

VENTAJAS Y LIMITACIONES DE LA EVALUACION PROBABILISTICA DE RIEGOS PARA CENTRALES NUCLEARES

SEGURIDAD

A. Birkhofer

Tal y como anunciábamos al dar la información sobre la Asamblea Anual de la SNE, previamente a la misma, el profesor Birkhofer impartió una lección magistral que a continuación presentamos a todos aquellos que no pudieron estar presentes.

INTRODUCCION

Hay una gran variedad de opiniones acerca de los propósitos y de las posibilidades de los análisis de riesgo. Unos consideran estos análisis como una cura milagrosa para la solución de todos los problemas de seguridad. Otros, los consideran como el medio con el que el «grupo de presión nuclear» engaña al público. Ninguno de estos puntos de vista extremos es correcto. Si se quiere dar respuesta a las preguntas sobre las posibilidades de los análisis de riesgos, se

sis de accidentes, se basa principalmente en análisis de seguridad determinísticos clásicos. Está basado en el concepto del accidente base de diseño. Estos, son accidentes que no se deben excluir, pero que son muy improbables. Estos análisis determinan los requerimientos para el diseño de los sistemas de seguridad. El método determinista, usado comúnmente en la tecnología, ha demostrado ser útil también en la tecnología nuclear. Sin embargo, los requerimientos de seguridad en este área, son más estrictos que los normales. En la República Federal de Alemania, los procedimientos están expuestos, en detalle, en los criterios de seguridad, reglamentación y normas.

Los criterios de seguridad requieren también los métodos probabilísticos según su desarrollo actual. En la práctica, este requerimiento ha llevado al desarrollo de análisis de fiabilidad para los sistemas de seguridad importantes.

Además, en los últimos años ha aumentado el número de propuestas que piden suplementar los clásicos análisis de seguridad por medio de investigaciones probabilísticas.

Parece que los conceptos «determinístico» y «probabilístico» se confunden a menudo, incluso por los expertos. El significado de estos aspectos, se puede describir con un ejemplo: supongamos que un ingeniero civil tiene que realizar un análisis de tensiones para un edificio elevado. Entre otros factores, tiene que considerar la velocidad máxima posible del viento y la carga inducida por la nieve, y tiene que incluir estos factores en sus cálculos. Podría usar datos estadísticos meteorológicos de la zona, seleccionar los valores más pesimistas, añadirles unos valores razonables como márgenes de seguridad y, después, diseñar el edificio según estas hipótesis. En la práctica, este trabajo se simplifica porque las hipótesis de carga y los márgenes de seguridad están ya suficientemente desarrollados en las normativas y en la reglamentación. Si no se cometen errores en los cálculos ni en la construcción del edificio, no es de esperar ningún fallo debido al viento o a la nieve. En este caso, el ingeniero civil ha utilizado un método determinístico. Ha realizado sus cálculos bajo condiciones extremas, fijadas determinísticamente. Las hipótesis se han tomado de tal forma, que un fallo en el edificio puede quedar totalmente excluido. Sin embargo, el fallo no está excluido según las leyes de la naturaleza. Aunque haya una probabilidad muy pequeña, se puede exceder incluso una hipótesis de carga muy pesimista.

El profesor A. Birkhofer (en el centro) durante su Conferencia en la TESIIM. Le acompaña M. Barandiarán (derecha) y J. L. Hernández Varela (izquierda).



Adolf BIRKHOFER, nacido en Munich en 1934, es Profesor de Dinámica y Seguridad de Reactores desde 1971, en la Technical University de Munich y General Manager de la Gesellschaft für Reaktorsicherheit (GRS) desde 1977. Dipl.-Ing., Electrical Engineering por el Institute of Technology, Munich, 1958. Estudios de Theoretical Physics en la Universidad de Innsbruck, Austria (1958-1961). Dr. Phil. en 1964. De 1958 a 1963, actividades industriales. Desde 1963, investigación en el terreno de la Dinámica y Seguridad de Reactores en la Technical University of Munich.

Es miembro de Reactor Safety Commission (RSK) de la República Federal de Alemania desde 1965 (Presidente, 1974-77); del Comité Safety of Nuclear Installations (CSNI) DE LA OCDE desde 1969 (Presidente, 1978-82); del Scientific and Technical Comité (STC) de las Comunidades Europeas; Enquete-Commission «Zukünftige Kernenergie-Politik» del Parlamento Alemán; American Nuclear Society (ANS); Nuclear Safety Standard Commission (KTA); Asociación de Ingenieros Alemanes (VDI). Recibió el premio Otto-Hahn de Frankfurt (Alemania), en 1976.

deben distinguir por lo menos tres áreas de aplicación.

La primera de ellas está relacionada con la aplicación de los análisis de riesgos en la tecnología de la seguridad de los reactores. Este trabajo trata, principalmente, de este aspecto.

Otra área es la implicación de los análisis de riesgo en las decisiones políticas y, una tercera es su efecto en el público en general. Estos dos últimos se discutirán sólo brevemente.

SIGNIFICADO DE LOS ANALISIS DE RIESGOS EN LA TECNOLOGIA DE SEGURIDAD NUCLEAR

Las centrales nucleares se han construido y licenciado antes de que nadie pensara en realizar análisis de riesgos. Por tanto, el análisis de riesgos no es un pre-requisito para las evaluaciones de seguridad. El proceso de licenciamiento, al menos en lo concerniente a los análisis

Los métodos probabilísticos tratan de cuantificar estas probabilidades. Para hacer esto, se deben estimar las probabilidades de que haya ciertas velocidades de viento o cargas de nieve que sean superadas o que el edificio no resista ciertas cargas. Se debe tener en cuenta las variaciones en la resistencia del acero y del hormigón. Como resultado de todo esto se obtiene la probabilidad de fallo del edificio.

No existe contradicción entre los métodos determinístico y probabilístico. Un profano entenderá más fácilmente la frase: «Este accidente se puede excluir de acuerdo con la experiencia humana», que la afirmación «la frecuencia esperada de ocurrencia de este accidente es más pequeña que 10^{-4} o 10^{-5} , por año». En la realidad, sin embargo, ambas frases describen el mismo estado de cosas.

En este ejemplo, las probabilidades se pueden estimar por medio de una evaluación directa de las estadísticas meteorológicas. Para otras muchas aplicaciones, es necesario aplicar métodos analíticos para calcular, por ejemplo, la falta de disponibilidad de sistemas de seguridad altamente fiables.

Aunque en estos casos, los resultados probabilísticos encierran grandes incertidumbres, pueden permitir en muchos casos un mejor juicio sobre el nivel ganado o de seguridad. La ventaja del método probabilístico se hace incluso más clara cuando se tiene que comparar la seguridad de sistemas diferentes.

La aplicación más consecuente de los métodos probabilísticos se ha hecho en análisis de riesgos. En los Estados Unidos, el «Estudio sobre seguridad de los reactores» WASH-1400, ha presentado por primera vez una investigación de este tipo al público. El objetivo de este estudio ha sido cuantificar los riesgos asociados a los accidentes en reactores de agua ligera. Ha sido publicado en 1975. Posteriormente, grupos contrarios a la energía nuclear han realizado los máximos esfuerzos para rebatir el estudio.

Estas confrontaciones han desembarcado, por parte de la NRC, en la formación de un grupo para la revisión de la evaluación de riesgos. El informe de este grupo, también llamado informe Lewis, ha criticado alguna de las partes del estudio WASH-1400. Sin embargo, al mismo tiempo este informe sugería la inclusión de métodos probabilísticos de una forma más importante en la evaluación crítica y como mejora del proceso de licenciamiento.

Parece que, especialmente el accidente de TMI en marzo de 1979, ha reavivado el interés por el análisis de probabilidad de riesgos. Varias comisiones en los Estados Unidos, que han investigado el accidente, sugieren enfáticamente un aumento del uso del análisis de riesgos de una forma más o menos profunda para treinta centrales nucleares de los Estados Unidos. Básicamente, estos análisis se han realizado utilizando los métodos desarrollados en el

WASH-1400. En algunos casos, se han desarrollado, sin embargo, nuevos métodos, por ejemplo, en la evaluación probabilística de incidentes externos, particularmente en los análisis de los defectos de los terremotos.

También se han realizado análisis de riesgo en otros países. En la República Federal de Alemania se han realizado análisis de riesgos para una central nuclear alemana y para un emplazamiento alemán, inmediatamente después de la publicación del WASH-1400. Para facilitar la comparación con los resultados del WASH-1400, la fase A de este estudio de riesgo alemán, ha utilizado de manera intensiva los métodos del WASH-1400. Los resultados del análisis se publicaron en 1979. Actualmente, las investigaciones continúan en la segunda fase del estudio. Se ha puesto especial interés en una investigación más detallada de las secuencias de los accidentes y en la inclusión de los recientes resultados de la investigación sobre la seguridad. Por ejemplo, se han mejorado los métodos aplicados al análisis de los accidentes con fusión del núcleo y a la determinación de la cantidad de material radiactivo liberado.

Actualmente se están realizando análisis probabilísticos sobre el concepto de un reactor de alta temperatura con las condiciones de un emplazamiento alemán. Los resultados de la primera fase de este estudio se han publicado el año pasado. Sin embargo, no es un análisis de riesgos completo, sino un intento de identificar las contribuciones más importantes a los riesgos por medio del uso de métodos probabilísticos.

Hay unas circunstancias particulares que caracterizan el análisis de riesgo para el SNR-300, prototipo alemán de reactores rápidos reproductores. Este estudio, denominado «Análisis orientado hacia los riesgos», se realizó siguiendo las sugerencias del comité de la energía nuclear, para el futuro de la República Federal Alemana y se terminó en abril de este año. El propósito de este estudio era el tener una comparación pragmática entre los niveles de seguridad del SNR-300 y los de un reactor moderno de agua ligera. Creo que este análisis ha sido el primero que se ha utilizado directamente en el proceso político de toma de decisiones. La situación parece comparable a la del llamado «Estudio Sizewell», realizado en Gran Bretaña. Este análisis de riesgo se ha desarrollado durante la preparación del informe público que, entre otros temas discutirá la seguridad de un reactor de agua a presión, que está proyectado en Sizewell.

Se podría preguntar por qué los análisis de riesgos han encontrado una aplicación tan grande, particularmente en el área de la seguridad de los reactores. Ciertamente, una de las razones es el miedo extendido de que los accidentes en las centrales nucleares pueden producir daños considerablemente mayores que los accidentes en otras industrias.

Aparentemente, el potencial de accidentes en las tecnologías establecidas se juzga de acuerdo con los daños que han ocurrido realmente y éstos se confunden a menudo con los máximos daños posibles.

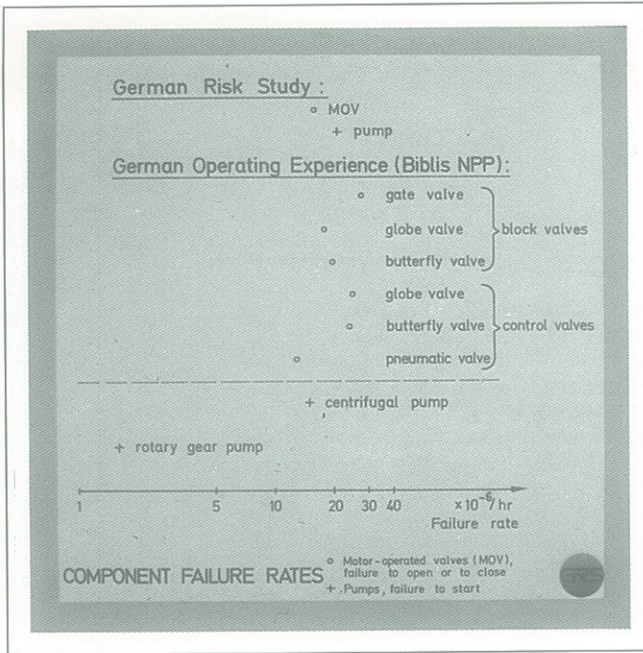
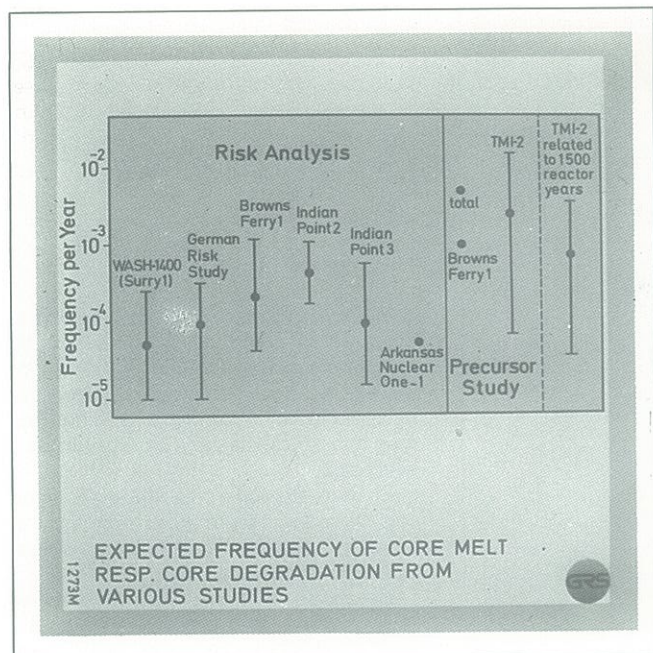
En contraste con esto, la discusión acerca de los peligros de la energía nuclear se concentra mucho más en lo que pudiera haber ocurrido si... La comparación del accidente químico en Seveso y el accidente nuclear en TMI, puede servir de ejemplo: aunque Seveso ha producido una gran preocupación al público, no ha habido apenas discusión acerca de la posibilidad de un daño mucho mayor. En contraste con esto, la discusión pública acerca del accidente de TMI a menudo implicaba que simplemente la suerte había evitado un accidente mucho más grave, habiéndose podido producir daños apocalípticos.

Hay un efecto negativo en el extraordinario récord de seguridad de las centrales nucleares: como hay muy poca experiencia de accidentes, la discusión acerca de los posibles daños está fuertemente influenciada por las especulaciones. Respecto a las evaluaciones técnicas de los sistemas de seguridad, no se puede aprender de accidentes reales. La posible realimentación por medio de la experiencia negativa para realizar mejoras de seguridad, se tiene que reemplazar por investigaciones analíticas de secuencias de accidentes concebibles o posibles, pero que nunca ocurrieron.

En primer lugar, estas investigaciones se pueden restringir a los análisis de ciertas situaciones, para estudiar la influencia de varios sistemas de seguridad sobre la secuencia de accidentes y los daños posibles.

El modelar razonablemente estas situaciones en una evaluación de seguridad sólo es posible si existe algún dato acerca de su frecuencia esperada. Ambas, la investigación de las situaciones de accidente y la estimación de las frecuencias de ocurrencia esperada, son los objetivos de los análisis de riesgo. En este sentido, el análisis de riesgo va más lejos de los criterios habituales de seguridad porque está principalmente interesado en secuencias de accidentes, que son sólo concebibles si se suponen fallos en los sistemas de seguridad.

Si los sistemas de seguridad de una central nuclear funcionan según diseño, no se producirán daños fuera de la central incluso en caso de accidente, ya que el material radiactivo queda retenido. Sólomente se pueden esperar contribuciones significativas al riesgo en el caso de que los mecanismos de seguridad fallen de tal manera que cantidades considerables de materiales radiactivos se liberen al exterior. Esto sólo puede ocurrir si las barras de combustible se dañan de forma severa, si hay fugas en la barrera refrigerante del reactor y si la contención falla. Los análisis de riesgo están principalmente interesados en los casos peores: la fusión del combustible nuclear y los daños que pueden resultar



de este tipo de accidentes. Por tanto, en un primer paso, el análisis de riesgo tiene que investigar los modos y las frecuencias esperadas de los accidentes con fusión del núcleo. A pesar de que el accidente de TMI produjo daños importantes en el núcleo, no se produjo fusión, por lo que estos análisis tienen que basarse en gran medida en investigaciones teóricas.

No creo que los métodos de análisis de árboles de sucesos y árboles de fallo que se usan en los estudios de riesgos se tengan que discutir en detalle en este momento. Lo que haré más bien, será comparar y discutir los resultados de algunos estudios.

La figura 1 muestra los resultados de varios estudios que han estimado la frecuencia esperada de fusión del núcleo o de daño severo al mismo. Además de la media, la varianza y los valores medios de frecuencias estimadas, el gráfico muestra los correspondientes intervalos de confianza del 90 por 100 hasta el límite en que están disponibles. La parte de la izquierda del gráfico muestra las frecuencias de fusión del núcleo, obtenidas por los análisis de riesgos.

El lado de la derecha del gráfico muestra los resultados de un estudio reciente desarrollado en los Estados Unidos, el «estudio precursor». Este estudio ha tratado de extrapolar la frecuencia esperada de daños severos al núcleo debidos a sucesos anormales en centrales nucleares en los Estados Unidos. Apparentemente, hay una discrepancia entre los resultados de las investigaciones analíticas y los resultados obtenidos en el estudio precursor. Esto hace suponer inmediatamente la existencia de contradicciones. Al interpretar análisis de riesgos, se tiene que tener en cuenta las grandes incertidumbres que hay en sus resultados. Sin embargo, las variaciones considerables en las frecuencias estimadas de fusión en el núcleo también indican que las características específicas de

diseño de las plantas son más importantes que lo que se supuso en el pasado. Este punto de vista está también reforzado por la comparación del WASH-1400 y del estudio de riesgos alemán. Ambos estudios determinan las contribuciones principales al riesgo para varias secuencias específicas de accidentes que resultan de las características de diseño de las centrales de referencia.

Para ambas centrales de referencia, las fugas pequeñas contribuyen de una manera importante a la frecuencia de fusión en el núcleo. En Surry 1, la causa principal para esto, fue el fallo aleatorio del sistema de refrigeración de emergencia del núcleo. Para Biblis B, por el contrario, fue el fallo de los sistemas de evacuación de calor secundario, producido por error del operador, que determinó la imposibilidad de realizar la recirculación a baja presión.

En el caso de Surry, el accidente de pérdida de refrigerante fue el principal contribuyente a las frecuencias de liberación que produjeron escapes severos, mientras que en el caso de Biblis B, este accidente fue menos significativo.

Creo que las diferencias en las frecuencias estimadas para las fusiones del núcleo reflejan, en gran medida, los diferentes diseños de las plantas.

La pregunta ahora es, si el estudio precursor no estará demostrando que los resultados de los estudios de los análisis de riesgos son demasiado optimistas.

En este estudio se han evaluado los LER de las centrales nucleares de Estados Unidos desde el año 1969 hasta el 1979, para determinar los sucesos que pueden ser considerados como precursores de los accidentes de daño en el núcleo.

Se han escrutado aproximadamente 19.000 sucesos. Como consecuencia de esto, se han seleccionado 169 para una evaluación más detallada. Estos sucesos han sido analizados utilizando las técnicas del análisis probabilístico de riesgo

para determinar, entre otras cosas la frecuencia esperada total de los accidentes con daños severos al núcleo. Tres sucesos contribuyeron con un 84 por 100 en el resultado final de $4,5 \times 10^{-3}$ por año. El accidente de TMI, por sí sólo, contribuyó el 50 por 100 y el de Browns Ferry, alrededor del 20 por 100.

El accidente de TMI es el único que realmente ha resultado en daño severo al núcleo después de 432 reactor-año de operación en los Estados Unidos.

La frecuencia esperada de fusión del núcleo no puede estar por debajo del inverso de esta cifra. Esto quiere decir que estas estimaciones dependen de manera decisiva de la disponibilidad de experiencia operativa. Si el suceso, como es el caso, ha ocurrido sólo una vez, las estimaciones incluyen incertidumbres muy grandes.

Parece más apropiado considerar los 1.500 reactor-año de operación de todos los reactores de agua ligera del mundo que sólo los 432 de los Estados Unidos. En este caso, la frecuencia esperada de daños severos al núcleo estimada del accidente de TMI, se reduciría en un factor de 3,5 hasta un valor de 7×10^{-4} , por año.

Mientras tanto, el Instituto de Operaciones de Centrales Nucleares (INPO) ha analizado el estudio precursor en Estados Unidos. El INPO determina que, sobre las bases de diseño actual de las centrales nucleares, el estudio precursor ha subestimado la frecuencia de fusión en el núcleo en un factor total de 30.

La razón principal de esto se ha atribuido al hecho de que la fiabilidad de los sistemas no se ha determinado considerando las características de diseño específicas de cada central.

La experiencia ha demostrado que los análisis de riesgo, a pesar de las incertidumbres que existen en todas las cifras estimadas, contribuyen de manera significativa a la mejora de las evaluaciones de seguridad y a un aumento de

la seguridad en las centrales. Esto es particularmente cierto para la parte técnica de las investigaciones, principalmente para la secuencia de sucesos y para los análisis de fiabilidad. Desde luego, también en este campo hay problemas que se hallan, sólo parcialmente, resueltos. Algunos de ellos van a ser discutidos a continuación, a la luz de la experiencia que se ha ganado en el estudio de riesgo alemán.

- Banco de datos para el fallo aleatorio de componentes.

Las incertidumbres en los bancos de datos de los análisis de fiabilidad tienen una considerable influencia en las variaciones de los resultados de los análisis. Estos datos son los que describen la cantidad de fallos en los componentes y la influencia de los trabajos de mantenimiento en la fiabilidad de los mismos.

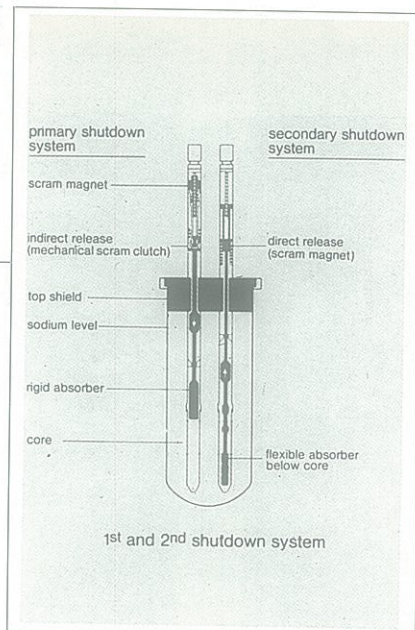
También en el contexto del análisis de riesgos alemán, se ha tratado de aumentar el banco de datos para los fallos de componentes independientes. Se han recopilado y evaluado los datos publicados en la literatura técnica, del mismo modo que se han recogido datos de las centrales eléctricas, es decir, tanto de las centrales nucleares como de las no nucleares.

En la figura 2 se comparan los datos sobre válvulas motorizadas y bombas, incluyendo el arranque del motor y los mecanismos de control usados en el estudio de riesgos alemán y los de la experiencia de operación de la central nuclear de Biblis. Los datos de operación que se muestran para estos componentes, encajan bien con los datos usados en el estudio de riesgos. En algunos casos, la cantidad de fallos se ha subestimado considerablemente.

- Fallos de modo común.

Además de los fallos independientes de los componentes individuales, se tienen que considerar los fallos de componentes redundantes producidos por una causa común.

De manera genérica, estos fallos son conocidos por el nombre de «fallos de modo común». Estudios realizados en los Estados Unidos muestran que las dependencias funcionales no reconocidas entre los componentes redundantes son la causa más importante para los fallos de modo común. Estas dependencias funcionales se pueden evitar en gran manera, por medio de separación funcional y espacial de los sistemas de seguridad redundantes. Las dependencias funcionales restantes se pueden considerar y evaluar por medio de análisis de fiabilidad suficientemente detallados.



Otras causas de los fallos de modo común pueden ser los errores en la planificación, fabricación, operación o mantenimiento. Aunque se tomen las medidas para que no ocurran estos fallos, no se pueden excluir totalmente. Como los fallos de modo común ocurren muy raramente y, si ocurren, se toman medidas para que no se repitan, la cuantificación de la probabilidad de ocurrencia de un fallo de modo común es muy difícil. En el estudio de riesgos alemán se ha tratado de deducir estas probabilidades de la experiencia de operación en las centrales nucleares alemanas.

Los problemas para la evaluación del fallo de modo común han demostrado ser muy importantes en los análisis de riesgos del SNR-300.

En el SNR-300, el calor de desintegración se puede evacuar por medio de la convección natural, incluso después de un fallo total de todos los componentes activos como bombas o ventiladores. Debido a las características del sistema, como baja presión del refrigerante, es muy improbable que una fuga en la barrera de presión del primario resulte en una pérdida de refrigerante significativa.

El SNR-300 está equipado con dos sistemas de parada que son redundantes y diversos hasta un grado muy alto. Cada uno de estos dos sistemas es a su vez redundante y está actuado por su propio sistema de protección del reactor. El diseño particularmente fiable de los sistemas de parada rápida (scram) considera el hecho de que un fallo en el scram del reactor rápido reproductor podría producir una excursión de potencia con la subsiguiente destrucción del núcleo.

Debido a la capacidad de evacuar el calor residual de forma pasiva y debido también al alto grado de redundancia y diversidad en el diseño de los sistemas de parada rápida del reactor, la destrucción del núcleo producida por fallos de

componentes independientes es extremadamente improbable. Se obtendría una probabilidad de fallo de 10^{-10} por actuación de los sistemas de parada rápida, incluso utilizando unos métodos muy conservativos en la evaluación probabilística.

En esta situación, los fallos de modo común son decisivos para prejuzgar la fiabilidad del sistema, aunque no se encuentren causas concretas.

Utilizando métodos muy pesimistas, se ha obtenido una probabilidad de fallo de 10^{-7} por actuación de los sistemas de parada rápida del SNR-300. Más del 99 por 100 de esta cifra viene de los fallos de modo común.

Los problemas que se han encontrado al realizar esta evaluación, se ilustran en la figura 3.

Para el SNR-300, hay un factor de 10^{-7} entre la frecuencia de los iniciadores principales de accidente, en este caso la suma de todos los transitorios de operación y la frecuencia de destrucción del núcleo. Para los fallos de evacuación del calor de desintegración, esta cifra es incluso más pequeña. Puede ser, sin embargo, subdividida en un fallo de $2,5 \times 10^{-6}$ para los sistemas activos y de 10^{-2} para los sistemas pasivos de evacuación de calor residual. Para los reactores de agua a presión, el factor entre la frecuencia esperada de una fuga pequeña como accidente iniciador y la fusión del núcleo es de 2×10^{-4} , para cada actuación. El fallo de los sistemas diseñados para mitigar la pérdida de agua de alimentación es de alrededor de 4×10^{-6} . Sin embargo, en este caso se ha supuesto que los suministros normales de energía eléctrica están disponibles, ya que la pérdida de la energía eléctrica exterior se ha considerado de forma separada.

Para las secuencias de accidentes más importantes, los fallos de los sistemas en el SNR son más bajos que en el caso de un reactor de agua a presión, al menos en un factor de alrededor de 10^{-3} . Bajo estas circunstancias, es obvio que las incertidumbres obtenidas en el estudio SNR-300 tienen que ser considerablemente mayores que en el estudio de riesgos de los reactores de agua a presión. Con fallos de 10^{-7} por actuación se alcanzan algunos límites en los análisis de fiabilidad. En el caso de probabilidades tan pequeñas, las probabilidades de fallos de componentes pasivos deben también de considerarse. La determinación empírica y analítica parece más difícil que la determinación de las probabilidades de fallo de los componentes activos.

Mannesmann presente en la construcción de Centrales Nucleares

Sta. M.^a de Garoña

Nuevos sistemas de tuberías

Ascó I y II

Circuitos primarios

Lemóniz I y II

Circuitos primarios

Almaraz I y II

Circuitos primarios

Vandellós I y II

Sistemas de tuberías (3.200 ton.)
componentes de soportes

Trillo I y II

Plantas llave en mano de:
Pretratamiento de Agua Bruta
Desmineralización Agua de
Aportación
Tratamiento de Vertidos Químicos
Desmineralización de Purgas de
Condensadores
Tratamiento de Residuos Radiactivos

Domicilio Social:

Conde de Peñalver, 45, 1.^o
Apartado 50.555 MADRID-6
Teléf.: 401 01 04
Telex 44193 MIIR-E

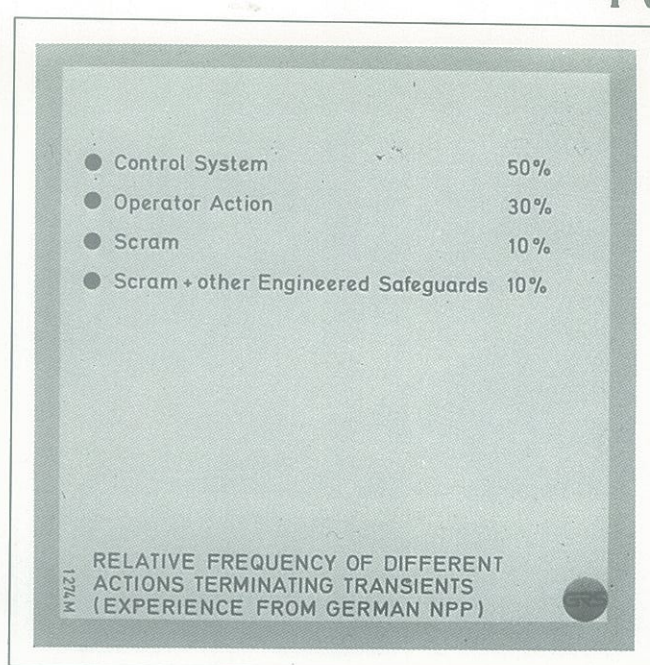
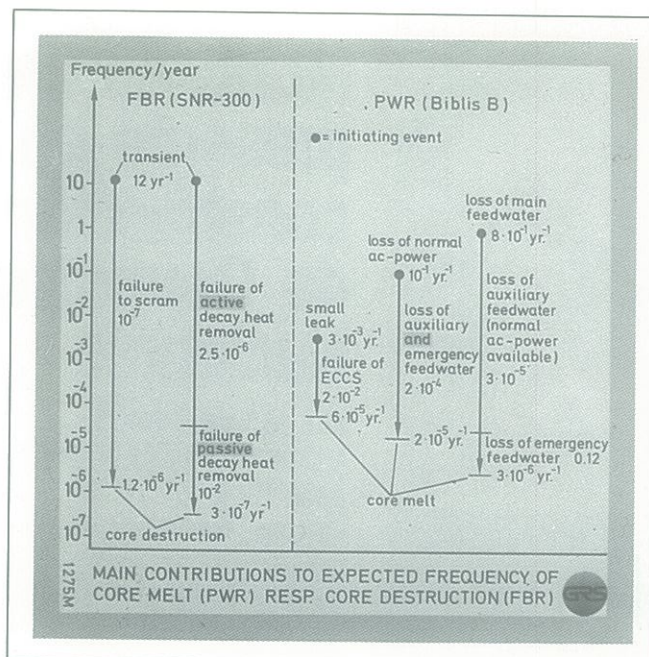
Fábrica:

Km. 16.500 Ctra. Madrid-Barcelona
San Fernando de Henares
Madrid



MANNESMANN

INDUSTRIA IBERICA S.A.



Errores humanos

Las experiencias de operación y los análisis de riesgos muestran que los errores humanos pueden contribuir de forma significativa al riesgo en las centrales nucleares.

Los errores de los operadores durante la operación normal pueden producir transitorios. Los errores de mantenimiento y los errores de los operadores después de la iniciación de un accidente, pueden hacer que su control sea más difícil.

Es particularmente difícil evaluar la fiabilidad humana para controlar las perturbaciones y los accidentes de forma cuantitativa. La importancia de la influencia humana en la terminación de un transitorio se puede ver en la lista siguiente. Esta lista indica las fracciones relativas de las acciones que han controlado los transitorios con éxito, de acuerdo con la experiencia:

50 por 100 por medio de los controles y las limitaciones.

30 por 100 por medio de acciones del operador.

10 por 100 por medio de la parada rápida del reactor (scram).

10 por 100 por medio de la parada rápida del reactor y otras acciones del sistema de seguridad.

El relativamente alto tanto por ciento de los casos en que los transitorios se han terminado por medio de las acciones de operador, demuestra la gran flexibilidad del personal de operación.

En el estudio alemán de riesgos, sólo se han considerado los errores humanos en el control de las perturbaciones de los accidentes que podrían derivarse de las probabilidades por el fallo de las acciones manuales descritas en el manual de operación. Las acciones manuales no planificadas que pueden afectar la secuencia del accidente de una forma favorable o desfavorable, no se han cuantificado. La experiencia muestra que en

la mayoría de los casos, el personal de operación ha identificado correctamente la situación durante las ocurrencias anormales. En este caso, esto significa que si se ha elegido la estrategia apropiada para la terminación del accidente, los errores tácticos, como empujar el botón incorrecto, tienen una importancia pequeña. En la mayoría de los casos, estos errores son identificados por el sistema de control y hay suficiente tiempo para corregirlos.

Las acciones que se deben llevar a cabo de forma rápida, en general, son iniciadas y controladas por sistemas automáticos.

A pesar de esto, la contribución más importante al riesgo en el estudio alemán, vino de los errores de operación durante el control del accidente. Las acciones manuales específicas requeridas al equipo de operación en el caso de la planta de referencia, han sido muy complicadas y largas. Consecuentemente, estas acciones manuales (enfriamiento de 100°K/h , activación de los sistemas de emergencia de agua alimentación) han sido reemplazados por sistemas automáticos. Por tanto, la evaluación de estas acciones no causará problemas significativos a las centrales nucleares de diseño actual.

Además de la fiabilidad de los sistemas de seguridad, un análisis de riesgos tiene que investigar las secuencias de los accidentes que se producirían en caso de fallo de estos sistemas. Esto no puede llevarse a cabo sin simplificaciones. En casi todos los análisis de secuencias de accidentes, ha de suponerse en cuanto a los sistemas que o bien están funcionando o que han fallado totalmente. Fallos parciales han de ser tratados como fallos totales. Análisis más detallados de secuencias de accidentes y la consideración de la dependencia del tiempo, producirían una cantidad de trabajo adicional considerable.

Las simplificaciones importantes que

se tienen que hacer en los estudios de riesgos están ilustradas en la figura 4. Partiendo de un número representativo de sucesos iniciadores, se estudian en detalle varias secuencias de sucesos y se determinan las probabilidades de fallo de los sistemas de seguridad que son necesarios para el control de los accidentes.

Esta parte del análisis se describe de forma esquemática en la parte superior del gráfico.

La gran cantidad de secuencias de sucesos que dependen del funcionamiento correcto o no del sistema de seguridad requerido, está clasificado de una forma basta. Excepto en el caso de fallos en la vaina del combustible, el estado del núcleo del reactor se considera o como intacto, o como totalmente fundido. En el estudio de riesgos alemán, como en otros estudios, se supone de antemano la fusión total del núcleo en el caso de que los requerimientos relativos a la efectividad de los sistemas de seguridad, de acuerdo con el proceso de licenciamiento, no se cumplan.

Los estudios de riesgos han reconocido la necesidad de distinguir estados intermedios entre el del núcleo suficientemente refrigerado y el de fusión total, particularmente en relación con los análisis de los accidentes de pequeñas fugas. La descripción de las secuencias de este accidente requiere modelos que permitan el cálculo de la extensión de los daños al núcleo, dependiendo de las condiciones de refrigeración del mismo.

El accidente de TMI ha reforzado la importancia de estas investigaciones. Durante el accidente, el núcleo se calentó hasta temperaturas a las que las guías de las varillas de combustible fallaron y los elementos combustibles de la parte superior del núcleo se destruyeron.

Para describir las cargas en la contención de una forma más realista, es necesario un análisis más detallado de las

secuencias de accidente que conducen a daños en el núcleo, o incluso a la fusión del mismo. De nuevo, el accidente de TMI ha demostrado que la contención es una barrera muy importante para la actividad. Aunque cantidades considerables de materiales radiactivos se liberaron del combustible a la contención, sólo una pequeña cantidad se escapó a la atmósfera.

Los análisis de riesgos realizados hasta ahora, han analizado las secuencias de los sucesos que producen daños en el núcleo de la misma forma que los accidentes de fusión que producen un fallo en la contención. En contraste con esto, la contención se puede ver como una barrera independiente, siempre y cuando se pueda evacuar el calor residual del núcleo dañado.

La parte inferior del gráfico muestra los modos de fallo de la contención considerados hasta ahora en los análisis de riesgo de los reactores de agua a presión. Estos análisis requieren la evaluación de las probabilidades de fallo. Esta evaluación incluye la investigación de varios procesos físicos, que son importantes en el transcurso del accidente. Las incertidumbres en los modelos usados que influyen a la incertidumbre de los resultados se pueden estimar sólo de forma muy basta.

La liberación de cantidades importantes de material radiactivo es sólo posible si la contención falla desde el principio del accidente. En este contexto, se ha progresado últimamente de un modo considerable en la evaluación de las explosiones de vapor. Una secuencia de accidente que lleve a un fallo inmediato de la contención debido a la explosión del vapor, es muy improbable. Los experimentos y las investigaciones teóricas han demostrado que la probabilidad de tal secuencia de accidentes es considerablemente más pequeña de lo que se había supuesto en el WASH-1400 y en el estudio de riesgos alemán. Algunos expertos, incluso afirman que se puede excluir la posibilidad de una explosión de vapor que pueda poner en peligro la integridad de la contención.

De acuerdo con los resultados del estudio de riesgos alemán, la secuencia de accidente más probable que lleva al fallo de la contención, se debe a la sobrepresurización, un día después de la iniciación del accidente. Investigaciones recientes llevadas a cabo en la fase B del estudio, han demostrado que sólo se debe esperar el fallo en la contención debido a la sobrepresión, después de 3 ó 4 días. Esta mejora sobre los resultados de la fase A del estudio, se debe princi-

palmente a un mejor modelado de la transmisión de calor entre el núcleo fundido y el hormigón en la última fase del accidente de fusión del núcleo.

Los cálculos de liberación de esta secuencia de accidente muestran que la mayor parte de los materiales radiactivos originados por el núcleo fundido, quedan retenidos dentro de la contención debido al proceso de laminación, antes del fallo de la misma por sobrepresión.

En el contexto del análisis de riesgo se ha discutido la conveniencia de la instalación de sistemas adicionales de seguridad. Tales sugerencias tienen que ser comprobadas cuidadosamente, ya que conceptos adicionales de diseño podrían poner en peligro el funcionamiento de los sistemas de seguridad ya existentes. El accidente de TMI demostró que los sistemas de seguridad pueden funcionar incluso cuando los límites de diseño se han excedido. Sin embargo, se debe conceder una gran importancia a las medidas preventivas que están diseñadas para evitar las secuencias del accidente, que lleva al daño en el núcleo.

Son muy recomendables las posibles mejoras para orientar a los operadores durante un accidente, especialmente las que muestren muy claramente el estado de la planta.

Las discusiones acerca de los análisis de riesgos, a menudo plantean la pregunta de si se han considerado las incidencias importantes y todas las secuencias de accidente que son significativas para el riesgo. En principio, de manera inductiva, no hay posibilidad de demostrar que los análisis son completos.

Por tanto, se tiene que confiar en los análisis sistemáticos y en la experiencia y el conocimiento de los analistas.

Para juzgar si los análisis son o no completos, es importante comparar continuamente las investigaciones teóricas y la experiencia práctica de operación, para comprobar si hay secuencias de accidente importantes que se hayan despreciado y para ver si los nuevos resultados requieren una corrección de los análisis.

Particularmente, este problema de la evaluación de los fallos de modo común y el de la influencia de los errores humanos son los responsables de que algunas personas vean los análisis de fiabilidad y de riesgos más como un arte que como una ciencia. Evidentemente, el buen juicio y la intuición de los analistas son una parte muy importante en estos análisis.

A pesar de estos problemas, el análisis de riesgos constituye una herramien-

ta importante para la evaluación de seguridad, si se aplica apropiadamente. Esto es particularmente cierto para los análisis de los sistemas de seguridad.

Los análisis de fiabilidad probabilística permiten un mejor juicio sobre los diseños importantes para la seguridad que los análisis de fiabilidad, basados en criterios determinísticos. Aun así el criterio de fallo simple, en su uso normal, está basado también en consideraciones probabilísticas: el fallo independiente de un componente individual se considera como un fallo creíble; se excluye, sin embargo, el fallo simultáneo de dos componentes fiables. Esto se hace, no obstante, sin cuantificar la fiabilidad real de los diferentes componentes. Se supone que van a fallar de la misma forma un componente fiable probado frecuentemente que un componente menos fiable y difícil de probar. Los análisis de fiabilidad probabilística permiten juzgar mucho mejor la influencia de los componentes individuales en la falta de disponibilidad del sistema.

Un análisis de fiabilidad extensivo también hace posible el considerar las interacciones de varios sistemas. La experiencia demuestra que los problemas aparecen con frecuencia en las interfaces entre los diferentes sistemas y donde se solapan las distintas ciencias. Este tipo de problemas son mucho más fácilmente identificables en los análisis de riesgos que en las investigaciones de seguridad determinísticas.

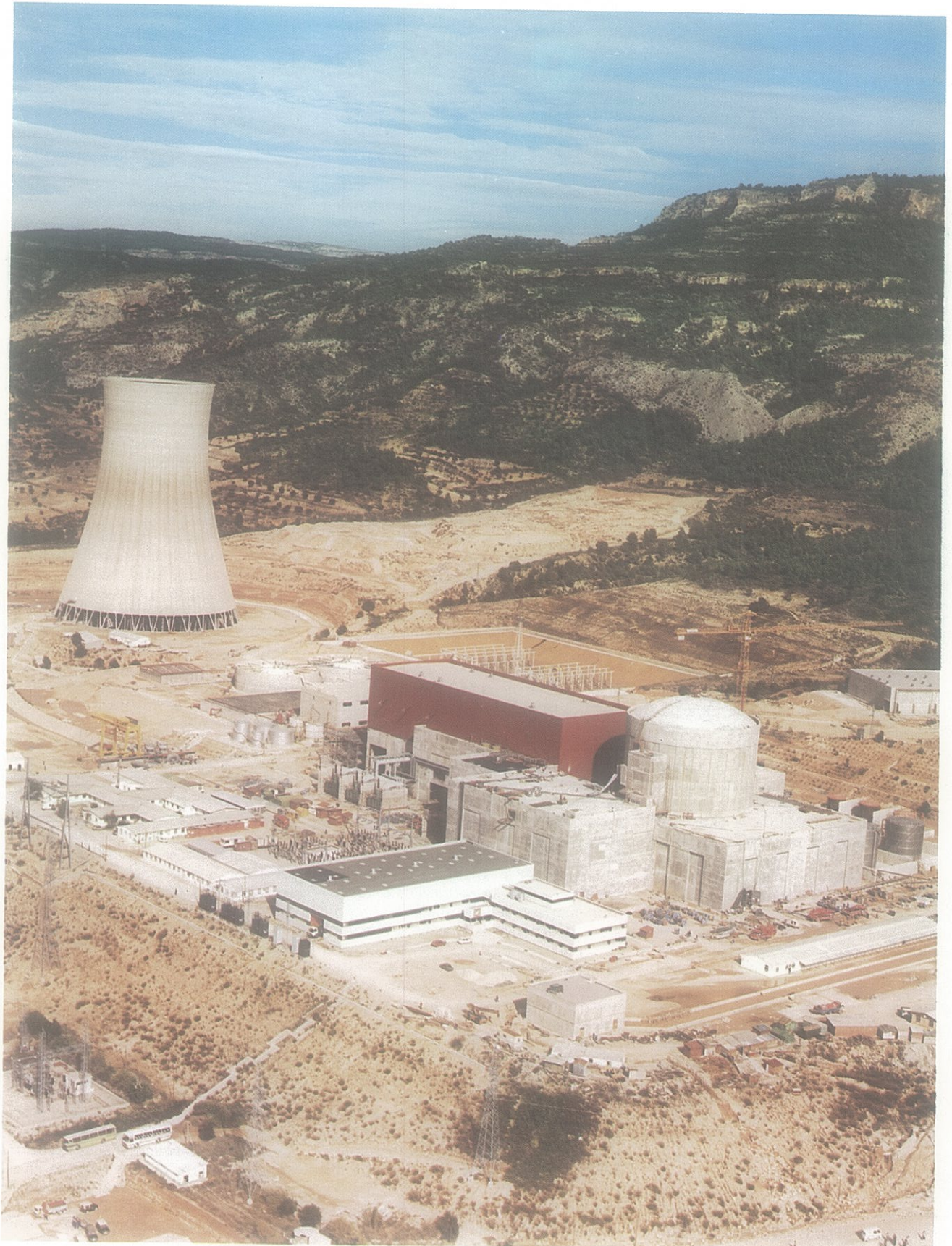
Los análisis de fiabilidad sobre las interfaces de sistemas permiten un mejor juicio sobre la importancia para la seguridad de los diferentes sistemas. Por ejemplo, el estudio alemán de riesgos ha llegado a la conclusión de que el sistema secundario es de considerable importancia en el control de transitorios y de fugas pequeñas. Por tanto, la distinción en una central entre parte nuclear y convencional, no es razonable desde el punto de vista de la seguridad.

El utilizar los análisis de fiabilidad puede también determinar en qué situaciones las acciones manuales son importantes para el control de los accidentes. Se puede entonces decidir si tales medidas se deben automatizar. Sin embargo, estas decisiones pueden ser difíciles en algunas ocasiones.

La secuencia de acciones automáticas se debe orientar de acuerdo con las trayectorias predeterminadas para los accidentes. Para esto, se necesita investigar si puede ocurrir una secuencia de accidente tal que produzca una actuación del sistema automático de forma incorrecta.

DURO-FELGUERA

DIVISION MONTAJES



C.N. Cofrentes

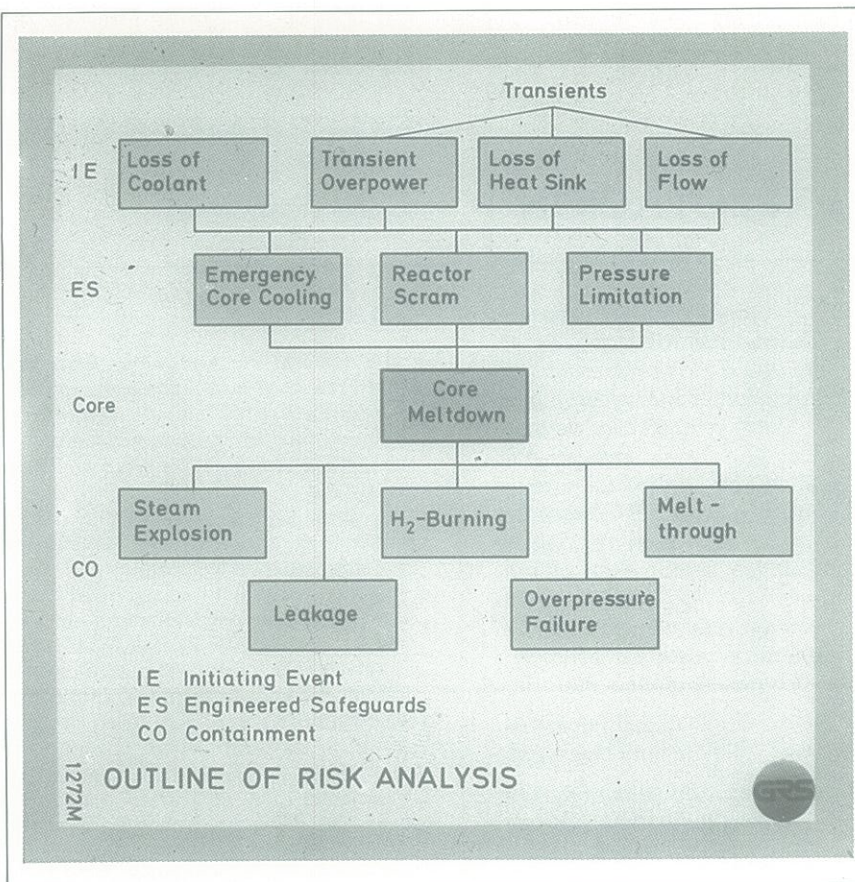
Este caso se ha encontrado en el estudio alemán de riesgos en el análisis de transitorios anticipados sin scram. En estos transitorios, se supone un fallo del sistema de parada por barras (scram) del reactor. Ahora se ha reconocido que las válvulas de control del sistema de agua de alimentación principal a los generadores de vapor, cerrarán tan pronto como se produzca el disparo del reactor por el sistema de protección, aunque el scram falle mecánicamente.

Las investigaciones sobre los sistemas automáticos de operación han demostrado que en estos casos también cerrarán las válvulas auxiliares de control. Por tanto, no hay control sobre el caudal de agua de alimentación, y la terminación del transitorio anticipado sin scram, será más difícil. En este ejemplo, la actuación automática de los componentes de los sistemas operativos influye sobre componentes importantes a la seguridad que se necesitan para el control de los accidentes. La modificación de los sistemas de operación automáticos diseñados para una operación más fácil de la central, puede de forma no intencional afectar al control de los accidentes.

Para aumentar la aplicación de los métodos probabilísticos, es muy importante realzar evaluaciones intensivas de la experiencia de operación. Ayudará a aumentar el banco de datos de los análisis de fiabilidad de componentes y de los sistemas. También puede servir para comprobar la lista de los sucesos considerados como iniciadores y para complementarlos, si es necesario. Es importante la investigación de las experiencias de operación en lo concerniente a perturbaciones ocurridas en la realidad, que pueden causar accidentes severos. Aunque el estudio precursor desarrollado en los Estados Unidos muestra que los resultados cuantitativos basados en las experiencias de operación disponibles en el presente, están sujetos a incertidumbres, estas experiencias pueden servir para afirmar y suplementar los análisis teóricos, particularmente si se han realizado para una central específica.

Además de para las evaluaciones de seguridad, como se ha discutido arriba, los métodos probabilísticos también se pueden utilizar para comprobar el diseño de la planta en función de los objetivos cuantitativos de seguridad. Las propuestas para tales objetivos se discuten ahora en todo el mundo.

Debido principalmente a las incertidumbres en los datos y también en los modelos, se debe tener mucha precaución cuando se trate de substituir o de



complementar las evaluaciones de seguridad determinísticas por los métodos probabilísticos.

CONCLUSIONES

Concluyendo, se han mencionado las ventajas y los inconvenientes de los análisis de riesgos en el área política y sus efectos en el público.

El análisis de riesgos puede ser muy importante en el contexto de las decisiones políticas, por ejemplo, en la utilización de nuevas tecnologías. Sin embargo, parece haber más limitaciones que en el área de análisis de sistemas técnicos.

Por una parte, el riesgo asociado con la utilización de una tecnología nueva, es sólo un aspecto de los muchos que se tienen que considerar al tomar decisiones políticas. Además, la mayor parte de los políticos no son capaces de apreciar o evaluar los métodos y las hipótesis que se utilizan para la obtención de los resultados de los análisis de riesgos. **Por tanto, deben de confiar en el juicio de los expertos, por lo que la situación no difiere esencialmente de la situación existente con las evaluaciones clásicas de seguridad.**

Para finalizar, algunas observaciones sobre las posibles influencias de los análisis de riesgos en la opinión pública.

Existe la evidencia de que la opinión pública sobre la energía nuclear no está influida de una forma importante por los resultados de los análisis de riesgos. Por un lado, los problemas de seguridad no son puntos clave para el rechazo o la aceptación de la energía nuclear. Además, los análisis de riesgos, informan al público para que tome conciencia de que los daños que se producen por los accidentes nucleares, no se pueden excluir. Aunque también se muestra que las probabilidades de estos daños, son extremadamente pequeñas. Es difícil, no obstante, dejar claro el significado de probabilidades tan pequeñas.

Del mismo modo, una evaluación extensiva tecnológica, no debe quedar limitada a la investigación de las consecuencias negativas de esta tecnología. Además de los peligros, las ventajas no deben ignorarse. Hoy, creo que no está dándose suficiente importancia a este aspecto. Algunos argumentos parecen implicar que las tecnologías sólo sirven para propósitos de autosatisfacción, y que sus riesgos son, básicamente, inaceptables. El problema principal, sin embargo, es mantener un equilibrio entre los riesgos naturales y los riesgos causados por la civilización, a un nivel tan bajo como sea posible. Nadie puede seriamente negar que la ciencia y la tecnología han contribuido de forma significativa a reducir los peligros y el riesgo para los seres humanos y para el medio ambiente.