

Análisis de modos y efectos de falla expandido: Enfoque avanzado de evaluación de fiabilidad

Manuel Perdomo Ojeda

correo electrónico: mperdomo@instec.cu

Instituto Superior de Tecnología y Ciencias Aplicadas (InSTEC), La Habana, Cuba

Artículo Original

Jesús Salomón Llanes

correo electrónico: jsalomon@instec.cu

Instituto Superior de Tecnología y Ciencias Aplicadas (InSTEC), La Habana, Cuba

Resumen

Los métodos cualitativos de evaluación de la fiabilidad y el riesgo han probado ser una herramienta útil para la toma de decisiones. El artículo presenta las características principales de un nuevo enfoque, el análisis de modos y efectos de falla, para unir las bondades de los métodos cualitativos y algunas de las fortalezas importantes de los cuantitativos. Este nuevo enfoque se implementó en el programa informático ASeC, y mediante él se realizó un estudio de fiabilidad detallado a un sistema de extinción de incendios, que incluye, a diferencia de la metodología tradicional, el análisis de fallas de causa común, y de dependencias funcionales. Los resultados se compararon con los de un análisis de fiabilidad por árbol de fallas del mismo sistema, utilizando el software ARCON. Se mostró la importancia del nuevo enfoque de análisis de modos y efectos de fallas expandido, en la obtención de resultados objetivos para la toma de decisiones basadas en la fiabilidad de sistemas complejos.

Palabras claves: análisis de modos efectos y criticidad de fallas, evaluación de la fiabilidad, evaluación del riesgo, análisis de sistemas, análisis de modos y efectos de fallas expandido

Recibido: 8 de febrero del 2016 Aprobado: 14 de julio del 2016

INTRODUCCIÓN

Los métodos cualitativos de evaluación de la fiabilidad y la seguridad, conocidos también como métodos de análisis de peligros de los procesos (PHA en inglés), han probado ser una herramienta útil para la toma de decisiones, bajo situaciones de escasa disponibilidad de datos. Sin embargo, estos suelen presentar insuficiencias de rigurosidad y cierto grado de subjetividad, que los hacen menos atractivos que sus similares de naturaleza cuantitativa. Por otro lado, la ventaja de no depender de datos estadísticos para obtener resultados fidedignos y su grado de detalle y facilidades descriptivas les dan la fortaleza principal, pero aun así queda sin resolver el problema de sus debilidades respecto del modelado

de dependencias, aspecto clave en la fortaleza de los métodos cuantitativos, como el análisis probabilista de seguridad (APS) [1,2].

Las ventajas que representa el empleo de los métodos cualitativos en el área de evaluación de riesgos, ha mantenido el interés en mejorarlos, actuando sobre aquellas debilidades que han sido bien identificadas. Así, se han realizado esfuerzos en ese sentido para técnicas tales como el análisis de modos y efectos de fallas (FMEA, por sus siglas en inglés) y el análisis de peligros y operabilidad (HAZOP, por sus siglas en inglés), reconocidas entre las de mayor uso y fortalezas.

El FMEA y su variante semicuantitativa: análisis de modos, efectos y criticidad de fallas (FMECA, por sus

siglas en inglés), han sido usados para asegurar la calidad de productos y procesos, para aumentar la seguridad de estos y evaluar su fiabilidad, aplicándose a sistemas eléctricos, mecánicos y de instrumentación y control, presentes en industrias como la química [3], la automotriz [4], en aerogeneradores [5], en centrales nucleares, para la determinación de los sucesos iniciadores de accidentes [6], en la mejora de la seguridad y calidad de prácticas de radiodiagnóstico de tumores [7] y de radioterapia [8], así como, en la industria militar y la aeronáutica.

Tras la edición en 1980 del procedimiento MIL-STD-1629A [9], como guía para la ejecución de los análisis FMECA, este ha sido ampliamente usado durante décadas sin experimentar variaciones, sin embargo, también se han reconocido debilidades presentes en esta metodología que tienen el potencial de afectar los resultados del análisis. En tal sentido, Estorilo y Posso proponen en [4] un método para resolver las irregularidades en el llenado de las hojas de trabajo del FMEA de proceso, empleado en la industria automotriz como requerimiento de calidad de los productos de los suministradores. En tanto, Arabian-Hoseinabadi, Oraee y Tavner plantean en [5] una modificación de las escalas de severidad, ocurrencia y detección, que fueron previamente establecidas en [9], para adaptarlas mejor a las condiciones de las turbinas de las máquinas aerogeneradoras. En otras prácticas, sin embargo, se ha aplicado siguiendo su metodología tradicional, como se documenta en los trabajos de Sawant, Dietrich y otros [7] y de Yang, Cao y otros [8].

Por su parte, la técnica HAZOP ha sido ampliamente usada en los análisis PHA de la industria de procesos, fundamentalmente en las industrias química y petroquímica. Su importancia para la seguridad de la industria ha hecho que en países como Gran Bretaña, Noruega y Estados Unidos de América (EE.UU.), se haya legislado su uso. Por ejemplo, en EUA su empleo quedó establecido desde 1992 en la norma OSHA 29 CFR Part 1910 [10]. Dada la complejidad del HAZOP es común encontrar numerosas guías y procedimientos escritos, que facilitan su empleo, como los establecidos en [11]. Pero al igual que el FMEA, a esta poderosa técnica de análisis también se le han reconocido debilidades importantes, que han sido objeto de mejoras. Ello puede verse en el trabajo realizado en [12] por Dunjó y otros, en el que se analiza la evolución histórica del HAZOP, a partir de la revisión de 166 documentos bibliográficos que muestran la variación sufrida por esta técnica, tanto para poder tratar en los modelos aquellas cuestiones específicas de la tecnología, que hasta entonces no habían sido consideradas, como para incluir la incidencia de los factores humanos, siendo esto último una de las principales críticas realizadas a la metodología tradicional.

Por ejemplo, para ayudar a resolver el problema del gasto significativo de tiempo que conlleva este tipo de

estudio, y su alta dependencia con el grado de experiencia del equipo de analistas, Rossing y otros desarrollaron en [13] un asistente informatizado denominado Functional HAZOP, que reduce considerablemente el esfuerzo involucrado, y agrega conocimiento al proceso de análisis permitiendo así, a analistas de poca experiencia realizar aportes importantes al estudio; ello se logra en gran parte modelando la instalación a través de módulos, de modo que las líneas con la misma función sean analizadas una sola vez. En otro trabajo [14], Cagno y otros afirman que el HAZOP es el enfoque más apropiado para gestionar los riesgos típicos de una industria en la etapa más compleja del proyecto: la puesta en servicio, desarrollando para ello una nueva metodología analítica, denominada Multilevel HAZOP (HzM), que combina la metodología tradicional con el HAZOP humano (human HAZOP), la técnica de análisis por árbol de eventos (ETA) y las técnicas de análisis de fiabilidad humana THERP y HEART. Este último enfoque permite la implementación de medidas más efectivas para reducir los riesgos, dado que determina con mayor precisión las secuencias de fallas donde hay desviaciones con consecuencias negativas, pero complica considerablemente el proceso de análisis, aun cuando se aplique la variante reducida (Two steps Multilevel HAZOP, HzM2S).

Llama la atención que no se encontró en la literatura consultada sobre estas metodologías ningún trabajo relativo al tratamiento de las dependencias, aun cuando se conoce que estos aspectos dominan el riesgo en instalaciones complejas con funciones y sistemas redundantes. Por ello se estimó conveniente ampliar la consulta hacia las metodologías implementadas en programas informáticos del estado del arte, dedicados a los análisis cualitativos de riesgo, dentro de los que se encuentran Leader software, de ABS Consulting [15]; y SCRI de Dinámica Heurística, S.A. [16]. Como resultado se constató que dicho problema tampoco está tratado en estos programas.

El presente trabajo persigue mostrar las características principales de un nuevo método de naturaleza semicuantitativa, implementado en el programa ASeC (ASeC_FMEAE) [17], que logra reunir las bondades de los métodos cualitativos y algunas de las fortalezas más importantes de los métodos cuantitativos más completos, dentro de las que está la posibilidad de realizar análisis de fallas de causa común y de dependencias funcionales, cuyos fundamentos se establecen en la sección 2 de este trabajo. Mediante esta herramienta novedosa se realiza un estudio de fiabilidad detallado a un sistema de extinción de incendios, que incluye ambos tipos de análisis antes mencionados, no presentes en la metodología tradicional, cuyas preparación y adaptación para su estudio aparece en la sección 3. Los resultados del análisis de criticidad mediante ASeC_FMEAE se comparan con los del análisis

de fiabilidad por árbol de fallas del mismo sistema, utilizando el software ARCON, mostrándose la utilidad del nuevo enfoque, a través de la discusión de estos resultados en la sección 4.

MATERIALES Y MÉTODOS

El método FMEAe (FMEA expandido) surge para dar solución al problema descrito en la introducción de este trabajo, dedicado fundamentalmente al tratamiento de las dependencias entre componentes y aquellas debidas a las funciones de apoyo (por ejemplo, alimentación eléctrica, control y mando), aunque algunas modificaciones se han implementado también en los métodos de análisis de criticidad. Las nuevas facilidades incorporadas en FMEAe que incrementan las potencialidades de la técnica tradicional, se resumen a continuación:

- a) Determinación de los sucesos básicos de causa común y estimación de sus probabilidades de ocurrencia.
- b) Determinación de las dependencias funcionales entre componentes.
- c) Análisis de importancia de causas de falla.
- d) Análisis de importancia por tipos de componentes.

Con las potencialidades descritas en los incisos a) y b) se logra acercar la técnica tradicional de FMEA a las bondades analíticas del árbol de fallas y árbol de eventos. La relevancia de esta novedad radica en que los modos de falla de causa común suelen ser dominantes en sistemas redundantes, contribución que se acrecienta aún más, cuanto mayor sea el grado de esta redundancia, mientras que las dependencias funcionales por equipos compartidos son parte importante de los puntos débiles del diseño de instalaciones complejas, hallados mediante los APS. Las novedades señaladas en c) y d) representan una fortaleza tanto para el propio FMEA tradicional, como para cualquiera de las técnicas cualitativas o cuantitativas, pero no se abordan en este trabajo. La metodología de FMEAe está implementada en el software ASeC [17]. Algunas de las bondades de su aplicación práctica se presentan más adelante, a través de los resultados del análisis de fiabilidad detallado de un sistema de extinción de incendios.

Determinación de los sucesos básicos de causa común y estimación de sus probabilidades de ocurrencia

Este procedimiento consiste en determinar de modo automatizado los componentes-modos de falla que cumplen funciones redundantes, que experimentan fallas por causa común. El algoritmo de análisis incluye las siguientes tareas generales:

- Se parte de un listado genérico de componentes, basado en la experiencia operacional y en estudios previos publicados. Un listado típico a considerar aparece en el capítulo 5 de [19], el cual se puede modificar para incluir otros componentes que,

basado en la experiencia específica, justifiquen su inclusión.

- De esta lista, se seleccionan como candidatos a análisis de fallas de causa común (FCC), aquellos que son redundantes e idénticos, definiéndose hasta 3 grados de dependencia, en función de la cantidad de atributos compartidos por los mismos. El grupo G1 comparte solo atributos internos, como por ejemplo, modo de operación, modo de falla y modo de control. Grupos G2 y G3 comparten atributos de G1 más atributos externos (por ejemplo, local de trabajo, condiciones de trabajo), siendo G3 el grupo más restrictivo, es decir, al que pertenecen aquellos componentes que comparten todos los atributos, internos y externos.
- Se afecta la tasa de falla o, alternativamente, la probabilidad de falla o indisponibilidad de los candidatos, mediante un factor BETA (β) genérico (factor β cuyo valor se corrige según el grado de redundancia de los componentes generadores aplicando la ecuación (5-1), Capítulo 5, de la referencia [19]).
- Los valores genéricos postulados (sin corregir de acuerdo con el grado de redundancia) del factor BETA según el grado de dependencia es el siguiente:
 - $\beta (G1) = 0,10$
 - $\beta (G2) = 0,15$
 - $\beta (G3) = 0,20$
- Para postular el valor $\beta (G1)$ se toma como referencia el valor medio de los factores β estimados en estudios de fallas de causa común en componentes activos de sistemas en centrales nucleares [19]. Se asume de manera conservadora que un aumento en el grado de dependencia incrementa en un 50 % el valor de dicho factor, y de ahí se obtienen los valores $\beta (G2)$ y $\beta (G3)$.
- Se agregan los modos de fallas de causa común en la hoja de trabajo para que participen en la evaluación del FMEA o análisis de criticidad, junto al resto de los modos de falla simples, por cualquiera de los tres métodos incluidos.

En la figura 1 se aprecia que los últimos 3 componentes-modos de falla del sistema se refieren a fallas de tipo FCC. Estos modos de falla participan también en el análisis de criticidad, de modo similar a cómo participarían en un modelo de árbol de fallas. La diferencia fundamental con este último es que aquí han sido determinados automáticamente por el software, mediante un algoritmo que utiliza los nuevos campos agregados en la Hoja de Trabajo. El panel ubicado en el extremo inferior izquierdo (figura1) indica que estas tres fallas tipo FCC, que involucran a 9 modos de falla, pertenecen a dos grupos de diferente grado de dependencia (3 componentes de grado G1 y 6 componentes de grado G3), información que puede ser verificada por el usuario desplegando la casilla correspondiente en el código ASeC.

Sistema: SISTEMA DE EXTINCIÓN DE INCENDIOS **ID:** SEI-001 **Planos de Ref.:** FIG.13.1-1

Subsistema: **ID:**

Datos Técnicos

No.	Componente	Modelo	Interfaces	Función	Reserv.	C	Estado	Condiciones de Trabajo	Ubicación
19	V4	VM-300	EE5,RL-106	Permitir paso de fluido ante demanda	200%	A	1: Abierto/AUTO (válvula, botón)	Presión normal	Local002
20	V7	VM-300	EE5,RL-107	Permitir paso de fluido ante demanda	200%	A	6: Cerrado/AUTO (válvula, botón)	Presión normal	Local003
21	CM-B1*8*10	PM-100		Suministro de flujo de líquido a presión	100%	2	20: Espera/AUTO (bombas, ver)	Presión normal	Local002
22	CM-B1*9*11	PM-100		Suministro de flujo de líquido a presión	100%	3	20: Espera/AUTO (bombas, ver)	Presión normal	Local002
23	CM-V2*13*14	VC-200		Bloqueo de fluido/evitar derivación	100%	4	6: Cerrado/AUTO (válvula, botón)	Presión normal	Local002

Datos de Fallos y Efectos

No.	Modo de Fallo	Cód.G.	Tasa F.	T.Obs.	T.Rep.	Controles	Causas	FPC	FOC	EA	CA	ES	CS	ED	CD
19	Falla a mantener la posición (D)	VM	2,0E-7	720	20	2: Probado periódicamente	Falla mecánica/Unión/Acoples	1						2	
20	Falla a abrir (D)	VM	1,0E-5	720	20	2: Probado periódicamente	Falla eléctrica/Interruptor	1	2					2	
21	Falla a arrancar (S)	PM	3,6E-7	720	20	2: Probado periódicamente	Falla eléctrica/Interruptor	0,60	1					3	
22	Falla a operar dado que arrancó (R)	PM	3,6E-6	12		4: En operación/No reparable	Alta vibración	1	2					3	
23	Falla a abrir (D)	VC	3,6E-8	720	20	2: Probado periódicamente	Corrosión	1	1					3	

Observaciones

No.	Observaciones
19	Válvula motorizada a la descarga de las líneas de B1 y B2.
20	Válvula motorizada a la descarga de la línea de B3.
21	Falla de causa común de las bombas B1, B2 y B3 a arrancar ante
22	Falla de causa común de las bombas B1, B2 y B3 a operar duran
23	Falla de causa común a abrir de las válvulas de retención V2, ...

Generadores de Fallos Causa Común

Código	Cantidad
B1.S	G3 6
B2.S	G2
B3.S	G1 3

No. de Componente-modos de fallo: 23

Fig. 1. Hoja de trabajo FMEAE, mostrando los componentes-modos de falla del 19 al 23.

Antes de pasar al análisis de criticidad de los componentes-modos de falla, se procede a determinar el efecto de cada uno de ellos. Este proceso lo realiza el analista, de forma similar que en un FMEA tradicional. En este caso, FMEAE divide el análisis en tres categorías: Efectos ambientales, efectos sobre la seguridad, y efectos sobre la disponibilidad de la instalación o sistema objeto de análisis. Los tres tipos de efecto se clasifican mediante una escala de cinco tipos de efectos o severidades, desde 1 (leve) a 5 (catastrófico). El ejemplo de la figura 1 muestra que para este caso solo existen efectos sobre la disponibilidad (valores numéricos que aparecen en la columna ED de la tabla de Datos y Efectos de Fallas). Cuando se aplica el método de los modelos de fiabilidad de componentes, la matriz de criticidad se completa multiplicando los grados de severidad (ED_i) por la probabilidad de ocurrencia del modo de falla (q_i) que es función, a su vez, del modo de control del componente (por ejemplo, no controlado, probado periódicamente y monitorizado continuamente) y por un factor (FPM_i) que depende del modo de operación (automático, manual remoto, manual local), como se aprecia en la ecuación (1).

$$IRCD_i = (q_i)(ED_i)(FPM_i) \quad (1)$$

Donde $IRCD_i$, ($0 \leq IRCD_i \leq 1$), es el índice de riesgo de disponibilidad del componente-modo de falla i , q_i es la probabilidad de ocurrencia del componente-modo de falla i , ED_i es el efecto sobre la disponibilidad que presenta el componente-modo de falla i al ocurrir, FPM_i es el factor de ponderación debido al modo de operación del componente

que define el modo de falla i (auto, manual remoto, manual local). A diferencia de la metodología tradicional de FMEA, en FMEAE se establece un indicador para evaluar la fiabilidad/riesgo del sistema. Para ello se emplea el IRS (Índice de Riesgo del Sistema) que se calcula según la ecuación (2) como el promedio de los valores de los índices de riesgo de cada componente-modo de falla, (IRC_i), determinados mediante la matriz antes descrita.

$$IRSd = \sum_{i=1}^n \frac{IRCd_i}{n} \quad (2)$$

Donde $IRSd$ es el índice de riesgo sobre la disponibilidad del sistema.

De acuerdo con la siguiente escala este valor de IRS (IRS_a , IRS_s , IRS_d , para cada uno de los tipos de efectos evaluados en FMEAE) clasifica la fiabilidad/riesgo del sistema en zonas que van desde la condición de 'Alta fiabilidad/Bajo riesgo' hasta 'Baja fiabilidad/Alto riesgo':

- $IRSd \leq 1,0E-3$: el índice de riesgo del sistema tiende a la excelencia.
- $1,0E-3 < IRSd \leq 2,0E-3$: el índice de riesgo del sistema se aleja de la excelencia en un rango tolerable.
- $2,0E-3 < IRSd \leq 4,0E-3$: el índice de riesgo del sistema presenta una incipiente degradación.
- $4,0E-3 < IRSd \leq 8,0E-3$: el índice de riesgo del sistema está degradado.
- $8,0E-3 < IRSd \leq 2,4E-2$: el índice de riesgo del sistema se acerca a la zona crítica.
- $2,4E-2 < IRSd \leq 7,2E-2$: el índice de riesgo del sistema está en la zona crítica.

- $7,2E-2 < IRSd \leq 2,2E-1$: el índice de riesgo del sistema es muy crítico.
- $2,2E-1 < IRSd$: el índice de riesgo del sistema es extremadamente crítico.

La escala anterior se basa en las dos premisas siguientes: para definir el índice de fiabilidad de un sistema ideal se toma como referencia el requerido en instalaciones que aplican buenas prácticas, como es el caso de las centrales nucleares, por ejemplo, de tipo CANDU ($Q=1,0E-03$) y, por otro lado, se asume como valor ideal para los efectos evaluados, el valor mínimo de la escala de efectos de FMEAe ($EA=1$; $ES=1$; $ED=1$). De esta forma, se comienza con la meta de $IRCd=1,0e-03$, y se van degradando esos valores, incrementándose periódicamente hasta alcanzar el límite superior, ($IRCd=2,2E-01$), por encima del cual se considera que la fiabilidad (o el riesgo) del sistema es extremadamente crítica. La evaluación de criticidad de los componentes-modos de falla se realiza mediante el Índice de Importancia Relativa del componente ($IIRi$), como presenta la ecuación (9) en [17]. Para facilitar la toma de decisiones, los valores de importancia relativa $IIRi$ se ordenan decrecientemente por su contribución al IRS, de acuerdo con el criterio presentado en la página 85 de [17].

Determinación de las dependencias funcionales entre componentes

Este análisis se realiza empleando la información contenida en los nuevos campos agregados a la Hoja de Trabajo, como son 'Interfaces' y 'C' (canal de acoplamiento de a redundancia). Su objetivo es alertar a los revisores del diseño o la operación de la instalación o sistema objeto de estudio, sobre la posibilidad de un aumento de la frecuencia de fallas por dependencias funcionales entre componentes diferentes (por servicios comunes o compartidos). El algoritmo de análisis incluye las siguientes tareas generales:

- Determinación de los grupos de dependencias, que se refieren a los componentes o ítems de la hoja de trabajo que tienen coincidencias de interfaces.
- Determinar el grado de la dependencia (GDF) dentro del grupo de componentes similares.
- Determinar el grado de importancia de las dependencias (GID) del grupo de componentes dado.

El GDF se define dentro de un mismo grupo de componentes (por ejemplo, bombas diésel, válvulas operadas por aire, etc.) y se calcula mediante la ecuación (3).

$$GDF = \frac{i}{m} \quad (3)$$

Donde GDF es el grado de dependencia funcional de un grupo dado de componentes, i es el número de interfaces que coinciden para componentes diferentes del grupo dado, m es el número total de interfaces de los componentes del grupo dado. Una vez determinado

el GDF, la dependencia existente se clasifica de acuerdo con su grado de importancia (GID), según criterios que dependen de combinaciones formadas entre la magnitud anterior y la redundancia del componente involucrado.

RESULTADOS

Preparación del FMEAe para aplicarlo a un sistema de extinción de incendios

El sistema objeto de estudio se muestra en la figura 2. Se refiere a un sistema de seguridad con alto grado de redundancia, que se encuentra en régimen de espera y debe activarse al recibir la señal automática de ocurrencia de un incendio en la instalación industrial a la que protege. Las consideraciones para el análisis se exponen a continuación:

- Toda la información de partida para llenar los datos técnicos y de fallas y efectos de la Hoja de Trabajo de FMEAe, aparece en el Capítulo 6, epígrafe 6.1a) (resumido en tabla 6.1-1), epígrafe 6.1b) (resumido en tabla 6.1-2) y epígrafe 6.1c) de la referencia [19].
- Se incluyen los errores humanos preaccidentales en aquellos equipos que se desalinean para prueba o mantenimiento, de modo que puedan quedar en posición incorrecta en el momento que sean demandados.
- Los sucesos básicos de falla de causa común (FCC), se determinan automáticamente por el software (FMEAe en ASeC).
- No se incluyen los sucesos especiales, dado que estos solo se usan para el modelado por Análisis de Árbol de Fallas (FTA).
- Se descartan las fallas a cerrar de las válvulas de retención para evitar derivación de fluido, por su baja probabilidad de ocurrencia.
- Se asume que el sistema ocupa 3 recintos diferentes, estando los componentes principales ubicados de acuerdo con la distribución que muestra la tabla 1.

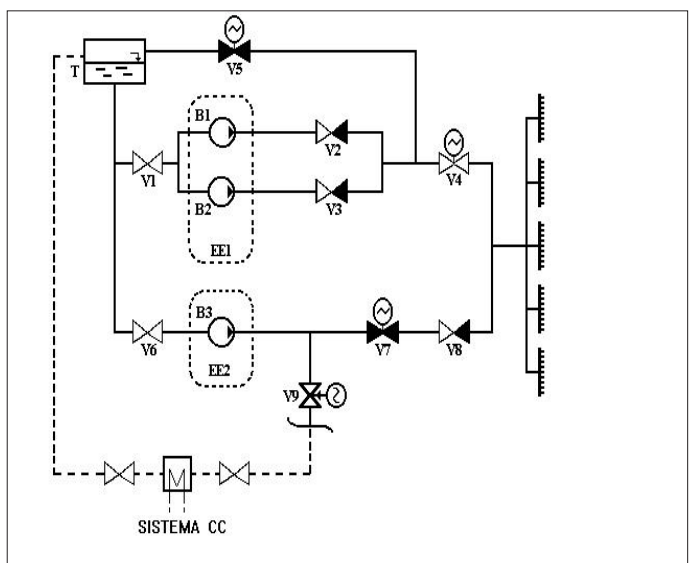


Fig. 2. Esquema simplificado de un sistema de extinción de incendios.

Tabla 1

Distribución de equipos por recinto

Recinto	Equipos ubicados
Local 001	T, V1, V6
Local 002	B1, B2, V2, V3, V4, V5
Local 003	B3, V7, V8, V9

Resultados de la determinación de la criticidad de los componentes-modos de falla, incluyendo las fallas de causa común

La figura 3 presenta los resultados del análisis de criticidad del sistema de la figura 2, aplicando el método de Modelo de Fiabilidad de Componentes, que parte de las tasas de falla, tiempos medios de reparaciones, modos de operación y de control, y grado de redundancia de los componentes-modos de falla del sistema, completados en la Hoja de Trabajo mostrada en la figura 1. En este caso, aplicando el algoritmo para la determinación de las FCC descrito en la sección 2, cumplen las condiciones de candidatos a FCC las bombas B1, B2 y B3 y las válvulas de retención V2, V3 y V8 (modos de falla No. 21 a), 23, figura 1). Se aprecia que aproximadamente el 65 % de los modos de falla incluidos en el análisis son no críticos, en tanto, solo aproximadamente el 4 % de estos resultaron de criticidad muy alta, y un 13 % de criticidad alta, lo que confirma el comportamiento esperado de la distribución de las contribuciones al riesgo de los componentes-modos de falla en sistemas, que cumple el principio de Pareto.

Resultados de la determinación de la criticidad de los componentes-modos de falla, sin incluir las fallas de causa común

En la figura 4 se muestran los resultados del análisis de criticidad de los modos de falla del sistema de la figura 2, pero en este caso sin la participación de las FCC. Aquí se observa que el perfil de fiabilidad del sistema cambia, siendo ahora dominantes los errores humanos sobre las válvulas V1 y V6 (V1.M y V6.M).

Resultados de la determinación de las dependencias funcionales

En la figura 5 se presentan los resultados del análisis de dependencias funcionales del sistema, realizado de acuerdo con el algoritmo descrito en el epígrafe 2. Según las características de diseño asumidas para este ejemplo, el perfil de dependencias funcionales indica que el grupo 2, conformado por las bombas, tiene una interfaz (alimentación eléctrica, EE1) que provoca dependencia entre las bombas B1 y B2. Como B1 y B2 son redundantes, pero pertenecen a un grupo de redundancia de grado 3 (B1, B2 y B3), y B3 no comparte la misma alimentación eléctrica que sus redundancias, se obtiene un GID Medio (M, amarillo), lo que no es tan riesgoso para la disponibilidad del sistema, que si hubiese sido determinado de Crítico (rojo) o Extremo (marrón), pero debe tomarse en consideración.

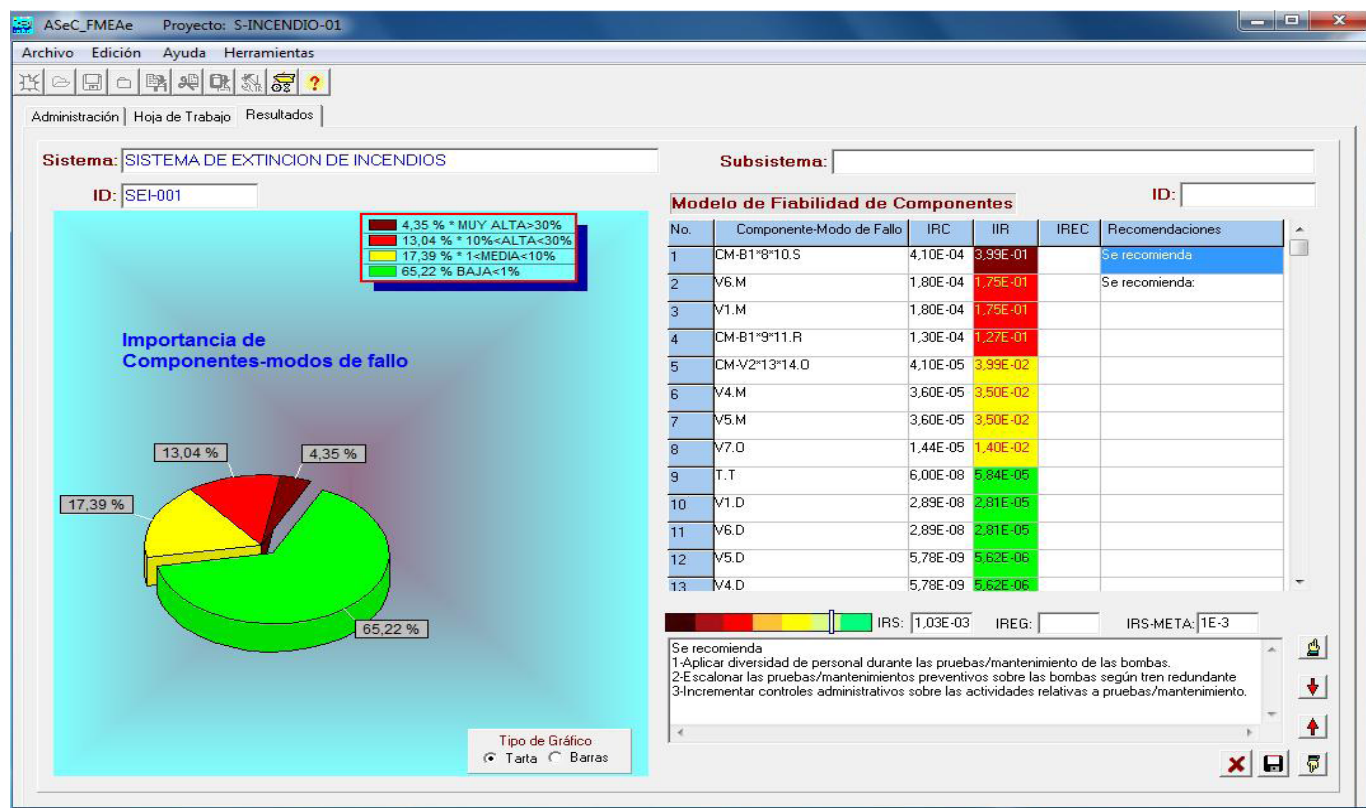


Fig. 3. Hoja de Resultados FMEAE. Criticidad de componentes-modos de falla (incluyendo las FCC).

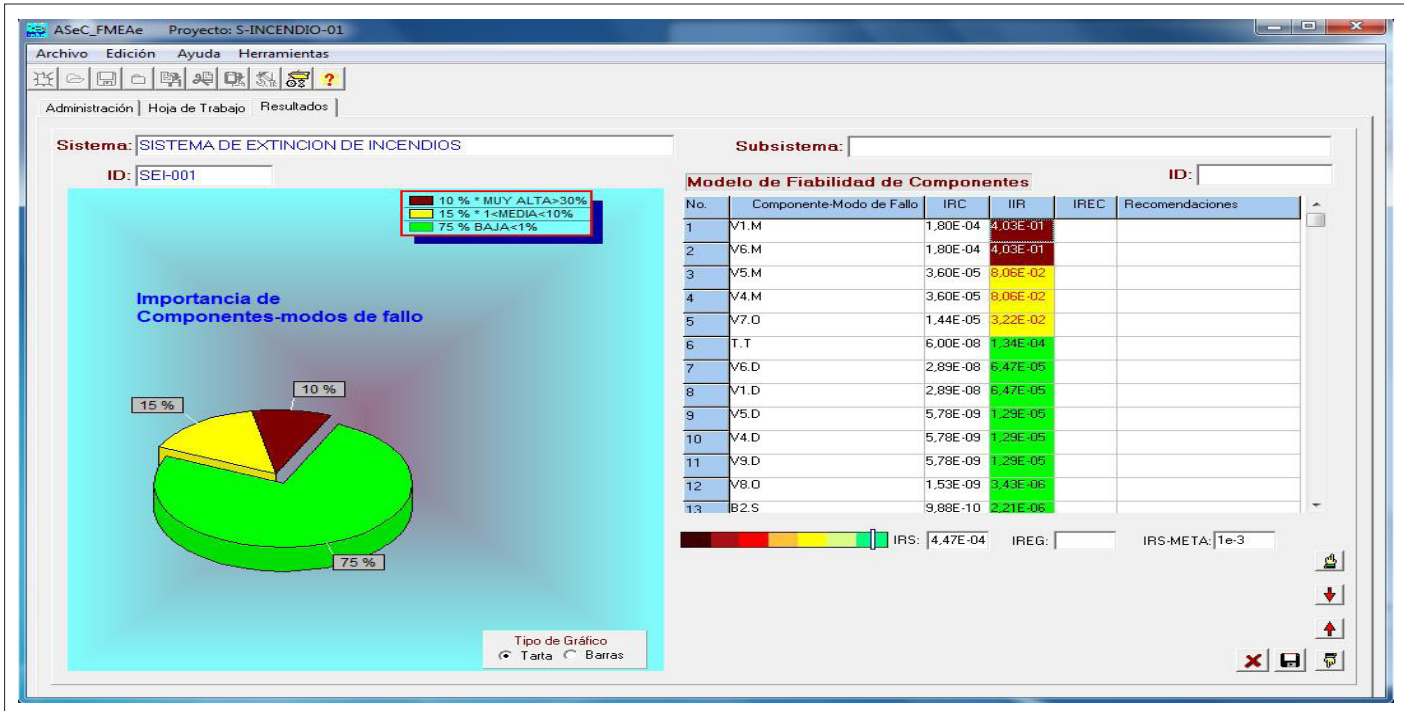


Fig. 4. Hoja de Resultados FMEAe. Criticidad de componentes-modos de falla (sin incluir las FCC).

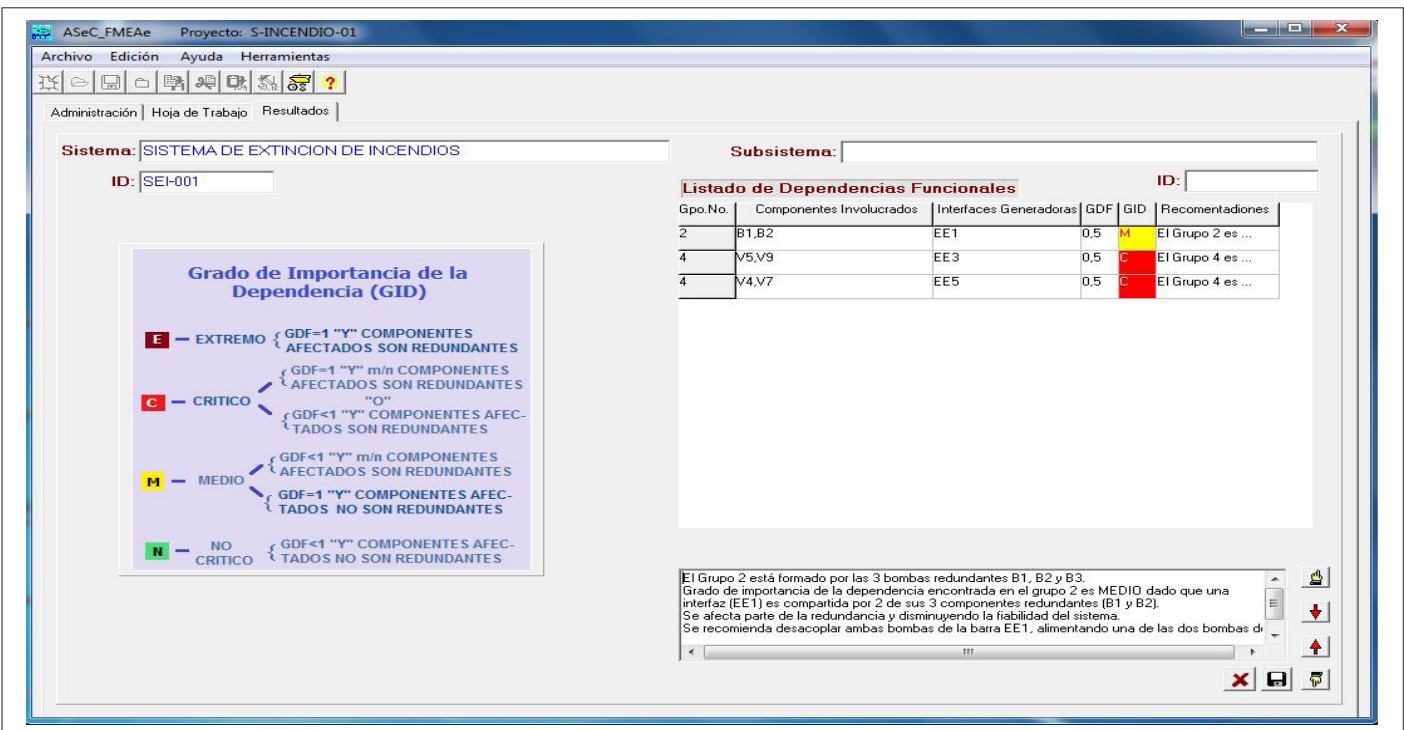


Fig. 5. Hoja de Resultados FMEAe. Importancia de dependencias funcionales.

DISCUSIÓN

Discusión de los resultados de la determinación de la criticidad de los componentes-modos de falla

La fiabilidad del sistema está dominada por las FCC y los errores humanos. Así, en la figura 3 puede verse que la FCC de las bombas a arrancar ante la demanda (CM-B1*8*10.S) contribuye al índice de riesgo del sistema

(IRS) en un 39,9 % (Muy Alta, de acuerdo con la escala presentada en la sección 2). Le siguen en orden decreciente los errores humanos a dejar en posición incorrecta a las válvulas manuales V1 y V6 (V6.M, V1.M; 17,5 %, Alta), y la FCC de las bombas B1, B2 y B3 a operar durante la misión (CM-B1*9*11.R; 12,7 %, Alta). En menor grado de criticidad están la FCC a abrir de las válvulas de retención

(CM-V2*13*14.O; 3,99%, Media), los errores humanos a dejar las válvulas V4 y V5 en posición incorrecta (V4.M, V5.M; 3,5 %; Media) y la falla a abrir de la válvula V7 (V7.O; 1,4 %, Media).

Este resultado es el esperado en sistemas con alta redundancia y sin diversidad, siendo solo los errores humanos y las FCC los sucesos que tienen el potencial para deteriorar la misma. Las diferencias fundamentales entre el perfil de fiabilidad del sistema obtenido con FMEAe (figura 3) y aplicando el método de árbol de fallas (Capítulo 6, [19]), se deben a que en este último se utilizan sucesos especiales y otras facilidades de modelado como es la ineficiencia de pruebas, mientras que en el primero se agrega el aporte de los efectos de las fallas. No obstante, en ambos casos, coinciden los elementos de la lista de componentes-modos de falla dominantes.

Es importante notar que el valor del índice de riesgo del sistema (IRS) calculado mediante la ecuación (2) de la sección 2, se incrementa 2,3 veces (de 4,47E-4 a 1,03E-3, figuras 4 y 3, respectivamente) cuando son incluidos los aportes de las FCC, demostrándose la contribución importante de estos eventos en el decremento de la seguridad o fiabilidad de sistemas con redundancia incluida.

La limitación fundamental radica en que, tanto la escala de evaluación del IRS, como los valores de los factores β para el cálculo de las tasas de falla de causa común, son valores genéricos postulados de la experiencia operacional de instalaciones donde existen buenas prácticas y necesitan ajustarse a casos específicos diferentes. No obstante, las causas que tributan a estas fallas son similares independientemente del tipo de instalación, por lo que el objetivo fundamental es llamar la atención sobre estos aspectos, y si se justifica pueden realizarse estudios de sensibilidad cambiando los valores en un rango que represente el caso actual. En el caso del IRS, se espera corregir la escala con la experiencia de aplicación del método a objetos variados.

Discusión de los resultados de la determinación de las dependencias funcionales

Quedó demostrada la importancia de este tipo de análisis para complementar las evaluaciones de fiabilidad y riesgo, empleando métodos semicuantitativos lo que se considera una fortaleza del método FMEAe. El resultado mostrado en la figura 5, implica que si fallase la alimentación eléctrica EE1 sería afectada apreciablemente la confiabilidad del sistema, pero quedaría disponible la bomba B3. Esta característica puede tomarse como una fortaleza de diseño del sistema de la figura 2, detectada por el análisis del FMEAe. En el caso del grupo 4, que incluye las válvulas motorizadas, existe una interfaz que provoca dependencia funcional entre las válvulas V5 y V9, las cuales de fallar abiertas derivan caudal importante a través de las líneas de prueba de B1/B2 y de B3 (ver esquema

de la figura 2). Ello ocurre cuando falla la alimentación eléctrica EE3, de aquí que, a diferencia del caso anterior, se está en presencia de un GID crítico (C, rojo), pues la dependencia afecta completamente a la redundancia, lo que puede notarse como una debilidad importante en el diseño del sistema. El otro problema detectado se refiere a las válvulas V4 y V7, que comparten la misma alimentación eléctrica (EE5). Como ambas son redundantes, al fallar la EE5, dejan al sistema indisponible, de ahí que el GID sea crítico (C), lo que también se refiere a una debilidad importante de diseño. Ninguno de los métodos de análisis y evaluación de la fiabilidad realiza este tipo de estudios tan importante para evaluar la fiabilidad del diseño de sistemas complejos, lo que representa una importante potencialidad del FMEAe.

CONCLUSIONES

El análisis exhaustivo de la fiabilidad del sistema redundante de extinción de incendios por el método de FMEAe, que incluye las Fallas de Causa Común y dependencias funcionales, arrojó resultados muy similares al realizado por el método de árbol de fallas. Se detectaron las principales debilidades y potencialidades de diseño del sistema analizado. Queda demostrada la utilidad de poder hacer análisis complementarios al análisis de fiabilidad tradicional, como herramienta de enfoque integral de apoyo para tomas de decisiones concernientes a la seguridad o fiabilidad de sistemas complejos. El método FMEAe brinda a los analistas de fiabilidad y riesgo una herramienta poderosa con la combinación de las bondades de los métodos cuantitativos y de los cualitativos, para realizar estudios detallados de fiabilidad/riesgo de sistemas de complejidad considerable, permitiendo obtener resultados similares e incluso más integrales que por el método de Árbol de Fallas.

REFERENCIAS

1. INTERNATIONAL ATOMIC ENERGY AGENCY. "Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants". *IAEA Safety Standards*. Specific Safety Guide No. SSG-3. 2010. ISSN: 1020-525X. ISBN 978-92-0-114509-3. Vienna, Austria. Disponible en: http://www-pub.iaea.org/mtcd/publications/pdf/te_1200_prn.pdf [Consultado: Abril 2014].
2. VILARAGUT, LLANES, Juan José; FERRO FERNÁNDEZ, Rubén *et al.* "Análisis probabilista de seguridad de tratamientos de radioterapia con un acelerador lineal de uso médico". *Revista NUCLEUS*, Dic. 2010, núm. 48, pp. 16-20. ISSN: 0864-084X. Disponible en web: <http://scielo.sld.cu/cgi-bin/wxis.exe/iah/> [Consultado: Abril 2014].
3. AGUILAR OTERO, José R.; TORRES ARCIQUE, Rocío; MAGAÑA JIMÉNEZ, Diana. "Análisis de modos de falla, efectos y criticidad (AMFEC) para la planeación

- del mantenimiento empleando criterios de riesgo y confiabilidad". *Tecnología, Ciencia, Educación*, vol. 25, núm. 1, 2010, pp. 15-26. ISSN: 0186-6036. Instituto Mexicano de Ingenieros Químicos A. C. Monterrey, México. Disponible en web: <http://www.redalyc.org/articulo.oa?id=48215094003> [Consultado: mayo 2014].
4. **ESTORIO, Carla; POSSO, Richard K.** "The reduction of irregularities in the use of process FMEA". *International Journal of Quality and Reliability Management*. 2010, vol. 27, núm. 6, pp. 721-733. Emerald Group Publishing Limited. ISSN: 0265-671X. Disponible en web: <http://www.emeraldinsight.com/journals.htm?articleid=1864948> [Consultado junio 2014].
 5. **ARABIAN HOSEYNABADI, H.; ORAEE, H.; TAVNER, P. J.** Failure Mode and Effects Analysis (FMEA) for wind turbines. *Electrical Power and Energy Systems*, 32 (2010), p. 817-824. ELSEVIER, 2010. ISSN: 0142-0615. Disponible en web: <http://www.sciencedirect.com/science/article/pii/S0142061510000281> [Consultado: junio 2014].
 6. INTERNATIONAL ATOMIC ENERGY AGENCY. "Safety assessment and verification for nuclear power plants". Safety standard series núm. NS-G-1.2. *IAEA Safety Guide*, pp.83. IAEA, Vienna: 2001. ISBN: 92-0-101601-8. Disponible en web: http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1428_web [Consultado: junio 2014].
 7. **SAWANT, Amit; DIETRICH, Sonja; SVATOS, Michelle; KEAL, Paul.** "Failure mode and effect analysis-based quality assurance for dynamic MLC tracking systems". *Medical Physics*. Dec. 37(12) 6466 (2010). American Association of Physicists in Medicine. Disponible en web: <http://dx.doi.org/10.1118/1.3517837> [Consultado: Mayo de 2015].
 8. **YANG, F.; CAO, N.; YOUNG, L.; et. al.** "Validating FMEA output against incident learning data: A study in stereotactic body radiation therapy". *Medical Physics*. 2015, núm. 42, pp. 2777, American Association of Physicists in Medicine. Disponible en web: <http://dx.doi.org/10.1118/1.4919440> [Consultado: Mayo de 2015].
 9. DEPARTMENT OF DEFENSE. MILITARY STANDARD. "Procedures for performing a failure mode, Effects and Criticality Analysis". *MIL-STD-1629A. AMSC N3074*. Washington DC, USA. November 24, 1980. Disponible en web: <http://sre.org/pubs/Mil-Std-1629A.pdf> [Consultado: julio de 2014].
 10. OCCUPATIONAL SAFETY AND HEALTH ADMINISTRATION. "Process Safety Management of Highly Hazardous Chemicals, Explosives and Blasting Agents, Final Rule". 29 *CFR Part 1910*. OSHA 7-1-07 Edition. USA, 2007. Disponible en web: http://www.osha.gov/pls/oshaweb/owasrch.search_form?p_doc_type=STANDARDS&p_toc_level=1&p_keyvalue=1910 [Consultado: octubre de 2014].
 11. AMERICAN INSTITUTE OF CHEMICAL ENGINEERS-CENTER FOR CHEMICAL PROCESS SAFETY. "Guidelines for Hazard Evaluation Procedures: with worked examples". AIChE-CCPS, 2nd. ed. 1992. ISBN: 0-8169-0491-X, New York, USA. Disponible en web: <http://www.abebooks.com/9780816904914/Guidelines-Hazard-Evaluation-Procedures-Worked-081690491X/plp>. [Consultado: julio de 2014].
 12. **DUNJÓ, Jordi; FTHENAKIS, Vasilis et. al.** "Hazard and Operability (HAZOP) analysis. A literature review". *Journal of Hazardous Materials*, 173 (2010) pp. 19-32. ELSEVIER, 2009. Disponible en web: <http://www.ncbi.nlm.nih.gov/pubmed/19733970>. [Consultado: sep-tiembre de 2014].
 13. **ROSSING, Netta Liin; LIND, Morten et. al.** "A functional HAZOP methodology". *Computer and chemical engineering*, 34 (2010), pp. 244-253. ELSEVIER. ISSN: 0098-1354. Disponible en web: <http://www.sciencedirect.com/science/article/pii/S0098135409001793> [Consultado: septiembre de 2014].
 14. **CAGNO, E.; CARON, F.; MANCINI, M.** "Risk analysis in plant commissioning: the multilevel HAZOP". *Reliability engineering and system safety*, 77 (2002), pp. 309-323. ELSEVIER, 2002. Disponible en web: <http://www.sciencedirect.com/science/article/pii/S0951832002000649> [Consultado: septiembre de 2014].
 15. ABS Consulting. *Leader 2015 software*. ABSG Consulting Inc., Houston, Texas, USA. Copyright 2000-2015. Disponible en web: <http://www.absconsulting.com>. [Consultado: Marzo 2015].
 16. Dinámica Heurística, S.A. de C.V. *Software SCRI-HAZOP, SCRI-FMEA, SCRI-What/If*. Monterrey, NL, México. 2010-2013. Disponible en web: <http://www.dinamicaheuristica.com> [Consultado: Mayo 2014].
 17. **RODRÍGUEZ GUAL, Maritza; PERDOMO OJEDA, Manuel et al.** "ASeC software application based on FMEAs in a mechanical samples positioning system on a radial channel for irradiations in a nuclear research reactor with continuous full-power operation". *International Journal of Ecosystems and Ecology Science (IJEES)* [on-line]. 4(1), 2014, pp 81-88. ISSN: 2224-4980. Disponible en web: http://www.researchgate.net/profile/Ilir_Morina/publication/265786164_Monuments_of_Nature_of_Mirusha_River_Basin/links/541b489a0cf2218008c1ce55.pdf. [Consultado: septiembre de 2014].

18. MOSQUERA, Genaro; RIVERO, Jesús.; SALOMÓN, Jesús *et. al. Disponibilidad y Confiabilidad de Sistemas Industriales*. 1995, Ediciones Universitarias UGMA, Barcelona, Venezuela. 156 pp. ISBN: 980-00-0889-6.
19. PERDOMO, Manuel; FERRO, Rubén. *Tratamiento de las fallas dependientes y las acciones humanas en los análisis de confiabilidad y riesgo de la industria convencional*. 2001, Ediciones Universitarias UGMA, Barcelona, Venezuela, 189 pp. ISBN: 980-00-1689-9.

AUTORES

Manuel Perdomo Ojeda

Ingeniero en Energética Nuclear, Máster en Instalaciones Energéticas y Nucleares, Profesor Auxiliar, Departamento de Ingeniería Nuclear, Facultad de Ciencias y Tecnologías Nucleares, Instituto Superior de Tecnologías y Ciencias Aplicadas (InSTEC), La Habana, Cuba.

Jesús Salomón Llanes

Ingeniero Electricista, Doctor en Ciencias Técnicas, Profesor Titular, Departamento de Ingeniería Nuclear, Facultad de Ciencias y Tecnologías Nucleares, Instituto Superior de Tecnologías y Ciencias Aplicadas (InSTEC), La Habana, Cuba

Expanded Failure Mode and Effects Analysis: Advanced Approach for Reliability Assessments

Abstract

The qualitative methods for risk and reliability assessment have proved to be a useful analytical tool in support of decision-making processes. This paper shows the key aspects of a new approach developed in the failure mode and effects analysis method, in order to link the kindness of the qualitative methods and some of the more important strengths of the quantitative ones. This new approach of analysis was implemented in the ASeC computer code, by means of which it was carried out a detailed reliability analysis of a fire extinction system that includes, in contrast to the traditional technique, common cause failures analysis and functional dependences analysis. The results are compared with those, which have been obtained using the fault tree analysis, by means of the ARCON computer code. Finally, the relevance of the new approach in reliability-concerned decision-making processes, it is shown, through the results of the analysis by applying the expanded failure modes and effect analysis method.

Key words: failure mode effects and criticality analysis, reliability assessment, risk assessment, system analysis, expanded failure mode and effects analysis