia.

Los análisis de incertidumbre pretenden extrapolar la incertidumbre asociada a los parámetros que definen la probabilidad de aparición de los sucesos básicos a la probabilidad de aparición de cada secuencia y a la frecuencia de los estados de daño considerados por determinación de sus funciones de distribución asociadas. De entre los métodos más utilizados para realizar este proceso, destaca el Método de Monte Carlo implementado, en varios códigos informáticos.

El análisis de sensibilidad consiste en la variación de hipótesis y parámetros que pudieran tener un impacto significativo en los resultados. Este análisis resulta un complemento del análisis de incertidumbre en lo que respecta a los modelos e hipótesis utilizados en el estudio.

El análisis de importancia proporciona información sobre la mayor o menor significación de los sucesos básicos individuales y conjuntos mínimos de fallo en los resultados. Existen diversas medidas de importancia con diferente significado cuya selección debe realizarse de acuerdo con los objetivos buscados en el estudio.

TAREA IX. ANALISIS DE SUCESOS EXTERNOS

Los sucesos externos, tales como incendios e inundaciones son contribuyentes potencialmente significativos a la frecuencia de daño al núcleo, debido fundamentalmente a la posibilidad de originar fallos de causa común en los equipos y/o iniciar algún transitorio o accidente con pérdida de uno o más sistemas de mitigación.

El análisis de estos sucesos es muy específico, ya que su aparición, progresión e impacto dependen de la situación, configuración y medios de protección particulares de la planta objeto de estudio.

El método general a utilizar consistirá en la realización de un análisis preliminar, bajo hipótesis conservadoras, que permita determinar aquellas áreas de la planta susceptibles de verse más afectadas por la aparición de un suceso de este tipo y, por añadidura, contribuir más significativamente a la frecuencia de daño al núcleo. Para aquellas situaciones potencialmente más significativas deberá efectuarse un análisis más detallado y realista.

TAREA X. ELABORACION DEL INFORME FINAL

La gran cantidad de información utilizada y generada en el transcurso de un APS requiere un esfuerzo notable de sistematización, normalización y síntesis a la hora de elaborar el informe final del estudio. En nuestra opinión este informe debe estar constituido por un volumen principal y unos apéndices.

El volúmen principal debería contener la descripción general del proyecto en cuanto a organización. objetivos y medios empleados, hipótesis principales consideradas y resultados obtenidos. La utilización de tablas y gráficos resulta muy aconsejable. En los apéndices, uno para cada tarea del APS, se describiría con detalle los diferentes aspectos considerados en cada una de estas tareas y su resultados específicos.

Adicionalmente, creemos necesario comentar brevemente dos actividades tan importantes como las ya mencionadas para el buen desarrollo de un proyecto de APS. Estas actividades son la Garantía de Calidad Técnica y la Informática del Proyecto.

La Garantía de Calidad Técnica interna del Proyecto tiene por misión controlar, desde el punto de vista técnico, la adecuación a los procedimientos del trabajo que se desarrolla en el mismo.

Indudablemente, un APS no podría llevarse a cabo sin contar con unas adecuadas herramientas informáticas de aplicación específica y real al desarrollo de este tipo de estudios según el alcance y método comentados. En nuestra opinión y desde nuestra experiencia, no basta únicamente con disponer de un potente código de análisis de árboles de fallos y tratamiento de funciones booleanas, ya que todas las tareas del APS, muy relacionadas entre sí, precisan y generan una información y unos cálculos específicos que de no estar automatizado su tratamiento convenientemente originaría un mayor volúmen de recursos requeridos para su desarrollo, un mayor periodo de tiempo para su finalización e impedirían o, cuanto menos, dificultarían considerablemente cualquier actualización futura del estudio.

BIBLIOGRAFIA

Plan de Proyecto del Análisis Probabilista de Seguridad de CN Cofrentes, octubre, 1988.

Propuesta de servicios de ingeniería para la realización del Análisis Probabilista de Seguridad de CN Ascó, mayo, 1988.

Plan de Proyecto del Análisis Probabilista de Seguridad de CN Almaraz, junio, 1987.

Probabilistic Safety Analysis Procedures Guide. NUREG/CR-2815, enero, 1984.

Interim Reliability Evaluation Program Procedures Guide. NUREG/CR-2728, enero, 1983.

Systematic Human Action Reliability Procedure (SHARP). EPRI NP-3583, junio, 1984.

Notas del Curso sobre Análisis Probabilístico de Seguridad impartido en el Instituto de Estudio de la Energía y del Medio Ambiente, 1986.