

METODOLOGÍA DE FCC Y FCC SUCEOS INICIADORES DE SISTEMAS SOPORTE



BEGOÑA PEREIRA PAGÁN

Experta en análisis de datos y fallos de causa común
EMPRESARIOS AGRUPADOS INTERNACIONAL (AIE)



JOSÉ MIGUEL GARCÍA GUTIÉRREZ

Técnico Superior de Análisis de Riesgos (APS).
ASOCIACIÓN NUCLEAR ASCÓ VANDELLÒS (ANAV)

Un **Análisis Probabilista de Seguridad**, en adelante APS, es un estudio de carácter probabilista que, mediante un modelo que refleja el comportamiento de la central, permite establecer la frecuencia esperada de daño al núcleo o de liberación de productos radiactivos al exterior para dicha planta. Es, por tanto, una herramienta que analiza tanto el diseño de la central como los procedimientos de la misma, así como su práctica operativa con el objeto de identificar qué puede dar lugar a un accidente y cómo éste podría evolucionar.

Por **fallo dependiente** se entiende un suceso en el que se produce el fallo relacionado de varios componentes ante una misma demanda o dentro de un determinado intervalo de tiempo por una misma causa. En otras palabras, un fallo dependiente relaciona a un grupo de sucesos, donde la probabilidad de fallo del sistema no puede expresarse mediante el producto de las probabilidades de los sucesos individuales.

Llamamos **fallo de causa común** (FCC) a un fallo dependiente en el que dos o más componentes fallan simultáneamente o en un determinado espacio de tiempo como resultado directo de una causa común compartida “residual” no contemplada en los modelos (Figura 1).

Es importante destacar que el estudio de fallos de causa común se centra en los componentes llamados activos, cuya operación o función depende de una fuente externa motora y que están normalmente operando o pueden cambiar de estado bajo condiciones normales de operación o en respuesta a condiciones de accidente.

Grupo de componentes de causa común es la definición de un conjunto de componentes susceptibles de tener un FCC debido a la misma causa. Normalmente, se emplean algunos criterios para definir estos grupos: mismo tipo de componente y modo de fallo (arranque, operación, apertura, cierre, etc.), mismo fabricante, idénticas prácticas de mantenimiento, y, muy importante, misma función requerida.

El **mecanismo de acoplamiento** es un medio para explicar cómo una causa de fallo se propaga afectando a múltiples componentes o equipos. Las tres grandes categorías en que se clasifican los mecanismos de acoplamiento son: funcional, espacial y humano.

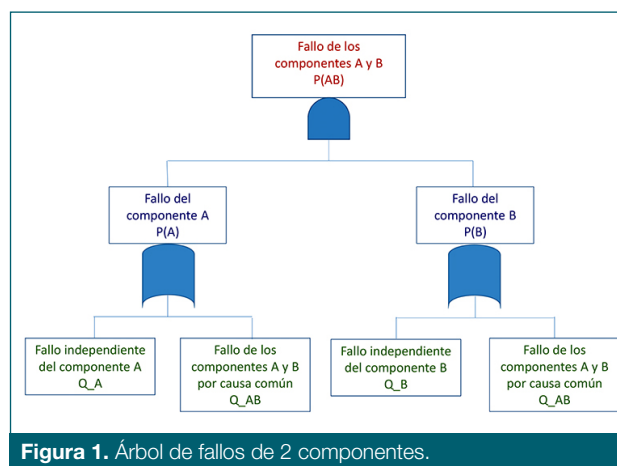


Figura 1. Árbol de fallos de 2 componentes.

Existen varias clasificaciones de las **causas de fallos de causa común**, básicamente se dividen en dos categorías principales: las debidas a errores o fallos durante el diseño y la construcción; y las que surgen durante la operación de la central.

Las **defensas básicas** contra los fallos de causa común son la redundancia¹, separación funcional², separación física³, diversidad⁴ y separación en el tiempo (sustitución de equipos o realización de pruebas / mantenimientos de forma escalonada). Existen otros factores que son determinantes, como las **medidas defensivas** que implanta la propia central: por ejemplo, la vigilancia y mantenimiento de los equipos de manera adecuada, un control de calidad efectivo, entrenamiento del personal, el uso de equipos cualificados, etc.

A principios de la década de 1980, varias organizaciones realizaron grandes investigaciones en el área de los FCC. EPRI (Electric Power Research Institute) publicó una base de datos inicial de sucesos de FCC ocurridos en CCNN en 1985 (EPRI NP-3967 [1]). En 1988, la NRC (U.S. Nuclear Regulatory Commission) y EPRI juntaron sus esfuerzos, resultado de los cuales fueron documentos como el EPRI NP-5613 y el NUREG/CR-4780, titulados "*Procedures for Treating Common Cause Failures in Safety and Reliability Studies*" [2, 3]. El propósito era establecer las etapas a seguir en el análisis de FCC.

Posteriormente, EPRI actualizó su base de datos a 1990 (EPRI TR-100382 [4]), empleando la clasificación que habían proporcionado los dos documentos anteriores (EPRI NP-5613 y NUREG/CR-4780). Mientras tanto, también se desarrollaban las bases para tratar de cuantificar los FCC mediante modelos paramétricos, así como las hipótesis para trasladar los sucesos con una determinada población a sus equivalentes con una población superior o inferior (*mapping up* o *mapping down*) y, también, una mejora en la recogida e interpretación de los potenciales sucesos de FCC a partir de la experiencia operativa. Todo ello con la ventaja de empezar a disponer de herramientas informáticas para desarrollar bases de datos.

Las lecciones aprendidas durante esta etapa y los avances tecnológicos motivaron el desarrollo de dos nuevos informes:

- NUREG/CR-5485 [5] que proporcionó un análisis de FCC que integraba los aspectos cualitativo y cuantitativo a partir de la experiencia operativa y las características de diseño de los componentes, en un procedimiento paso a paso hecho para que los analistas del APS modelaran de forma más adecuada los FCC.

¹Es la existencia de múltiples componentes o trenes, cada uno de los cuales es capaz de cubrir el 100% de la función que se requiere.

²Un requisito importante para conseguir un beneficio completo es que todas las redundancias del sistema no dependan de componentes comunes, señales o suministro eléctrico. Esta condición es necesaria para evitar que un fallo único en un servicio común suponga el incumplimiento de la función de todo un sistema.

³Normalmente se hace mediante una separación física (distancia) y con barreras protectoras (paredes, cubículos o salas separadas, etc.).

⁴La diversidad de equipos implica, por tanto, que un sistema dispone de trenes o componentes redundantes que no son idénticos (por ejemplo, en el caso de un sistema de AFW (*Auxiliary Feed Water*) de una central PWR (*Pressurized Water Reactor*) que disponga de dos trenes con bombas motorizadas y un tren con una turbobomba).



Figura 2. Central nuclear de Vandellòs II

- NUREG/CR-6268 [6] que proporcionó una guía para recoger, clasificar y codificar sucesos de causa común (reeditada y revisada en 2007).

En los APS de las centrales de Ascó y Vandellòs II, se utilizó el EPRI TR-100382 [4], para cuantificar los FCC, aplicando ya el modelo paramétrico de las Múltiples Letras Griegas (MGL por sus siglas en inglés, *Multiple Greek Letters*) con las hipótesis mencionadas y haciendo un análisis de aplicabilidad de los sucesos recogidos en él.

Los métodos paramétricos utilizan la hipótesis de que un porcentaje constante de los fallos que se producen sobre un componente es debido a FCC. Esto implica que una fracción de la probabilidad de fallo de los componentes puede ser asociada a fallos por una misma causa que haría igualmente fallar al resto de los componentes del grupo considerado, independientemente de su número.

Para sucesos básicos de dos redundancias se ha venido utilizando el método del factor β . Para un número superior de redundancias se suelen emplear los métodos de los factores α o de las Múltiples letras Griegas (MGL), aunque también existe el método del parámetro básico.

A medida que se fue avanzando en los esfuerzos para cuantificar los sucesos de FCC, se fueron comparando metodologías, para ver cuál era la más apropiada (Tabla 1).

Para cubrir aún más las necesidades de datos de FCC, la NRC e INL (Idaho National Laboratory) desarrollaron un procedimiento para la recogida y análisis de datos de FCC que incluía la identificación, codificación, estimación paramétrica y un sistema informático para el almacenamiento y análisis de los sucesos. Este sistema, llamado programa *Integrated Data Collection and Coding System* (IDCCS) está desarrollado en Access y suministra al usuario las tablas que contienen los datos de los análisis de FCC. El alcance del estudio abarca desde 1997 hasta el presente (la experiencia anterior no estaba disponible) y se alimenta de dos focos de información:

- Las bases de datos de INPO (Institute for Nuclear Power Operations) que contienen información de las CCNN de EEUU:
 - *Nuclear Plant Reliability Data System* (NPRDS) desde 1997.
 - *Equipment Performance and Information Exchange* (EPIX) de 1997 a 2012.

Metodología de estimación de FCC	Descripción	Características
Método del parámetro básico	Se basa en la hipótesis de que las probabilidades de los fallos independientes y de causa común son simétricas. Es útil para explicar las similitudes y diferencias de los modelos alternativos de fallo de causa común.	Difícil de estimar los parámetros a partir de la experiencia de explotación.
Factor Beta	Es un modelo sencillo. Se ha utilizado para modelar dependencias entre componentes redundantes e idénticos de un mismo sistema.	Para sistemas con más de dos componentes o trenes, la aplicación directa del factor beta no permite distinguir entre los posibles fallos parciales que se puedan dar entre las redundancias. Esto supone ser bastante conservador y podría ser adecuado cuando se quiere emplear valores de screening para cuantificar sucesos básicos de baja significación en el riesgo.
Múltiples Letras griegas (MGL)	Está basado en el método del factor beta, pero puede distinguir entre sucesos que afectan a un gran número de redundancias.	Normalmente se aplica a grupos de FCC de cualquier tamaño. Hay fuentes de datos genéricas que proporcionan valores para los distintos parámetros, pero no trata de forma óptima las posibles incertidumbres.
Factores alfa	Bastante similar al método de las múltiples letras griegas, salvo que trata mejor el tema de las incertidumbres. También permite con menos complejidad que el anterior, considerar los fallos según existan pruebas escalonadas o no escalonadas.	También se aplica a grupos de FCC de cualquier tamaño y hay fuentes de datos genéricas que proporcionan valores para los distintos parámetros.

Tabla 1.

- INPO *Consolidated Event System* (ICES) de 2012 a 2020.
- INPO *Industry Reporting and Information System* (IRIS) desde 2019.
- Los informes de sucesos notificables de la NRC (Licensee Event Reports, LERs) contenidos en la base de datos Sequence Coding and Search System (SCSS), desarrollada por el Oak Ridge National Laboratory (ORNL).

La base de datos de FCC resultante se encuentra en la página web de la NRC, en el apartado de *Reactor Operational Experience Results and Databases*, como una actualización del NUREG/CR-6268 [6] y se identifica como *CCFParameterEstimates* seguido del año de fecha de corte superior del análisis. Se actualiza cada 2 años desde 2003, siendo la versión más reciente la de 2021 [7], cubriendo sucesos desde 1997 a 2020. En la página web se pueden ver las estimaciones realizadas para los dos métodos paramétricos de más consenso: factores α y el de múltiples letras griegas (MGL, *Multiple Greek Letters*).

Los criterios necesarios para hacer estas estimaciones a partir de la experiencia operativa también están disponibles (Idaho National Laboratory. *System and Component Descriptions, Boundaries, and Failure Modes*, [8]) y abarcan los siguientes aspectos:

- Definiciones del tipo de componente analizado.
- Límites físicos del tipo de componente.
- Modos de fallo.
- Sistemas en los que se encuentran.
- Parámetros de FCC (definiendo su incertidumbre con el tipo de distribución, media, mediana, estimadores de máxima verosimilitud y percentiles del 5%/95%).

El tamaño de los grupos de FCC va de 2 a 6 componentes en general, en algún caso llega a 8.

Para hacer las estimaciones de los parámetros a partir de la experiencia operativa se tienen en cuenta varios factores:

- Próxima causa del fallo (error de diseño, procedimiento inadecuado, condiciones ambientales extremas).
- Factor de acoplamiento: basado en la condición de que se pueda producir el fallo de m de n componentes por una causa compartida.

- Factor de degradación del componente que representa la probabilidad del grado de fallo del componente durante la operación para la que es requerido.
- Factor de tiempo: es un factor de peso que tiene en cuenta si los múltiples fallos se pueden producir en un intervalo corto o cercano en el tiempo, a medio o a largo plazo, dependiendo de si el fallo se detecta de forma inmediata (por ejemplo, con una alarma, o que una bomba deje de dar caudal) o hasta que se le realiza una demanda, prueba o ronda de inspección.
- Tipo de relación entre el fallo de un componente y sus redundantes: letal si el fallo afecta a todos los componentes del grupo, de la misma forma, por una causa clara, y no letal (el resto de los casos).

Por lo tanto, se deben resaltar dos aspectos importantes en el análisis de los FCC: existe una estructura bien definida de cómo se debe hacer, pero también hay un cierto nivel de incertidumbre asociada a la subjetividad del análisis. Aun así, se ha intentado objetivar este proceso, requiriéndose un gran conocimiento y experiencia por parte de los analistas.

ANAV se planteó la posibilidad de utilizar la fuente de datos de *CCFParameterEstimates*, más actualizada para la obtención de parámetros genéricos, sin la necesidad de realizar análisis de aplicabilidad, o *mapping-up* o *mapping-down*, factores de peso, etc., que implicaba el utilizar los datos de la base de datos de EPRI TR-100382 [4]. Pero, adicionalmente, dadas las ventajas del método de los factores α frente al de las MGL (mejor modelo para tratar las probabilidades de k -de- m componentes, tratamiento adecuado de la incertidumbre y menos complejidad para considerar los fallos según estén sometidos los equipos a pruebas escalonadas o no escalonadas), se decidió también migrar de metodología de MGL a factores α . (Figura 3).

Otro aspecto relevante que contribuyó a tomar esta decisión fue que el programa empleado para cuantificar los modelos de APS, *Risk Spectrum*, estaba preparado para calcular directamente las probabilidades / tasas de FCC, introduciendo directamente los factores α e identificando si los grupos de FCC estaban sometidos a pruebas escalonadas o no, descontando el valor asignado a estos sucesos de los datos de probabilidad / tasa de fallo independiente, evitando de esta forma contabilizarlos dos veces (en muchos APS, dada

Q_k es la probabilidad o tasa de fallo, según el modelo esté en demanda o en función del tiempo respectivamente, de k componentes específicos debido a un suceso de causa común, donde $1 \leq k \leq m$.

La probabilidad o tasa de fallo total Q_t de un componente específico puede ser obtenida a partir de los valores Q_k mediante la siguiente expresión:

$$Q_t = \sum_{k=1}^m \binom{m-1}{k-1} Q_k$$

- Pruebas no escalonadas:

$$Q_k^{(m)} = \frac{k \alpha_k^{(m)}}{\binom{m-1}{k-1} \alpha_t^m} Q_t = f_{cc} Q_t$$

- Pruebas escalonadas:

$$Q_k^{(m)} = \frac{\alpha_k^{(m)}}{\binom{m-1}{k-1} \alpha_t^m} Q_t = f_{cc} Q_t$$

Donde:

$$\alpha_t^{(m)} = \sum_{k=1}^m k \alpha_k^{(m)}$$

Se define $\alpha_k^{(m)}$ como la fracción de la frecuencia total de los sucesos de fallo que tienen lugar en el sistema afectando a cualesquiera k componentes en un grupo de m

Figura 3. Metodología de factores alfa FCC.

la pequeña contribución de las probabilidades / tasas de FCC frente a los mismos datos del fallo independiente, se empleaban para estos últimos los valores globales de fallo, es decir, la suma de ambas contribuciones de forma conservadora).

Finalmente, otra cuestión importante en el APS era la de considerar o no FCC en operación en la estimación de la frecuencia de los sucesos iniciadores de sistemas soportes con trenes alternantes. Hasta ese momento, se había postulado la posibilidad de que fallara(n) la(s) bomba(s) que estaba(n) en operación y que, al arrancar la(s) redundante(s), en espera, también pudiera(n) hacerlo por una misma causa. Sin embargo, no parecía razonable asumir un mismo estatus en ambos equipos; unos podrían haber estado en funcionamiento días o semanas, y a los otros se les requería que cumplieran su función durante la secuencia de accidente (24 horas, tiempo para llevar la planta a parada segura).

Se habían planteado diferentes hipótesis para evitar que una situación tan improbable alterara los resultados del APS.

Una opción fue la de considerar que sólo un 10% de este tipo de fallos podrían acoplarse con un mismo mecanismo de fallo; otra fue asignar al factor de causa común de todo el grupo un valor genérico calculado a partir de considerar que todos los componentes fallarían en operación por una causa común residual con una frecuencia determinada a partir de la experiencia operativa (no ha ocurrido un fallo de causa común de todas las bombas de sistemas de refrigeración), lo cual llevó a una estimación similar a la del LOCA grande. Incluso se planteó el analizar los tiempos medios de reparación de una bomba, entendiendo que, si se conseguía dejarla operativa antes de esas 24 horas (secuencia de accidente), aunque se produjera el fallo de otra bomba, no sería un suceso iniciador al haber sido recuperada.

EPRI, en 2021, editó el *Technical Report 3002020764* [9], y analizó esta cuestión. En su apdo. 3.3.4.3 *Potential Solutions for the Treatment of CCF SSIE*, explica que los datos analizados en el INL RADS⁵ incluyen sucesos acaecidos entre los años 1988 y 2020; en 2952 años-reactor han ocu-

rido 5 sucesos⁶ para la pérdida total o parcial de agua de servicios. Y señala que ninguno de esos iniciadores de fallo de causa común implicó a componentes normalmente en operación y componentes en espera que fallasen al ponerlos en operación.

La conclusión es que existe una fuerte evidencia en la experiencia operativa (cero sucesos de FCC en 25.900.000 horas) para descartar la postulación de FCC en aquellos grupos que contengan bombas en funcionamiento y bombas en espera, para un modelo que represente un suceso iniciador de sistemas soporte.

Adicionalmente, el documento define en su apdo. 3.2.1.3 *Based on Active/Passive Failure Mode Characterization*, entre otros, como dos modos de fallos activos, pero distintos, los siguientes:

- Fallo a operar durante el tiempo de misión tras una demanda con éxito.
- Fallo de componentes normalmente operando a continuar haciéndolo.

En ambos casos se trata de un fallo en operación, pero las condiciones son completamente diferentes.

A raíz del análisis de EPRI, ANAV decidió suprimir en los modelos de sucesos iniciadores de sistemas soporte este tipo de fallos de causa común.

REFERENCIAS

- [1]. EPRI NP-3967. Classification and Analysis of Reactor Operating Experience Involving Dependent Events. EPRI, Palo Alto, CA: 1985.
- [2]. EPRI NP-5613, NUREG/CR-4780. Procedures for Treating Common Cause Failures in Safety and Reliability Studies. Vol. 1 Procedural Framework and Examples. EPRI, Palo Alto, CA: 1988.

⁶Loss of RBCCW (Reactor Building Closed Cooling Water) due to stem/disk separation of the RBCCW heat exchanger temperature control valve (2001), fish intrusion affecting 2 units (2003), fire event (2010) y Loss of condenser heat sink due to failure of non-safety bus (2019).

⁵Risk Analysis and Data System

- [3]. EPRI NP-5613, NUREG/CR-4780. Procedures for Treating Common Cause Failures in Safety and Reliability Studies. Vol. 2 Analytic Background and Techniques. EPRI, Palo Alto, CA: 1988.
- [4]. EPRI TR-100382. A Database of Common-Cause Events for Risk and Reliability Applications. EPRI, Palo Alto, CA: 1992.
- [5]. NUREG/CR-5485. U.S. Nuclear Regulatory Commission. Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment. November 1998.
- [6]. NUREG/CR-6268. U.S. Nuclear Regulatory Commission. Common-Cause Failure Database and Analysis System. Revision 0 (INEEL/EXT-97-00696), Vol. 1–4, September 2007 (ADAMS Accession No. ML072970404).
- [7]. INL/EXT-21-62940. CCF Parameter Estimations 2020 Update. Zhegang Ma, and Kelly J. Kvardfordt. Idaho National Laboratory. November 2021.
- [8]. Idaho National Laboratory. System and Component Descriptions, Boundaries, and Failure Modes. <https://nrc.nrel.gov/publicdocs/CCF/CompBoundaries.pdf>. Accessed 2021.
- [9]. EPRI 3002020764. Consideration of Common Cause Failures in Risk Informed Decision-Making. 2021.■