TERCER EJERCICIO

GRUPO A - SEGURIDAD NUCLEAR

TEMA 29

Conceptos de fiabilidad y disponibilidad. Función de tasa de fallos. Fallos en espera y en demanda. Fiabilidad Humana. Tipos de acciones humanas erróneas

Contenido

Resumen

Los APS cuantifican el riesgo de la instalación en cuanto a la frecuencia anual de fusión del núcleo (nivel 1) y la frecuencia de excedencia de cada categoría de liberación (nivel 2). Para ello se definen los escenarios accidentales, las posibles evoluciones de la instalación y se estudia de forma detallada la probabilidad de que los sistemas necesarios para la mitigación de esos escenarios dejen de cumplir su función de seguridad. Para ello es preciso determinar los parámetros de fiabilidad y de disponibilidad de los equipos.

Intuitivamente, la fiabilidad de un equipo representa su capacidad para realizar la función para la que está diseñado en condiciones de operación normal o de accidente. El estudio cuantitativo de la fiabilidad de equipos y componentes lleva a la determinación de distintos parámetros de fiabilidad, a saber, su tasa de fallos en espera o en operación y la probabilidad de fallos en demanda. Ello proporciona elementos necesarios para determinar la probabilidad de que el equipo falle en su cometido de seguridad. Otros mecanismos por los que un determinado equipo puede no completar su cometido de seguridad es por estar fuera de servicio al estarse realizando operaciones de prueba o mantenimiento previstas.

Los datos de fiabilidad no deben tomarse como números aislados, sino como representantes de una función de distribución, normalmente la media o la mediana. Las distribuciones de probabilidad asignadas a los parámetros se propagan posteriormente para proporcionar una distribución de la frecuencia de daño al núcleo, resultado de los APS de nivel 1.

La aplicación de estos conceptos en los APS se concreta en la tarea de Análisis de Datos, en la cual se determinan los valores de la frecuencia de sucesos iniciadores, indisponibilidades por pruebas periódicas y mantenimientos (preventivo y correctivo), sucesos básicos de fallo independiente y de fallo de causa común y sucesos especiales.

Una de las tareas asociadas a los Análisis Probabilistas de Seguridad consiste en el estudio de la influencia de fallos en las actuaciones de los operadores en la mitigación de los accidentes, y la cuantificación de la probabilidad de que esos fallos ocurran.

Las acciones que realizan los operadores se clasifican en cinco tipos:

Tipo 1 las que se producen con anterioridad a un suceso iniciador, que dejan indisponibles o perjudican la actuación de sistemas de mitigación

Tipo 2 las que conducen por sí solas o en combinación con otras circunstancias a la ocurrencia de un suceso iniciador

Tipo 3 Las acciones que realizan los operadores en el seguimiento de procedimientos basados en síntomas

Tipo 4 Las que realizan los operadores siguiendo procedimientos en los que es necesario el diagnóstico de la situación

Tipo 5 Las acciones de recuperación no procedimentadas.

En la cuantificación de la probabilidad de fallo de los distintos tipos de acciones humanas en los APS españoles se ha seguido la técnica dada por EPRI en el *Procedimiento sistemático de fiabilidad de las acciones humanas* (Systematic Human Action Reliability Procedure, SHARP), y se ha usado la *técnica para la predicción de la tasa de error humano*, (Technique for Human Error Rate Prediction) elaborada por los laboratorios nacionales Sandia bajo los auspicios de la US NRC.

Para la estimación de las probabilidades de error humano, las actuaciones humanas se separan en su parte cognitiva y manual. La primera se refiere a los procesos de decisión que pueden llevar a no detectar la necesidad de la acción o a tomar las decisiones de manera tardía. El tiempo disponible para ello es un parámetro fundamental. Para el análisis de la actuación manual se realiza una descomposición en tareas simples para las que se tienen valores estándar provenientes de la literatura.

1. INTRODUCCIÓN

La fiabilidad de los equipos instalados en centrales nucleares se garantiza mediante

- un adecuado diseño, haciendo uso de códigos y normas industriales aceptadas en el mundo nuclear o recomendadas o impuestas por la legislación,
- una instalación y puesta en funcionamiento de acuerdo a las especificaciones del fabricante y a las normas ingenieriles aplicables, el correcto mantenimiento durante la vida del componente, y la adecuada garantía de calidad en todas las fases anteriores.

La realización de los APS conlleva un estudio detallado de los sistemas que intervienen en la ocurrencia, gestión y mitigación de accidentes. Partiendo de la extensa familiarización con la planta, se llevan a cabo las tareas de selección de los sucesos iniciadores que deben considerarse, el análisis de su evolución (delineación de secuencias) y la determinación de los equipos y acciones de los operadores necesarios para su gestión, dando lugar al análisis de sistemas y al análisis de fiabilidad humana, respectivamente. Para calcular la frecuencia con que se espera ese daño es necesario calcular la probabilidad de que los sistemas requeridos para desarrollar las funciones de seguridad que mitigan cada accidente no cumplan su función de seguridad según se modela en los criterios de éxito de los árboles de sucesos.

Resulta necesario en primer lugar conocer la frecuencia esperada con la que pueden ocurrir los sucesos iniciadores que desencadenan las secuencias accidentales.

Para obtener probabilidad de que un sistema no cumpla su función de seguridad para mitigar la ocurrencia de un suceso iniciador debe obtenerse una descripción de sus posibilidades de fallo en función de combinaciones de fallo de los componentes que lo forman, atendiendo al papel que juega cada uno de éstos en el funcionamiento de aquél. De los métodos posibles para obtener la cuantificación de la fiabilidad de sistemas (árboles de fallo, diagramas de bloque, sistemas de Markov), en los APS se usa el método deductivo de los árboles de fallo.

Otro mecanismo por el que un sistema puede no cumplir su misión de seguridad es por encontrarse fuera de servicio por estar sus componentes siendo sometidos a pruebas o mantenimientos.

Es en la tarea de datos donde se cuantifican la frecuencia de sucesos iniciadores y los parámetros y distribuciones de fiabilidad a que responden los equipos de la central.

Las probabilidades de los errores del personal de la planta en la operación, calibraciones, etc. se obtienen en la tarea de fiabilidad humana.

Desde el punto de vista del cálculo de la fiabilidad, debe tenerse en cuenta que los sistemas requeridos para mitigar las consecuencias de un suceso iniciador deben operar durante un tiempo específico después de ocurrido un suceso iniciador. Dichos sistemas pueden clasificarse en dos tipos: sistemas en espera y sistemas en operación normal:

- Sistemas en espera son los que no están normalmente en operación y son requeridos para mitigar las consecuencias de un suceso iniciador de modo inmediato. Su característica principal es que deben cambiar de estado al ser requeridos: válvulas que deben abrir, bombas que deben arrancar, etc. Deben responder a la demanda, y se necesitará calcular el fallo a entrar en funcionamiento en caso de demanda (fallo a la demanda). También se necesitará calcular el fallo a su funcionamiento continuado (fallo en operación) durante el tiempo de misión que se les haya asignado.
- Existen sistemas en operación normal cuyo funcionamiento debe continuar para la mitigación del accidente estudiado. Es el caso tanto de sistemas cuyo funcionamiento es requerido directamente, como el de sistemas que son soporte de otros. No se necesita el cálculo del fallo a la demanda, pero sí el del fallo en operación durante el tiempo de misión que se les haya asignado.

Los datos que se obtienen no deben tomarse como números aislados, sino como representantes de una función de distribución, normalmente la media o la mediana. A este valor se acompaña una medida de la incertidumbre en ese dato, que se expresa como la dispersión de la distribución. A cada suceso básico se le asigna por tanto además de la probabilidad puntual una función de distribución que permite la realización de cálculos de incertidumbre para proporcionar un intervalo de confianza a la frecuencia de daño al núcleo. Estas distribuciones se obtienen de bases de datos que recogen la experiencia operativa de la industria en general y la nuclear en particular, y en algunos casos son corregidas mediante técnicas bayesianas que incorporan la experiencia operativa de la planta.

2. CONCEPTOS DE FIABILIDAD Y DISPONIBILIDAD

2.1 Conceptos generales; modos de fallo

Antes de definir los conceptos, conviene establecer algunas ideas previas. Consideremos un componente cuyos posibles estados son funcionamiento normal o fallo; el cambio de estado supone la transición de uno a otro, y se considerará este salto en un instante de tiempo t determinado. Si el componente pasa del estado *funcionamiento normal* a *fallado*, se dice que el componente ha fallado en el tiempo t. Este instante de fallo no es, obviamente, conocido *a priori*, sino estocástico.

Si el componente es reparable, permanecerá en el estado fallado el tiempo necesario hasta que se complete la reparación. En este instante, el componente pasará del estado fallado al de funcionamiento normal, transición que recibe el nombre de reparación. El tiempo de reparación incluye el tiempo que se tarda en detectarse el fallo, el tiempo de comprobación y el de reparación y pruebas necesarias. El tiempo de reparación resulta ser también estocástico. Se puede suponer que el componente, una vez reparado se encuentra plenamente en su estado de funcionamiento normal, es decir, se considera que el componente es *tan bueno como nuevo*. Esto permite considerar solo dos estados, *sano*, y *fallado*.

A la hora de analizar los sistemas en función de su capacidad de actuar para mitigar un accidente, no se tiene en cuenta únicamente si éstos están en un estado de

funcionamiento normal o de fallo. Puede producirse la indisponibilidad también por *descargos* de los componentes del sistema por hallarse en mantenimiento o en pruebas. Esta *indisponibilidad* interviene también en la fiabilidad de los sistemas, y debe tenerse en cuenta en los árboles de fallo. Estas indisponibilidades son en su mayor parte *deterministas*, ya que los periodos de mantenimiento y las pruebas a que debe someterse cada componente están determinadas por el fabricante, por el programa de mantenimiento de la instalación y por las Especificaciones Técnicas de Funcionamiento.

2.2 Fiabilidad

Consideremos un componente no reparable, es decir, cuya única transición es de un estado normal a un estado de fallo.

Comenzando en un instante t = 0 en el que el componente se encuentra en un estado normal de funcionamiento, se define la fiabilidad en el instante t, R(t), como la probabilidad de que el componente no haya experimentado ningún fallo en el intervalo [0,t], es decir, que el primer fallo del componente se produzca en un instante posterior a t.

$$R(t) = P(T_{\text{fallo}} > t)$$

La curva de fiabilidad R(t) es una curva de supervivencia, monótona decreciente, puesto que el componente está sano en t = 0, y no se duda de que fallará en algún momento.

A partir de la fiabilidad se definen los siguientes conceptos:

Infiabilidad en t, F(t). Probabilidad de que un componente sano en t = 0 falle antes de instante t. R(t) + F(t) = 1.

Densidad de probabilidad de fallo en t, f(t), igual a la derivada de la fiabilidad respecto del tiempo, de tal manera que f(t)dt es la probabilidad de fallo del componente entre t y t + dt sabiendo que estaba nuevo en t = 0, pero sin imponer condiciones en t. Se dice que es una densidad no condicionada.

Tasa de fallos en t, r(t) o h(t). Su producto por dt es la probabilidad de fallo del componente entre t y t + dt condicionada a que el componente estaba sano en t. Sus propiedades se discuten más adelante.

Tiempo medio hasta el fallo (MTTF) se define como la esperanza matemática del tiempo de fallo.

2.3 Indisponibilidad

Denotada por Q(t), se define como la probabilidad de que el componente se encuentre fallado en el instante t, dado que se encuentra en el estado sano en t = 0. Se pueden definir valores medios y asintóticos.

La evaluación del impacto de un componente sobre el estado de un sistema se hará mediante una de las siguientes magnitudes:

Infiabilidad para componentes no reparables

Indisponibilidad para componentes reparables requeridos en un instante t

Indisponibilidad media para componentes reparables cuyo funcionamiento se requiere durante un intervalo

3. FUNCIÓN TASA DE FALLOS

3.1 Componentes no reparables

La tasa de fallos de un componente no reparable se ha definido como la probabilidad de fallo por unidad de tiempo condicionada a que el componente no ha fallado hasta el tiempo t. Usando esta definición puede relacionarse la función tasa de fallos con la infiabilidad y con la densidad de probabilidad de fallos.

$$F(t) = 1 - \exp\left(-\int_0^{\infty} h(\tau)d\tau\right)$$

En el caso de que la tasa de fallos sea constante en el tiempo, r(t) = λ, se tiene,

$$R(t) = \exp(-\lambda t)$$

$$f(t) = \lambda\, exp(-\lambda t)$$

La experiencia operacional suministra una curva característica de la evolución con el tiempo de la tasa de fallos, la llamada *curva de la bañera*, que presenta tres zonas bien diferenciadas (ver Figura 1)

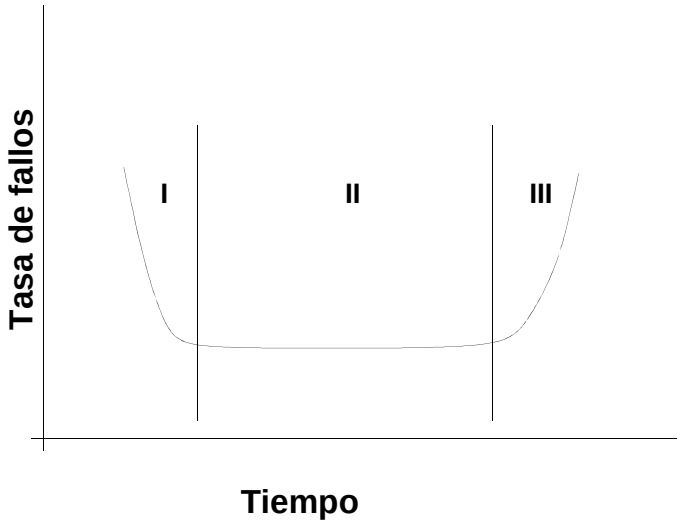

Figura 1: Curva de la bañera

I. Recoge los fallos infantiles o incipientes, con tasas de fallos rápidamente decrecientes y que se producen en un periodo muy corto de la vida del componente. Estos fallos provienen generalmente de un deficiente control de calidad o de fallos de fabricación. Los fallos incipientes generalmente se eliminan mediante el *periodo de rodaje*

II. Corresponde a una tasa de fallos aproximadamente constante, de forma que la densidad de probabilidad de fallo, como se ha visto más arriba, es exponencial. Esta región es conocida como el tiempo de vida útil del componente y es la aproximación más generalizada para los componentes empleada en los APS (para componentes que fallan en el tiempo, es decir, para fallos en operación o en espera). Los tiempos de inspección y mantenimiento se diseñan para conseguir que los componentes operen durante ese tiempo.

III. La tasa de fallos crece rápidamente. Corresponde a un proceso de envejecimiento de componente que dispara su tasa de fallos.

4. FALLOS EN ESPERA Y EN DEMANDA

El fallo de un componente a completar su misión puede deberse a dos causas:

- fallo del componente
- componente fuera de servicio debido a pruebas periódicas o a mantenimientos preventivos o correctivos.

4.1 Fallo de un componente

A cada componente se le asocia un modo de fallo que se asignará a cada uno de los siguientes tipos: en espera, en operación o en demanda. Para cada uno de ellos se usa un modelo distinto de fiabilidad. Las definiciones de los modos de fallo son como sigue:

Fallo a la demanda en componentes cuya demanda de acción supone un cambio de estado, que puede fallar por motivos independientes del tiempo.

Fallo en operación en componentes que deben funcionar correctamente de forma continuada durante un determinado tiempo, que se denomina tiempo de misión; pueden considerarse componentes reparables o no reparables, y en el caso de ser reparables se considera que su fallo se detecta inmediatamente.

Fallo en espera en componentes que no se encuentran en funcionamiento durante la operación normal, pero que deber estar disponibles en caso de ser requeridos; se considera que sus fallos no se detectan hasta requerirse su funcionamiento o en pruebas o mantenimientos.

4.1.1 Fallos a la demanda

Se considera cada demanda como el resultado de un experimento de Bernouilli, en el que los dos posibles resultados son fallo (el componente no responde a la

demanda) y éxito (el componente responde a la demanda). Se hacen por tanto las siguientes hipótesis:

a) en cada demanda el resultado es independiente del obtenido en la demanda anterior

b) cada demanda tiene únicamente dos posibles resultados (éxito y fallo)

c) la probabilidad de fallo en cada demanda es constante (igual a p)

La obtención del valor de p se hace acudiendo a la estadística de respuesta a la demanda de los componentes, y la indisponibilidad es Q = p.

4.1.2 Fallo en operación

Sistemas no reparables. La indisponibilidad es igual a la infiabilidad. Para componentes con tasas de fallo constantes, la fiabilidad es $R(t) = e^{-\lambda t}$ y la indisponibilidad,

$$Q(t) = 1 - R(t) = 1 - e - \lambda t$$

siendo t el tiempo de misión. En la aproximación del suceso raro, dada por $\lambda t \ll 1$, y desarrollando en serie de Taylor a primer orden, la indisponibilidad se aproxima por

$$Q(t) = \lambda t$$

4.1.3 Fallos en espera.

El fallo de estos sistemas se detecta al solicitarlos o en las pruebas o revisiones de mantenimiento. Si T es el intervalo de vigilancia, es decir, el tiempo entre pruebas, la indisponibilidad está dada por

$$Q(t) = \frac{1 - e^{-\lambda t}}{\lambda t}$$

que, en la hipótesis del suceso raro, suele aproximarse por

$$Q(t) = \frac{\lambda t}{2}$$

5. DISTRIBUCIONES TÍPICAS DE LA FUNCIÓN DENSIDAD DE PROBABILIDAD DE FALLOS

Para obtener resultados numéricos de la probabilidad de fallo de los componentes, se acude a distintos modelos para esa probabilidad en función de las características del componente, en particular en función del modo de fallo y del conocimiento experimental sobre su fiabilidad.

Se distinguirá entre variables aleatorias discretas y continuas. Las primeras se utilizan para modelar fallos que no dependen del tiempo, como los fallos a la demanda o la ocurrencia de sucesos discretos en un intervalo de tiempo, y se caracterizan por una función de distribución discreta como la distribución binomial y la distribución de Poisson. Las segundas se usan para representar el fallo de componentes en los que el tiempo, como variable continua, tiene un papel fundamental y se describen mediante una función de densidad continua, como la distribución exponencial, la distribución lognormal, la distribución gamma y la distribución beta.

6. LA TAREA DE ANÁLISIS DE DATOS

El principal objetivo de la tarea de Análisis de Datos en un Análisis Probabilista de Seguridad (APS) es suministrar los datos necesarios para cuantificar los modelos desarrollados. En la actualidad, los APS se realizan en varios ámbitos, atendiendo a los posibles escenarios de operación de la planta:

El APS nivel 1, que comprende APS a Potencia, que a su vez incluye la operación de la planta conectada a red, arranque (puesta en marcha) y disponible caliente; y APS en Otros Modos, que incluye los Estados Operacionales (EOP) de la central cuando se encuentra en parada. El APS nivel 2 que corresponde al análisis de los accidentes con liberación de productos radiactivos a la contención y al medio ambiente.

Las necesidades de datos son similares en cada uno de estos análisis y se diferencian sólo cuando éstos se ven afectados por los diferentes modos o estados operacionales (por ejemplo, las indisponibilidades de componentes sujetos a Especificaciones de Funcionamiento son distintas si la planta se encuentra a potencia o en parada). Lógicamente, el alcance de los datos también se ve afectado por los distintos escenarios, bien sea porque se postulen diferentes accidentes (en parada no tiene sentido hablar de disparo del reactor y sí de LOCA en RHR) o en función de los sistemas requeridos para mitigarlos. Básicamente, los datos son requeridos en dos áreas:

- En los árboles de sucesos delineados en la tarea de Análisis de Secuencias de Accidente.
- En los árboles de fallo desarrollados en la tarea de Análisis de Sistemas.

Los datos pueden, así mismo, dividirse en dos grupos:

- Frecuencias de sucesos iniciadores.
- Sucesos básicos, entendiendo como tales a aquellos que no requieren un ulterior desarrollo en los correspondientes árboles. Éstos, a su vez, pueden subdividirse en:
    - Indisponibilidades por pruebas periódicas y mantenimientos (preventivo y correctivo).
    - Sucesos básicos de fallo independiente y de fallo de causa común.
    - Errores humanos.
    - Sucesos Especiales: corresponden a aquellos sucesos que no es posible incluir en las categorías anteriores (por ejemplo, sucesos que

representan la política rotacional de trenes en sistemas con más de una redundancia) o que suponen simplificaciones en los modelos.

De los datos anteriores, las probabilidades asociadas a errores humanos se estudian y estiman en la tarea de Fiabilidad Humana.

6.1 Estimación de frecuencias de sucesos iniciadores

En las tareas de Familiarización con la Planta o de Análisis de Secuencias de Accidente (dependiendo de cada central) se identifican los posibles sucesos que iniciarían una secuencia de accidente que puede dar lugar al daño al núcleo. Estos sucesos iniciadores se agrupan en función de los requisitos de mitigación de la planta. En general, podemos hablar de diferencias entre un APS a potencia y un APS en otros modos:

Nivel 1 APS a Potencia. Los grupos de sucesos iniciadores, atendiendo a la frecuencia esperada de ocurrencia, se pueden clasificar en:

- Sucesos que, como iniciador, no han ocurrido nunca en centrales nucleares: como puede ser Rotura de Vasija, LOCA grande o Rotura Múltiple de Tubos de Generador de Vapor (PWR).
  Al no disponer de experiencia operativa alguna sobre estos sucesos, se suele acudir a fuentes de datos genéricas, (por ejemplo, el WASH–1400, Ref. 1, para Rotura Mecánica de Vasija o el NUREG/CR-5750, Ref. 2, para diferentes sucesos iniciadores) o a una estimación estadística, basada en los años de operación de reactores, en los que nunca se ha producido tal evento. Es decir, para estimar la frecuencia media se utiliza la expresión $F = (2N + 1)/2T$, siendo $N = 0$ sucesos y T el número de años–reactor considerados. Se hace la hipótesis de que la frecuencia se distribuye con una función gamma.
- Sucesos poco frecuentes: que han ocurrido al menos una vez en alguna central nuclear similar a la que se está analizando (por ejemplo: Rotura de un tubo de un Generador de Vapor, Rotura de Líneas de Agua de Alimentación Principal o de Vapor Principal).
  En este caso, la frecuencia se estima como $F = N/T$, siendo N igual al número de sucesos que se han producido en las centrales nucleares que se consideran aplicables a la que se está analizando y T el número de años–reactor.
- Sucesos frecuentes o relativamente frecuentes: corresponden a sucesos que ocurren en las centrales nucleares (por ejemplo, disparo del reactor, pérdida de agua de alimentación y/o condensado, pérdidas de energía eléctrica exterior).
  Esto supone que la experiencia de la propia central analizada debe ser la que pese en la estimación de la frecuencia de estos sucesos iniciadores, bien porque ésta es suficiente y no es necesario recurrir a la de otras plantas, o bien, porque tras estimar la frecuencia basada en la experiencia de otras centrales, se haga un análisis bayesiano con el objeto de adaptar dicha frecuencia genérica a la de la planta analizada. La estimación de la frecuencia se hace de forma análoga a la del apartado anterior. Normalmente y a medida

que la experiencia de una central aumenta, estas frecuencias se estiman exclusivamente con la experiencia de la central que se analiza.

- Sucesos iniciadores con características especiales de diseño: corresponden a sucesos que dependen del diseño de la propia central (por ejemplo: LOCAs de interfase, Pérdida del sistema de refrigeración de componentes; Pérdida del sistema de Agua de Servicios Esenciales).
  Para estos sucesos se realiza un árbol desarrollado de fallos de cada situación. Este modelo conduce a ecuaciones booleanas que se cuantifican conociendo el valor medio de cada suceso básico (variable), con datos basados en juicios de expertos, genéricos, tratados bayesianamente o estimados directamente a partir de un análisis de la experiencia específica de planta según sea el caso. En algunas ocasiones, un grupo de sucesos iniciadores puede estar formado por sucesos que se engloban en distintas partes de la clasificación anterior. Estos casos se tratan separadamente y, posteriormente, se suman sus frecuencias.

APS en otros modos. Cada central divide los modos de operación que se atraviesan durante las paradas de recarga en diferentes Estados Operacionales de Planta (EOP) a los que aplican determinados sucesos iniciadores.

Básicamente, los sucesos se tratan de forma análoga al apartado anterior, pudiéndose encontrar Grupos de Sucesos Iniciadores referidos a las operaciones en parada que no han ocurrido nunca, poco frecuentes y frecuentes o relativamente frecuentes (LOCA en RHR, Pérdida del tren de RHR en servicio, LOCA en RCS, pérdidas de energía eléctrica exterior) o que se estimen mediante modelos específicos de planta. Finalmente, a las frecuencias estimadas se les aplica un factor que representa la probabilidad de que la planta se encuentre en los EOP que aplica cuando se produce un determinado suceso iniciador para determinar la probabilidad final de cada grupo.

6.1.1 Necesidad de análisis de experiencia operativa

Para el APS a Potencia, es necesario analizar todos los disparos ocurridos en la planta, así como aquellos sucesos que, dependiendo de las circunstancias, podrían dar lugar al disparo de la misma (por ejemplo, pérdidas de energías eléctricas exteriores) independientemente de que éstas se produzcan en cualquier modo de operación de la central. En este caso es necesario conocer el tiempo que la central estuvo en los modos de operación aplicables al APS a Potencia en el periodo de análisis del APS.

Análogamente, para el APS en Otros Modos, además de ser aplicables los sucesos de pérdida de energías eléctricas exteriores, es necesario revisar la experiencia de la central para cubrir dos objetivos: detectar posibles escenarios que no hayan sido contemplados “a priori” y contabilizar el número de sucesos ocurridos aplicables a los iniciadores postulados. En este caso es necesario conocer el tiempo que la central estuvo en cada Estado Operacional (EOP) aplicable al APS en Otros Modos en el período de análisis del APS.

6.1.2 Fuentes documentales

1. De la planta.

   Para analizar los disparos e incidentes de la planta se ha de acudir, en principio, a la siguiente documentación:

- Informes de Disparos.
- Informes de Sucesos Notificables e Informes Especiales.
- Libros de Operación de Sala de Control.

Para identificar el tiempo de cada modo de operación o estado operacional de la planta (EOP) se puede acudir, en función de los datos que recojan, a los Libros de Operación de Sala de Control e Informes Mensuales de Explotación.

2. Fuentes de Datos Operacionales de Centrales Extranjeras.

   Entre las fuentes de datos que los APS utilizan para analizar la experiencia de sucesos poco o relativamente frecuentes, se pueden citar las siguientes:

- Nuclear Power Experience Reports (NPEs).
- Base de datos World Association of Nuclear Operators (WANO).
- NUREG basados en la experiencia de centrales de EEUU.
- VGB: Base de datos de experiencia operativa de centrales KWU.

6.2 Sucesos básicos

Como se ha dicho anteriormente, se entiende por suceso básico aquél que no requiere un desarrollo posterior.

6.2.1 Indisponibilidades

Se entiende por indisponibilidad la probabilidad de que cuando es requerido un componente o conjunto de ellos (tramo), no puedan realizar la función para la que son requeridos. Las indisponibilidades pueden ser debidas a Pruebas Periódicas, Mantenimientos Preventivos (entendiendo por éstos los programados) o Mantenimientos Correctivos (entendiendo por éstos los no programados, sea cual sea la causa: fallos, reparaciones, medidas preventivas no programadas, modificaciones de diseño, etc.).

En general, las indisponibilidades se calculan como T_i/T_t siendo T_i el tiempo de indisponibilidad y T_t el tiempo total considerado, definido por el periodo analizado en el APS en los modos de operación al que aplica.

Las indisponibilidades de tramos o componentes redundantes (mismo sistema, trenes distintos) se pueden promediar siempre que su experiencia sea similar, de forma que T_i es el tiempo indisponibilidad total grupo en el periodo analizado y T_t viene dado por el producto del número de componentes por el tiempo total de cada uno $T_t = N \times T$.

Indisponibilidades debidas a pruebas periódicas y mantenimientos preventivos
Corresponden a actividades programadas cuya frecuencia y duración se mantiene más o menos estable y que se pueden estimar de varias maneras:

a) A partir de datos reales de planta: cuando existen datos de operación de la central, la indisponibilidad se calcularía, igual que en el caso anterior, como relación entre el tiempo empleado y el tiempo total.

b) A partir de las duraciones de indisponibilidad estimadas en cada actividad y frecuencias definidas en los procedimientos de prueba o gamas de mantenimiento preventivo.

Indisponibilidades por mantenimiento correctivo Siempre que se disponga de experiencia de planta, se calculan de la forma indicada anteriormente: $T_t/N \times T$, siendo N el número de tramos o componentes redundantes y T el tiempo considerado en los modos aplicables.

Análisis de Experiencia de Explotación y Fuentes de información Las fuentes de información más importantes, necesarias para el cálculo de indisponibilidades por pruebas periódicas/mantenimientos preventivos y mantenimientos correctivos, así como para la identificación de fallos y estimación del número de horas de funcionamiento o espera y de demandas de los componentes modelados, son:

- Informes de Sucesos Notificables (ISN) y Libros de Control de Inoperabilidades.
- Sistema de Gestión de Mantenimiento y órdenes de trabajo.

6.2.2 Sucesos básicos de fallo independiente

Los sucesos básicos de fallo están definidos por tipos de componentes y modos de fallo asociados. Los límites de componentes se definen al principio del proyecto en función de las necesidades de modelación y de la disponibilidad de los datos, en colaboración conjunta entre las tareas de Análisis de Sistemas y de Análisis de Datos. Se pueden citar como ejemplos los siguientes:

6.2.3

Tipo de Componente	Modos de Fallo
Bomba motorizada	Fallo al arranque
	Fallo en operación
Generador Diesel	Fallo al arranque
	Fallo en operación
Válvula motorizada	Fallo a la apertura
	Fallo al cierre
	Fallo a permanecer abierta
	Fallo a permanecer cerrada
Interruptor de potencia	Fallo a la apertura
	Fallo al cierre
	Apertura espuria

Relé	Fallo a la energización Fallo a la desenergización Desenergización espuria
Genérico	Pérdida de función

Los sucesos básicos de fallo independiente se tratan de igual manera en los APS a Potencia y Otros Modos.

Cuantificación. Probabilidades y Tasa de fallo. Modelos. Atendiendo al modo de fallo hablaremos de probabilidades o de tasas de fallo.

- Cuando el componente cambia de estado al ser requerido (está parado y se arranca, está abierto y se cierra o viceversa) el modo de fallo está asociado a la demanda y, por tanto, se necesita conocer la probabilidad de fallo en demanda representada por P (/d).
- Cuando el modo de fallo del componente está vinculado a un tiempo de exposición al fallo, se necesita conocer la tasa de fallos representada por λ (/h). En este último caso, se puede diferenciar entre tasa de fallos en misión (λ_m) y tasa de fallos en espera (λ_e).

Los sucesos básicos de fallo emplean los parámetros anteriores usando un modelo que tendrá en cuenta las particularidades del propio componente. Los modelos a los que se asocian los sucesos básicos son tres: Demanda, Misión y Espera.

- Modelos en Demanda y en Espera (asociados a modos de fallo en demanda)

  Cuando el modo de fallo requerido está asociado a la demanda, si se produce el fallo, éste puede ser debido a la propia demanda del equipo o haberse producido durante el tiempo que estuvo en "espera" (intervalo entre demandas, normalmente, intervalo de pruebas). Si el intervalo de tiempo es pequeño, se asume que el fallo se debe al propio cambio de estado, es decir, a la demanda; en ese caso, la indisponibilidad asociada al suceso básico será directamente la probabilidad en demanda.

  Cuando este intervalo de tiempo es mayor, es más probable que el fallo se deba a la espera que a la propia demanda (por ejemplo, acumulación de suciedad en contactos).

- Modelos en Misión y en Espera (asociados a modos de fallos horarios). La tasa de fallo en misión corresponde a modos de funcionamiento en los que, al producirse el fallo, éste se detecta de forma inmediata. La tasa de fallo en espera, al contrario, corresponde a componentes y modos de funcionamiento en los que, al producirse el fallo, éste no se detecta de forma inmediata y hay que esperar a que su funcionamiento sea requerido para saber si el componente está fallado o no.

Las indisponibilidades asociadas a los sucesos básicos de fallo en misión y espera son:

- Misión: $1 - \exp(-\lambda_m t_m)$, siendo λ_m la tasa de fallos en misión y t_m el tiempo en que es requerido el funcionamiento del componente (normalmente, la duración de la secuencia de accidente, generalmente 24 horas).
- Espera: $1 - [(1 - \exp(-\lambda_e t_p))/\lambda_e t_p]$, siendo λ_e la tasa de fallos en espera y t_p el tiempo entre pruebas del componente.

Base de Datos Genérica de Componentes En el apartado anterior hemos visto cómo se estiman las indisponibilidades de los sucesos básicos de fallo independiente, en función del modelo. Para ello se necesitan conocer los datos asociados al modo de fallo, es decir, las probabilidades y tasas de fallo. El objetivo del APS es representar la realidad de la planta y, por lo tanto, los datos han de reflejar su experiencia de explotación tanto como sea posible. Sin embargo, la planta puede no disponer de información suficiente para determinar las probabilidades y tasas de fallo de todos los componentes modelados en el APS. Por ello, en función de los tipos de componentes y modos de fallo definidos al inicio del proyecto, se elabora una Base de Datos Genérica de Componentes que, a partir de fuentes de datos genéricas, nos permita obtener los parámetros de partida deseados.

Son varias las fuentes de datos existentes, las cuales pueden dividirse en dos tipos: las que se basan en sucesos ocurridos en diversas plantas, cuyos estimadores puntuales e incertidumbre han sido o deben ser calculados, y las que presentan directamente estimaciones basadas en consensos de expertos. En todas ellas, la calidad radica en la claridad de las definiciones de los límites de componentes, en lo detalladas que sean las descripciones de los modos de fallo y en la representatividad de los datos con respecto a los componentes de la planta.

En principio, se emplea una base de datos genérica y de consenso lo más amplia y aceptable que sea factible. En dicho sentido, las bases de datos utilizadas en los programas de la NRC del NUREG 1150 vol.1 –ASEP del NUREG/CR–4550 Rev. 1 e IREP del NUREG/CR–2728– se consideran aceptables para su uso en APS. El NUREG/CR-6928, contiene datos y estimaciones de la industria americana.

En el caso de que para algún tipo de componente y sus modos de fallo no haya datos disponibles, se toman los valores de otros componentes que tengan unas características y modos de fallo similares. Este criterio aplica, por ejemplo, a componentes tales como compuertas motorizadas de ventilación que se asocian a válvulas motorizadas, ya que los modos de fallo son análogos.

En general, las bases de datos proporcionan la distribución asociada al dato genérico.

Datos específicos: tratamiento bayesiano y estimación directa Esta subtarea se encarga de analizar la experiencia de explotación de la central al objeto de identificar fallos y estimar los números de horas de funcionamiento o espera y de demandas de los componentes modelados. Las fuentes de documentación son las mismas que las utilizadas en la identificación de mantenimientos correctivos y ambos trabajos se

deben hacer de forma conjunta haciendo un análisis profundo y exhaustivo de los datos recopilados. Los datos necesarios para este análisis son:

- Detección de todos los trabajos no programados sobre los componentes modelados en el APS, susceptibles de impedir el funcionamiento de éstos.
- Horas de funcionamiento y demandas de los componentes modelados en el APS.

Criterios de fallos catastróficos Para efectuar una adecuada clasificación de los mantenimientos analizados, se procede a establecer criterios de fallos catastróficos, en los que se identifican qué estados del componente le impedirían realizar la función para la que es requerido en el APS y qué situaciones corresponderían a fallos incipientes o estados degradados que no impedirían el funcionamiento del mismo en las condiciones de un accidente.

Estimación clásica / Tratamiento Bayesiano Una vez analizados los datos específicos de planta, obtenidos los fallos y las horas de funcionamiento/espera o demandas, según sea el modelo, y agrupados los sucesos básicos en familias se procede a efectuar un ajuste bayesiano sobre los mismos o una estimación directa de las probabilidades/tasas de fallos en función de la experiencia. Siempre que se dispone de suficiente experiencia se debe hacer una estimación directa de los parámetros por medio de su Estimador de Máxima Verosimilitud (MLE).

El estimador para la probabilidad de fallo a la demanda corresponde a $P = n/D$, donde n es el número de fallos aplicable y D es el número de demandas del componente. El estimador para la tasa de fallos es $\lambda = n/T$, donde n es el número de fallos aplicable y T el tiempo total de operación del componente.

Cuando la experiencia es pequeña o no significativa, se acude al tratamiento bayesiano, en donde se toman como funciones *a priori*, las contenidas en la Base de Datos Genérica de Componentes, y como funciones de *verosimilitud* o evidencia los fallos, demandas y horas obtenidos del análisis de la experiencia de explotación.

Cuando no se dispone de experiencia, se emplea directamente el dato de la Base de Datos Genérica de Componentes.

7. SUCESOS BÁSICOS DE FALLO DE CAUSA COMÚN (FCC)

7.1 Definición y clasificación

Un fallo de causa común está definido como el fallo simultáneo o indisponibilidad de más de un componente debido a una misma causa que no puede ser modelada de forma explícita. Estos fallos están modelados como sucesos básicos de causa común en los árboles de fallo de los diferentes sistemas.

Se entiende por mecanismo de acoplamiento el medio para explicar cómo una causa se propaga afectando a múltiples componentes o equipos. Los sucesos básicos de fallo de causa común se tratan de igual manera en los APS a Potencia y Otros Modos, pudiendo variar exclusivamente el alcance de componentes de plantas requeridos en uno u otro análisis.

Para incorporar al modelo los grupos de componentes identificados en la fase anterior se establecen sucesos básicos de fallo de causa común (FCC) que intervienen en el modelo provocando el fallo del componente. Su indisponibilidad (es decir, probabilidad de que cuando se vaya a requerir un equipo éste falle por una causa común a varios componentes) se calcula mediante una adecuada representación paramétrica y un análisis de datos.

8. DEFINICIÓN Y OBJETIVOS DEL ANÁLISIS DE FIABILIDAD HUMANA

El análisis de fiabilidad humana (FH) es un método por el cual se realiza un análisis sistemático de las acciones que el personal de la planta lleva a cabo o puede tener que llevar a cabo para controlar los accidentes. Este tipo de análisis permite la identificación, descripción, modelación y cuantificación de los errores humanos *creíbles* que son significativos para el riesgo de la instalación. Se parte de la premisa de que los operadores actúan acorde a su entrenamiento, excluyéndose actos de vandalismo o sabotajes.

En el contexto de un Análisis Probabilista de Seguridad (APS), el objetivo de la tarea de Fiabilidad Humana es analizar la influencia del ser humano en el riesgo asociado con la operación de las centrales nucleares.

En los APS los análisis de fiabilidad humana se realizan para los distintos modos de operación (a potencia y en parada), para sucesos iniciadores internos y externos (incendios, inundaciones). El peso de los análisis de fiabilidad humana en la interfase y en los niveles 2 es mucho menor que en el nivel 1.

8.1 El error humano

En los APS, se considera un *Error Humano* una acción humana realizada fuera de los márgenes de tolerancia dados por los criterios de éxito de los sistemas de la planta.

Los errores humanos modelados en un APS incluyen errores que reducen la disponibilidad de sistemas, que tienen como resultado un suceso iniciador, que no impiden la progresión de un accidente o que empeoran la progresión de un accidente.

Se supone que los errores humanos pueden ocurrir antes de un suceso iniciador (preiniciadores), pueden causar el suceso iniciador (iniciadores) o pueden ocurrir después del suceso iniciador (post-iniciadores), mientras el personal de la planta está tratando de mitigar las consecuencias de un accidente.

8.2 Normativa

Para verificar la calidad de los Análisis Probabilistas de Seguridad, la industria americana, con el apoyo y la participación de la NRC promovió la edición del estándar ASME/ANS-RA-S-2002 *Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications*, que recibió addenda hasta realizarse una actualización en 2008 y del cual la versión más reciente está dado por las Addenda ASME/ANS-RA-Sa 2009. La NRC ha editado la

Regulatory Guide 1.200 *An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities* que contiene la posición reguladora sobre la forma aceptable de demostrar la calidad de los APS para aplicaciones reguladoras que hagan uso de los resultados de los APS. El estándar de ASME establece tres Categorías de calidad de los APS en función del cumplimiento de ciertos requisitos. En cada aplicación debe determinarse qué Categoría debe cumplir el APS para poderse usar en esa aplicación, pudiendo llegar a especificar distintas Categorías aplicables para distintas partes del Análisis de Riesgo (distintos modelos de APS) asociados con la aplicación.

El estándar ASME/ANS-RA-Sa 2009 establece la categorización mediante requisitos de alto nivel (*High Level Requirements, HLR*) que se desarrollan en requisitos soporte (*Supporting Requirementes, SR*). El cumplimiento con estos requisitos permite asignar la categoría de calidad al APS de forma que pueda utilizarse en apoyo de una solicitud informada por el riesgo u otra aplicación de los APS.

9. PROCEDIMIENTO SISTEMÁTICO DE FIABILIDAD DE LAS ACCIONES HUMANAS

Como resultado del esfuerzo de investigación para incorporar las interacciones humanas en el APS, el EPRI, Electric Power Research Institute (California) ha desarrollado el procedimiento sistemático de fiabilidad de las acciones humanas (Systematic Human Action Reliability Procedure), conocido por sus siglas en inglés, SHARP 32[5].

SHARP pretende ser un marco para la incorporación de las interacciones humanas en el APS con un enfoque sistemático que considera un conjunto de pasos (ver más abajo). SHARP no proporciona de forma explícita los métodos de cuantificación, sino que hace referencia a otros documentos disponibles.

La metodología SHARP ha sido usada en todos los APS realizados por las centrales nucleares españolas; una visión esquemática puede verse en la Figura 2.

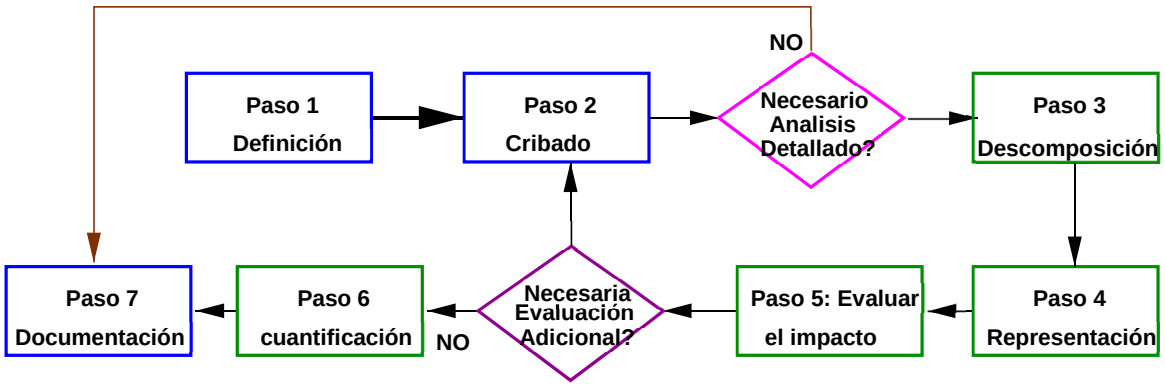

Figura 2: Esquema de los pasos para la realización de un análisis de fiabilidad humana siguiendo SHARP.

9.1 Paso 1: Definición e Identificación

Durante la operación normal de una central nuclear tienen lugar varias intervenciones humanas. El examen de las acciones que pueden causar o agravar incidentes proporciona la siguiente clasificación útil para los APS, que es la que se encuentra en [5].

Tipo 1 Antes de que tenga lugar el suceso iniciador

Tipo 2 Acciones que inducen el suceso iniciador

Tipo 3 Después del suceso iniciador, mientras se siguen Procedimientos de Operación en Emergencia (POE)

Tipo 4 Acciones que se realizan después del suceso iniciador, en las que se siguen procedimientos que no están basados en síntomas

Tipo 5 Acciones de recuperación que se hacen después del suceso iniciador y no están directamente contempladas en los POE.

Para ilustrar las fases de las acciones humanas después de un suceso iniciador, consideremos la Figura 3: Fases de una acción humana, tras un suceso iniciador. En ella, el estímulo inicial y la detección y la ejecución final en el tiempo disponible y las tareas manuales son características de las acciones de tipo 3, mientras que el diagnóstico y la selección de estrategia lo son de las de tipo 4.

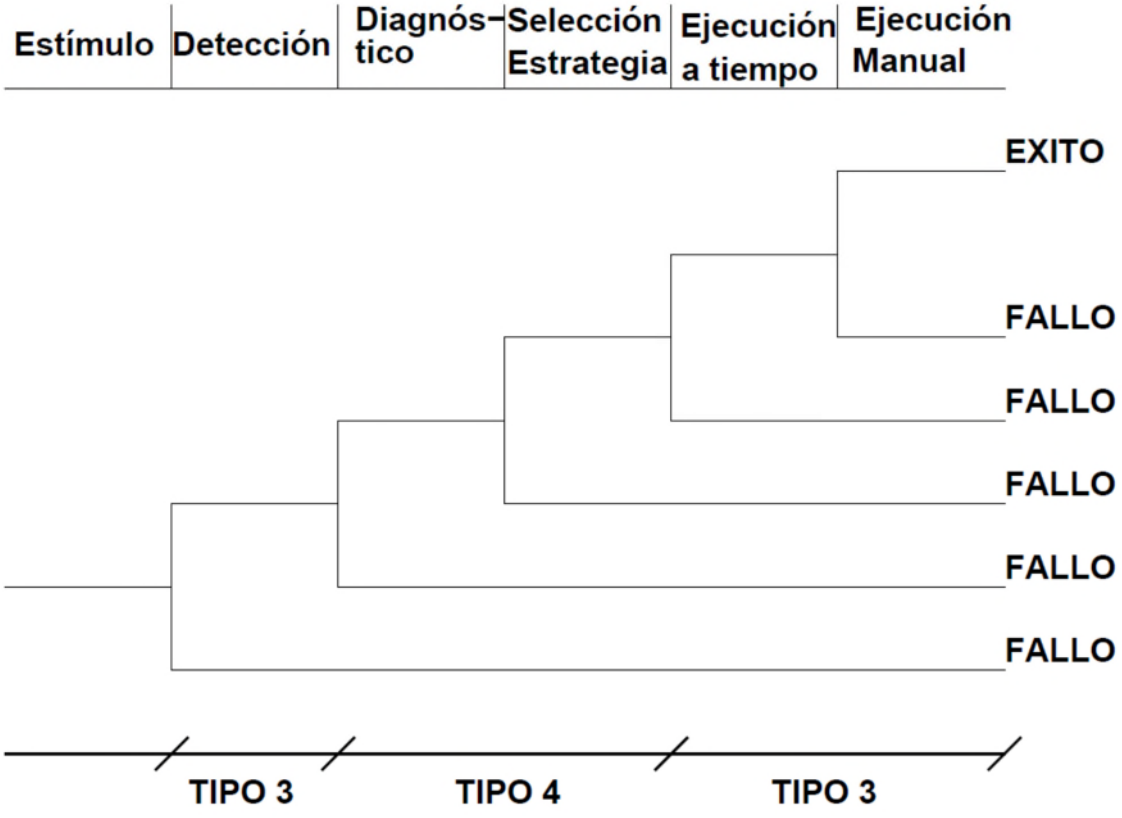

Figura 3: Fases de una acción humana, tras un suceso iniciador

Puede verse por tanto que los errores de las acciones de tipo 1 reducen la disponibilidad de los sistemas importantes para la seguridad. Las acciones humanas de tipo 2 provocan un suceso iniciador o incrementan su frecuencia de ocurrencia. Un error del operador durante la progresión de un accidente (tipos 3 a 5) implica que el operador no impide la progresión del accidente o contribuye a que se agraven las condiciones del mismo.

En lo que sigue se mirará más en detalle cada uno de los tipos de error.

9.1.1 Errores humanos de tipo 1

Se definen los errores humanos de tipo 1 como aquellos que tienen lugar antes de la ocurrencia de un suceso iniciador y que pueden reducir la disponibilidad de sistemas por causa de un mal alineamiento tras un mantenimiento o una prueba, de una incorrecta calibración de un canal de instrumentación, etc. Las acciones que se investigan son aquellas que implican un cambio de estado, tales como

1. Pruebas periódicas realizadas sobre equipos de seguridad
2. Procesos de calibración de instrumentación relacionada con equipos de seguridad
3. Acciones de mantenimiento correctivo y preventivo periódico.

La identificación de las acciones de tipo 1 se realiza revisando todas las acciones humanas descritas más arriba, y todos los procedimientos y prácticas operativas de la instalación referidas a las pruebas, mantenimiento, calibraciones y realineamiento de sistemas para la operación.

Ejemplos de errores de tipo 1 son,

- Posición incorrecta de una válvula del sistema de Agua de Alimentación Auxiliar después de realizar un mantenimiento.
- Posición incorrecta de las válvulas manuales de suministro de nitrógeno a las válvulas de alivio de los generadores de vapor después de un mantenimiento preventivo, de causa común porque el trabajo fue realizado por un único equipo de instrumentistas.
- Calibración incorrecta de un canal de presión en la contención que proporciona la señal automática para el arranque de la ducha de la contención (equipo de calibración).

Dentro de los errores de tipo 1 debe incluirse también el incorrecto alineamiento de aquellos componentes que no son directamente el objeto de una prueba, pero cuyo realineamiento es necesario para la realización de la misma y existe posibilidad de que queden mal alineados. Así, pueden excluirse aquellas actividades para las que existe una prueba funcional de la configuración requerida tras la actividad.

9.1.2 Errores humanos de tipo 2

Se definen los errores de tipo 2 como aquéllos que inducen la ocurrencia de un suceso iniciador o incrementan la frecuencia de ocurrencia de un suceso iniciador.

Su determinación está íntimamente relacionada con las tareas de identificación de sucesos iniciadores y de cálculo de su frecuencia.

Los métodos principales para la identificación de las acciones de tipo 2 son

Análisis de la experiencia operativa Se revisan los registros históricos de experiencia operativa de la planta y de otras plantas buscando acciones de los operadores que hayan dado lugar a un transitorio.

Análisis sistemático Una fuente importante de información para identificar acciones de tipo 2 es la estructura jerárquica de causas de disparo. El análisis de modos de fallo y sus efectos (FMEA, Failure Mode and Effects Analysis) es otra posible fuente. Adicionalmente, se debe revisar las tareas de seguimiento de carga, de operación y pruebas relacionadas con el arranque y parada de la planta y con el mantenimiento y pruebas que necesitan realineamientos durante la operación.

Los errores de tipo 2 también pueden dividirse en tres categorías según den lugar directamente a un suceso iniciador (*tipo 2 puro*) o deban combinarse con otros fallos humanos o de componentes para dar lugar al iniciador (*tipo 2 compuesto*).

Tipo 2A son fallos latentes producidos en la ejecución de tareas que inducen una anomalía en el funcionamiento de la planta que permanece indetectada durante algún tiempo. Estos son similares a los errores de tipo 1 en cuanto a la fuente del error se refiere (una mala operación en una tarea habitual), pero contribuyen también a la frecuencia del iniciador.

Tipo 2B son iniciadores puros, es decir, provocan directamente el transitorio.

Tipo 2C también son sucesos compuestos en los que la planta no responde adecuadamente a la anomalía, es decir, en una situación en la que la planta está en una situación anormal; por esta razón se clasifican como de tipo 2 y no como de tipo 3, 4 o 5.

Para dejar clara esta clasificación, piénsese en los siguientes ejemplos:

- Apertura de una válvula del presionador en el transcurso de una reconexión eléctrica (tipo 2A).
- Desbloqueo temprano de un permisivo P-11 (tipo 2B).
- Error al cerrar una válvula del presionador abierta inadvertidamente (tipo 2C).
- Error al reconectar un cargador de emergencia antes de la pérdida de una barra de corriente continua.
- Disparo de turbina involuntario (tipo 2B).

9.1.3 Errores humanos de tipo 3

Los errores llamados de tipo 3 son aquellos que puede cometer el turno de operación mientras se realizan las acciones contenidas en los Procedimientos de Operación en Emergencia basados en síntomas durante la mitigación de un suceso iniciador. Incluyen errores en los que el operador se salta una acción procedimentada, no la realiza a tiempo o lo hace incorrectamente.

Son los miembros del turno de operación quienes básicamente pueden cometer este tipo de errores. Una clasificación amplia de las actividades que pueden llevar a este tipo de error es,

- Fallo en el apoyo a un automatismo
- Fallo en la operación manual de un equipo
- Fallo en el control de procesos.

Para la identificación de las acciones de tipo 3, deben analizarse todas las actuaciones de los operadores en respuesta a un iniciador. Por tanto deben analizarse los procedimientos existentes en la planta para la mitigación de accidentes. Estas incluyen,

- Procedimientos de Operación en Emergencia
- Procedimientos de Fallo
- Procedimientos de Operación Especiales
- Procedimientos de Operación Generales

En el análisis de las acciones de tipo 3 se realiza una evaluación detallada de las tareas a realizar, lo que incluye

- Identificación de las tareas críticas o tareas necesarias para que la acción tenga éxito.
- Práctica operativa (procedimientos de estructuración del turno de operación, instrumentación, factores ambientales, interfaces)
- Otras acciones relacionadas con las tareas.

Son ejemplos de estas acciones,

- Fallo del operador en las acciones de apoyo al arranque automático del sistema de agua de alimentación auxiliar.
- Error humano en el realineamiento a recirculación con el sistema de inyección de alta presión después de un LOCA pequeño.
- Error humano en la maniobra de Purga y Aporte (*Feed & Bleed*) tras un disparo con pérdida del sumidero de calor.
- Error humano en el control del sistema de agua de alimentación auxiliar después de un disparo del reactor.
- Error humano en la desconexión de cargas tras un SBO.

9.1.4 Errores humanos de tipo 4

Este tipo de errores surge cuando el turno de operación trata de mitigar un suceso iniciador, e incluyen

- Diagnóstico incorrecto que normalmente se asocia a errores en la identificación del iniciador o del estado de la planta
- Selección de la estrategia incorrecta, ligado a errores del turno de operación en la decisión de las funciones de seguridad a proteger y de los sistemas para hacerlo después de la identificación correcta del suceso iniciador.

La identificación del diagnóstico erróneo requiere la evaluación, para cada suceso iniciador o estado de la planta, de qué otros iniciadores o estados pueden producir

síntomas similares. Para los errores de selección de estrategia deben evaluarse las estrategias posibles que puede adoptar el turno de operación en cada iniciador identificado en cada estado de la planta.

Ejemplos de errores de tipo 4 de mal diagnóstico son

- Los ocurridos en el accidente de TMI
- Los identificados en la *Matriz de confusión* (Oconee NPP):
    - Rotura de línea de vapor dentro de la contención y pequeño LOCA
    - Alto caudal de agua de alimentación auxiliar y rotura de la línea de vapor fuera de la contención.

Una selección errónea de la estrategia ocurre, por ejemplo, en

- el realineamiento de la inyección de alta presión al modo recirculación demasiado pronto
- confusión en la planificación para el alineamiento de las válvulas para establecer la recirculación.

Este tipo de error humano se ha analizado en muy pocos APS, y es considerado poco significativo desde que las centrales nucleares adoptaron procedimientos de operación basados en síntomas, puesto que no hay necesidad de diagnosticar el iniciador y los POE conducen al turno de operación a la estrategia correcta en cada caso. Un diagnóstico erróneo es posible en plantas que no disponen de procedimientos basados en síntomas.

9.1.5 Errores humanos de tipo 5

Estos hacen referencia a errores del turno de operación en la realización de actividades encaminadas a la mitigación de un iniciador, pero que no están previstas en los POE.

Estas acciones de recuperación fallidas aparecen, por ejemplo, en

- un fallo en la detección de una anomalía
- diagnóstico incorrecto
- selección de la estrategia inadecuada
- restricciones de tiempo que inducen fallos en la ejecución de acciones.

La identificación de la recuperación de acciones tiene lugar después de la cuantificación preliminar de las secuencias, y se centra en los conjuntos mínimos de fallo (MCS) significativos para el daño al núcleo. Estas acciones se insertan directamente en los MCS y no en los Árboles de Sucesos o de Fallos.

9.2 Paso 2: Cribado

El objetivo del cribado es seleccionar las acciones humanas más importantes relacionadas con el riesgo de la planta con el objetivo de hacer un análisis detallado. El cribado consiste en tres etapas:

- Asignación de probabilidades conservadoras de error humano (valores de cribado) a las acciones identificadas en el Paso 1.

- Cuantificación preliminar de las secuencias accidentales usando esas probabilidades de cribado.
- Selección de errores para el análisis detallado aplicando criterios cualitativos y cuantitativos.

9.3 Paso 3: Descomposición

En este paso se descomponen las acciones humanas en tareas y subtareas. Este proceso se desarrolla para acciones seleccionadas para el análisis detallado.

Debe analizarse cada acción para identificar qué tarea puede llevar al fallo (tareas críticas). De esta manera se reduce la complejidad de paso de cuantificación, mejorando también la estimación de los valores de la probabilidad de fallo, al pasar de una acción compleja a un conjunto de tareas simples.

En el caso de acciones procedimentadas la identificación de tareas y subtareas se hace de acuerdo a los pasos y sub-pasos de los procedimientos de la planta.

En este paso también se identifican los factores de forma (Performance Shaping Factors, PSF) más importantes que pueden influir en la acción bajo estudio y en otras acciones relacionadas. Ejemplos de PSF y acciones relacionadas consideradas en los análisis de acciones humanas de tipos 1 y 3 son,

Errores humanos de tipo 1

- PSF:
  - Calidad de los procedimientos aplicables, si existen.
  - Número de componentes y funciones de cada uno en el equipo de trabajo.
  - Entrenamiento del personal.
  - Características de las herramientas y del equipo a usar.
  - Nivel de estrés asociado con la actuación.
  - Frecuencia de manipulación (pruebas, mantenimiento, etc.).
- Acciones relacionadas: Verificaciones (comprobaciones visuales) y pruebas funcionales, y sus frecuencias.

Errores humanos de tipo 3

- PSF:
  - Estructura del turno de operación.
  - Distribución de tareas entre el personal de la sala de control.
  - Entrenamiento y experiencia.
  - Carga de trabajo y nivel de estrés.
  - Calidad de la interfase hombre-máquina.
  - Calidad de los procedimientos aplicables.
  - Ergonomía de las herramientas de ayuda a la operación (alarmas, sistemas de presentación de parámetros, sistemas de comunicaciones, etc.).
  - Escenario (nivel de emergencia).

  - Tiempo disponible (intervalo en el cual la acción debe hacerse correctamente).
  - Tiempo que se tarda en realizar la acción correctamente.
- Acciones relacionadas: acciones previas, simultáneas o posteriores que pueden tener influencia.

9.4 Paso 4: Representación

El analista de fiabilidad humana intenta clarificar las relaciones entre las tareas que componen una determinada acción por medio de una representación gráfica. Con este paso se trata de reflejar posibles caminos de fallo como ayuda en la evaluación del impacto y para facilitar el proceso de cuantificación.

En el análisis de fiabilidad humana de los APS se contemplan dos formas de representación:

- El Árbol de acciones del operador (*Operator Action Tree*, OAT) para distinguir la parte cognitiva de la parte manual de la acción (ver la Figura 4).
- La técnica para la predicción de la tasa de error humano (*Technique for Human Error Rate Prediction*, THERP) [6] proporciona el árbol de fallos de fiabilidad humana (*HRA event tree*), que es una forma de árbol de fallos en el que cada rama representa un proceso de decisión binario (por ejemplo, comportamiento correcto o incorrecto). Este árbol de fallos de fiabilidad humana se aplica al análisis de la parte manual de las acciones (ver Figura 1).

9.5 Paso 5: Evaluación del impacto

Una vez obtenida la información detallada de cada acción significativa, ésta se revisa para determinar si es necesario hacer cambios en los modelos probabilistas desarrollados (iniciadores, árboles de fallos y se sucesos, secuencias, dependencias, etc.) antes de la cuantificación final.

Por ejemplo, puede ser necesario reestructurar las estructuras lógicas del APS por las siguientes causas:

- Identificación de errores de causa común por un patrón mal calibrado usado en la calibración de varios canales de instrumentación.
- Acciones que requieren la misma instrumentación.
- Inhibición de la actuación automática de un sistema.

9.6 Paso 6: Cuantificación

El objetivo del paso 6 de SHARP es el cálculo final de la probabilidad de error de las acciones humanas importantes.

En la actualidad, los APS españoles usan la herramienta HRA Calculator, de EPRI, para el cálculo de la probabilidad de error humano. Esta herramienta integra todos los PSAF aplicables a las acciones humanas para su cuantificación. La cuantificación de la parte cognitiva de la acción se realiza mediante la correlación Human Cognitive

Reliability/Operator Reliability Experiment Model (HCR/ORE) o la Caused-Based Decision Tree (CBDT) (ver más abajo).

La NRC ha publicado recientemente la metodología IDHEAS, que es un sistema completo para la cuantificación de la probabilidad de error humano para los APS, aplicado a sus modelos propios [7].

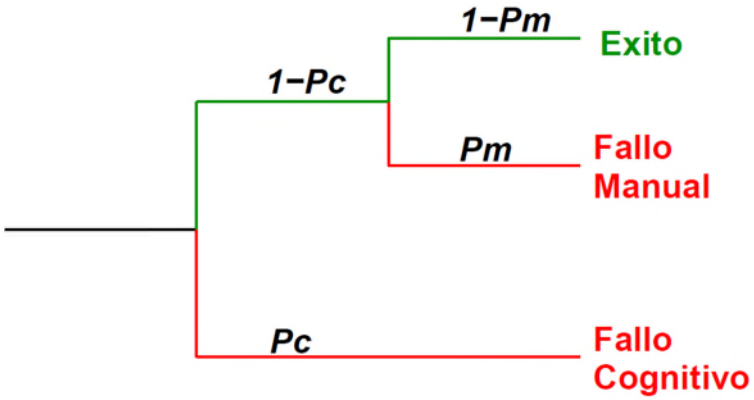

Figura 4: Descomposición de la acción humana en parte cognitiva y parte manual.

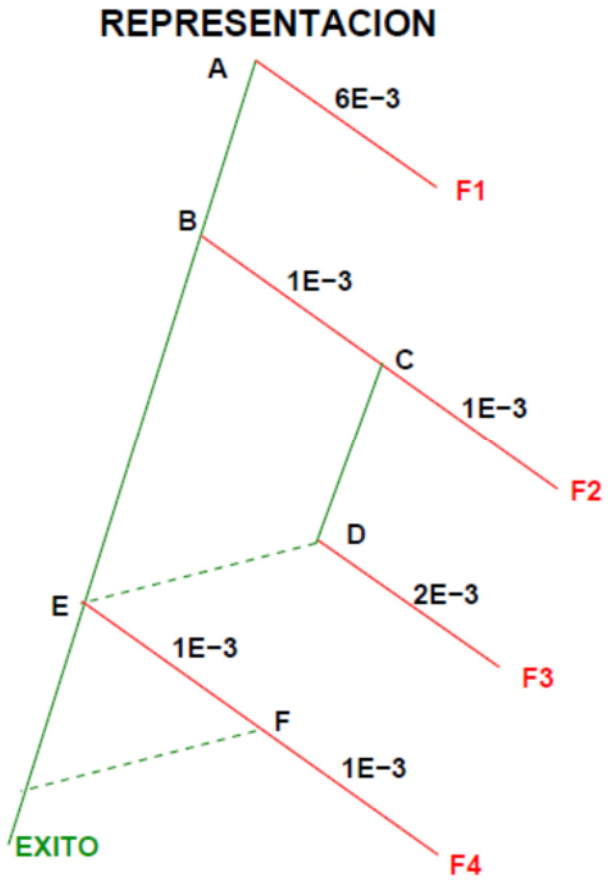

Figura 5: Ejemplo de representación de la parte manual de una acción en los APS

9.7 Documentación

Toda la información necesaria para que el análisis se pueda seguir debe incluirse en el informe final, conteniendo los métodos y resultados y con la descripción clara de las hipótesis del análisis.

10. ANÁLISIS DE DEPENDENCIAS

El objetivo del análisis de dependencias es la identificación de las dependencias entre las acciones humanas. Estas dependencias pueden ser debidas a distintos mecanismos (personal, procedimientos, herramientas o equipo usado, instrumentación, tiempo compartido, etc.). La identificación de dependencias puede hacerse *a priori*, antes de la cuantificación o *a posteriori*, después, analizando los conjuntos mínimos de fallo de las secuencias. La cuantificación de las dependencias puede ser específica, si hay suficiente información, o directamente por medio de las tablas de THERP. A menudo se usa una combinación de ambos métodos.

El NUREG-1921 [8] incluye una aproximación válida para la determinación del nivel de dependencia entre dos acciones humanas (completa, alta, moderada, baja o nula) que tiene en cuenta si las acciones las tiene que realizar un mismo turno (ej. sólo se aplica dependencia nula si el tiempo transcurrido entre los estímulos que requieren la realización de ambas acciones supera la duración de un turno); si existen elementos cognitivos comunes en su realización (ej. si las acciones las realiza un único turno y están requeridas en el mismo paso del procedimiento seguido en respuesta al iniciador o se realizan en respuesta al mismo estímulo), la secuencia temporal en la que se presentan las condiciones que las requieren (ej. si las señales para su realización son simultáneas o si la que requiere la segunda acción se presenta antes de haber completado la primera de ellas); el tiempo entre estímulos para su realización (cuanto más separados, menor posibilidad de dependencia); los recursos humanos disponibles para su realización; si las acciones se realizan o no en la misma zona (ej. en Sala de Control o fuera de ella); y el nivel de estrés. A partir de los niveles de dependencia asignados, la probabilidad de los sucesos dependientes puede cuantificarse aplicando las expresiones incluidas en THERP.

11. FIABILIDAD HUMANA EN LOS APS DE INCENDIOS

Las características específicas de los accidentes iniciados por incendios han llevado a la NRC junto con la industria americana, representada por EPRI, a establecer una metodología concreta para la realización de la tarea de fiabilidad humana en los análisis probabilistas de incendios. Esta metodología ha quedado plasmada en el NUREG-1921 [8].

El alcance del análisis de fiabilidad humana en incendios se centra en los Sucesos de Error Humano (SEH) posteriores al iniciador. Éstos se agrupan en las categorías siguientes:

- SEH de sucesos internos: sucesos que dan cuenta de acciones provenientes de o asociadas con el APS de sucesos internos, que típicamente hacen uso de los Procedimientos de Operación en Emergencia normales (no específicos de incendios)
- SEH de respuesta al incendio: Sucesos que reflejan el fallo de las acciones añadidas al APS de incendios, típicamente de procedimientos de operativos de respuesta ante incendios, planes o pre-planes de respuesta al incendio. Estas acciones incluyen las asociadas con el abandono de la Sala de Control.
- SEH que corresponden a la respuesta indeseada a las actuaciones espurias o a señales espurias de instrumentación

En el NUREG-1921 se proporcionan pautas para analizar el nuevo contexto que representa la existencia de un incendio en la central que induzca un iniciador de APS. Se tiene en cuenta que al quemarse cables de potencia o instrumentación pueden producirse actuaciones espurias o fallos inducidos por el incendio a los que el turno de operación deberá dar respuesta usando los procedimientos de incendios, los de operación en emergencia o una combinación de ambos.

Para la cuantificación de la probabilidad de error humano, el NUREG-1921 considera aceptables dos metodologías de análisis cognitivo y de ejecución:

1. Metodología de EPRI, que reúne los tres métodos siguientes:
   - Caused-Based Decision Tree (CBDT) [9], aproximación estándar al análisis cognitivo, incluyendo la decisión, diagnosis y el proceso de toma de decisiones.
   - Como complemento a lo anterior, la modelación del proceso cognitivo de acciones en las que tiene influencia el tiempo se hace por medio del método HRC/ORE [10] (Human Cognitive Reliability/Operator Reliability Experiment.
   - Los aspectos de ejecución y modelación se basan en THERP.
2. Metodología de la NRC: ATHEANA. Este método ofrece un proceso estructurado para la identificación de aspectos críticos de éxito y fallo asociados con operaciones anormales. ATHEANA no se limita a un conjunto específico de PSF o condiciones de planta, permitiendo acomodar fácilmente PSF específicos de incendio y sus contextos.

12. REQUISITOS DE ALTO NIVEL REQUERIDOS EN EL ASME/ANS RA-S-1.1–2022

En el estándar ASME/ANS-RA-Sa 2009 [11] los requisitos de alto nivel para los análisis de fiabilidad humana se establecen para tipos de acciones humanas.

Acciones anteriores al iniciador

HLR-HR-A Debe usarse un proceso sistemático para identificar aquellas actividadesrutinarias específicas que, si no se completan correctamente pueden afectar a la disponibilidad del equipo necesario para realizar las funciones modeladas en el APS.

HLR-HR-B El cribado de las acciones que no necesitan tenerse en cuenta explícitamente en el modelo debe basarse en el análisis de cómo las prácticas operativas de la central limitan la probabilidad de error en tales actividades.

HLR-HR-C Para las acciones que no se criban, debe definirse un suceso básico de error humano que caracterice el impacto del fallo como indisponibilidad de un componente, sistema o función modelada en el APS.

HLR-HR-D La evaluación de las probabilidades de los fallos humanos anteriores al iniciador debe realizarse usando un proceso sistemático que contemple las influencias específicas de la instalación y de cada actividad en el comportamiento humano.

Acciones posteriores al iniciador

HLR-HR-E Debe usarse una revisión sistemática de los procedimientos para identificar el conjunto de respuestas del operador requeridas para cada una de las secuencias accidentales.

HLR-HR-F Deben definirse los sucesos de error humano que representen el impacto de no llevar a cabo adecuadamente la respuesta requerida, de una manera consistente con la estructura y detalle de las secuencias accidentales.

HLR-HR-G La evaluación de la probabilidad de los sucesos de error humano debe realizarse usando un proceso bien definido y autoconsistente que tenga en cuenta las influencias específicas de la planta y de cada escenario en el comportamiento humano y tenga en cuenta las dependencias potenciales entre sucesos de fallo de acciones humanas dentro de la misma secuencia accidental.

HLR-HR-H Las acciones de recuperación (en conjuntos mínimos de fallo o en escenarios) deben modelarse sólo si se ha demostrado que la acción es posible y viable para los escenarios donde se aplican. La estimación de la probabilidad de fallo debe tener en cuenta las dependencias con fallos de acciones humanas anteriores del escenario.

Comunes a ambos tipos de acciones

HLR-HR-I La documentación del análisis de datos debe ser consistente con los requisitos soporte aplicables.

Adicionalmente, en el HLR-QU-C para la tarea de cuantificación, referido a la verificación de que las dependencias se han tenido en cuenta adecuadamente, se contempla un procedimiento para identificar las dependencias de acciones humanas.

13. Bibliografía

[1] Atwood, C.L., y otros. Handbook of Parameter Estimation for Probabilistic Risk Assessment. NUREG/CR-6823, SAND2003-3348P, 2003

[2] Grinstead C.M., Snell J.L. Introduction to Probability. American Mathematical Society, 2000.

[3] Høyland A., Rausand, M. System Reliability Theory. John Wiley & Sons, Inc., 1994.

[4] Thompson, W.A., Point Process Models with Applications to Safety and Reliability. Chapman-Hall, 1988.

[5] G.W. Hannaman, A.J. Spurgin, et al., Systematic Human Action Reliability Procedure (SHARP). EPRI NP-3583, 1984.

[6] A.D. Swain and H. E. Guttmann, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Applications, NUREG/CR-1278, Sandia National Laboratories, 1983 (THERP).

[7] NRC. Integrated Human Event Analysis System for Event and Condition Assessment (IDHEAS-ECA) (NUREG-2256) https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr2256/index.html

[8] EPRI 1023001 y US NRC. NUREG-1921. EPRI/NRC-RES Fire Human Reliability Analysis Guidelines, 2012

[9] EPRI, Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment, 1992. TR-100259.

[10] Reliability Experiments Using Nuclear Power Plant Simulators. EPRI, Palo Alto, CA: 1990. NP-6937, as supplemented by EPRI TR 100259.

[11] ASME-ANS Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications ASME/ANS RA-S-1.1–2022, mayo, 2022