UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

Facultad de Química

División de Estudios de Postgrado

Aplicación de la Teoría de la Confiabilidad al Diseño y Construcción de Plantas Nucleares de Potencia

T E S I S

Que para obtener el grado de:

MAESTRIA EN CIENCIAS NUCLEARES

P r e s e n t a :

Julio Fournier González

1982

I N D I C E

F I G U R A S

RESUMEN

En la aplicación de la teoría de la confiabilidad al problema de la seguridad de las plantas nucleares de potencia se consideran tres clases de confiabilidad :

Confiabilidad intrínseca
Confiabilidad operacional
Confiabilidad humana

Se postula la existencia de defectos y errores humanos remanentes de concepto, diseño, manufactura, construcción, instalación y pruebas como origen de configuraciones anómalas ocurridas en la explotación del sistema planta-operador al encadenarse con eventos transitorios con probabilidad de causar eventos indeseables a través de mecanismos que se han tratado de identificar en este trabajo.

Se discuten algunas características de los reactores de potencia de agua ligera y de alta temperatura enfriados por gas desde el punto de vista de la vulnerabilidad a la formación de configuraciones anómalas.

Se describen conceptualmente sistemas avanzados no existentes aún, de respaldo a la función humana del operador, como medio de disminuir las probabilidades de ocurrencia de eventos indeseables .

Se discute la información reciente y se presentan, a modo de conclusión, sugestiones finales de acuerdo a las condiciones de nuestro país.

Se incluye como anexo, la postulación de la existencia de defectos remanentes en los proyectos nucleoeléctricos.

1. INTRODUCCION

1.1. INTRODUCCION

Desde que el hombre aprendió a utilizar materiales para realizar sus objetivos, aprendió también a seleccionar y alterar los materiales para adecuarlos a casos específicos.

Todas aquellas características, propiedades y cualidades de materiales alterados por el hombre y de los artefactos construídos con ellos para usos específicos, pueden englobarse en el concepto "calidad".

La calidad de un material o de un artefacto se juzga en el grado en que sea adecuado para su uso específico, precisamente desde el punto de vista del usuario, no a juicio del diseñador, ni del fabricante ni del vendedor.

Si se establecen determinados requerimientos que deben cumplir en forma general determinada clase de artículos o sea se establecen normas, el proceso a través del cuál se intenta cumplir con esas normas se llama "un proceso de control".

Cuando este proceso de control se aplica en la fabricación de productos para cumplir con las normas de calidad especificadas se llama "control de calidad".

El Control de Calidad en la fabricación, es el proceso regulador a través del cuál se miden las características, propiedades y cualidades del producto en forma directa o indirecta mediante inspecciones, mediciones y pruebas destructivas y no destructivas para verificar que es adecuado para el uso especificado, se hacen comparaciones con las normas establecidas y se actúa en --

las diferencias.

En el Control de Calidad se aplican metodologías de la Estadística para planear los muestreos, intervalos y puntos de medición en las etapas y líneas de la producción masiva de la industria moderna.

En determinados productos, por las exigencias especiales de su uso, se requiere además la constatación de la calidad en forma similar a la auditoría financiera, conocida en inglés como "Quality Assurance", traducida al español como "Garantía de Calidad" y es la actividad de proporcionar, a todos a quienes concierne, la evidencia necesaria para establecer la confianza de que la función del Control de Calidad se ha realizado en forma adecuada.

El interés principal de los usuarios del producto es obtener la máxima efectividad de su uso. Desde este punto de vista se ha desarrollado la Teoría de la Confiabilidad que estudia la regularidad general que deben mantenerse durante el diseño, experimentación y manufactura, aceptación y uso de componentes y sistemas para obtener la máxima efectividad de uso.

Esta nueva disciplina principió a utilizarse durante la segunda guerra mundial en el diseño y fabricación de las bombas V-1 y V-2 lanzadas por Alemania. Actualmente, ya en pleno desarrollo, se emplea en forma extensa en las industrias de defensa, aeroespacial, electrónica y de computadoras.

De acuerdo con los Criterios Generales de Diseño establecidos como normas a las Plantas Nucleares de Potencia se aplica esta Teoría a la determinación de la confiabilidad y verificación de los sistemas de protección del Reactor.

12 OBJETIVO

El propósito de este trabajo, definido antes de los acontecimientos de la Planta Nucleoeléctrica Three Mile Island cercana a Harrisburg, Pa., USA, es mostrar el estado actual del arte sin circunscribirse a las aplicaciones probabilísticas ya realizadas extensivamente y a partir de las definiciones básicas de la Teoría de la Confiabilidad; se considera a la Planta Nucleoeléctrica y al personal que la opera, combinados en un sistema para tratar de encontrar direcciones para la búsqueda de soluciones al problema de la Seguridad de la Industria Nuclear.

1.3 JUSTIFICACION

Actualmente está en proceso de construcción la primera Planta Nucleoeléctrica de nuestro país. Iniciará su operación comercial en la primera mitad de la década de los 80's y alcanzará la mitad de su vida económica en el año 2000.

En ese año las dos terceras partes de la energía eléctrica que se producirá en México serán generadas por plantas termoeléctricas que queman hidrocarburos y por nucleoeléctricas que consumen uranio a las que el Plan de Energía de México asigna una capacidad probable de 20,000 MWe. (referencia 1).

La instalación de 20,000 MWe nucleares en nuestro país, improbable en la situación actual, está supeditada, además, al restablecimiento en el ámbito internacional de la competividad de las plantas nucleoeléctricas perdida en algunos paises por las circunstancias que se comentan y discuten en este trabajo.

Por supuesto todas las Plantas Nucleoeléctricas deberán cumplir con todos los requisitos y criterios de seguridad que establez-

can los organismos autorizados para regular el uso pacífico de la energía nuclear y ser confiables en todos los aspectos del - diseño, la construcción y la operación para que sean seguras y productivas.

Desde este punto de vista se justifica discutir la aplicación - de la Teoría de la Confiabilidad al Sistema Operador-Planta Nucleoeléctrica.

2. EL PROBLEMA DE LA SEGURIDAD

Durante la operación de un Reactor de fisión controlada de cualquier tipo, se genera un inventario de materiales radioactivos producidos por las fisiones de núcleos y por la activación de - materiales que capturan neutrones.

Parte de este inventario comprende materiales que, por tener vidas medias largas, por producirse en cantidades apreciables y - por sus características químicas, pueden amenazar la salud pública si se liberan a la biósfera, por lo que deben mantenerse confinados mediante artificios de contención; la integridad de estos artificios es amenazada a su vez por la energía liberada - por los materiales radioactivos que se degrada a calor de decaimiento por lo que debe protegerse mediante artificios de enfriamiento y para mitigar las consecuencias de pérdida de integridad de la contención se proveen diversos artificios adicionales y medidas de emergencia.

A este efecto, desde el inicio del uso pacífico de la energía - nuclear se ha desarrollado una filosofía de seguridad, única -- por su consistencia, aplicada internacionalmente para salvaguardar la salud pública y se han establecido disposiciones legales

para el diseño, construcción y operación de Plantas Nucleoeléctricas.

Los procedimientos actuales de Licenciamiento de Plantas Nucleoeléctricas se caracterizan por suposiciones conservadoras y márgenes adicionales de seguridad; predominan los análisis determinísticos de accidentes y eventos postulados con apoyo adicional en análisis probabilísticos del comportamiento de los sistemas relacionados con la seguridad basados en las técnicas de confiabilidad ya incorporadas en los códigos y normas establecidas específicamente para Plantas Nucleoeléctricas, como son los análisis de modos y efectos de fallas en formas cualitativa y cuantitativa, árboles de fallas, diagramas de bloques y fallas funcionales en modo común en condiciones normal de transitorios y de accidentes (referencia 2).

En el diseño y cálculo se consideran los factores del sitio tales como sismicidad, meteorología, hidrología, geología, densidad de población y otros. Se establecen los parámetros seguros de operación, se implementan sistemas de seguridad física, procedimientos administrativos, procedimientos contra sabotaje y planes de emergencia. Se documentan los análisis de seguridad, la constatación de la calidad de la fabricación y construcción y los procedimientos de operación, mantenimiento, inspección en servicio y auditorías de seguridad.

Se capacita teóricamente al personal de operación y se le entrena prácticamente en simuladores y Plantas reales antes de obtener la calificación y licencia de operación.

Estos procedimientos y otros no mencionados han permitido llegar al estado actual de la explotación comercial de Plantas Nucleoeléctricas sin lesión directa de personas del público pero

sin evitar, en casos aislados, daño serio al equipo, pérdidas de generación, serias pérdidas económicas y, como consecuencia de haber ocurrido liberación no controlada de productos de fisión a la biósfera en el evento TMI-2 del 28 de marzo de 1979, pérdidas de confianza en los procedimientos y mecanismos de seguridad tal como fueron utilizados hasta esa fecha (ref. 3).

3 TEORIA DE LA CONFIABILIDAD

3.1 DEFINICIONES BASICAS

De acuerdo con B.V. Gnedenko se define: "La Teoría de la Confiabilidad es la nueva disciplina científica que estudia la uniformidad general que debe mantenerse durante el diseño, experimentación, manufactura, aceptación y uso de componentes y sistemas para obtener la máxima efectividad de su uso" (referencia 4).

De acuerdo con la Arinc Research Corporation el concepto Confiabilidad se define:

"La Confiabilidad es la probabilidad de que el Sistema considerado se comportará satisfactoriamente cuando menos por un período dado de tiempo cuando se usa bajo condiciones especificadas" (referencia 5).

Por Sistema entendemos lo que el Webster Collegiate Dictionary define como: "Elementos de interacción e interdependencia regulares que forman un todo unificado" (referencia 6).

3.2 RELACIONES FUNCIONALES

Representamos la probabilidad de comportamiento satisfactorio, o

sea la confiabilidad mediante R(t) y la tasa o razón de falla - mediante h(t).

De acuerdo con las leyes de la probabilidad definimos un evento E compuesto de dos subeventos independientes E_1 y E_2.

E_1: No ocurre falla antes del tiempo t.

E_2: No ocurre falla entre el tiempo t y el tiempo t + dt

E: No ocurre falla antes del tiempo t + dt

Como E es un elemento compuesto, de acuerdo con la ley del producto de probabilidad tenemos:

$$Pr\ (E) = Pr\ (E_1) \cdot Pr\ (E_2) \quad (1)$$;

sustituyendo los símbolos de las probabilidades tenemos puesto que:

$$R\ (E_2) = 1 - h\ (t)\ dt \quad (2)$$

$$R\ (t+dt) = R\ (t)\ [1-h\ (t)\ dt] \quad (3)$$

o sea:

$$d\ R\ (t) = -\ R\ (t)\ h\ (t)\ dt \quad (4)$$

que nos da:

$$h\ (t) = \frac{-\ d \ln (R(t))}{dt} \quad (5)$$

y resulta:

$$R\ (t) = e^{-\int_o^t h(t)\,dt} \quad (6)$$

Se ha observado experimentalmente en ciertos componentes que - la razón de falla h (t) es alta al principio de su vida útil y

disminuye a un valor constante al terminar el periodo llamado - de asentamiento, este valor constante se conserva hasta llegar al periodo de desgaste o vejez en que la razón de falla aumenta rápidamente, la relación funcional (6) es aplicable en todo --- tiempo de la vida del componente. En el periodo medio cuando - la razón de falla es constante la ecuación (1) toma la forma

$$R(t) = e^{-\lambda t} \qquad (7)$$

en la que λ representa a la razón constante de falla.
La ecuación (7) indica la probabilidad de funcionamiento satisfactorio en el período de tiempo de 0 a t con una razón constante de falla.

La probabilidad de falla en el período de tiempo de 0 a t sería:

$$f(t) = 1 - R(t) = 1 - e^{-\lambda t} \qquad (8)$$

Tomando la primera derivada tenemos:

$$F'(t) = f(t) = \lambda e^{-\lambda t} \qquad (9)$$

que es la función exponencial de densidad de falla.

Si se desarrolla en serie la forma exponencial de la confiabilidad tenemos:

$$R(t) = e^{-\lambda t} = 1 - t + \frac{(t)^2}{2!} - \frac{(t)^3}{3!} + \ldots \qquad (10).$$

Para valores pequeños de λt podemos considerar que:

$$R(t) \approx 1 - \lambda t \qquad (11)$$

Se han establecido programas para recoger y sistematizar esta - dísticamente la información experimental y en condiciones de -- operación real del comportamiento de componentes para consti --

tuir bancos de información sobre confiabilidad en constante crecimiento, principalmente en aplicaciones militares y espaciales.

A la fecha, existe para aplicaciones nucleares el Sistema NPRDS (Nuclear Plant Reliability Data System) del Edison Electric Institute (referencia 7).

3.3 CONFIABILIDAD INTRINSECA

Con la información experimental es fácil calcular las confiabilidades de componentes simples y determinar tiempos de sustitución antes de falla, vida útil, etc.

Para cuantificar la confiabilidad de sistemas simples los cálculos son comparativamente simples, pero al aumentar el número de componentes en el sistema los cálculos crecen desmesuradamente en complejidad. Naturalmente esto ha dado lugar a una enorme cantidad de literatura sobre métodos para cuantificar la confiabilidad tales como árboles de fallas, tablas lógicas, análisis Monte Carlo, síntesis de circuitos, diagramas lógicos, hasta llegar al establecimiento de guías y normas aplicables al análisis de la confiabilidad de los sistemas de protección de plantas nucleoeléctricas.

Los análisis de confiabilidad no se limitan a obtener la confiabilidad numérica de un sistema, en la fase del diseño muestran las alternativas que alcanzan el objetivo numérico de confiabilidad, permiten identificar las áreas vulnerables que es necesario modificar por arreglo diferente de componentes o por sustitución. Muestran además la susceptibilidad de sistemas a las fallas en modo común cuando se toman en cuenta factores causales tales como condiciones normales y anormales de los medios -

ambientales interior y exterior incluyendo deficiencias de diseño y errores de operación y mantenimiento.

La confiabilidad número calculada por los procedimientos de las guías y normas ya establecidas permite obtener:

- La confiabilidad de la planta nucleoeléctrica en sus diferentes condiciones y configuraciones de operación normal, transitorios y accidentes.

- Las confiabilidades de los sistemas individuales de protección de la planta que combinadas dan la confiabilidad de la planta.

- Definición de los métodos de operación y mantenimiento.

- Identificación de las áreas vulnerables desde el punto de vista de la confiabilidad.

- Calificación de la efectividad de las pruebas de capacidad de funcionamiento de los sistemas de protección.

- Calificación de la efectividad de la frecuencia de las pruebas y del mantenimiento planeado de los sistemas de protección.

- Identificación de las áreas de falla en modo común.

- Una mejor idea de las consecuencias de las acciones del operador.

Esta confiabilidad numérica calculada por procesos de manejo de información estadística se llama confiabilidad intrínseca .

3.4 CONFIABILIDAD OPERACIONAL

No es posible anticipar todas las condiciones adversas durante la operación tales como deficiencias en la calidad cuyo control no es perfecto, como no lo es el conocimiento de los materiales ni el conocimiento del comportamiento humano, en consecuencia, la confiabilidad que se obtiene en la operación real de una planta o sea:

La confiabilidad operacional es inferior a la confiabilidad intrínseca de la planta.

Al obtener información real de operación del comportamiento de sistemas y componentes, deberá considerarse, como un proceso continuo, la realización de análisis de confiabilidad para determinar qué cambios de diseño o modos de operación hay que efectuar para obtener la confiabilidad deseada.

Este proceso continuo debe incluir el intercambio de experiencias en todas las plantas.

3.5 CONFIABILIDAD HUMANA

En la conducta humana existe una tendencia al error generalmente sensitiva al número de decisiones, operaciones o cualquier otra medida de actividad, de aquí que a mayor número de operaciones y decisiones realizadas mayor será el número de errores observados.

En tanto los humanos estemos constituidos físicamente y sicológicamente como lo estamos, habrá fallas, equivocaciones, omisiones y otros eventos imprevistos.

El sistema compuesto por la Planta Nucleoeléctrica y el Operador (palabra en la cual englobamos toda intervención humana en el funcionamiento de la Planta) es un sistema complejo que realiza funciones múltiples cuyas configuraciones cambian en tiempos determinados y en tiempos aleatorios, cuyos sistemas pueden desacoplarse y reacoplarse en diversas formas. Es claro que los errores del Operador pueden afectar la confiabilidad de la Planta y que cualquier mejora en la confiabilidad del propio Operador puede contribuír positivamente a la Seguridad de la Planta.

Las calificaciones del Operador pueden dividirse en factores relacionados con:

Conocimientos técnicos
Conocimiento de la Planta
Habilidad real de Operación
Aspectos humanos.

Sin detallar los rigurosos y estrictos procesos del licencia miento del personal que opera la planta podemos decir que si el Operador posee una apreciación correcta de los procesos que tienen lugar en un reactor y que conoce cómo y por qué un reactor responde a los diversos estados en que puede encontrarse, está entonces calificado desde los puntos de vista de conocimiento técnico y de seguridad:

El Operador calificado debe conocer la propia Planta en gran detalle, incluyendo las normas y límites de operación segura, los procedimientos de prueba, mantenimiento, de estados transitorios y accidentes y los procedimientos de emergencia.

La habilidad real del Operador se demuestra mediante exámenes en los que debe operar la Planta satisfactoriamente bajo la ob-

servación del examinador.

Por supuesto el Operador ha sido entrenado en operación de simuladores de operación normal, en estados transitorios y de accidente y de reactores reales de las mismas características del reactor de la Planta que va a operar bajo la supervisión directa de un operador ya licenciado.

La calificación de los aspectos humanos, probablemente la mas importante, es la más difícil de estimar y no siempre se incluye, en los análisis de confiabilidad de un sistema, la probabilidad de errores humanos.

Generalmente se supone que no hay errores de diseño, que las pruebas que hace el operador no introducen fallas en el sistema, que siempre se alcanzan los objetivos de pruebas y que el mantenimiento y las reparaciones se realizan a la perfección, se obtiene pues, la confiabilidad intrínseca.

Cuando se considera el sistema hombre-máquina se asigna una probabilidad a los errores del Operador estimada o respaldada por estudios de tiempo y movimientos de ingeniería y estadísticas de experimentos para intentar encontrar una razón de falla humana similar a las razones de falla de componentes.

En el diseño de Plantas Nucleoeléctricas se toman en cuenta los factores humanos y se analiza el comportamiento del Operador con base a tres parámetros:

a) Estímulo que lleva a:
b) Percepción, que integrada con información interna lleva a:
c) Acción efectiva.

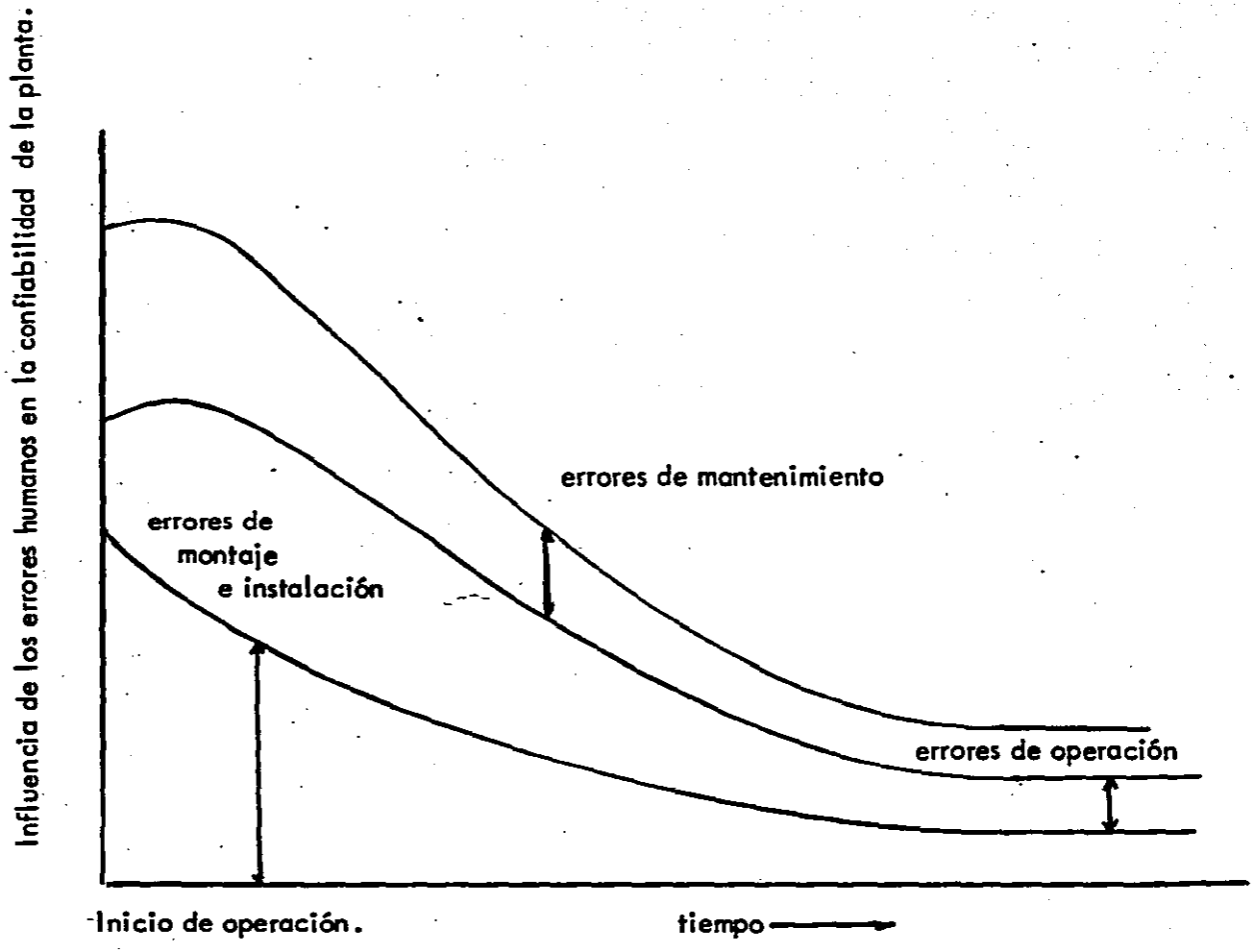

Influencia de los errores humanos en la confiabilidad de la planta.
errores de mantenimiento
errores de
montaje
e instalación
errores de operación
Inicio de operación.
tiempo

FIGURA 1.

Cualquiera de estos tres eslabones en la cadena del comporta -- miento del operador que no se realice, es fuente de error; por - ejemplo:

Un estímulo originado en el exterior no es tomado en cuen ta por el operador; ve pero no percibe, oye pero no escucha.
El operador recibe varios estímulos que no puede discrimi mar; está confundido.
El operador recibe el estímulo, pero no sabe lo que signi fica; está confundido.
El operador recibe el estímulo y entiende lo que significa pero no sabe que hacer; está confundido.
El operador conoce la acción que debe tomar pero no está en posibilidad física de realizarla; ha perdido el con -- trol del sistema.
El operador conoce y puede realizar la acción pero no la realiza en el tiempo y secuencia debida; se desconcierta.

Para lograr que el operador no pierda el control del sistema y- que esté siempre en posibilidad física de realizar actuaciones en los tiempos y secuencias debidas de modo confiable, el diseñador debe tomar en cuenta que exista un medio ambiental confor table para el operador que disminuya la posibilidad de distracciones y que ofrezca seguridad personal. Que haya retroalimentación al operador mediante señales que indiquen la respuesta - del sistema a sus acciones, que los controles, anunciadores, rótulos, luces, indicadores y dispositivos de actuación estén a su alcance y percepción para facilitar la operación.

Si los factores humanos indican probable insuficiencia en los - tiempos de reacción al estímulo para la realización de la ac -- ción manual, en comparación con la actuación automática, se deberá respaldar o reemplazar la acción manual con la actuación --- automática.

Los errores humanos que se cometen en todo el ciclo de la vida de la planta pueden clasificarse como:

Errores conceptuales
Errores de diseño
Errores en el control de calidad
Errores en montaje e instalación y pruebas
Errores en la operación y el mantenimiento

En la etapa de diseño es posible eliminar la mayor parte de los errores conceptuales lo mismo que en la etapa de montaje, instalación y prueba se detecta la mayoría de los errores de diseño y se corrigen los efectos de los errores conceptuales remanentes.

En la etapa de pruebas se detecta la mayoría de los errores de montaje e instalación.

Los efectos de los errores remanentes tienden a disminuír al inicio de la operación conforme se detectan los defectos y se corrigen, lo mismo que los efectos de los errores de operación y mantenimiento conforme gana habilidad el personal de operación y mantenimiento.

En la operación comercial las razones de errores de operación se estabilizan al igual que las del mantenimiento al quedar establecido el mantenimiento predictivo.

En forma similar a la información de comportamiento de componentes se han establecido programas y bancos de datos sobre el comportamiento humano. NASA - Data Book for Human Factors *engineering*. Vol1 Nov. 1969 Washington DC 755-245 USA. Fitts P. M. Human Performance, Brooks Cole Publishing Co. Belmont CA. 1968 USA.

4. ESTADO ACTUAL DE LA APLICACION

Las técnicas de confiabilidad, cuya extensa aplicación ya se ha mencionado, han sido utilizadas en la elaboración de dos monumentales trabajos que analizan la Seguridad de las Plantas Nucleares:

El Estudio de la Seguridad de los Reactores Nucleares de Estados Unidos (WASH-1400) conocido como el Reporte Rasmussen y El Estudio Alemán sobre los Riesgos de las Centrales Nucleares realizado bajo la dirección del Profr. Dr. A. Birkhofer.

Ambos trabajos concuerdan y concluyen que las probabilidades de una catástrofe originada por una Planta Nuclear son muy pequeñas.

Se han publicado además numerosos trabajos sobre análisis de riesgos y beneficios que concuerdan en la existencia permanente de riesgos en toda actividad humana y, aunque los márgenes de incertidumbre en la cuantificación de riesgos son considerables y la aceptabilidad de riesgos muy discutible, se ha obtenido información valiosa siempre que en su interpretación se tengan en cuenta las limitaciones de la metodología.

Entre esos trabajos destacan en interés los que buscan la optimización de la protección radiológica tomando en cuenta el costo de la protección y el costo del detrimento a la salud causado por las radiaciones. No menos interesantes son los trabajos que señalan que hay un límite en la búsqueda de seguridad en el cuál, la introducción de más protección a un sistema para mejorar la seguridad introduce, a fin de cuentas, otros riesgos adicionales que cancelan la aparente ventaja obtenida.

Esta situación es análoga a una de las contradicciones básicas de la tecnología moderna ya encontrada en las cuantificaciones de la confiabilidad; por una parte se presentan problemas de -- complejidad creciente que hay que resolver, lo que lleva a complejidad creciente de los sistemas que se usan para resolverlos disminuyendo la confiabilidad y por otra parte los requisitos - de comportamiento confiable de esos sistemas son cada vez mas - estrictos. Para resolver esta contradicción hay dos caminos: - aumentar la confiabilidad y calidad de los elementos individuales que componen el sistema y buscar configuraciones de siste - mas complejos confiables con elementos de baja confiabilidad soportados por métodos de mantenimiento durante el servicio para conservar la confiabilidad.

Mediante estos procedimientos se ha logrado a la fecha, alta -- confiabilidad intrínseca en sistemas complejos cuya confiabilidad operacional es ahora sensible a la confiabilidad humana.

5. DISCUSION DE RESULTADOS

Para tratar ahora la interpretación que debe darse a los resultados obtenidos con las técnicas actuales de confiabilidad conviene evitar algunas fuentes importantes de confusión y error - dividiendo analíticamente las "cosas" en dos dominios: ideacional y fenomenological.

Esta división y cualquiera otra distinción son artificiales y - no nos dicen nada del mundo real cualquiera que este sea, sim - plemente están enfocadas a un propósito -facilitar nuestra en-- cuesta y nada más. Aquellas "cosas" consideradas pertenecien - tes al dominio fenomenológico son aquellas que podemos observar, ya sean objetos o eventos (un eclipse solar, la posición de la

aguja de un instrumento de medición o la huella de una partícula en una cámara de niebla).

El dominio ideacional comprende aquellas "cosas" que no tienen existencia objetiva comunmente llamadas ideas.

Las "cosas" clasificadas como ideacionales pueden conocerse solo mediante alguna manifestación fenomenológica (por ejemplo alguien que expresa mediante sonidos lo que está pensando).

No tiene caso argumentar sobre la realidad relativa de las dos categorías ya que todas las categorías se derivan del dominio - ideacional.

Todos los fenómenos pueden categorizarse y en el proceso muchos de sus atributos dejan de percibirse. Todas las ideas necesi - tan alguna clase de expresión fenomenológica para que puedan -- transmitirse. La ciencia práctica se enfoca para permitirnos - tratar con una sola de estas categorías - el dominio fenomenológico, por esta razón una distinción analítica entre las cosas - que pueden observarse (objetos y eventos) debe claramente separarlas de aquellas cosas que no pueden observarse (ideas).

Utilizando esta distinción es posible separar los medios de explicación de la misma explicación y distinguir los modelos del mismo original.

No se supone que los modelos sean copias exactas del mundo real, sino simplificaciones tentativas que revelen información par -- cial para tratar de entender procesos y estimar predicciones de comportamiento.

En la modelación de un sistema real para analizar las fallas de sus componentes se pierden muchas características de las fallas,

no siempre se consideran las fallas graduales (paramétricas o - graciosas), ni las fallas alternas (intermitentes). Para sim - plificar el tratamiento matemático y en la carencia de una enor me cantidad de información acerca de muchísimas variables que - intervienen en la dinámica de un sistema, se prefiere el proce- dimiento binario de falla - no falla y los resultados de confia bilidad obtenidos mediante la modelación simplificada deben in- terpretarse como las tendencias estadísticas del comportamiento del modelo que es la representación parcial del sistema real.

Los modelos matemáticos y los modelos físicos tales como siste- mas piloto, simuladores y la información experimental concurren para aumentar el conocimiento sobre el comportamiento de los -- sistemas reales y si los hechos demuestran que las predicciones probabilísticas no concuerdan con la realidad, la falla no está en las herramientas ni en los cálculos, está en factores no con siderados, en conocimientos incompletos o no aplicados y a fi - nal de cuentas está en el factor humano.

6. FACTORES CRITICOS.

6.1 IDENTIFICACION DE FACTORES CRITICOS EN EL SISTEMA PLANTA-OPERADOR

Mediante la modelación simplificada de los subsistemas del sis- tema complejo multimodal que es la Planta Nucleoeléctrica se en cuentran las tendencias estadísticas del probable comportamien- to según el modelo.

Sabemos que la idea de una población infinita distribuida por - frecuencias de una o mas características es fundamental de todo trabajo estadístico y que de una experiencia limitada de alguna función o de individuos de un tipo dado, podemos obtener idea de la población hipotética infinita de la cual hemos obtenido nues tra muestra y tener idea de la naturaleza probable de muestras -

futuras a las cuales se van a aplicar nuestras conclusiones, si las siguientes muestras están de acuerdo con esta expectativa, la expectativa se hace mas probable y si una última muestra no está de acuerdo con esta expectación, inferimos que ha sido obtenida, en el lenguaje de la estadística, de una población diferente.

Si la confiabilidad intrínseca de un sistema complejo multimodal obtenida con apoyo estadístico es elevada, si el personal de operación está calificado como en el caso de una planta nucleoeléctrica y, a pesar del historial de las demás plantas, ocurre un evento indeseable como el evento TMI-2 podemos inferir que el sistema complejo multimodal, que puede asumir diferentes modos de operación y estados distintos en la configuración de elementos y subsistemas, se ha configurado en un sistema complejo fuera de la población a la cual se aplicó el modelo para estimar la confiabilidad intrínseca; por lo tanto su comportamiento no sigue la lógica para la cual han sido capacitados los operadores y ha abierto la posibilidad de ocurrencia del evento indeseable.

El origen de las configuraciones anómalas del sistema complejo multimodal está en los errores remanentes de concepto, diseño, manufactura, construcción, instalación, montaje y pruebas y en los errores de omisión y actuación en la operación y el mantenimiento de la Planta.

Durante la puesta en servicio y la operacion no todos los errores remanentes y de omisión o actuación generan inmediatamente las consecuencias que los harían evidentes; algunos de ellos no se detectan y permanecen ignorados; en el lenguaje de la confiabilidad, existen en el sistema en estado de "reserva alerta", listos para encadenarse con los eventos transitorios que ocurren durante la operación.

No todos los errores en reserva alerta pueden producir configuraciones anómalas antes o durante el evento transitorio al cual se encadenan; el operador tiene dominio de la situación y dispone, en caso extremo, de los sistemas de protección y de emergencia.

Dada la existencia de errores de este tipo, la probabilidad del encadenamiento es igual a la probabilidad de ocurrencia del evento transitorio.

Algunos errores en reserva alerta pueden producir configuraciones anómalas antes o durante el evento transitorio al cual se encadenan; el operador no identifica de inmediato la configuración anómala, ha perdido el dominio de la situación y sus acciones pueden interferir con la actuación automática de los sistemas de protección y de emergencia. Dada la existencia de errores de este tipo, la probabilidad del encadenamiento es igual a la probabilidad de ocurrencia del evento transitorio.

Las consecuencias dependen del grado de interferencia que ocurra en la actuación de los sistemas de protección y de emergencia por intervención del operador. En esta última situación identificamos como factores críticos a los errores remanentes y de omisión y actuación existentes en estado de reserva alerta con capacidad de producir configuraciones anómalas del sistema complejo multimodal y a la falta de identificación inmediata de la configuración anómala por parte del operador cuyas ulteriores acciones no son las apropiadas.

6.2 EL ACCIDENTE TMI-2

El accidente ocurrido a las 4 horas a.m. el miércoles 28 de mar

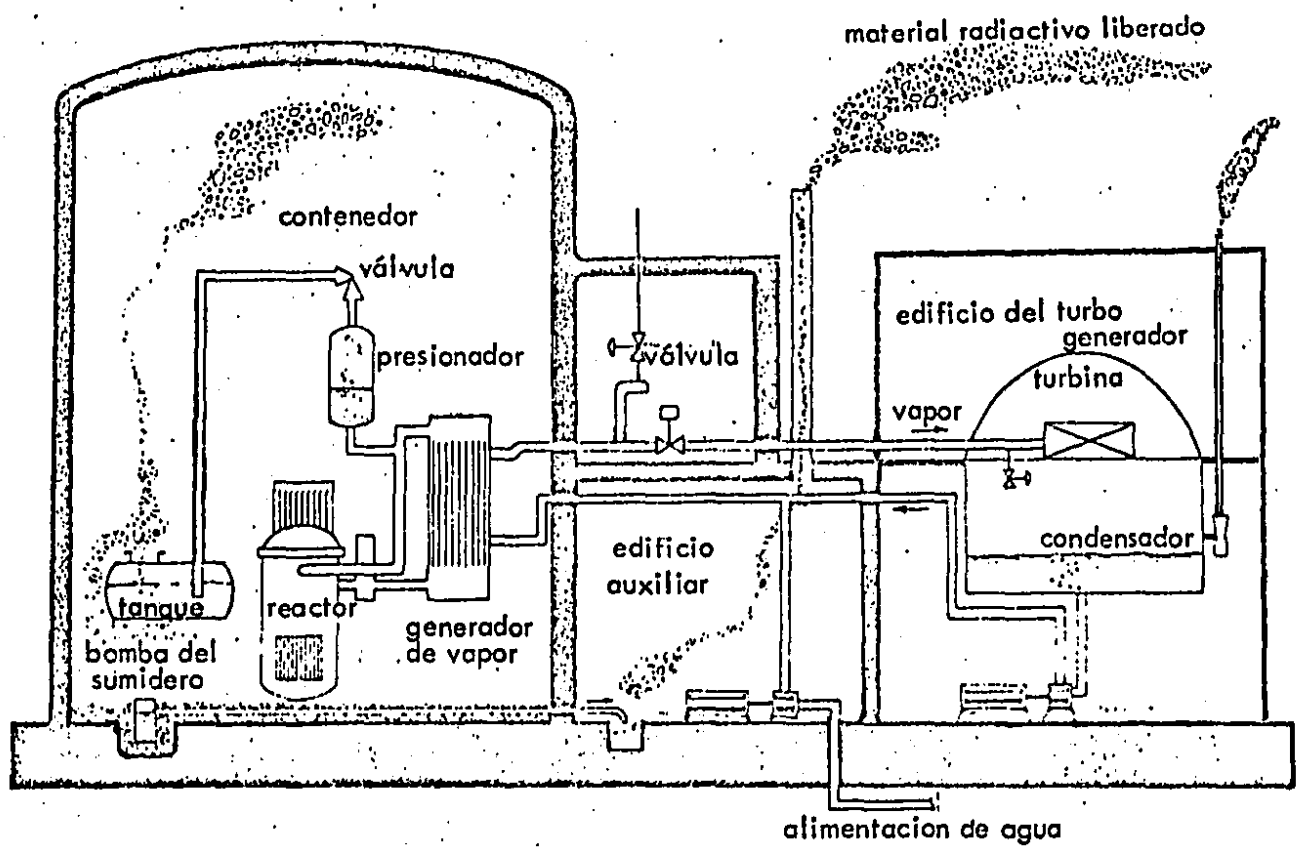


FIGURA 2. TRAYECTORIAS DEL MATERIAL RADIACTIVO LIBERADO.

zo de 1979 en la unidad 2 de la Planta Nucleoeléctrica Three Mile Island en las cercanías de Harrisburg Pa. U.S.A., hizo evidente que las consecuencias de los incidentes aparentemente leves ocurridos en las Plantas Nucleoeléctricas no se habían investigado adecuadamente y que era necesario examinar a fondo la seguridad.

Este error se detectó a través de sus consecuencias que pusieron en relieve la insuficiente atención que se había prestado en todos los niveles y sectores de la industria nuclear a la operación sin riesgos y en particular al elemento humano y su papel fundamental en la prevención y respuesta a los accidentes. El tema de la seguridad operacional en el uso pacífico de la energía nuclear desde este desafortunado accidente entró en revisión que continúa hasta estas fechas.

6.2.1 SECUENCIA DE EVENTOS

Según el Reporte Especial del 6 de abril de 1979 de la American Nuclear Society la secuencia de los eventos de este accidente fué la siguiente:

- "Cerca de las 4 a.m., el sistema principal de agua de alimentación de Three Mile Island - 2 funcionó mal aparentemente como resultado de falla, ya fuera del desmineralizador o del suministro del aire a una válvula operada por aire.

- Con el sistema principal de agua de alimentación fuera de operación, el sistema auxiliar de agua de alimentación debía arrancar automáticamente.

No realizó su función, sin embargo, porque un cierto número de válvulas en el sistema auxiliar se habían dejado inadvertidamente cerradas después de una prueba del sistema días antes del accidente.

- Sin suministro de agua de alimentación, se secaron los generadores de vapor y como resultado se elevaron la temperatura y la presión del enfriador primario. Se disparó el turbogenerador. El aumento de presión generó una señal que puso al reactor en scram, (apagado rápido de emergencia).

- En segundos, la presión en el circuito primario se elevó a 1.625×10^7 pascal (2355 psi) disparando una válvula de alivio en la parte superior del presionador. El enfriador primario, así aliviado, fué conducido por tubería a un tanque de apagado, localizado dentro del contenedor. La válvula falló y quedó en la posición de abierta con liberación continua del enfriador fuera del sistema.

  Esta falla y la falla del sistema principal de agua de alimentación (ambas de naturaleza mecánica) unidas al mal funcionamiento del sistema auxiliar de agua de alimentación ocasionaron el inicio del incidente.

- El sistema de emergencia de enfriamiento del núcleo arrancó automáticamente a los dos minutos en la secuencia del accidente y principió a elevarse el nivel del enfriador. En unos cuantos minutos, el indicador de nivel del presionador, según reporte, empezó a dar erróneamente lecturas elevadas y de hecho se salió del límite superior de la escala - aún cuando en realidad

debía haber indicado la situación opuesta. Un operador manualmente paró la actuación automática primero en una de las bombas de inyección a alta presión (ECCS) y unos pocos minutos después a la otra. Se supone que hizo esto para evitar que el presionador llegara a ponerse "sólido" (lleno totalmente de agua); si el presionador se llena, se pierde el control de la presión.

- Dos minutos después del primer paso del ECCS según se reporta, el enfriador primario del reactor entró en -- evaporación relámpago.

- También después del primer paso del ECCS, las bombas del sumidero del sótano del contenedor empezaron automáticamente a funcionar (la aislación del contenedor en TMI-2 no es automática con la iniciación del ECCS solamente hasta que la presión en el contenedor ha alcanzado cuatro psig).

  Varios minutos después se estableció el flujo de agua de alimentación aumentando la presión en los generadores de vapor.

- Con flujo libre a través de la válvula de alivio del presionador, el tanque de apagado continuó llenándose y a quince minutos en la secuencia del accidente se -- abrió su disco de ruptura liberando finalmente más de 40000 litros de enfriador primario al piso del contenedor del cual fué bombeada a un tanque de almacenamiento en el edificio auxiliar donde el agua se derramó -- otra vez al excederse la capacidad del tanque que ya estaba parcialmente lleno. A través del sistema de -- ventilación del edificio principiaron a escapar al me-

dio ambiente los isótopos radioactivos de Kriptón, xenón y iodo; los filtros de ventilación retuvieron los gases nobles.

- La liberación de enfriador primario del sistema primario continuó a través de la válvula de alivio del presionador abierta originando una baja en la presión primaria. Una hora quince minutos después del transitorio inicial y con presión cercana de 1300 psi se dispararon manualmente dos bombas de enfriador en el circuito de un generador de vapor, aparentemente para evitar cavitación y el daño resultante a las bombas. Las --- otras dos bombas se dispararon también manualmente 25 minutos después. A este punto el sistema del reactor quedó sin convección forzada y sin sumidero de calor.

- Se recuperó el control del sistema de alivio del presionador y se puso en funcionamiento otra vez el ECCS. Se cree, sin embargo que el nivel del enfriador había bajado tanto, que parte del núcleo había quedado descubierto con daño substancial resultante al combustible. Aún cuando se registraron temperaturas bastante altas en el núcleo, no se cree que haya ocurrido realmente fusión.

- A las tres horas se notó que habían ocurrido fugas del primario al secundario en el generador de vapor "B" -- abriendo una trayectoria para más material radioactivo del sistema secundario al medio ambiente. El generador de vapor "B" fué consecuentemente aislado; el generador de vapor "A" permaneció en funcionamiento.

- Se ha postulado que el daño substancial del combustible combinado con altas temperaturas resulta en la for

mación del reactor de una burbuja de gas consistente - en hidrógeno (de la reacción de zircaloy con agua) y - productos gaseosos de fisión.

La burbuja presenta un problema en la realización del enfriamiento: Si se reduce la presión en el sistema -- primario la burbuja se expansiona y posiblemente invalida el modo de enfriamiento (e.g., causando cavita -- ción en las bombas).

- El hidrógeno también presentó un problema en el contenedor. En las fases iniciales del accidente la pre -- sión había subido sobre la presión atmosférica. Des - pués se detectó el hidrógeno y si se permite que se -- acumule tiene potencial de ocasionar una explosión.

- En la tarde del miércoles se restableció el enfriamiento del núcleo dañado mediante la activación de una delas bombas de enfriador primario en el circuito "A" -- usando el generador de vapor "A" como sumidero de ca - lor. El proceso de desgasificación involucró la ex -- tracción del gas disuelto en el enfriador en la rama - fría del sistema primario y rociándolo a través del -- presionador y descargándolo al contenedor. Esto redujo eventualmente el tamaño de la burbuja pero agregando hidrógeno al contenedor. En el 3 de abril funcionó un recombinador de hidrógeno fuera del contenedor y -- principió a bajar gradualmente la concentración de hidrógeno (2.3 por ciento al fin del día 1o. abril, 2.1 por ciento en la mañana del 4 de abril). Se espera -- que la concentración baje al 1% en abril 15.

- Al tiempo de redactar este reporte, algunas temperaturas arriba del núcleo estaban en exceso de 200°C, re -

quiriendo que la presión primaria se mantenga a cerca de 6.9×10^6Pa (1000 psi).

El procedimiento de alcanzar el apagado frío preferido hasta el 6 de abril es continuar el enfriamiento por - circulación bombeada hasta el 11 de abril y después pa sar a "circulación natural" en el sistema primario con agua "sólida" en el secundario. No se considera el -- uso del sistema de remoción del calor residual(RHRS) ".

6.2.2 EJEMPLOS DE ERRORES Y FALLAS INDUCIDAS POR EL FACTOR HUMA NO.

De acuerdo con la información anterior de la ANS en el Reporte Especial sobre el accidente TMI-2 se pueden citar ahora, ejem - plos de errores que pueden originar configuraciones anómalas no identificadas inmediatamente por el operador cuyas acciones pue den tener consecuencias indeseables.

1 Se mencionó anteriormente el error remanente de aten - ción insuficiente presentada por la industria nuclear a la operación sin riesgos y a la participación del e- lemento humano.

Este error de concepto, en el accidente TMI hizo posi- bles la ocurrencia, la permanencia y las consecuencias del error de operación en estado de reserva alerta que consistió en dejar cerradas las válvulas de descarga - del sistema auxiliar de agua de alimentación a los ge- neradores de vapor.

2 Este error de operación cometido en el circuito secun- dario no nuclear, se encadenó con el evento transito -

rio inicial de alta probabilidad de ocurrencia que había incapacitado al sistema principal de agua de alimentación de los generadores de vapor. Aunque se corrigió por el operador ocho minutos después del inicio del accidente, éste ya había realizado acciones de interferencia con la actuación automática de los sistemas de emergencia y protección por falta de identificación inmediata de la configuración anómala producida por el error de operación. La actuación automática de los sistemas de protección del turbogenerador y del reactor habían parado el turbogenerador y puesto al reactor que operaba al 98% de potencia en estado de apagado rápido de emergencia produciendo unicamente calor residual de decaimiento a los treinta segundos del inicio del accidente.

3 Las acciones de interferencia por parte del operador consistieron en parar manualmente las bombas de inyección a alta presión del sistema de emergencia de enfriamiento del núcleo suspendiendo la actuación automática. La interferencia del operador se basó en la indicación falsa de la instrumentación del nivel dentro del presionador que se había salido de escala probablemente por la turbulencia producida por la descarga de vapor y agua a través de la válvula de alivio abierta en la parte superior del presionador. Esta válvula se quedó abierta y la bloqueó el operador a las dos horas veinte minutos después del inicio del accidente.

4 Entre la primera y la segunda hora después del inicio del accidente el operador paró las cuatro bombas que circulan el enfriador del reactor después de que se había restablecido la alimentación auxiliar a los genera-

dores de vapor. Se supone que en las siguientes horas ocurrió el daño al combustible iniciando la reacción - metal-agua y ocurrió el derrame de material radiactivo; aunque a las cinco horas del inicio del accidente se - aisló al contenedor primario ya había ocurrido liberación de radioactividad al medio ambiente.

5 La indicación falsa dada por la instrumentación del nivel del líquido en el presionador originada por las - condiciones de turbulencia de la evaporación relámpago y tomando en cuenta que posteriormente regresó a la escala puede interpretarse como un error de diseño en - la instrumentación.

6 La falla de la válvula de alivio en la posición de --- abierto pudo originarse en calibración incorrecta, defectos de manufactura, error de aplicación, error de - diseño o causas diversas.

7 En el diseño no se consideró la instalación permanente en el sistema primario de dispositivos de venteo de gases incondensables. Estos dispositivos eliminan, en condiciones de emergencia, la interferencia de los gases incondensables con los procedimientos de enfria -- miento, disminuyen las probabilidades de explosión por hidrógeno al enviarlo junto con los gases radiactivos a áreas de tratamiento controlado.

8 En el diseño no se consideró la instalación, dentro -- del contenedor primario, de un sumidero de calor que - realizara las funciones de cancelación de la presión - en el contenedor primario, presión que inició el bom - beo de material radiactivo fuera de la contención al -

edificio auxiliar. Estos sumideros de calor son: en - los reactores Westinghouse el sistema de condensación por hielo y en los reactores General Electric la alber ca de cancelación de la presión.

9 En la mayoría de las Plantas Nucleoeléctricas actual - mente en operación, las salas de control no presentan al operador información suficiente en forma integrada, que permita diagnosticar un estado anómalo con rapidez; en el caso TMI-2 no hubo indicación directa del estado de la válvula de alivio que falló, los parámetros críticos se registraron en bandas de gráficas difíciles - de leer aunque adecuadas para análisis post-mortem; -- los anunciadores no estaban agrupados por funciones ni por secuencias de operación ni orden de prioridad además del etiquetado inconsistente de los controles y -- anunciadores.

Defectos de este tipo, atribuibles a deficiente diseño, son los que originan la confusión del operador o sea: errores humanos de diseño originan errores humanos de- actuación.

6.2.3 COMENTARIOS

En las fuentes consultadas sobre el accidente TMI-2 se encontró información confusa, incompleta y contradictoria. El Reporte - Especial de la ANS fué uno de los primeros y no coincide con -- los diversos análisis, reportes e informes posteriores que se - contradicen y muestran inconsistencias.

No se pretende que la descripción del evento TMI-2 sea exacta - como no lo son las conjeturas que aquí se presentan. La postu-

lación de defectos y errores humanos remanentes, actuaciones consecuenciales inapropiadas y fallas inducidas por la intervención humana tampoco describe toda la situación real, simplemente se utiliza como una herramienta para el objetivo de este trabajo.

La NRC desde los primeros reportes indicó que el accidente TMI-2 hacía evidente la gran dificultad confrontada por el operador de una planta PWR para entender y controlar apropiadamente el curso de un accidente con rotura pequeña en el sistema primario con la concurrencia de otras condiciones anormales y recomendó que se realizaran a la brevedad más análisis de transitorios y accidentes en los PWR que involucran inicialmente o en algún tiempo durante su curso, una rotura pequeña en el sistema primario con la seguridad de que estos análisis demostrarían, como ya lo había demostrado el accidente TMI-2, que el operador necesita información adicional sobre el estado del sistema para que pueda seguir el curso de un accidente y estar así en capacidad de responder en forma apropiada.

Por su parte el OIEA convocó la Conferencia Internacional del 20 al 24 de octubre de 1980 en Estocolmo Suecia donde se trataron los problemas de la seguridad nuclear que el accidente TMI-2 había hecho pasar al primer plano enfocados a:

- Las funciones de la Dirección de las compañías eléctricas y su personal técnico.
- La calificación y capacitación del personal operador.
- La idoneidad de los procedimientos operacionales en caso de emergencia.
- La evaluación y utilización de la experiencia de explotación y la zona de contacto hombre-máquina.

Se insistió principalmente en la Dirección de la explotación de las Plantas Nucleares con responsabilidad y calificación cre -- cientes del personal directivo, y la capacitación de los operadores.

Cabe hacer notar que con anterioridad al accidente TMI-2, ha -- bían ocurrido incidentes importantes en Plantas Nucleares que - no llamaron la atención internacional sobre la insuficiencia de la filosofía de seguridad en la forma en que fué aplicada tales como:

AÑO	PLANTA	CAUSA	DEFECTO
1957	WINDSCALE Producción de Plutonio de Inglaterra.	Liberación de calor por la energía Wigner del grafito. Error en operación por falta de procedimientos de operacion Error de diseño con instrumentación insuficiente.	Destrucción del Reactor
1966	ENRICO FERMI Reactor rápido 430 MWt Estados Unidos de América.	Oclusión del flujo de sodio por desprendimiento de dos de flectores. Error de cambio de ingeniería y falta de control de calidad.	Destrucción del núcleo del reactor.
1974	WURGASSEN 640 MWe RFA	Error humano de operación Error de diseño Falla de equipo	Daños en la contención
1975	BROWNS FERRY 1100 MWe EUA	Procedimiento inadecuado Error humano	Incendio que - afectó los cables eléctri - cos de tres unidades.

1980	SAINT LAURENT 480 MWe Francia	Falla de instrumentación y arranque inadecuado. Error humano	Daño al encamisado en algunas barras de combustible.

7. POSIBLES MEJORAS A LA CONFIABILIDAD OPERACIONAL

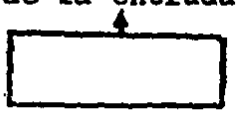
7.1 METODO DE ARBOLES DE FALLAS

El método de árboles de fallas que fué desarrollado y utilizado para el calculo probabilístico de la confiabilidad intrínseca - puede emplearse en otras formas diferentes para investigar las posibilidades de mejorar la confiabilidad operacional, mediante esta técnica las fallas que contribuyen a que tenga lugar un -- evento indeseable, se organizan deductivamente y representan - gráficamente incluyendo sus efectos.

Para esta representación se utilizan los siguientes símbolos:

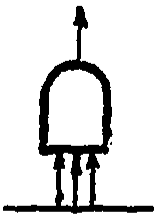
a) Círculo. Representa una falla básica 

b) Rombo. Representa un evento producido por fallas que se toma como básico en un árbol dado de fallas. 

c) Rectángulo. Representa un evento resultante de la combina -- ción de los eventos representados por los símbolos anteriores, relacionados lógicamente a través de la entrada y salida por puertas lógicas. 

d) Puerta lógica "Y". Representa la intersección de conjuntos, esto es, el evento resultante ocurre si y solo si ocurren todos los eventos concurrentes.

AL EVENTO RESULTANTE



TODOS LOS EVENTOS CONCURRENTES

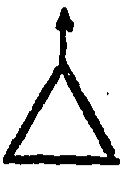
e) Puerta lógica "O". Representa la unión de conjuntos, esto es, el evento resultante ocurre si ocurre uno cualquiera o más - cualesquiera de los eventos concurrentes:

AL EVENTO RESULTANTE

CUALQUIERA O CUALESQUIERA
DE LOS EVENTOS CONCURRENTES

f) Puertas de transferencia. Representan eventos resultantes de árboles de fallas que se transfieren a otros árboles para evitar repeticiones.

TRANSFERENCIA DE



TRANSFERENCIA A

Para construir el árbol de fallas se principia por definir el evento indeseable en forma clara y precisa como el evento indeseable principal y solo el único principal del árbol de fallas.

A continuación se definen, como las ramas principales del árbol, a los eventos que llevan directamente al evento principal y se conectan con la puerta lógica correspondiente.

Se desarrollan las ramas secundarias del árbol para conectar a los subeventos con los eventos ya conectados con el evento principal y asi se prosigue en los siguientes niveles de ramas y eventos conectados a través de las puertas lógicas correspondientes hasta llegar a los eventos fundamentales (fallas básicas) o a una puerta de transferencia que proviene de otro subárbol ya desarrollado. (Referencia 7).

7.2 APLICACION Y OBJETIVOS

En la aplicación de esta metodología al cálculo probabilístico de la confiabilidad intrínseca se asignan probabilidades de ocurrencia a los eventos básicos y aunque en teoría es posible encontrar exactamente las posibilidades de ocurrencia de los demás eventos incluyendo al evento indeseable principal, en la práctica, dado el obstáculo presentado por el enorme número de combinaciones posibles, se siguen métodos aproximados para calcular la probabilidad del evento principal.

En el caso presente utilizamos esta técnica para investigar las posibilidades de mejorar la confiabilidad operacional para intentar en primera instancia:

1ª La eliminación o disminución de las probabilidades de ocurrencia de los eventos indeseables inducidos por el factor humano.

2ª Disminuir la vulnerabilidad de los sistemas de la planta a la formación de configuraciones anómalas inducidas por defectos de manufactura, errores remanentes de concepto, diseño, manejo, instalación, montaje, pruebas, operación y mantenimiento.

3ª Discutir las posibilidades de medición de las variables y parámetros del proceso en forma directa o indirecta y las alteraciones inducidas por las condiciones anormales procesando la información en forma digerible por el operador.

4ª Discutir las posibilidades de obtener diagnósticos tempranos de las condiciones precursoras a los eventos indeseables.

5ª Discutir las posibilidades de la automatización de actuaciones de seguridad con prioridad sobre las actuaciones manuales si el operador no reacciona a tiempo oportuno por limitación humana.

Para construír los árboles de falla adecuados a estos propósitos generalizados a los tipos actuales de reactores, principiamos por definir como evento indeseable principal, al evento ocurrido en TMI-2; la liberación no controlada de material radiactivo al medio ambiente que puede originarse por la ocurrencia de dos --- eventos originados por falla de la contención combinada con la falla en el control de los efluentes radiactivos de los productos de fisión no contenidos o por la falla del control de los -- efluentes radiactivos procedentes de los desechos radiactivos o

de incidentes en el recambio de combustible.

7.3 ARBOL DE LA LIBERACION NO CONTROLADA DE MATERIAL RADIACTIVO AL MEDIO AMBIENTE.

Evento 1: Liberación no controlada de material radiactivo al medio ambiente.

Evento 11: Combinación de los eventos 111 y 112

Evento 12: Falla de control de efluentes de desechos radiactivos y recambio de combustible originada por la concurrencia de otros eventos a la puerta lógica de transferencia 3.

Evento 111: Falla de la contención originada por la concurrencia de otros eventos a la puerta lógica de transferencia 1.

Evento 112: Falla del control de efluentes radiactivos del edificio del reactor originada por la concurrencia de otros eventos a la puerta lógica de transferencia 2.

El evento indeseable "falla de la contención" es el resultado de la concurrencia de otros eventos a la puerta lógica de transferencia 1 tales como la falla de la primera barrera de contención ya que la falla del encamisado permitió que productos de fisión se mezclaran con el enfriador primario; fallas de la segunda barrera de contención o sea el paso del enfriador contaminado con los productos de fisión a través de la descarga de vapor y agua por la válvula de alivio que falló en la posición abierta y a través de las fallas en los tubos de los generadores de vapor

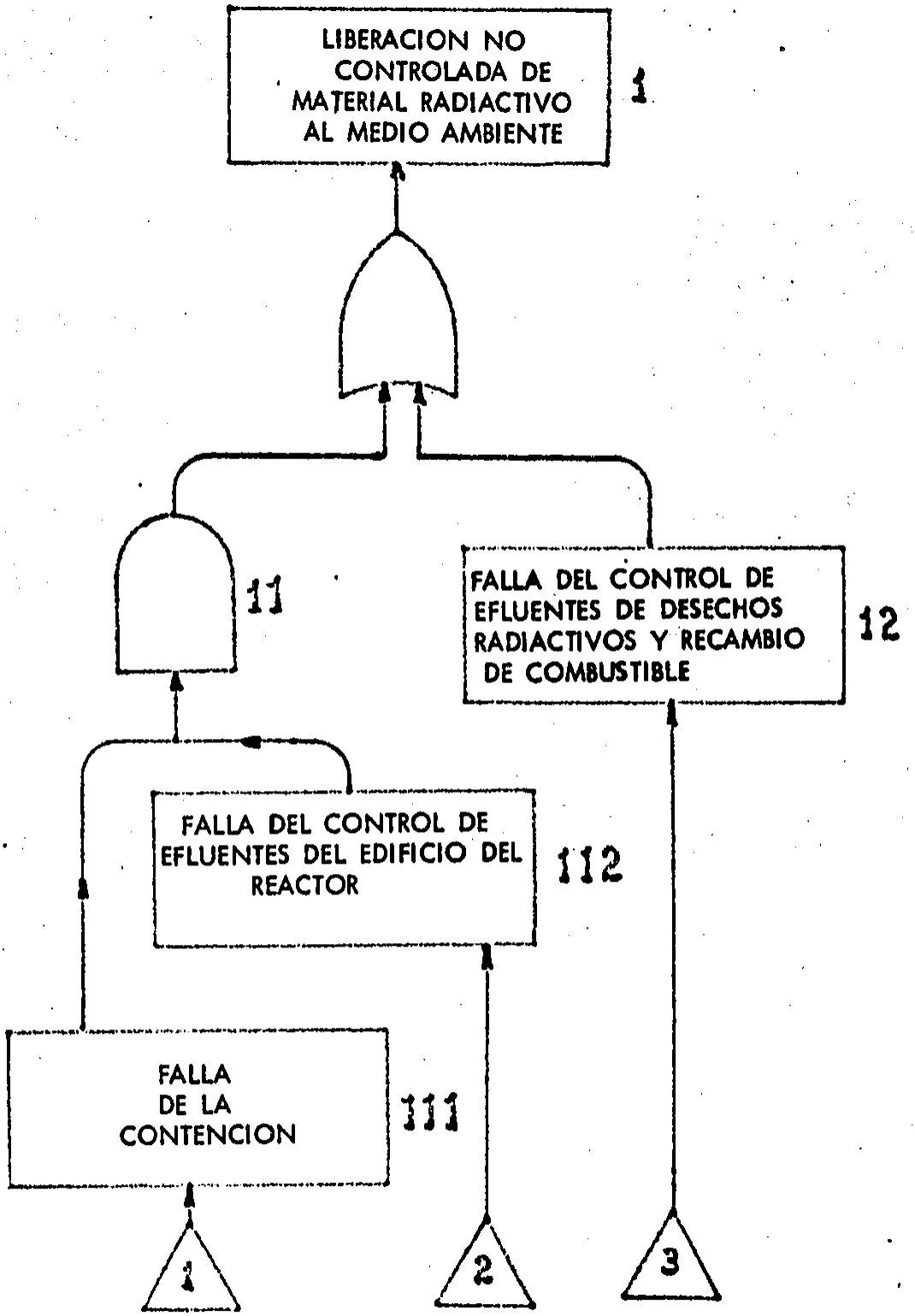


FIGURA 3 ARBOL DE LA LIBERACION NO CONTROLADA DE MATERIAL RADIACTIVO AL MEDIO AMBIENTE

que amenazaron contaminar los sistemas secundarios, violación de la tercera barrera por medio del bombeo del drenaje de los derrames de enfriador contaminado debidos a la rotura del disco limitador de presión del tanque de apagado, el drenaje pasó del edificio del reactor a un tanque receptor en el edificio auxiliar.

Los efluentes del edificio del reactor deben controlarse, tanto el tanque de recepción como los filtros del sistema de ventilación del edificio auxiliar fueron insuficientes, el edificio auxiliar se contaminó y a través de la descarga de los filtros se liberaron gases nobles y iodo radiactivos al medio ambiente esta falla de control de los efluentes del edificio del reactor contaminados con productos de fisión puede considerarse como consecuencia de errores remanentes de diseño que concurren a través de la puerta lógica de transferencia (2). Esta falla y la falla de la contención se unen en la puerta lógica (Y) para producir el evento indeseable principal a través de la puerta "o".

Queda otra posibilidad de ocurrencia del evento indeseable principal por medio de la ocurrencia de otros eventos que concurran a través de la puerta lógica de transferencia (3) para ocasionar la falla del control de efluentes procedentes del tratamiento de desechos radiactivos y de accidentes durante los recambios de combustible. La ocurrencia de esta falla concurre al evento indeseable principal a través de la puerta lógica "o". Cualquiera de las dos concurrencias a la puerta lógica "o" ya sea por las fallas combinadas de la contención y del control de efluentes del edificio del reactor o por la ocurrencia de la falla del control de los efluentes procedentes del tratamiento de desechos y accidentes de recambio originarán la liberación de materiales radiactivos al medio ambiente.

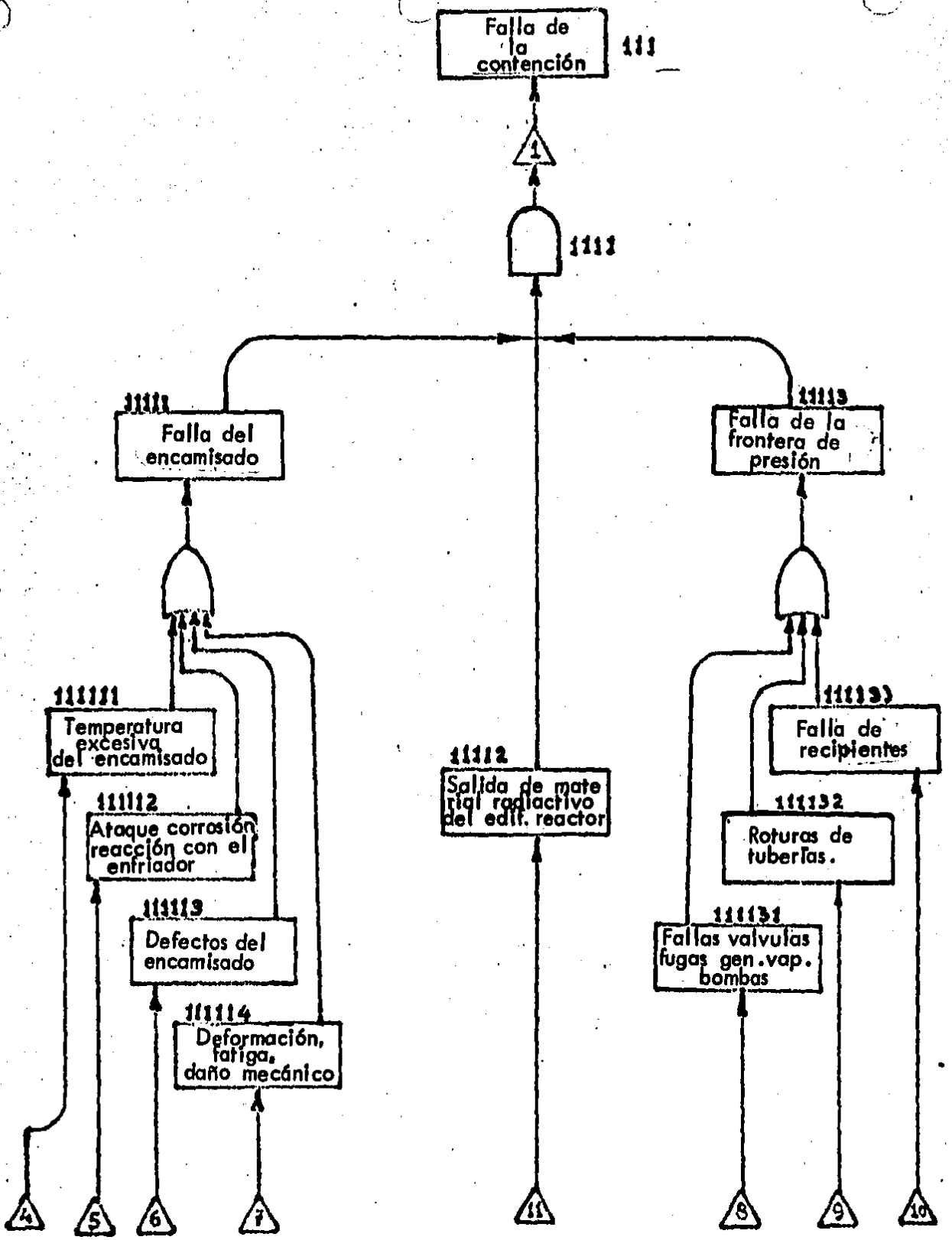


FIGURA 4 ARBOL DE FALLA DE LA CONTENCION POR COMBINACION DE LAS FALLAS DEL ENCAMISADO, DE LA FRONTERA DE PRESION Y DE LA CONTENCION DEL EDIFICIO DEL REACTOR.

7.3.1 ARBOL DE FALLA DEL ENCAMISADO

La mayor parte del inventario de material radiactivo en el interior del sistema primario está formado por los productos de fisión contenidos por la primera barrera constituida por el propio combustible y su encamisado. La menor parte de este inventario está en suspensión en el enfriador originado por la migración de productos de fisión a través del encamisado y la activación de las impurezas y productos de corrosión suspendidos en el enfriador y son capturados en el sistema de desmineralización y enviados al sistema de tratamiento de desechos radiactivos.

A la falla del encamisado concurren a través de la puerta lógica "o" cuatro eventos de los cuales basta uno para producir la falla.

Temperatura excesiva del encamisado.
Ataque por corrosión o reacción con el enfriador
Defectos del encamisado
Deformación y fatiga del encamisado por hinchamiento del combustible irradiado o choques térmicos o daño mecánico.

Estos cuatro eventos son a su vez la consecuencia de la concurrencia de otros eventos a las puertas lógicas de transferencia    y  respectivamente.

7.3.2 FALLA DE LA FRONTERA DE PRESION DEL SISTEMA PRIMARIO

En caso de falla de la primera barrera de contención, o sea la falla del encamisado, los materiales radiactivos que contaminan al enfriador quedan contenidos por la segunda barrera de contención constituida por la frontera de presión del sistema primario.

Esta frontera pierde su integridad si hay fugas en los componentes del sistema primario tales como válvulas, bombas o generadores de vapor, o por roturas de tuberías o por fallas o roturas de recipientes; a la ocurrencia de estos tres eventos indeseables concurren, a través de tres puertas lógicas de transferencia 8, 9 y 10, otros eventos indeseables conectados con las puertas lógicas y , o según el caso formando más árboles de fallas.

7.3.3 FALLA DE LA CONTENCION FORMADA POR EL EDIFICIO DEL REACTOR

El edificio del reactor está construido de modo de actuar como una tercera barrera de contención de los materiales radiactivos.

Al efecto tiene un revestimiento metálico interior para dar hermeticidad que está equipado con un sistema de penetraciones para permitir el paso de cables de energía eléctrica, cables de instrumentación y control, líneas de aire para actuaciones de control, compuertas para el paso de personal y equipo, penetraciones para el paso de tuberías de alimentación y vapor, sistemas de control de la atmósfera, sistemas de drenaje y sistemas de aislación; además de la determinación de los niveles de radiactividad en el interior del edificio del reactor, hay un sistema de detección de fugas en todas las soldaduras del revestimiento metálico del edificio.

Los eventos indeseables que pueden ocasionar la ocurrencia de la violación de esta tercera barrera concurren a través de la puerta lógica 11 conectados según el caso, con las puertas lógicas "O" y "Y" formando más árboles de fallas.

7.3.4 FALLA DEL CONTROL DE EFLUENTES DEL EDIFICIO DEL REACTOR

Los efluentes del edificio del reactor, están sujetos a medición de los niveles de radiactividad para determinar los procedimientos de manejo y control en el edificio auxiliar mediante los sistemas de tratamiento de materiales radiactivos.

La pérdida de este control puede originarse por errores remanentes de diseño tales como:

Insuficiencia en capacidad disponible de almacenamiento de efluentes del edificio del reactor.

Insuficiencia en capacidad de tratamiento de efluentes del edificio del reactor.

Falta de capacidad para enviar los efluentes radiactivos del edificio auxiliar a los sistemas de tratamiento de - desechos.

Estos eventos indeseables en estado de reserva alerta ocasionaron en el caso TMI-2 la pérdida del control de los efluentes radiactivos procedentes del edificio del reactor por violación de la tercera barrera, la concurrencia del evento indeseable principal: liberación no controlada de material radiactivo al medio ambiente.

7.3.5 ARBOL DE FALLA DEL CONTROL DE EFLUENTES DEL EDIFICIO DEL REACTOR

Evento 112: Falla del control de efluentes radiactivos del edificio del reactor.

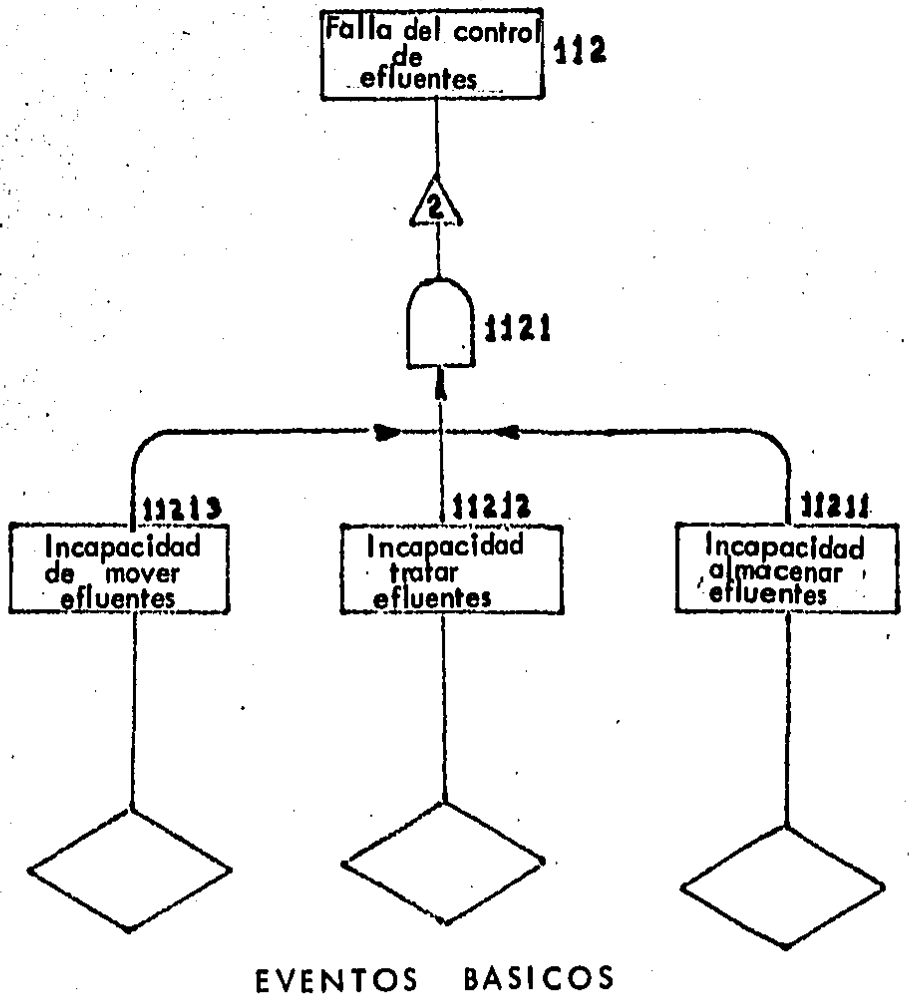


FIGURA 5 ARBOL DE FALLA DEL CONTROL DE EFLUENTES DEL EDIFICIO DEL REACTOR.

Evento 1121: Combinación de los eventos 11211, 11212 y 11213.

Evento 11211: Falta de capacidad para almacenar los efluentes radiactivos del edificio del reactor

Evento 11212: Falta de capacidad de tratamiento de los efluentes radiactivos del edificio del reactor.

Evento 11213: Falta de capacidad para transferir los efluentes -- del edificio del reactor al tratamiento de desechos radiactivos.

Estos tres últimos eventos se consideran como fallas básicas.

7.4 ELIMINACION O DISMINUCION DE LAS PROBABILIDADES DE OCURRENCIA DE LOS EVENTOS INDESEABLES.

El proceso de representar mediante árboles de falla las relaciones entre todos los eventos indeseables y las fallas básicas de los componentes elementales de los sistemas de una planta, puede generar una cantidad enorme de diagramas. Para el objetivo de este trabajo se limita este proceso a la eliminación o disminución de las probabilidades de ocurrencia de los eventos que pueden amenazar la integridad de las barreras de contención, considerando a cada barrera como si fuera la única y encontrar formas de hacerlas resistentes a las consecuencias de los eventos indeseables que no se pueden eliminar.

7.4.1 ARBOL DE FALLA DEL ENCAMISADO OCASIONADA POR TEMPERATURA EXCESIVA

La temperatura excesiva del encamisado es un evento indeseable -

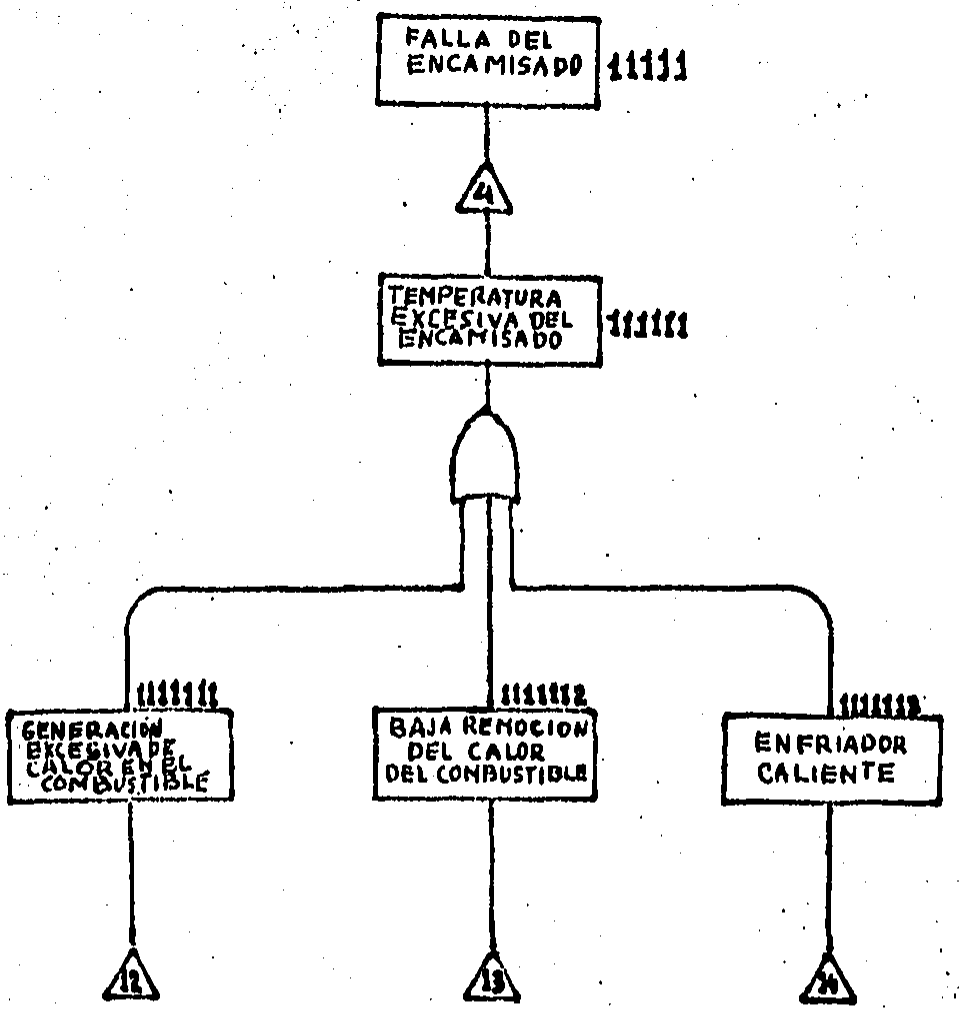


FIGURA 6 ARBOL DE FALLA DEL ENCAMISADO OCASIONADA POR TEMPERATURA EXCESIVA DEL ENCAMISADO.

ocasionado por la concurrencia de cualquiera de tres eventos: generación excesiva de calor en el combustible, baja remoción del calor del combustible, enfriador caliente que no extrae suficiente calor.

El calor se genera en el combustible en dos formas: calor inmediato producido por la fisiones y calor residual producido por el decaimiento radiactivo de los fragmentos de fisión tiempo después del acontecimiento de las fisiones.

El régimen del flujo de neutrones en un reactor crítico fija el régimen de fisiones y en consecuencia el nivel de potencia térmica del reactor, para elevar el nivel de potencia térmica se introduce reactividad positiva en el reactor ya sea por manipulación de las barras de control, por dilución del boro de la cuña química, por recirculación más rápida del moderador o por la entrada de moderador frío, esta reactividad positiva debe cancelarse a la llegada del reactor al nivel de potencia deseado de lo contrario el nivel sigue subiendo y en consecuencia la temperatura del encamisado excede los límites permitidos para operación segura causandose daños al encamisado y violación de la primera barrera.

La baja remoción del calor del combustible puede producirse por pérdida del enfriador, por baja circulación del enfriador, por oclusión que baja el flujo del enfriador o por cambio de estado del enfriador; como resultado aumenta la temperatura del encamisado.

Si el enfriador se calienta por pérdida de la transferencia de calor en los generadores de vapor o en los intercambiadores de calor, la diferencia de temperaturas del encamisado y del enfriador disminuye y en consecuencia disminuye la transferencia de calor del encamisado al enfriador y empieza a subir la temperatura

del encamisado hasta un punto de equilibrio que puede ser superior a los límites de operación segura.

Otros eventos posibles son la falta de sumideros de calor adecuados para extraer el calor del enfriador o la falla de los sistemas de emergencia por actuaciones erróneas del operador o por la presencia de gases no condensables que interfieren con la circulación forzada del enfriador conduciendo a su calentamiento.

Dependiendo de la elección de materiales para el encamisado del combustible y el enfriador pueden tener lugar reacciones entre los productos de fisión y el material del encamisado y entre el enfriador y el material del encamisado. Estos eventos concurren a la puerta de transferencia [5].

Dependiendo de la forma como esté constituido el material combustible pueden ocurrir interacciones entre el combustible y el encamisado: Estos eventos concurren a la puerta de transferencia [7].

La generación de calor en el combustible es su función primaria y puede dársele resistencia a la radiación y a la temperatura -- además de integridad mecánica en la forma de óxidos o carburos de uranio. La conductividad térmica no es suficiente para evitar grandes esfuerzos térmicos resultantes que pueden fracturar al combustible. Tanto los óxidos como los carburos retienen la mayoría de los productos de fisión y la razón de difusión de los gases es pequeña abajo de los 1000°C.

Los reactores de agua ligera utilizan óxidos de uranio con encamisado de aleaciones de zirconio. En los dos tipos de reactores de agua ligera es de importancia vital que nunca quede descubierto de agua el núcleo del reactor pues la temperatura del encami-

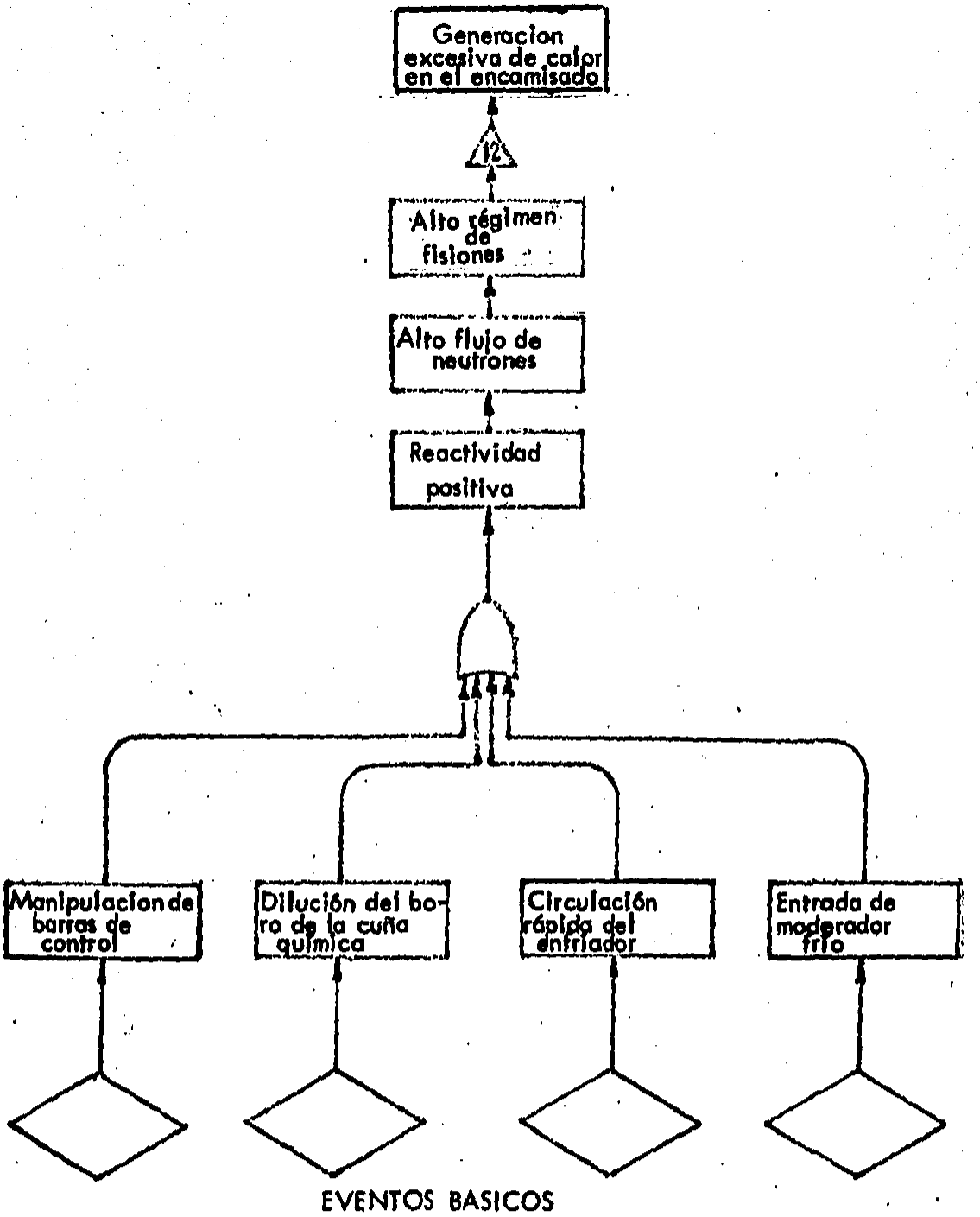


FIGURA 7 ARBOL DE LA GENERACION EXCESIVA DE CALOR EN EL COMBUSTIBLE

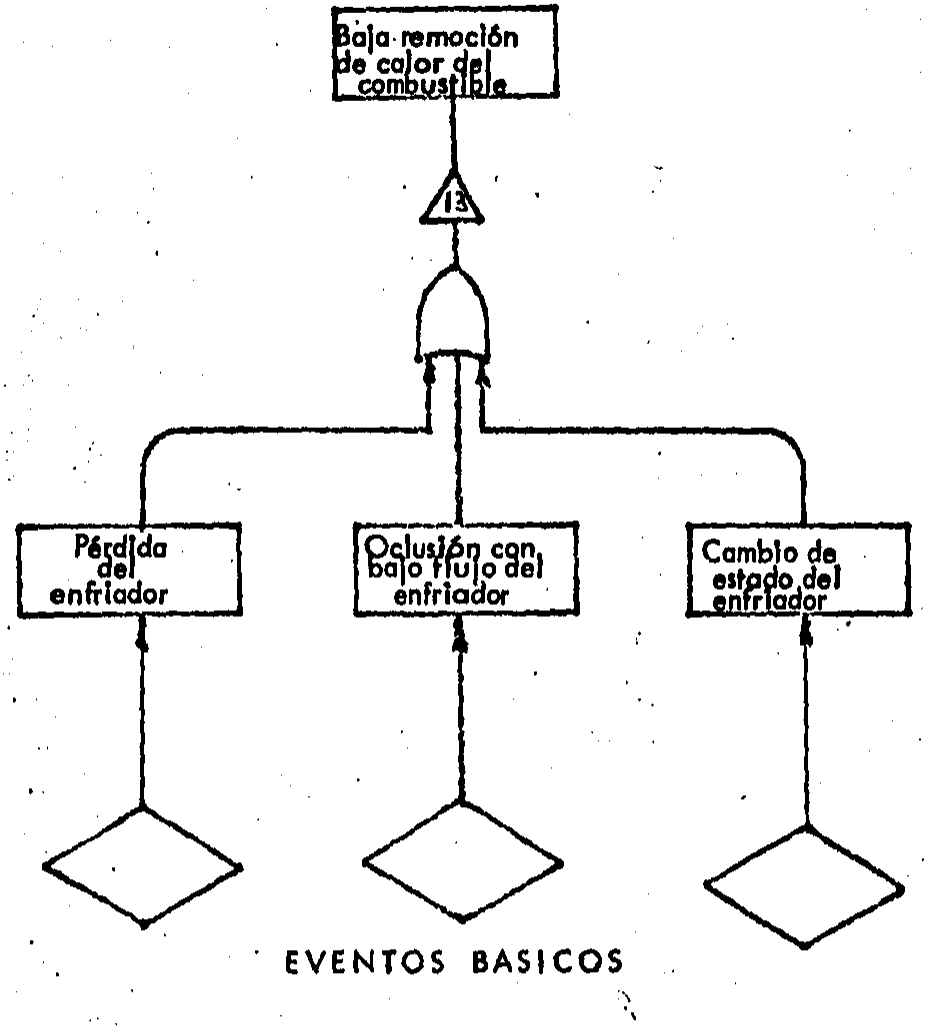


FIGURA 8 ARBOL DE LA BAJA REMOCION DE CALOR DEL COMBUSTIBLE

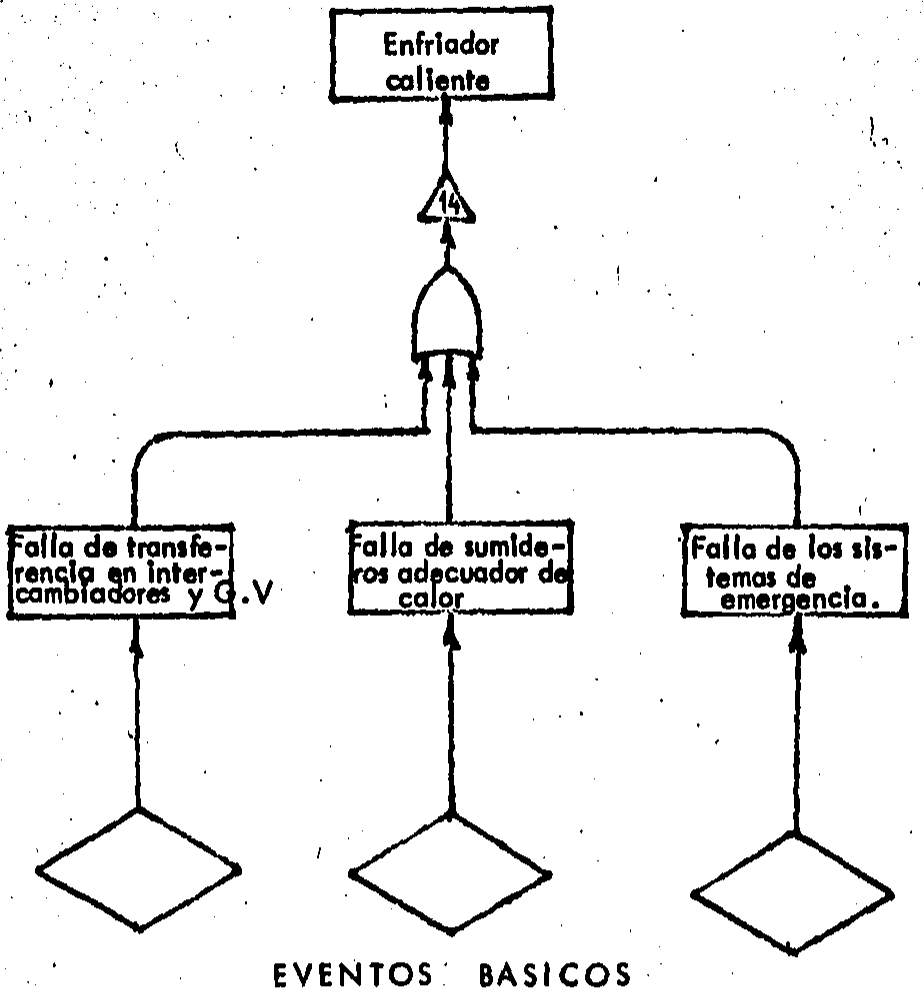


FIGURA 9 ARBOL DEL ENFRIADOR CALIENTE

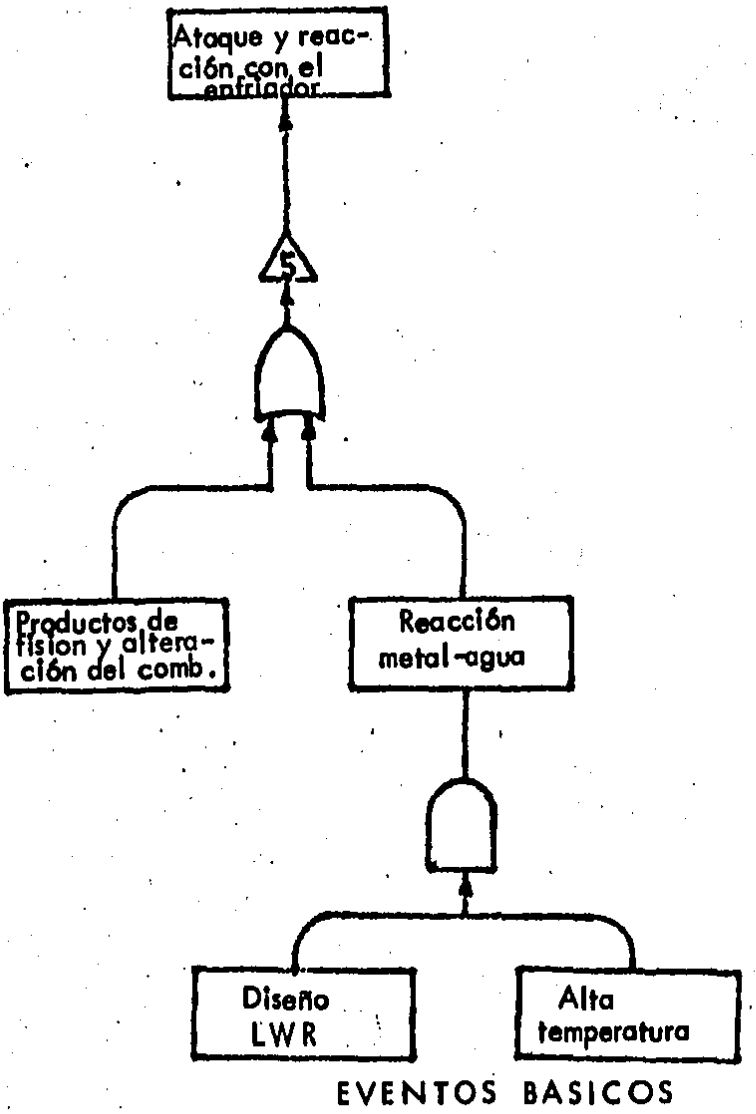


FIGURA 10 ARBOL DEL ATAQUE, CORROSION Y REACCION DEL ENCAMISADO CON EL ENFRIADOR

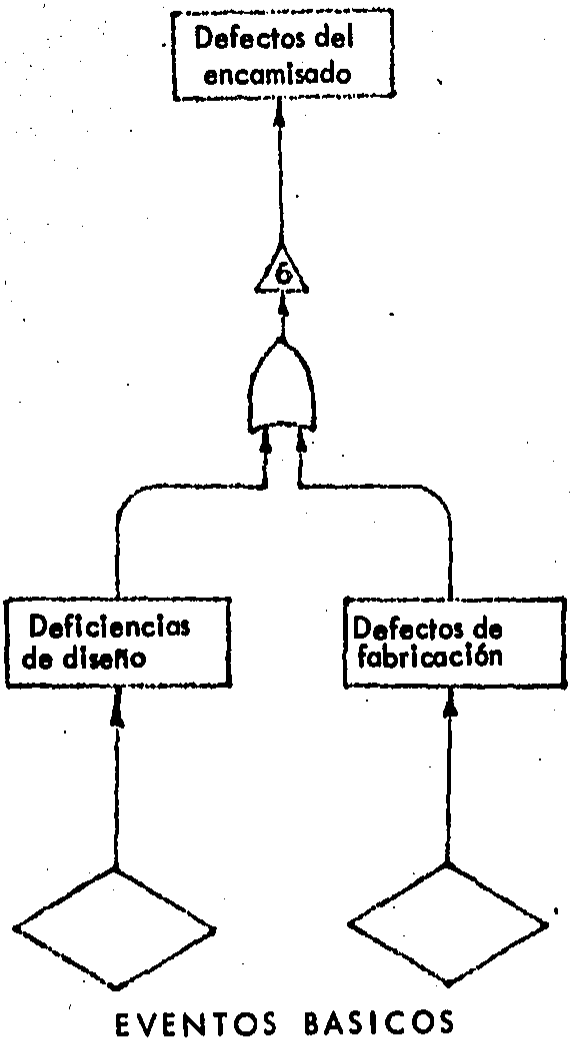


FIGURA 11 ARBOL DE LOS DEFECTOS DEL ENCAMISADO

sado sube rápidamente fundiendo la aleación de zirconio además - de producir la reacción metal - agua perdiéndose la integridad de la primera barrera de aquí que estos reactores deben estar -- previstos de las llamadas "características de ingeniería de seguridad" en forma redundante y diversificada incluyendo sumideros de calor dentro y fuera de la contención primaria para hacer a cualquier emergencia.

Los reactores del tipo de alta temperatura refrigerados por gas helio y moderados por grafito HGTR utilizan como combustible oxicarburo de uranio acompañado por carburo de Torio como material fértil en forma de esferillas de 100 a 500 um de diámetro del núcleo de combustible revestidos con carbón pirolítico de alta resistencia y carburo de silicio con espesor de 130 um. La pequeñez del núcleo combustible limita los choques térmicos, el revestimiento soporta altas temperaturas, el enfriador es inerte y el moderador es refractario al calor con excelentes propiedades de moderación.

El moderador de grafito tiene una capacidad de absorción del calor residual tal, que suponiendo que fallara totalmente al en - friamiento por helio, pasaría una hora antes de que el núcleo alcanzara 1650°C, el combustible de esferillas de oxicarburo de -- uranio y óxidos de torio revestidos con carbón pirolítico pueden soportar 2200°C que no se alcanzarían hasta después de 10 horas, tiempo amplio para restablecer el enfriamiento en contraste con los reactores de agua ligera en los que se daña el encamisado -- del combustible al minuto.

Naturalmente en estos reactores no existe la reacción metal-agua y no hay probabilidad del paso de eventos por la puerta de transferencia 5.

Dada la composición del combustible y su geometría las probabilidades del paso de eventos por la puerta de transferencia 7 que - dan reducidas a las probabilidades de las consecuencias de eventos externos tales como guerras, sabotaje y terremotos.

Las características de ingeniería de seguridad de estos reactores tienen menos complicaciones que las de los reactores de agua ligera y la condición física del refrigerante puede conocerse mediante la medición de dos parámetros interrelacionados: presión y temperatura sin las complicaciones de interfases líquido - vapor y no hay el riesgo de que el núcleo del reactor quede descubierto, de aquí que la información dada al operador por la instrumentación sea de fácil interpretación además del amplio margen de tiempo que tiene el operador para hacer diagnósticos de - situaciones en casos de emergencia con amplio margen de verificar la corrección de diagnósticos y actuaciones.

El fluido de trabajo está practicamente libre de radiactividad y el concreto con membrana metálica de hermeticidad proporciona -- blindaje al personal y simplifica la operación, el mantenimiento y las inspecciones en servicio.

El ahorro en costos permite asignar mas recursos a la reducción de efluentes radiactivos al medio ambiente mediante sistemas de purificación y recuperación del gas, como consecuencia, los reactores de alta temperatura enfriados con helio y moderados con -- grafito, liberan al medio ambiente mucho menos materiales radiactivos que los reactores de agua ligera con los cuales compiten - en costos de generación eléctrica por su mayor eficiencia térmica. (Referencia 8).

En estos reactores se aminoran las consecuencias de los eventos que pudieran concurrir a la puerta lógica de transferencia 3.

7.4.2 SISTEMAS AVANZADOS DE RESPALDO A LA FUNCION HUMANA

En los árboles de fallas se han presentado los eventos que amenazan la integridad de las barreras en forma incompleta mediante - la cual se pueden encontrar tres grupos de eventos:

Eventos originados por el factor humano
Eventos originados por fallas básicas
Eventos externos (citados en la discusión)

Por otra parte el Estudio Birkhofer realizado en Alemania cuantifica la contribución relativa de causas de la fusión del núcleo en la siguiente forma:

Errores humanos	63%
Fallas de componentes	23%
Fallas en modo común	14%

Teniendo en mente el factor humano, presente en todo momento desde la concepción del proyecto hasta su realización y explotación, las complejas relaciones entre eventos podrían representarse por centenares de árboles de fallas y de acuerdo con el tipo de reactor se podrían encontrar muchas formas diversas de diseñar características de ingeniería de seguridad y sistemas de instrumentación y control con puntos de mediciones y actuaciones automáticas ubicadas en lugares estratégicos en la lógica de los sistemas de manera de cancelar o mitigar las consecuencias de los --- eventos indeseables y para dar al operador en la sala de control la información completa sobre el estado de la planta, las configuraciones normales y anómalas de los sistemas, los datos de las variables y parámetros de procesos incluyendo sus tendencias.

Parte de esta información se dá al operador, en las actuales salas de control, a través de anunciadores, indicadores, registradores y alarmas visuales y acústicas; este cúmulo de señales y -

la complejidad introducida por el aumento de información y el poco tiempo tiempo disponible para que el operador diagnostique - las situaciones que requieren acción inmediata, sobrepasan la capacidad humana y deben buscarse otros medios de procesar la in - formación instrumental y presentarla en forma integrada al operador por medio de pantallas de tubos de rayos catódicos (CTR).

Los sistemas de proceso de información presentan en forma gráfica los márgenes de operación segura y el operador puede llamar a los controles de actuación automática, verificar las lógicas y - ordenar desde las pantallas las actuaciones de seguridad, sin - lentas y complicadas actuaciones manuales, con el respaldo de secuencias previamente programadas y de diagnósticos oportunos y rápidos que incluyen la verificación automática de los instrumentos.

La integridad de los sistemas de la planta debe protegerse me - diante un sistema de realización de pruebas que detecta, identifica y localiza en la fase temprana las fallas, dahdo al opera - dor las indicaciones en las pantallas incluyendo la predicción - de las tendencias de los procesos para que decida las actuacio - nes inmediatas a través de los diagramas interactivos mostrados en las pantallas.

El operador ve inmediatamente los efectos de sus actuaciones con las predicciones de las tendencias de los procesos que ha modificado. Los dispositivos de pruebas están interconstruídos en los equipos y componentes que supervisan en forma continua, pulsante o interruptiva para detectar la mayor cantidad posible de fallas tanto en los componentes en línea como en los que están en reserva activa, pasiva o en alerta, de entrada automática como sea -- compatible con las condiciones reales de operación o con las funciones simuladas para las pruebas.

Los paquetes de programas de computación para el sistema de pruebas dan la localización, jerarquía, identificación y los cambios lógicos correspondientes a las fallas detectadas. Llevan en memoria las frecuencias de las pruebas ya sean pulsantes o interruptivas, los tiempos de funcionamiento y ejecutan los cálculos de confiabilidad de tiempos disponibles antes de falla de los componentes y listando su reemplazo en los tiempos disponibles en los paros programados o su salida o entrada automática en línea por sustitución o reposición en los componentes en alerta automática.

El historial de pruebas está correlacionado con el historial de operación llevado por la computadora de proceso y se integran los dos historiales para procesar y dar la información detallada en los casos de fallas importantes incluyendo además de la localización, identificación y áreas afectadas por las fallas, los datos de los variables y de los parámetros de proceso y las condiciones meteorológicas y sísmicas en el momento que ocurrió o se detectó la falla.

La acumulación sistematizada de la experiencia operación puede ampliar los paquetes de programas para hacer mas precisas las predicciones de comportamiento y vidas útiles de componentes.

Al madurar esta sistematización será posible establecer el mantenimiento predictivo de la planta y la optimización de la operación, al tiempo que se mejora la seguridad al minimizar las probabilidades de confusión del operador.

Estos sistemas avanzados de instrumentación, control, integración de la información, sistematización de la experiencia y respaldo a la función humana que se han descrito conceptualmente, pese a su potencial y extensa gama de aplicaciones, no son de fá

cil realización ya que implican cambios en las actitudes y filosofías actuales de diseño de las características de ingeniería de seguridad ademas de la implementación de las actividades de investigación, diseño de prototipos de ensayo y pruebas hasta llegar a las líneas de producción de equipo y componentes con dispositivos interconstruidos para pruebas de funcionamiento durante su uso específicamente diseñados para dar la integración y presentación de información precisa, completa y oportuna en la forma requerida.

En la condición presente de sistemas y salas de control de diseño inadecuado, es viable introducir mejoras de fácil realización tales como la instalación de circuitos cerrados de televisión que permitan la supervisión visual de situaciones tales como posición de válvulas y de interruptores, fugas de vapor y derrames de líquidos en las diversas instalaciones de la planta; instalación de detectores y analizadores de vibraciones en el equipo rotatorio, tuberías y recipientes; redistribución de la sala de control y rearreglo de anunciadores, indicadores, registradores y alarmas, remarcado de carátulas indicando los márgenes de operación segura, semiautomatización para efectuar una serie de mandos en secuencia correcta con una sola actuación del operador, pruebas de pulso de circuitos eléctricos sin interferir con las funciones, verificación de calibración de instrumentos, reducción del número de anunciadores al concentrar la información, sustitución de los registradores que dan gráficas en cinta de papel por registradores de memorias magnéticas de archivos compactos y selección rápida de información por lectura en pantallas CRT con acoplamiento opcional a impresoras obteniendose consolas compactas de mando que facilitan al operador la percepción de la información.

Todas estas modificaciones contribuyen a la disminución de las probabilidades de ocurrencia del evento indeseable; confusión -- del operador causada por el cúmulo de señales y el poco tiempo disponible para su correcta interpretación.

La implantación completa de los sistemas avanzados de instrumentación, control, integración de la información, sistematización de la experiencia operacional, realización de pruebas, identificación de fallas y entrada automática en línea de componentes en reserva, además de minimizar efectivamente las probabilidades de errores por confusión, disminuyen las probabilidades de errores en el mantenimiento, tanto por la sustitución automática de componentes como por las predicciones precisas sobre la vida útil de componentes con base a la acumulación sistematizada de la experiencia operacional.

Al conseguir lo anterior, se disminuye la vulnerabilidad de los sistemas de la planta a la formación de configuraciones anómalas inducidas por confusión del operador y ahora hay que tomar en -- cuenta los factores humanos tales como errores de concepto de diseño y defectos de manufactura manejo, instalación, montaje y -- pruebas.

8. SISTEMATIZACION DEL CONTROL Y DE LA CONSTATACION DE LA CALIDAD EN LA INDUSTRIA NUCLEAR

Como ejemplo de la sistematización del control y de la constatación de la calidad que se puede hacer extensiva a otras áreas de la industria nuclear, con reducción notable de la influencia de factores humanos, se describe a continuación el control y la --- constatación de la calidad mediante la implantación ya lograda - de nuevas técnicas aplicadas a la producción comercial de combustible nuclear o sea la primera barrera de contención.

8.1 EL CONTROL Y LA CONSTATACION DE LA CALIDAD DE COMBUSTIBLES NUCLEARES.

El componente primario de un reactor nuclear es el combustible; cuando el combustible se dispone dentro del reactor en la configuración adecuada, sostiene una reacción en cadena de fisiones que genera calor y produce fragmentos de fisión radiactivos.

El problema de seguridad de los reactores nucleares es mantener confinados los materiales radiactivos evitando su liberación al medio ambiente. A ese efecto el combustible debe tener las siguientes características:

1. Transferir el calor generado por las fisiones al enfriador.
2. Contener a los productos de fisión.
3. Alcanzar el quemado previsto y tener la duración deseada.
4. Posibilidad de evaluar el contenido fisionable y ser probado antes de su uso.

Los materiales fisionables adecuados para fabricar combustibles nucleares son tres: U^{233}, U^{235} y Pu^{239}.

El U233 se produce por transmutación del Th232 y se ha utilizado en dos reactores de potencia del tipo HTGR en Peach Bottom y --- Fort Saint Vrain.

El U235 es el único material fisionable que existe en la naturaleza en el Uranio natural. Es el que se emplea en forma de U02 enriquecido en los reactores de agua ligera que son los que al presente predominan en el ámbito mundial.

El Pu239 se produce por transmutación del U238 y ha sido empleado en forma de Pu02 como parte de la recarga de combustible del reactor de agua ligera de San Onofre 1 California en 1970. Se le considera el combustible de los reactores avanzados de cría - del cercano futuro.

El U02 se sinteriza en forma de pastillas que se encamisan en tubos de Zircaloy que es una aleación de Zirconio seleccionada por tener:

1. Adecuadas propiedades mecánicas.
2. Baja absorción parásita de neutrones.
3. Compatibilidad con el enfriador y el combustible
4. Buena conductividad térmica.
5. Estabilidad frente a la radiación.
6. Facilidad de fabricación.
7. Tolerancia al veneno soluble en el enfriador.

Se toma en cuenta la reacción metal-agua que es posible a temperaturas superiores a la temperatura normal de operación.

El uso del acero inoxidable 304 como material de encamisado se - ha descontinuado porque permite la difusión del tritio generado en el combustible al enfriador.

Los métodos de inspección y prueba evolucionaron de las tecnologías de laboratorio a nuevas y poderosas técnicas aplicables a - la producción comercial de combustibles nucleares que pueden --- agruparse según las características del material y los fenómenos físicos o químicos en que se basan:

FENOMENOS FISICOS Y TECNICAS DE PRUEBA ASOCIADAS

I Radiación penetrante.

a) Radiografía y autoradiografía.

b) Espectrometría de centelleo.

c) Irradiación.

d) Calibración por intensidad o atenuación.

e) Difracción.

II Ondas sónicas y ultrasónicas.

a) Ecopulso (reflexión).

b) Resonancia.

c) Trasmisión.

III Penetración y presión.

a) Líquido penetrante.

1. Fluorescente.

2. Colorante

b) Gas penetrante (fugas)

c) Presión diferencial

IV Electricidad y magnetismo.

a) Fugas magnéticas (pruebas con partículas)

b) Calibración por inducción, capacitancia y atracción magnética.

c) Caida de potencial.

d) Corrientes parásitas

e) Triboelectricidad

V Optica.

a) Visual.

b) Microscopia.

c) Metalografía.

d) Espectroscopia.

VI Térmica.

a) Termoelectricidad.

b) Materiales termosensibles

VII Química.

a) Procedimientos húmedos. (incluye radioquímica)

b) Corrosión.

VIII Mecánica.

a) Calibrado.

b) Pesado.

c) Sometimiento a esfuerzos.

d) Tamaño de partículas

1. Distribución por tamaños

2. Area de superficie.

La implantación de estas técnicas en las líneas de producción requirió la preparación de operadores hábiles y con pleno conocimiento de los principios físicos y químicos como base para realizar la fase más difícil de las inspecciones y pruebas: la interpretación de la información obtenida.

Conforme se acumuló experiencia y fué creciendo la industria nuclear, fué posible iniciar la eliminación parcial de los factores personales en las pruebas mediante ayudas mecánicas, que ahorran tiempo, disminuyendo las probabilidades de error.

Se describe a continuación la fabricación actual de combustible nuclear para dar una idea del grado de madurez alcanzado en la industria nuclear en la automatización de procesos y control con sistemas de computación.

El material fisionable se recibe de la planta de enriquecimiento en la forma de UF_6 gaseoso y después de determinar su contenido fisionable y verificar su grado de enriquecimiento se convierte directamente en UO_2 en un horno mediante una reacción química en seco.

La conversión produce el UO_2 en la forma de un polvo que puede - sinterizarse con uniformidad en pastillas de calidad consistente, compactadas y que al quemarse en el reactor nuclear tienen una - densificación mínima como se ha comprobado en las 780 toneladas de pastillas cargadas en reactores en operación y que han cumplido con todos los requisitos de calidad.

Para garantizar la integridad del encamisado de Zircaloy, los tubos se inspeccionan después del primer conformado para verificar su integridad estructural y dimensional, se conforman en frío en tubos de alta calidad, se verifican sus características dimensionales y su integridad mecánica por ultrasonido mediante equipo - automático que captura la información de alta velocidad y anuncia al operador las decisiones de aceptación o rechazo.

Para asegurar que el combustible está libre de agua, se rectifican en seco en lugar del anterior esmerilado en húmero y se desgasifican en un horno de alta temperatura al vacío ya colocadas en el interior de los tubos todavía abiertos en los que se inserta un material absorbedor de hidrógeno.

Se verifica la sequedad de las pastillas por muestreo y los re - sultados se capturan para formar parte de la vasta cantidad de información para la documentación permanente del embarque de combustible.

Cada movimiento en el proceso de combustible está eslabonado al sistema de control del inventario de material con terminales de entrada en toda la planta; este sistema de computadora registra más de 12.5 millones de transacciones anuales de movimientos de uranio desde la llegada del UF_6 hasta el movimiento de una lata de polvo de un transportador a otro.

En esta forma se cumple con los reglamentos de salvaguardia de materiales nucleares y se lleva el sistema de control y contabilidad de materiales.

Este sistema, como parte del proceso de manufactura dá los programas y rutas de producción y otorga las libranzas de control de calidad, lo mismo que la facturación a clientes por embarques de polvo y combustible fabricado. Dá además las libranzas y certificaciones de garantía de calidad y de cumplimiento con las especificaciones de ingeniería. En cualquier punto del proceso se puede verificar el estado de la calidad del material especificado y también verifica el peso del material que va en cada barra de combustible en la estación de carga automática de UO_2.

Se realizan además una variedad de análisis químicos que incluyen análisis espectrográficos de la mayoría de los elementos de la tabla periódica y pruebas físicas desde la medición de las partículas del polvo hasta los estudios microfotográficos de las estructuras básicas de los cristales del metal.

Después de la carga los tubos se soldan con tapones de formas que corresponden a la posición en que serán distribuídos, ya en los ensambles de combustible, en el corazón del reactor.

Los tubos se inspeccionan por exploración activa con rayos gamma y las soldaduras por rayos X.

Se arman los ensambles de combustible que son verificados para - detectar fugas y sujetos a una inspección final antes de su empa que para embarque.

Algunas barras de combustible en las primeras cargas de combusti ble deben contener venenos quemables que limiten la elevada reac tividad inicial en forma tal que al quemarse se vaya reduciendo la limitación.

Este veneno quemable en forma de un óxido de gadolinio se sinte- riza en pastillas junto con el UO_2 y se carga automáticamente en los tubos según control programado.

En una barra dada pueden existir hasta siete zonas con diversos grados de envenenamiento.

Como doble comprobación en la precisión del cargado y de la cali dad, toda la barra se explora y mide el contenido y distribución del gadolinio que tiene propiedades paramagnéticas mediante un - magneto super conductor y se comprueba la densidad y los gramos de uranio verificando la presencia de los resortes y del mate -- rial capturador de hidrógeno en los plenums de las barras de com bustible.

Se mantiene completo rastreo de todas las barras cargadas seria- das en forma única con historias completas de las condiciones de como se procesaron, de los análisis químicos y pruebas físicas - de su localización en los haces de combustible documentadas en - microfilm durante toda la vida del combustible. El grado de con trol de calidad aplicado involucra más de un millón de verifica-

caciones para una carga típica de combustible de 750 haces.

En el próximo futuro, se pondrá a punto la inspección automática de pastillas con rayos laser. Esta inspección, usando la última palabra en la tecnología de circuítos integrados de alta velocidad permitirá identificar con precisión cualquier defecto en las pastillas y eliminarlas clasificándolas por tipo de defecto.

Respecto al control y constatación de la calidad del diseño de plantas nucleoeléctricas mediante la normalización del diseño, ya se ha realizado la ingeniería completa para cuatro plantas en sitios diferentes para empresas distintas con apoyo en avanzados sistemas de computación que eliminan gran parte de los planos y dibujos y que efectúan los cálculos de ingeniería tomando en cuenta los diferentes parámetros peculiares de cada sitio y cliente con ahorros de tiempo considerable con completo apego a los criterios de seguridad y eliminación de las interferencias físicas, revisiones y cambios de diseño originados en el proceso iterativo de la ingeniería convencional obteniéndose diseños de plantas más seguras y confiables.

9. COMENTARIOS, DISCUSION DE INFORMACION RECIENTE Y CONCLUSION.

9.1 Comentarios

Se ha postulado la existencia de defectos y errores humanos remanentes de concepto, diseño, manufactura, construcción, instalación y pruebas como origen de las configuraciones anómalas ocurridas en la explotación del sistema planta-operador al encadenarse con eventos transitorios con probabilidad de causar finalmente eventos indeseables a través de mecanismos que se han tratado de identificar en este trabajo.

Se han discutido algunas de las características de los reactores de agua ligera y de alta temperatura enfriados por gas respecto a la eliminación o disminución de las probabilidades de ocurrencia de eventos indeseables y de la vulnerabilidad de los sistemas de la planta a la formación de configuraciones anómalas.

En la descripción conceptual de los sistemas avanzados de respaldo a la función humana se han discutido las posibilidades de hacer accesible al operador la información de las configuraciones de la planta, del estado de las variables de proceso en forma integrada y digerible, de diagnósticos tempranos de las condiciones precursoras de eventos indeseables y las posibilidades de poner en acción por mando manual sencillo, secuencias automáticas de actuaciones correctivas complicadas y la necesidad de dar prioridad a las actuaciones automáticas sobre la actuación manual en condiciones de emergencia.

Antes de presentar las sugestiones finales, se transcribe y discute la información reciente tomada de las referencias que se citan a continuación:

Investigación del evento TMI-2 realizada por la NRC. Para realizar las investigaciones y evaluaciones del accidente TMI-2, la Comisión Reguladora Nuclear de los Estados Unidos (NRC), integró el grupo "TMI-2 Lessons Learned Task Force" cuyo propósito fué: "...identificar y evaluar aquellos aspectos correspondientes a la seguridad que se originaron por el accidente TMI-2 que requieren acciones de licenciamiento aplicables tanto a los reactores en operación al presente como a los que están pendientes de licencia de operación". (referencia 9).

La conclusión principal a que llegó este grupo fué que: "...aunque el accidente en TMI surgió de muchas fuentes, las lecciones aprendidas mas importantes caen en un área general que hemos escogido llamar seguridad operacional. Esta área general incluye los tópicos de la ingeniería de factores humanos, del entrenamiento y la calificación del personal de operación, de la integración del elemento humano en el diseño, la operación y la regulación del sistema de seguridad y la garantía de calidad de la operación".

Las recomendaciones finales dadas por este grupo fueron:

.1 Entrenamiento y calificación del personal
.2 Personal de la Sala de Control
.3 Horarios de trabajo
.4 Procedimientos de emergencia
.5 Verificación de la realización correcta de las actividades de operación
.6 Evaluación de la experiencia de operación
.7 Interfase hombre-máquina
.8 Estimación de confiabilidad del diseño final
.9 Revisión de las calificaciones y clasificaciones de seguridad
.10 Características de diseño de accidentes con daño al núcleo y fusión del núcleo.
.11 Objetivos de seguridad de las regulaciones relativas

al reactor

.12 Revisión de los objetivos del personal

.13 Grupo de respuestas a emergencias NRC

9.3 Investigación del evento TMI-2 realizada por la Comisión Kemeny.

La Comisión Kemeny, designada por el presidente de los Estados Unidos para evaluar el accidente TMI-2 concluyó después de seis meses de investigaciones que:
"para evitar accidentes tan serios como el TMI-2 son necesarios cambios fundamentales en la organización, procedimientos, prácticas y sobre todo en las actitudes, tanto de la NRC como, en la extensión de que las instituciones que investigamos son típicas, de la industria nuclear" (referencia 10).

El informe de la Comisión y los reportes del personal detallaron las bases que respaldan la anterior conclusión y reafirmaron que "...los problemas fundamentales (respecto a la seguridad de planta nucleares) son los problemas relacionados con las personas y no los problemas del equipo".

El reporte de Garantía de Calidad de la Comisión reportó que:

1. La organización, procedimientos y prácticas de la NRC no combinan la función gerencial, la ingeniería ni la revisión que garantice el comportamiento necesario - de la empresa generadora para minimizar las probabilidades de fallas del equipo y del operador para lograr la operación segura de la planta nuclear.

2. La falta de garantía de calidad o de una evaluación de la seguridad del equipo y operaciones de la planta no considerados como "relacionados con la seguridad" contribuyó en forma significativa a la ocurrencia del accidente TMI.

3. Falta de análisis detallados de seguridad y modos de falla en todos los sistemas de la planta para asegurar la confiabilidad y la seguridad de la planta.

4. Ingeniería de sistemas; las interacciones entre sistemas y la interacción entre el equipo y los operadores generalmente no han sido consideradas en el proceso de revisión de la NRC.

5. El presente sistema de reporte de eventos en la operación no asegura la difusión y utilización de información de fallas en la industria. No existe un análisis comprensivo de fallas y desviaciones ni un sistema de aplicabilidad de acciones correctivas a todos los sistemas y operaciones que afectan la confiabilidad y la seguridad de la planta.

6. Las prácticas actuales de la empresa generadora y la NRC no aseguran la adecuada preparación, revisión y ejecución de los procedimientos de mantenimiento por el operador.

7. NRC tiene un punto de vista muy limitado de los cambios hechos a la configuración de la planta. El control de la empresa generadora respecto a los cambios en el equipo relacionado con la seguridad parecen adecuados; la contribución a la configuración del equipo no relacionado con la seguridad es inadecuada.

8. No se hace uso pleno de las prácticas de gerencia, ingeniería, seguridad, confiabilidad y garantía de calidad en uso en otras industrias donde la seguridad y la confiabilidad son críticas.

9.4 Información dada por la Oficina de Prensa de la Casa Blanca (USA)

COMUNICADO DEL PRESIDENTE DE LOS E.U.A.

"...Una de las mejores fuentes potenciales de nuevos suministros de electricidad en las décadas venideras es la energía nuclear. Los Estados Unidos han desarrollado una fuerte base tecnológica en la producción de electricidad por medio de la energía nuclear. Desafortunadamente el Gobierno Federal ha creado un ambiente regulador que está obligando a muchas productoras de electricidad a descartar la energía nuclear como una fuente de nueva capacidad de generación, aún cuando los consumidores deban encarar como resultado tasas innecesariamente altas de electricidad La energía nuclear está maniatada en un pantano de regulaciones que no mejoran la seguridad pero que causan extensos retrasos de licenciamiento e incertidumbre económica.

Para corregir las presentes deficiencias del gobierno y para permitir que la energía nuclear aporte su contribución esencial a nuestras necesidades futuras de energía, estoy anunciando hoy una serie de iniciativas políticas:

1) Doy instrucciones al Secretario de la Energía para -- dar la inmediata atención prioritaria a recomendar mejoras en el proceso de licenciamiento y regulación nuclear. Anticipo que el Presidente de la Comisión Reguladora Nuclear dará los pasos para facilitar el licenciamiento de las plantas en construcción y de las que esperan licencias. En consistencia con la salud y seguridad públicas, eliminaremos los obstáculos innecesarios para el desarrollo de la generación corriente de reactores nucleares de potencia...
...Eliminar los problemas de regulaciones que han pesado en la industria nuclear sería de poca utilidad si el sector que genera electricidad no pudiera conseguir el capital necesario para la construcción de nuevas plantas generadoras. Hemos dado pasos significativos para mejorar el clima para la formación de capital

al paso de mi programa de recuperación económica. La tarifa de impuestos contiene substanciales incentivos para atraer nuevo capital a la industria". (referencia 11).

.5 Discusión

En los Estados Unidos las guías reguladoras se aplicaron principalmente a los reactores de agua ligera tipos BWR y PWR y por excepción a dos reactores del tipo HTGR enfriados con helio y moderados con grafito. El incremento desordenado de los requisitos incluidos en las guías regulaдoras (1.3 requisitos nuevos por cada día de trabajo en 1978) dió la apariencia de errático tratamiento sintomático y no causal de los problemas de seguridad de los reactores de agua ligera.

El cumplimiento de estos requisitos no anticipados, además de las penalizaciones en costos, de las demoras e incertidumbres que causaron, no mejoraron la seguridad de las plantas a las que hicieron cada vez mas complicadas con modificaciones imprevistas, dificultando el proceso de licenciamiento hasta hacer inaplazable la actuación correctiva de la máxima autoridad de los Estados Unidos. (referencia 12).

El hecho de que un proyecto nucleoeléctrico cumpla con las regulaciones y requisitos impuestos para lograr el licenciamiento no significa que con más y más regulaciones y requisitos aumente más y más la protección a la salud pública.

El hecho de que los cálculos probabilísticos demuestran la alta confiabilidad intrínseca de los proyectos nucleoeléctricos tampoco garantiza la confiabilidad operacional del sistema planta operador.

Las limitaciones de esos dos puntos de vista: la reglamentación del uso de un energético y el análisis actual de riesgos por el uso de un energético fueron percibidas con anterioridad al accidente TMI-2, por ejemplo en 1974 el Instituto de Investigaciones de la Energía Eléctrica (Electric Power Research Institute. EPRI) de Palo Alto, California U.S.A. llevó a cabo un estudio de tecnologías avanzadas no nucleares y su aplicación a la industria nuclear. Estos puntos de vista diferentes, evidenciaron varias deficiencias tales como:

a) Los requisitos de la AEC (Atomic Energy Comission) relativos a la garantía de calidad se limitaban al equipo relacionado con la seguridad.

b) Falta de identificación y análisis de los modos de falla del equipo.

c) Falta de utilización de la información de fallas

d) Control desbalanceado de la seguridad

e) Falta de productos y de abastecedores calificados.

f) Ocurrencias anormales causadas por el personal

g) Ciega confianza en las predicciones numéricas.

Actualmente el EPRI opera el Centro de Análsis de Seguridad Nuclear (Nuclear Safety Analysis Center NSAC) con el soporte y concurrencia de los fabricantes y de los propietarios de los Sistemas Nucleares de Suministro de Vapor en operación o en construcción para explorar plenamente desde muchos puntos de vista, las posibilidades de aplicación a problemas de diversas tecnologías selectas existentes y de probada eficacia y de desarrollar a ese mismo fin nuevas tecnologías.

Se debe mencionar también que los fabricantes de los Sistemas Nucleares de Suministro de Vapor no descuidaron los aspectos de ingeniería humana y que ofrecieron a las empresas productoras de electricidad opciones de salas de control con sistemas y consolas ensambladas y alambradas en fábrica con instrumentación completa verificada en bancos de prueba con eliminación de errores remanentes. Las ventajas de estas opciones no siempre fueron aprovechadas por diversos motivos, entre ellos el hecho de que cada mejora provocaba problemas de licenciamiento que se evitaban repitiendo diseños ya licenciados.

Actualmente se han identificado las áreas que presentan problemas, se han definido los grados de viabilidad de las soluciones y se ha estimado el impacto que causarían en las practicas actuales.

Considerando solamente dos áreas principales como la Ingeniería Humana y la Seguridad, la Confiabilidad y la Garantía de Calidad, se pueden citar algunos ejemplos:

Ingeniería Humana

a) Entenamiento y calificación de Operadores
   Medios: métodos, simuladores, técnicas de entrenamiento y procedimientos de calificación
   Impacto: reestructurar los programas presentes eliminando las deficiencias actuales.

b) Ayudas y herramientas para operadores
   Medios: ayudas visuales, herramientas analíticas como microprocesadoras de escritorio fuera de línea.
   Impacto: mínimo requiere revisión e implementación

c) Diseño de la sala de control y comportamiento operacional.

Medios: los señalados en descripción conceptual de los sistemas avanzados de respaldo a la función humana. (referencia 13)
Impacto: mayor. Realizable en la siguiente generación de reactores. Requiere aplicación de los factores antropométricos conocidos y ampliación de los conocimientos actualmente incompletos del comportamiento humano en condiciones diversas normales y adversas.

Seguridad, Confiabilidad y Garantía de Calidad

a) Análisis de riegos
Medios: enfoque organizado y estructurado de la ingeniería de seguridad.
Impacto: requiere reanálisis independiente de la actual postulación de eventos base de diseño y dar nuevos enfoques a los criterios de falla tales como el enfoque de "falla sin pérdida funcional" fundamentalmente diferente del criterio de falla única, y los análisis de riesgos en la operación, de circuitos espurios y de configuraciones anómalas que no han sido considerados plenamente en la industria nuclear.

b) Deficiencias en la seguridad, la confiabilidad y la garantía de calidad.
Medios: ingeniería de seguridad y confiabilidad basada en los nuevos análisis y enfoques citados en a).
Impacto: máximo. Requiere extenso trabajo y tiempo adicional en los análisis de riesgo bajo los nuevos enfoques que significan cambios en los criterios actuales. Investigación y desarrollo integral de la teoría de la confiabilidad intrínseca, humana y operacional con respaldo de la consolidación experimental en condiciones reales y simuladas del comportamiento humano, revisión de las prácticas del control y garantía de calidad en todas las etapas del proyecto nucleoe-

léctrico para lograr la reducción de la influencia del factor humano como se sugiere en el ejemplo citado del control y la constatación de calidad en la fabricación de combustible nuclear.

Conclusion

El evento TMI-2 obligó a considerar en nueva perspectiva las cuestiones de seguridad. Diversas Instituciones organizaron grupos de trabajo a ese efecto que concordaron en la identificación de deficiencias, propusieron medidas correctivas y propusieron medidas correctivas y desarrollaron programas de implementación aplicables a las plantas en operación o en término cercano a su licenciamiento, particularmente en la interfase planta-operador se enfocaron a las mejoras de las salas de control y a los factores humanos. Se tiene presente la preocupación de que estos programas,aplicables en cercano término a la corrección de notorias deficiencias, no conducen a la aplicación de los sistemas integrados de mayor relevancia respecto a la seguridad, los cuales requieren largo término de implementación y cambios completos, apenas en inicio, en las características de la industria nuclear.

Si se considera deseable el control manual de los reactores de potencia, estos deben ser del tipo de reactor simple, estable y "noble" que perdone errores por ser insensible a ellos, como el tipo HTGR que se ha descrito y que no requiere control por computadora en línea por estimar que los programas de control podrían ser demasiado complejos y poco confiables y que el operador quedaría aislado del reactor y no estaría preparado para entrar en acción en caso de accidente.

Si se considera que es más confiable el control por computadora que el control humano directo y

que la confiabilidad de las computadoras pueden mejorarse mediante diseños depurados ya verificados y que el accidente TMI-2 y la gran mayoría de otras fallas de operación pudieron evitarse con el control de computadora, este control tiene viabilidad de implantarse en los reactores del tipo LWR a pesar de las complicaciones introducidas por la automatización. (referencia 13).

Al presente se desarrollan varias ayudas de computadora - para informar al operador sobre los estados de operación de la planta tales como el sistema de indicación de los parámetros de seguridad (Safety Parameter Display System SPDS) en estudio en el ENSAC del EPRI. (referencia 14), el sistema de supervisión y análsis de disturbios (Disturbance Analysis and Surveillance System DASS) en el que trabajan dos grupos de Westinghouse y de Babcock & Wilcox a contrato con el EPRI y el Departamento de Energía, un sistema de análisis de disturbios con auspicio multinacional de Europa, se desarrolló en el Proyecto Halden en Noruega y fué la base del sistema STAR instalado en el reactor Grafenrheinfeld en Alemania Occidental (referencia 14). Tanto el sistema DASS como el STAR tienen el mismo objetivo, sus capacidades de diagnóstico son esencialmente secuencias preanalizadas de accidentes, cuando la computadora recibe señales de los sensores que analizados indica disturbio, da aviso de acciones correctivas. Si actúan - los sistemas automáticos de protección en caso de accidente el operador queda fuera de acción por 30 minutos en los que los sistemas automáticos tienen prioridad sobre - la actuación manual.

9.7 Se presentan ahora las sugestiones finales de acuerdo a las condiciones de nuestro país.

1a. El exceso de regulaciones y las posiciones conservadoras relativas a la seguridad están en proceso de revi

sión y mejoramiento en el ámbito internacional de la energía nuclear; toca a los organismos autorizados decidir cuáles de esas mejoras se adoptan en nuestro país.

2a. La función gerencial de los proyectos nucleares en todos sus aspectos debe centralizarse y disciplinarse; a diferencia de otros países en que la generación de electricidad la realizan empresas diferentes, es posible establecer en México una organización técnica competente que soporte los proyectos en todo su ciclo de vida.

3a. Incorporar las áreas de seguridad, confiabilidad y garantía de calidad desde el inicio de los proyectos, desarrollando técnicas de búsqueda y eliminación de fallas.

4a. Seleccionar y preparar personal altamente motivado para todas las actividades; personal que esté siempre alerta para detectar y corregir anomalías, evitando la tendencia individualista de establecer pequeños imperios.

5a. La realización de proyectos de alta tecnología tiene el efecto de magnificar las cualidades y defectos de una organización y solamente con eficiencia técnica y administrativa es posible realizar en los tiempos y presupuestos fijados plantas nucleares productivas y seguras.

A P E N D I C E

EXISTENCIA DE DEFECTOS REMANENTES EN LOS PROYECTOS NUCLEOELECTRICOS

Durante la puesta en servicio de una planta nucleoeléctrica la mayoría de las fallas que ocurren en los componentes de los sistemas sujetos por primera vez a las exigencias funcionales, son el resultado de desviaciones no detectadas con respecto a las especificaciones y requerimientos de diseño, suponiendo que este haya sido depurado de errores, ocurridas durante el proceso de fabricación, transporte, almacenamiento, construcción, erección y prueba o sean las operaciones de realización del proyecto.

En el comportamiento humano existe una tendencia al error generalmente sensible al número y complejidad de decisiones y operaciones realizadas.

Las operaciones de realización, inspección y pruebas de un proyecto nucleoeléctrico no son inmunes a este fenómeno y para cada una de las operaciones puede suponerse una probabilidad de error. Por otra parte no todas las operaciones de realización pueden inspeccionarse y aquellas que pueden pueden inspeccionarse no siempre pueden someterse a inspecciones repetidas y no todos los defectos pueden originar una falla ni son detectados todos los defectos que pueden originar una falla.

Si suponemos un proceso maduro en el que en las operaciones de realización se han eliminado los errores gruesos mediante procedimientos documentados depurados por la experiencia al igual que las funciones de inspección realizadas por personal experimentado en control y constatación de la calidad, podemos establecer los siguientes parámetros para encontrar una expresión general -

de las confiabilidades del proyecto.

R Es el conjunto de operaciones durante la fabricación, transporte, almacenamiento, construcción, erección, pruebas e -- inspección o sean todas las funciones de realización.

E_R Es la razón de las operaciones correctas al número total de operaciones realizadas (Eficiencia de realización)

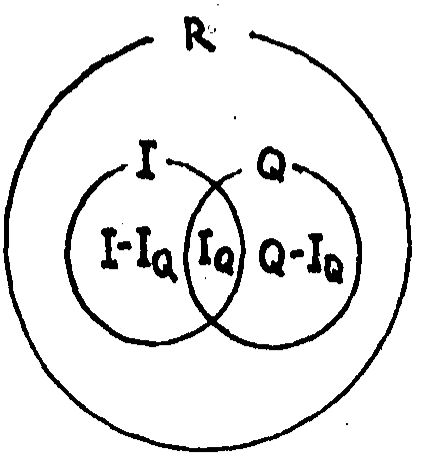
Q Es el conjunto de operaciones críticas que no deben tener - defectos que causen falla $Q \leq R$

I Es el conjunto de operaciones de realización sujetas a inspección $I \leq R$

I_Q Es la intersección de los conjuntos I y Q

E_I Es la razón de las operaciones erróneas detectadas en una inspección al número total de operaciones erróneas sujetas a inspección (eficiencia de inspección).

Las relaciones entre R, I, Q y la intersección I_Q se muestran en el siguiente diagrama.



Conjuntos:

R Todas las operaciones

I Operaciones inspeccionables

Q Operaciones críticas

I_Q Intersección de I con Q

La totalidad de los eventos del conjunto R está compuesta por los dos subconjuntos: R-I subconjunto de las operaciones no inspeccionables y I Subconjunto de las operaciones inspeccionables.

Si a cada uno de los eventos del conjunto R le asignamos una probabilidad, la totalidad de probabilidades será

$$1 = \{E_R + (1-E_R)\}^{R-I}\{[E_R + (1-E_R)][E_I + (1-E_I)]\}^{I} \qquad (1)$$

La primera expresión entre llaves representa la probabilidad de las dos condiciones posibles en una sola operación de realización (correcta o errónea), el exponente R-I es el número de tales operaciones que no son inspeccionables.

La segunda expresión entre llaves representa la probabilidad de las dos condiciones posibles en una sola operación inspeccionable (correcta o errónea) afectada o no por el nivel de eficiencia de inspección, el exponente I es el número de las operaciones inspeccionables. El subconjunto R-I contiene dos subconjuntos: $\{R-Q-(I-I_Q)\}$ y $\{Q-I_Q\}$
el primero contiene a las operaciones que no son inspeccionables ni críticas y el segundo contiene a las operaciones que no son inspeccionables pero si son críticas.

El subconjunto I también contiene dos subconjuntos, $I-I_Q$ y I_Q que consisten de las operaciones no críticas y críticos respectivamente.

Si consideramos solamente las operaciones críticas, la igualdad (1) toma la forma:

$$1 = \{E_R + (1-E_R)\}^{Q-I_Q} \{[E_R+(1-E_R)][E_I+(1-E_I)]\}^{I_Q} \qquad (2)$$

Como $I-E_R$ es la probabilidad de que una operación de realización no sea correcta y $I-E_I$ es la probabilidad de que la operación incorrecta no se detecte el producto de estas dos probabilidades nos dará $(I-E_R)$ $(I-E_I)$ la probabilidad de falla por esa operación y tenemos:

$$1 = \{E_R^{Q-I_Q} + (1-E_R^{Q-I_Q})\}\{[1-(1-E_R)(1-E_I)]^{I_Q} + 1-[1-(1-E_R)(1-E_I)]^{I_Q}\} \qquad (3)$$

En esta expresión (3) el primer término entre las primeras llaves es la probabilidad de que ninguna de las operaciones críticas de realización del subconjunto $Q-I_Q$ produzca fallas y el primer término entre las segundas llaves es la probabilidad de que ninguna de las operaciones de realización del subconjunto I_Q tenga defecto que haya pasado inadvertido en la inspección. La probabilidad conjunta de que no exista defecto en las operaciones de realización de los subconjuntos $Q-I_Q$ y I_Q o sea en el conjunto de operaciones críticas es:

$$P_R = E_R^{Q-I_Q}[1-(1-E_R)(1-E_I)]^{I_Q} \qquad (4)$$

Puede considerarse que esta expresión contiene la primera forma de ataque del problema de la confiabilidad del proyecto. El número de operaciones críticas de realización Q es sensible a los márgenes de diseño.

La probabilidad de error de realización E_R es sensible a la complejidad de las operaciones.

El número de operaciones críticas sujetas a inspección I_Q, es sensible al juicio analítico en el nuevo proyecto ayudado por la experiencia de los proyectos ya realizados. La eficiencia de inspección E_I es sensible a las condiciones en las que E_R y I_Q -

son sensibles. Cuando hay poco respaldo de experiencia la diferencia entre Q y I_Q es grande. Conforme la experiencia y el resultado de las inspeccionesypruebas progresan la diferencia disminuye al aumentar I_Q. El entrenamiento en las operaciones de realización puede elevar las eficiencias E_R y E_I.

En proyectos con bases sólidas de experiencia y organización la diferencia entre Q y I_Q puede ser pequeña desde el inicio y puede aproximarse temprano a cero en este caso se tiene un límite superior de la probabilidad de que en la realización del proyecto no se dejen defectos ocultos que ocasionen fallas en la explotación cuya expresión es:

$$\hat{P}_R = [1-(1-E_R)(1-E_I)]^{I_Q} \qquad (5)$$

hasta aquí hemos considerado que un defecto de realización produce una falla o bien no produce ninguna falla, en realidad se puede tener una distribución probabilística de fallas correspondiente a diversas clases de defectos y tenemos:

E_{Rj} probabilidad de que el defecto j no ocurra

E_{Ij} probabilidad de que el defecto j se detecte en caso de que ocurra.

Pj probabilidad de que el defecto j produzca una falla si ocurre y no se detecta (dependiendo de los márgenes de diseño y puede depender del tiempo).

Como se consideran todas las operaciones R, las que no están sujetas a inspección tienen valores de E_{Ij} iguales a cero y el límite superior toma la forma:

$$\hat{P}_R = \prod_{j=1}^{R} [1-(1-E_{Rj})(1-E_{Ij})P_j]$$

Si sumamos las probabilidades compuestas $(1-E_{Rj})(1-E_{Ij})$

Tenemos una expresión aproximada:

$$P_R \approx 1 - \sum_{j=1}^{n} (1 - E_{Rj})(1 - E_{Ij}) P_j$$

para el límite superior de la probabilidad de que en la realización del proyecto no se dejen defectos que ocasionen fallas en la explotación.

El límite inferior de la probabilidad de fallas será:

$$P_Q = \sum_{j=1}^{n} (1 - E_{Rj})(1 - E_{Ij}) P_j$$

La penúltima ecuación puede utilizarse para evaluar la sensibilidad de la confiabilidad de realización a los métodos de inspección y a los márgenes de seguridad de diseño de los cuales depende P_j.

La viabilidad de aplicación de este procedimiento en un proyecto real no es clara. El primer obstáculo es la obtención de la información básica en un medio en el que aún no se entiende bien el control y la constatación de calidad y al presente su alcance queda limitado a postular la existencia de defectos remanentes que pueden ocasionar fallas que a su vez pueden encadenarse a otros eventos y producir consecuencias indeseables.

R E F E R E N C I A S

1.- Plan de expansión del Sector Eléctrico al año 2,000. PESE 2,000. Comisión Federal de Electricidad. México 1978

2.- "Oversight Hearings on Nuclear Energy-Overview of the Major Issues" U.S. Congress, 94th Congress Serial No. 94-16 Apr. 28 29-Washington D.C. U.S.A. 1975.

3.- Nuclear News. April 6, 1979-TMI-2 Special Report. American Nuclear Society. Hinsdale, Illinois, U.S.A. 1979.

4.- B.Y. Gnedenko "Nadezhnosti". Soviet Encyclopedia. Vol. 2-pag. 348-353. Nauka Pres. Moscow, USSR 1963.

5.- ARINC Research Corporation "Reliability Engineering" pag. 6 Prentice Hall, Inc. Englewood Cliffs. New Jersey, U.S.A. 1944.

6.- Webster Unabridged Dictionary pag. 1853. Collins World. New York, N.Y., U.S.A. 1976.

7.- IEEE Std. 352-1975 Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems New York, N.Y. 10017, U.S.A. 1975.

8.- Harold M. Agnew "Gas Cooled Power Reactors". Scientific American Vol. 244 No. 6 pag. 43-51. June 1981, New York, N.Y. U.S.A. 1981.

9.- Nuclear Regulator y Commission. TMI-2 Lesson Learned Force. Final Report NUREG-0585. Washington D.C., U.S.A. 1979.

10.- J.Kemeny "Report of the President's Commission of the accident at Three Mile Island" Government Printing Office, Washington D.C., U.S.A. 1979.

11.- Office of the White House Press Secretary President's Communication. October 8, 1981. Washintgon, D.C., U.S.A. 1981.

12.- Outlook for Nuclear Power. Power Engineering. November 1981, pag. 70-78. Barrington. Illinois 60010, U.S.A. 1981.

13.- J.Fournier. Ciclo de Conferencias sobre energía nuclear. Conferencias 7 y 8: Puesta en servicio de una planta nuclear y automatización de una planta nuclear. Comisión Federal de Electricidad, México. Junio 1971.

14.- F.R. Mynatt. Nuclear Safety Research Since Three Mile Island. Science Vol. 216 No. 4542, pag. 131-135. Director of the Instrumentation and Control Division. Oak Ridge National Laboratory, Tennessee 37830, U.S.A.-April 1982.