

Banco de datos internacional de sucesos de fallo de causa común (ICDE)

M.^a R. Morales , B. Fernández Andújar y
M.^a B. Pereira

El Fallo de Causa Común (FCC) es un fallo dependiente en el que dos o más componentes fallan simultáneamente o en un corto espacio de tiempo como resultado directo de una causa común compartida. La causa compartida puede ser funcional o física.

Ante la baja frecuencia de este tipo de sucesos, algunos países miembros de la Agencia de Energía Nuclear (AEN) y de la Organización para la Cooperación y el Desarrollo Económico (OCDE) decidieron crear el proyecto *International Common-Cause Failure Data Exchange* (ICDE) con el fin de impulsar la cooperación multilateral en la recogida y el análisis de los datos de sucesos de FCC.

A Common Cause Failure (CCF) is a dependent event in which two or more components fail simultaneously or within a short space of time as a direct result of a shared common cause. The shared cause may be functional or physical.

Due to the low frequency of this type of events, some Member States of the Agency of Nuclear Energy (NEA) of the Organization for Cooperation and Economic Development (OECD) decided to create the project *International Common-Cause Failure Data Exchange* (ICDE) in order to encourage multilateral cooperation in the collection and analysis of data relating to CCF events.

INTRODUCCIÓN

Como *fallo dependiente* se entiende un suceso en el que se produce el fallo relacionado de varios componentes por una misma causa. El Fallo de Causa Común (FCC) es un fallo dependiente en el que dos o más componentes fallan simultáneamente o en un corto espacio de tiempo como resultado directo de una causa común compartida. La causa compartida puede ser funcional o física, por ejemplo, un mismo suministro de energía eléctrica, inundaciones internas, problemas de diseño, etc.

Normalmente, los Análisis Probabilistas de Seguridad (APS) deben tratar de forma explícita las dependencias funcionales y físicas. Los sucesos de FCC de los modelos APS representan aquellas causas compartidas residuales, es decir, que no están explícitamente modeladas.

Ante la baja frecuencia de este tipo de sucesos, algunos países miembros de la Agencia de Energía Nuclear (AEN, en inglés NEA, *Nuclear Energy*

Agency) y de la Organización para la Cooperación y el Desarrollo Económico (OCDE) decidieron crear el Proyecto *International Common-Cause Failure Data Exchange* (ICDE) con el fin de impulsar la cooperación multilateral en la recogida y el análisis de los datos relacionados con los sucesos de Fallos de Causa Común (FCC).

Actualmente, los países miembros son: Canadá, Corea del Sur, Finlandia, Francia, Alemania, España, Japón, Suecia, Suiza, el Reino Unido, República Checa y los Estados Unidos.

OBJETIVOS

Los objetivos iniciales del Proyecto ICDE fueron los siguientes:

- Recoger y analizar sucesos de FCC para entenderlos mejor, comprender sus causas y estudiar su prevención.
- Realizar análisis cualitativos de los sucesos de FCC, con el objeto de determinar cuáles son las mejores medidas preventivas o de mitigación de sus consecuencias.



M.^a ROSA MORALES CASTELLANOS
es licenciada con grado en Ciencias Exactas, especialidad Investigación Operativa, por la Universidad Complutense de Madrid. Funcionaria del Consejo de Seguridad Nuclear, asignada a la Unidad de Inspección.



BÁRBARA FERNÁNDEZ ANDÚJAR
es ingeniera industrial, especialidad Técnicas Energéticas, por la ETSIIM y máster en Ciencia y Tecnología Nuclear por la Universidad Politécnica de Madrid. Funcionaria del Consejo de Seguridad Nuclear, asignada al área de APS.



M.^a BEGOÑA PEREIRA PAGÁN
es ingeniera industrial, especialidad Técnicas Energéticas, por la ETSIIM de la Universidad Politécnica de Madrid. Responsable de Análisis de Datos de APS. Departamento de Seguridad de Empresarios Agrupados.

c) Establecer un mecanismo para el intercambio y acumulación de la experiencia obtenida en relación con los FCC, incluyendo el desarrollo de defensas contra su ocurrencia, tales como indicadores para inspecciones basadas en el riesgo.

A estos objetivos se ha añadido el de registrar características que faciliten la cuantificación de los sucesos básicos de Causa Común. Este punto presenta cierta complejidad debido a la dificultad de conseguir una homogeneización de los datos entre los distintos países.

El Proyecto ICDE pretende, por tanto, recoger todos los posibles sucesos de FCC, incluyendo tanto los completos (que se han llegado a producir) como parciales (o potenciales que no se han llegado a manifestar, pero cuyo fallo incipiente o estado de degradación se ha podido detectar). Se delimita como suceso aplicable: «El deterioro de dos o más componentes (con respecto al cumplimiento de una función específica) que se produce en un determinado intervalo de tiempo y que es el resultado directo de una causa compartida.»

ALCANCE Y CONTENIDO

Los componentes que se encuentran, en la actualidad, dentro del alcance del ICDE son:

- Bombas centrífugas.
- Generadores diesel.
- Válvulas motorizadas
- Válvulas de alivio / seguridad / alivio-seguridad.
- Válvulas de retención.
- Válvulas de aislamiento de vapor principal (MSIV).
- Baterías.
- Instrumentación de medida de nivel.
- Interruptores de potencia y de disparo del reactor.

Estado del ICDE a 2013

- 1681 sucesos de FCC.
- 127480 años-grupo de FCC (poblaciones de fallo de causa común).
- 12 tipos de componente + 2 en proyecto.
- 270 CCNN aportando información.
- 12 países.

- Mecanismos de accionamiento de barras de control.
- Cambiadores de calor.

Actualmente, están en desarrollo: ventiladores y componentes de instrumentación y control digital.

Básicamente, un suceso de FCC deberá ser interpretado para clasificarlo según su grado de fallo:

- Completo (C).
- Estado degradado (D).
- Incipiente (I).
- Estado operativo (W).

Y su tiempo de exposición al fallo:

- Misión.
- Intervalo de pruebas.
- Demandas reales.

Así mismo, antes de empezar a reportar sucesos de FCC, habrá que determinar la población susceptible de sufrirlos. En España se sigue la línea definida en los APS y, por tanto, el punto de partida para establecer el alcance del ICDE son los sucesos básicos de FCC modelados.

El ICDE introduce, no obstante, dos tipos posibles de poblaciones:

- Población observada (OP): componentes similares no necesariamente con una función redundante.
- Población expuesta (EP): población del suceso básico de FCC (con una función redundante).

Y recoge dos tipos de información:

- Sobre la población sujeta a FCC.
- Registro de identificación de la población, donde se define cada

grupo susceptible de FCC sobre el que se realiza un análisis de experiencia de explotación. Normalmente, se emplean algunos criterios para definir estos grupos: mismo tipo de componente, mismos modos de funcionamiento (arranque, operación, apertura, cierre, etc.), mismo fabricante, idénticas prácticas de mantenimiento, y, muy importante, misma función requerida.

- Registro estadístico de la población, donde se recogen los fallos independientes identificados para cada grupo de los anteriores, en función del modo de fallo modelado, así como sus horas o demandas (arranques, aperturas, cierres...)

- Sobre el suceso de fallo FCC.

- Registro del suceso FCC, donde se recoge toda la información que permita un análisis posterior del mismo.

ANÁLISIS DE SUCESOS DE FCC

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

- Fallos de diseño, fabricación o construcción: Se trata de un grupo de causas asociadas a sucesos o decisiones que tienen lugar antes de la explotación de la central, y por tanto, no relacionadas con su operación (especificaciones de diseño inadecuadas, diseño erróneo o inadecuado, construcción inadecuada o defectuosa).

- Causas propias de la operación de la planta (procedimientos inadecuados -ambiguos, incompletos o erróneos-, acciones humanas, condiciones de funcionamiento o ambientales extremas).

Los FCC se producen por la coexistencia de dos factores principales: la susceptibilidad que un componente presenta al fallo debido a una causa raíz concreta y el factor de acoplamiento (o **mecanismo de acoplamiento**) que crea la condición de que múltiples componentes se vean afectados

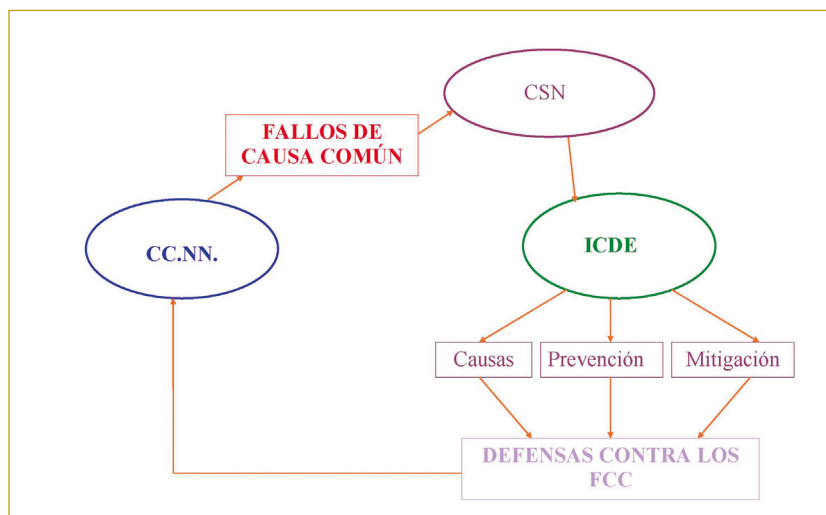


Figura 1.

Failure Cause	Process / Error / Immediate Cause of Failure			Symptoms of Failure	
Design	Engineering	Calculations errors in the capacity definition	Several charges are not considered	Insufficient capacity	
			Error in the definition of discharge voltage limit	Insufficient capacity	
	Construction	Inadequate selection for the component materials	Plates	Cracks / Breaks	
				Insufficient capacity (Premature aging)	
				Insufficient capacity (Loss of surface activity)	
			High acid concentration in the electrolyte	Insufficient capacity (Corrosion)	
				Short Circuit	
			Separators / Cells / Terminal connections	Decomposition of the electrolyte (Reaction with it)	
				Insufficient capacity (Loss of porosity)	
				Cracks / Breaks (Loss of plasticity or voltage mechanical stress)	
Maintenance / Test	Electrical	Incomplete recharge	Prolonged operation of cells with a low voltage reduce the capacity	Low density of th electrolyte	
		Float voltage		Low float voltage	
	Human	Blows during handling / bad manipulation		Cracks in cells	
		Entry of objects		Cracks in plates	
	-Direct actions	Short -circuit among plates			
	-Procedure	Lack os test / preventive maintenance (premature aging)		Insufficient capacity	
Other components	Charger / bar isolator / switchgear between the battery and charger			Loss of voltage	

Table 7.1 of ICDE Report (NEA/CSNI/R(2003)19: Battery Failures (causes, process, and symptoms)

Table 7.1 of ICDE Report (NEA/CSNI/R(2003)19: Battery Failures (causes, process, and symptoms)

Figura 2.

por la misma causa (por ejemplo, en el fallo de dos válvulas de alivio a la apertura por un mal tarado del punto de apertura debido a una inadecuada calibración: los factores de acoplamiento serían el procedimiento de calibración común y, tal vez, el mismo personal de mantenimiento; la causa raíz sería la mala calibración). Las defensas contra los fallos de causa común tienen la consecuencia inmediata de mejorar la fiabilidad de los componentes.

Las defensas básicas contra los fallos de causa común son las siguientes:

Redundancia es la existencia de múltiples componentes o trenes, cada uno de los cuales es capaz de cubrir el 100% de la función que se requiere. Básicamente, una redundancia significa la existencia de al menos un 100% alternativo de la capacidad de esa función o de un sistema para cumplir los requisitos funcionales específicos del mismo. El criterio de redundancia se emplea para alcanzar una alta fiabilidad en sistemas de seguridad, así como una gran disponibilidad en sistemas de producción y servicios. Se considera que un sistema cumple con el criterio de redundancia si puede operar con uno o más trenes fallados o indisponibles. Aunque, en principio, la aplicación del criterio de redundancia puede implicar independencia entre trenes, es prácticamente imposible

demostrar que no existe algún tipo de dependencia entre ellos.

Separación Funcional: un 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.

Separación Física: de trenes o componentes redundantes. Normalmente se establece una distancia entre los tramos redundantes o se emplean barreras protectoras (paredes, cubículos o salas separados, etc.). Con una separación física de los sistemas se protegen de forma efectiva las redundancias de las dependencias espaciales.

Diversidad: se puede dividir un sistema redundante en dos o más trenes conteniendo diferentes componentes con el mismo propósito funcional. La diversidad de equipos implica, por tanto, que un sistema disponga de trenes o componentes redundantes que no sean idénticos (por ejemplo, es el caso de un sistema de Agua de Alimentación Auxiliar que disponga de dos trenes con bombas motorizadas y un tren con una turbobomba).

Otras: separación en el tiempo (sustitución de equipos o pruebas / mantenimientos escalonados). La separación en el tiempo es una medida administrativa de protección

contra los problemas de diseño y envejecimiento. Esta defensa consiste, por ejemplo, en la instalación de nuevos equipos de una forma escalonada (no todos a la vez sino separados en el tiempo) o la realización de pruebas escalonadas en el tiempo. El ICDE recoge esta política de pruebas para cada grupo de FCC. Para que esta medida sea verdaderamente efectiva es importante disponer de un buen sistema de análisis de la experiencia de planta y de recogida de fallos. Se entiende que si se realizan pruebas

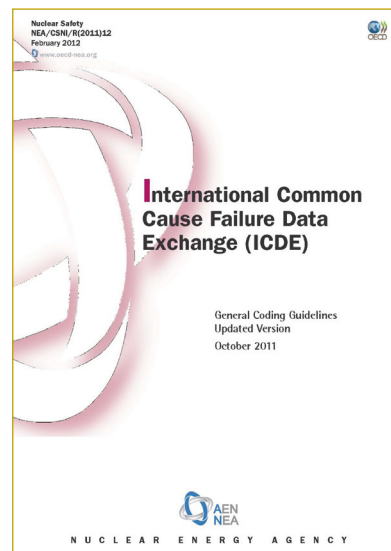


Figura 3.

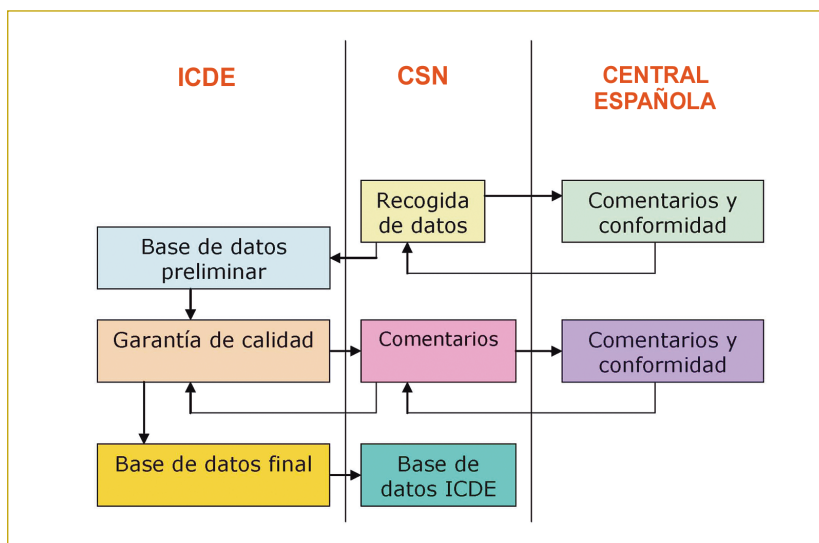


Figura 3. escalonadas en el tiempo y se detectase en una de ellas un fallo que se pudiese considerar de causa común real o potencial, se procedería a revisar los componentes redundantes al objeto de prevenir la ocurrencia del FCC sobre todo el grupo.

Un concepto importante en el análisis que el ICDE realiza sobre los sucesos de FCC es el factor tiempo. Si un suceso tiene un factor tiempo bajo (la influencia del tiempo se califica de baja) significa que entre el primer fallo y el siguiente (en un equipo redundante por la misma causa) habría

margen para que la planta detectase la anomalía y procediese a su eliminación. Por el contrario, un factor tiempo alto, prácticamente implica que no hay margen para evitar que un segundo componente (o más) presente la misma degradación.

RECOGIDA DE INFORMACIÓN

Para facilitar el proceso de recogida de información, el ICDE ha elaborado lo que denomina “Guías de Codificación” para cada uno de los tipos de componentes dentro de su alcance.

Normalmente, el procedimiento de trabajo consiste en que uno o más países proponen el análisis de un tipo de componente y, tras la aprobación del grupo, se encargan de elaborar una descripción general, identificando los sistemas a los que puede pertenecer, los límites físicos del componente (se incluye una figura del tipo de componente que facilite la comprensión de sus límites físicos), el periodo mínimo de recogida de datos, las excepciones que puedan existir (por ejemplo, en los fallos de los generadores diesel se excluyen aquellos que serían baidaseados en caso de emergencia), los posibles modos en que puede fallar u otras informaciones de interés (piezas falladas, posibles síntomas del fallo, etc.) Es decir, se elabora una “Guía de Codificación” del componente que, posteriormente, se somete al Grupo del ICDE para comentarios o aclaraciones, siendo finalmente editada.

Una vez establecida la Guía, se elabora un programa de recogida de la información en el que participan todos los países miembros. Durante el periodo de aporte de sucesos, se lleva a cabo también un proceso de Garantía de Calidad. El CSN aporta información a partir de lo recogido en los APS españoles y está sujeto, por tanto, a las actualizaciones de los mismos. En el proceso participan todas las centrales con las que se consensúa la información a reportar.

Failure Cause Categories		Failure symptoms	Percentage
Design			50%
1. Engineering process:	• Calculation errors in the capacity definition	• Insufficient capacity of the battery	4 %
2. Construction process	• Inadequate selection of component materials for the plates / electrolyte / separators / cells	• Insufficient capacity • Short-circuit • Low-voltage battery/cells	46%
Maintenance / Test			42 %
1. Physical failures in sub-components	• Electrolyte • Connections • Breaker / Switch	• Loss of density • Low level in the electrolyte • Insufficient tightening of connection • Corrosion or increasing of the resistance between terminal connections and wires • Discharge of the battery	20%
2. Electrical failures	• Incomplete recharge • Prolonged operation of cells with low voltage	• Low density of the electrolyte • Low-voltage battery/cells • Low floating voltage • Premature aging	12 %
3. Human - Direct actions	• Bad manipulations, blows during handling of entry of objects, etc.	• Cracks in cells or plates • Short-circuit	8 %
- Procedure	• Lack of test/preventive maintenance	• Premature aging • Low-voltage battery/cells	2 %
Other components		• Loss of voltage	6%
Unknown		• Loss of voltage	2 %

Tabla 1.

1ª Etapa: el CSN recoge información del análisis de experiencia operativa del APS de la central, seleccionando aquellos sucesos susceptibles de ser considerados potenciales o reales FCC.

2ª Etapa: se analizan los sucesos y se rellena el formato del ICDE en inglés. Se envían los sucesos analizados a la central para su aprobación. Este paso puede requerir iteraciones, ya que la central puede hacer comentarios que se deben resolver hasta que quede el suceso definitivo a enviar al ICDE.

3ª Etapa: se envían los sucesos al ICDE. En esta fase, el ICDE revisa la información aportada, pudiendo a su vez emitir comentarios. El CSN resuelve aquellos comentarios que no tengan una implicación mayor; el resto, en caso de que haya, serán reenviados a las plantas. Una vez pasado este proceso, el ICDE aprobará el suceso que será cargado a dicho banco de datos.

Una vez reportados todos los sucesos de FCC de un determinado tipo de componente por parte de los países que participan en él, los países líderes* los analizan desde el punto

*España ha sido país líder de los tipos de componentes batería e interruptor.

de vista cualitativo, es decir, investigan cuáles han sido las causas más comunes, qué tipo de defensas se podrían implantar o se han implantado para evitarlos o minimizarlos, qué síntomas del fallo hubo, qué tiempo transcurrió o podría transcurrir hasta el fallo de todos los componentes del grupo, cuál es la mejor forma de detección, etc...

Y para ello, requieren de la participación de todos los países participantes, organizando un *workshop* en el que distintos grupos comentan los sucesos ocurridos, sacando conclusiones que son transferidas a los encargados del tipo de componente para que lo incorporen en su informe. El informe, una vez redactado, se pasa a comentarios de todo el grupo. Tras este último proceso, se aprueba y es editado de forma pública por la OCDE.

A modo de ejemplo, en la Tabla 1 se muestra el análisis de los sucesos reportados -causas identificadas y síntomas del fallo- para el tipo de componente batería.

La mayoría de los sucesos fueron detectados durante pruebas o mantenimientos programados lo que reveló la importancia de mantener una adecuada política de los mismos como verdadera medida preventiva.

CONFIDENCIALIDAD

Por último, es preciso mencionar, como tema relevante, la confidencialidad del ICDE, siendo el coordinador nacional el responsable de mantenerla en su respectivo país. Dentro de cada uno de los informes públicos, se añade un párrafo similar al siguiente:

The confidentiality of the data is a prerequisite of operating the project. The ICDE database is accessible only to those members of the ICDE Project Working Group who have actually contributed data to the databank.

Los informes se pueden descargar desde la página de la OCDE/NEA:

www.nea.fr/html/nsd/docs/indexcsni.html.

BIBLIOGRAFÍA

- Nuclear Safety NEA/CSNI/R(2011)12. International Common-Cause Failure Data Exchange (ICDE). General Coding Guidelines. Update Version October 2011. February 2012.
- NEA/CSNI/R(2003)19. ICDE Project Report: Collection and Analysis of Common-Cause Failures of Batteries. December 2003.
- <http://www.oecd-nea.org/jointproj/icde.html>
- <http://www.nea.fr/html/nsd/docs/indexcsni.html>.■