FOCUS ARTICLE

EL ÁRBOL DE FALLOS Y EL ANÁLISIS DE IMPORTANCIA, DOS HERRAMIENTAS PARA LA OPTIMIZACIÓN DE LA GESTIÓN DE DISTINTOS TIPOS DE RIESGOS

Arturo Trujillo

Introduction

El árbol de fallos es una metodología desarrollada en la década de 1960, y utilizada ampliamente desde entonces para el análisis de riesgos. Habitualmente, asociamos el término "riesgo" a la pérdida de vidas humanas, a los daños al medio ambiente o a las pérdidas económicas. No obstante, cabe también reconocer otros tipos de riesgos, tales como el deterioro de la calidad de un producto, o de la imagen de una compañía, la pérdida de producción, o la indisponibilidad de una planta. En el presente artículo se describe brevemente la técnica del árbol de fallos aplicada al análisis de este tipo de situaciones, se muestra una aplicación práctica, y se introduce el denominado análisis de importancia como herramienta de gestión de riesgos.

EL ANÁLISIS MEDIANTE ÁRBOL DE FALLOS

El árbol de fallos es una técnica de análisis de fallos deductiva que parte de un evento indeseado en concreto y proporciona un método para determinar las causas de este evento y, lo que a menudo es todavía más importante, cómo se relacionan las causas con el evento final. Lógicamente es importante una elección adecuada del suceso indeseado (al que denominaremos "cabecera" del árbol). Si el suceso es demasiado general, el análisis se hace inmanejable; si es demasiado específico, el análisis no proporcionará información suficiente acerca del sistema estudiado. El suceso de cabecera acostumbra a estar relacionado con la seguridad de la planta o instalación, pero no siempre es así. De hecho, el método es completamente universal, y pueden analizarse con él diversos tipos de riesgos (daños a la calidad del producto, pérdida de producción, daños medioambientales, etc.). Algunos ejemplos de sucesos de cabecera de un árbol de fallos podrían ser:

- Rotura catastrófica de un reactor químico por sobrepresión originada por una reacción fuera de control.
- El vehículo no arranca cuando se gira la llave de contacto.
- Pérdida de calidad del producto (color) por temperatura excesiva durante el proceso de síntesis.
- Pérdida de producción por paro de planta originado por interrupción del suministro eléctrico.

En el presente artículo se utilizará un ejemplo para demostrar la potencia del método.

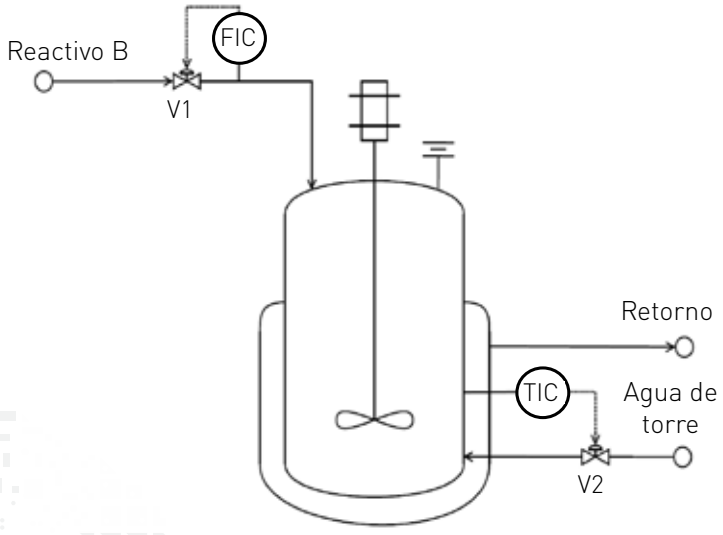


Figura 1. Esquema del sistema estudiado.

APLICACIÓN PRÁCTICA: UN EJEMPLO DE ÁRBOL DE FALLOS

El esquema de la figura 1 muestra el sistema que se analizará. Se trata de un reactor químico, dotado de un agitador, una camisa a través de la que se puede enfriar con agua de torre, así como un sistema de dosificación de un reactivo, y la instrumentación auxiliar necesaria. En este ejemplo se considerará que en el reactor se lleva a cabo una reacción del tipo:

Reactivo A + Reactivo B -> Producto + calor

Inicialmente se carga un disolvente en el reactor, así como el reactivo A y el catalizador de la reacción. Posteriormente se arranca la agitación y se va añadiendo controladamente el reactivo B. Un análisis de riesgos de proceso efectuado previamente detectó que en caso de perderse el control de la reacción se produciría un desprendimiento excesivo de calor en el reactor, que provocaría la vaporización del disolvente y consiguiente presurización. Por ello se ha dotado al reactor con las siguientes protecciones:

- El reactivo B se dosifica a caudal constante. El caudalímetro FIC actúa sobre la válvula automática V1 manteniendo el valor de caudal consignado por el operador.
- El reactor dispone de un sistema de enfriamiento mediante una camisa por la que circula agua de torre. La temperatura de la masa de reacción se controla al valor consignado por el operador mediante la sonda de temperatura TIC que, a su vez, actúa sobre la válvula automática de paso de agua V2. La válvula V2 tiene un tope mecánico para asegurar que circula un caudal mínimo de agua, independientemente de las indicaciones de TIC.
- Como última barrera, el reactor dispone de un disco de ruptura específicamente diseñado para una pérdida del control de temperatura de la reacción.

A fin de no complicar en exceso el ejemplo, se han considerado las siguientes hipótesis simplificadoras:

- Se considera que la operación correcta de cualquiera de los dos lazos de control disponibles (caudal del reactivo B y temperatura de la masa de reacción) es suficiente para mantener la seguridad de la reacción. Esto es:
    - El caudal mínimo garantizado por el tope mecánico de V2 es suficiente para enfriar el reactor siempre que se mantenga el control sobre el caudal del reactivo B.

- El sistema de enfriamiento del reactor tiene capacidad suficiente para enfriarlo, aun cuando se pierda el control del caudal del reactivo B.

- No se considera el error humano en el establecimiento de los valores de consigna de caudal del reactivo B ni de temperatura.
- No se considera la posibilidad de fallo del tope mecánico de la válvula V2.
- No se considera el error en el diseño de los sistemas; en particular, del disco de ruptura.
- Obviamente, el agitador es una parte importante del sistema de enfriamiento del reactor. No obstante, en este caso se ha considerado que el sobredimensionamiento del sistema de enfriamiento es tal que, incluso con el agitador parado, es suficiente para mantener el control de temperatura.

Se invita al lector a reanalizar el ejemplo teniendo en cuenta uno o varios de estos efectos.

CONSTRUCCIÓN DEL ÁRBOL DE FALLOS

En este ejemplo, el suceso que se pretende analizar es la sobre presurización (y eventual estallido) del reactor debido a la pérdida de control de la reacción. A este suceso se le denomina "cabecera" del árbol, se escribe como encabezamiento del árbol de fallos (ver figura 2) y es para el que se calculará la probabilidad de ocurrencia.

Para que se produzca esta sobrepresión inaceptable y subsiguiente estallido, es necesario que den dos sucesos simultáneamente:

- Que haya fallado el sistema de control de temperatura descrito en el apartado anterior.
- Que fallen las salvaguardas disponibles: fundamentalmente, que el disco de ruptura no se abra a la presión prevista.

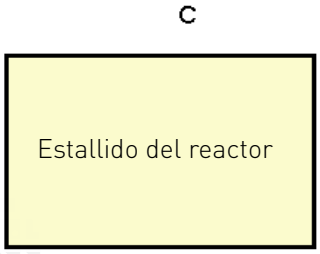
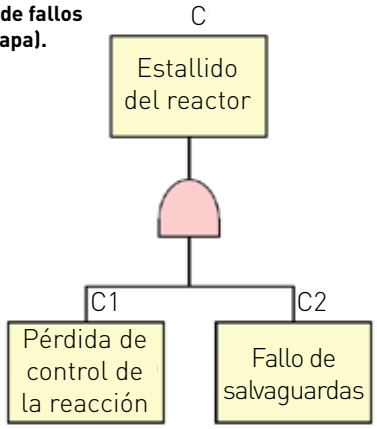


Figura 2. Árbol de fallos (primera etapa).

Dado que estos dos sucesos deben producirse simultáneamente, y el de cabecera no se producirá si no se dan ambos, se representan en el árbol enlazados con el suceso de cabecera a través de una puerta lógica "Y" (ver figura 3). El árbol en este punto puede leerse como "se producirá el suceso de cabecera si se dan la pérdida de control de la reacción Y el fallo de las salvaguardas disponibles".

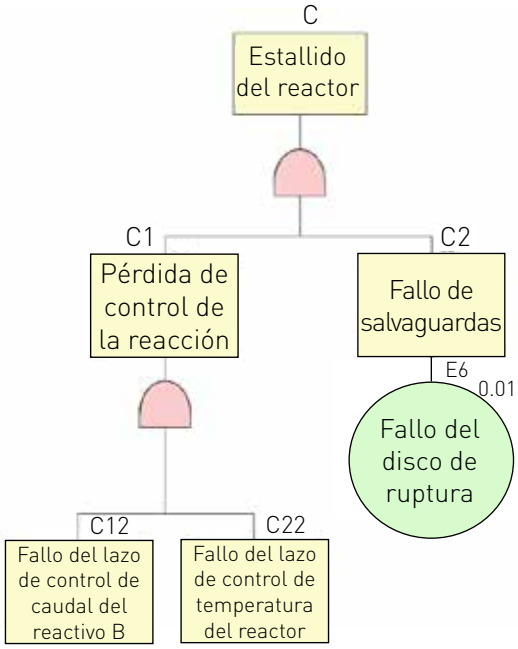
Figura 3. Árbol de fallos (segunda etapa).



El fallo (no apertura) del disco de ruptura es ya un evento suficientemente sencillo para el análisis que se pretende, por lo que se denomina "suceso elemental" y se representa como un círculo. En cambio, la pérdida de control de temperatura del reactor es todavía un suceso complejo, que se debe desarrollar más.

De la descripción anterior del proceso cabe deducir que la pérdida de control de la temperatura requiere el fallo simultáneo del lazo de control de caudal FIC-V1 y del lazo de control de temperatura FIT-V2. Así pues, al igual que se ha hecho en el paso anterior, ambos eventos se enlazarán mediante una puerta lógica "Y" (ver figura 4).

Figura 4. Árbol de fallos (tercera etapa).

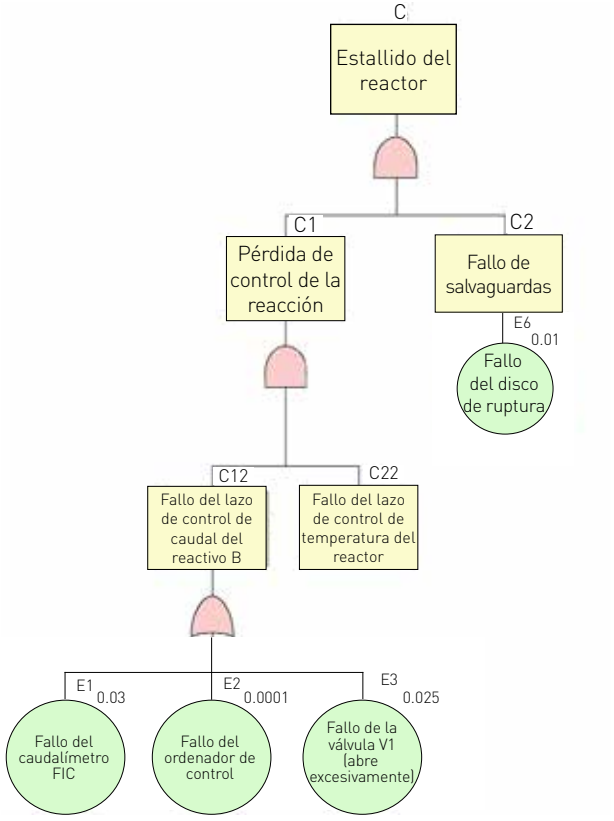


Ambos sucesos son todavía demasiado complejos para el análisis propuesto, por lo que debe proseguirse su desarrollo. Tomando el caso del fallo del lazo de control de caudal del reactivo B, puede concluirse que este puede ser debido al fallo de uno cualquiera de los siguientes componentes:

- El caudalímetro FIC indica un caudal inferior al que realmente está pasando.
- El ordenador de control de la planta no interpreta correctamente los datos del caudalímetro y ordena abrir en exceso la válvula V2.
- La válvula V2 se abre en exceso a pesar de recibir las señales correctas del ordenador de control.

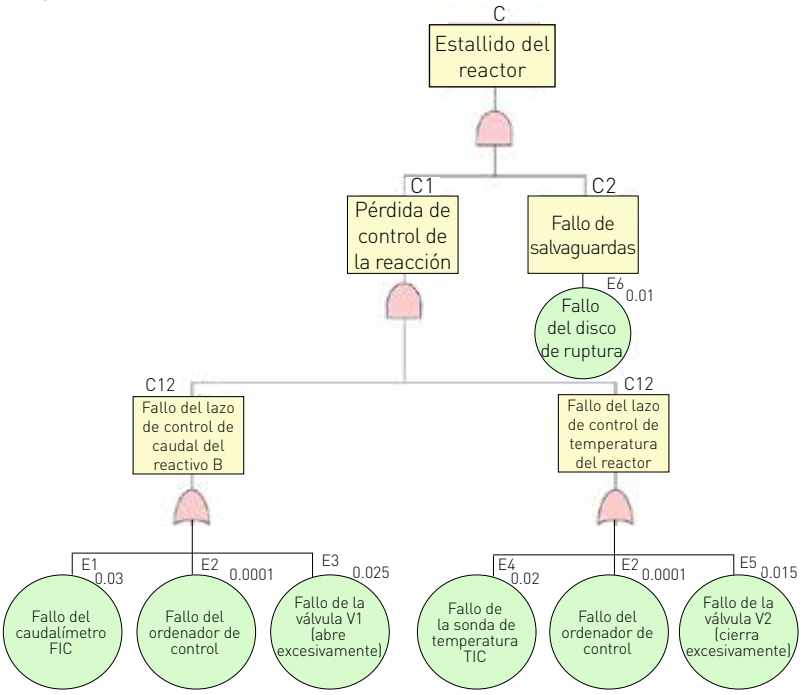
Dado que uno solo de estos tres eventos puede dar lugar a la pérdida del control de caudal de reactivo B, se enlazarán mediante una puerta lógica "O", tal como muestra la figura 5. Esta sección del árbol de fallos puede leerse como "la pérdida de control del caudal de reactivo B se produce si se da el fallo del caudalímetro FIC O el fallo del ordenador de control O el fallo de la válvula V1". Los tres sucesos identificados son ya suficientemente simples para el análisis que se pretende, por lo que se considerarán eventos elementales.

Figura 5. Árbol de fallos (cuarta etapa).



Obviamente, el lazo de control de temperatura es análogo al del de caudal de reactivo B, sin más que reemplazar FIC por TIC y V1 por V2 (en cambio, se considerará que el fallo del ordenador de control es común para ambos casos). Así, la figura 6 muestra ya el árbol de fallos en su situación final.

Figura 6. Árbol de fallos (final).



Desde luego, el árbol podría profundizarse más, analizando las causas de los eventos que hemos denominado elementales. En cualquier caso, el grado de profundidad en el desarrollo de los eventos dependerá de los objetivos del estudio. En general, un nivel como el mostrado en el ejemplo acostumbra a ser suficiente en la mayor parte de aplicaciones.

Una vez dibujado el árbol de fallos es conveniente completar una tabla tal como de la tabla 1, en la que se detalla el código de cada evento elemental, su denominación simplificada a efectos del dibujo del árbol, y una descripción más detallada, incluyendo el modo de fallo. Esto último es especialmente importante dado que la mayor parte de los componentes estudiados tienen más de un modo de fallo.

Debe destacarse que la elaboración del árbol de fallos se simplifica en caso de disponer de un análisis de seguridad de procesos (por ejemplo, un HAZOP) correctamente realizado. En efecto, normalmente el árbol adopta, en este caso, una estructura muy general:

Tabla 1. Sucesos elementales

Código	Nombre	Descripción
E1	Fallo del caudalímetro FIC	El caudalímetro FIC indica un caudal significativamente inferior al que realmente circula.
E2	Fallo del ordenador de control	El ordenador de control interpreta incorrectamente los datos de los sensores de campo, dando instrucciones erróneas a los elementos finales de control (válvulas).
E3	Fallo de la válvula V1 (abre excesivamente)	La válvula V1 se abre excesivamente a pesar de recibir una señal de control correcta desde el ordenador de control.
E4	Fallo de la sonda de temperatura TIC	La sonda de temperatura TIC indica una temperatura significativamente inferior a la que realmente tiene el reactor.
E5	Fallo de la válvula V2 (cierra excesivamente)	La válvula V2 se cierra excesivamente a pesar de recibir una señal de control correcta desde el ordenador de control.
E6	Fallo de disco de ruptura (no abre)	El disco de ruptura del reactor no se abre a pesar de haberse alcanzado su presión de diseño.

el suceso de cabecera está conectado, mediante una puerta "Y" a dos sucesos genéricos, "causas" y "fallo de salvaguardas". El suceso "causas" incluye las identificadas en el HAZOP (que posiblemente deban desarrollarse con mayor profundidad). A su vez, el suceso "fallo de salvaguardas" incluirá todas las identificadas en el HAZOP. La figura 7 muestra esta relación entre HAZOP y árbol de fallos para el caso del ejemplo.

ANÁLISIS CUALITATIVO DEL ÁRBOL DE FALLOS

El árbol de fallos constituye una representación de las posibles maneras en que puede alcanzarse el suceso de cabecera (en este caso, el estallido del reactor), a partir de los fallos de equipos y componentes. Esta representación puede también obtenerse en forma de ecuación equivalente. Para ello, basta con sustituir las puertas "Y" por el símbolo[1] "⊗ y las puertas "O" por el símbolo ⊕. Utilizando las tablas de aplicación de cada tipo de puertas (ver anexo) pueden deducirse fácilmente las siguientes reglas de operación:

$$A \oplus B = B \oplus A$$

$$A \oplus A = A$$

$$A \otimes B = B \otimes A$$

$$A \otimes A = A$$

$$A \otimes (B \oplus C) = A \otimes B \oplus A \otimes C$$

$$A \oplus (B \oplus C) = A \oplus B \oplus C$$

$$A \otimes (B \otimes C) = A \otimes B \otimes C$$

$$1 \oplus A = 1$$

$$1 \otimes A = A$$

$$0 \oplus A = A$$

$$0 \otimes A = 0$$

Figura 7. Relacion entre HAZOP y arbol de fallos

Session: (1) 03/10/2013 — Revision:
Node: (1) Reactor
Drawings:
Parameter: Presión — Intention:

PC	DESVIACIÓN	CAUSAS	CONSECUENCIAS	F	S	R	SALVAGUARDAS	RECOMENDACIONES	POR	F	S	R	DS
Más	Más Presión	1. Fallo del lazo de control de caudal del reactivo B por: : - Fallo del caudalímetro FIC : - Fallo del ordenador de control. : - Fallo de la válvula V1 (abre excesivamente)	1.1. Estallido del reactor. Riesgod e exposición personal y de daños materiales.	4	4	M	1.1.1. Disco de ruptura.	1.1.1. -		2	4	B	
		2. Fallo del lazo de control de temperatura del reactor por: : - Fallo de la sonda de temperatura TIC : - Fallo del ordenador de control. : - Fallo de la válvula V2 (cierra excesivamente)	2.1. Estallido del reactor. Riesgod e exposición personal y de daños materiales.	4	4	M	2.1.1. Disco de ruptura.	2.1.1. -		2	4	B	
Menos	Menos Presión	3. Sin causas previsibles.											

[1] En una buena parte de la literatura sobre este tema se utilizan los símbolos "x" y "+" para representar, respectivamente, las puertas "Y" e "O". En el presente artículo se ha preferido no utilizar esta nomenclatura, pues puede inducir a la confusión con las multiplicaciones y sumas habituales.

En el caso del ejemplo, la ecuación del árbol puede desarrollarse paso a paso como sigue:

$$C = C1 \otimes C2$$

$$C = (C12 \otimes C22) \otimes C2$$

$$C = [(E1 \oplus E2 \oplus E3) \otimes (E4 \oplus E2 \oplus E5)] \otimes E6$$

Interesa, por motivos que serán evidentes inmediatamente, reagrupar la ecuación anterior de la forma siguiente:

$$C = E1 \otimes E4 \otimes E6 \oplus E1 \otimes E5 \otimes E6 \oplus E2 \otimes E6 \oplus \oplus E3 \otimes E4 \otimes E6 \oplus E3 \otimes E5 \otimes E6$$

Como puede verse, se obtiene una "O" de varios términos, cada uno de los cuales es el "Y" de varios sucesos elementales. Aunque puede parecer sumamente farragosa (de hecho, lo es), esta forma de representación es mucho más informativa que el propio árbol de fallos, aunque éste resulta más fácil de construir a partir de la realidad física.

Cada uno de los términos de la ecuación anterior recibe el nombre de "corte mínimo del árbol de fallos" (o *minimal cut set*, en la denominación inglesa frecuentemente empleada). Cada corte mínimo representa una forma distinta en que puede llegar a producirse el suceso de cabecera. Así, por ejemplo, el primer corte mínimo de árbol de la ecuación anterior significa que puede producirse el estallido del reactor si fallan simultáneamente el caudalímetro FIC (E1), la sonda de temperatura TIC (E4) y el disco de ruptura (E6). Igualmente, el quinto corte nos indica que puede estallar el reactor si fallan simultáneamente el ordenador de control (E2) y el disco de ruptura (E6). Cualquier árbol de fallos puede reducirse a un conjunto de cortes mínimos. Es decir, somos capaces de identificar cada una de las combinaciones de eventos elementales que, caso de producirse simultáneamente, darían lugar al evento de cabecera.

El conjunto de cortes mínimos ya permite alguna inferencia cualitativa acerca de la fiabilidad del sistema. Así, el número de cortes mínimos aumenta (combinatoriamente) con la complejidad del árbol (y, por tanto, del sistema). A su vez, el número de sucesos elementales en cada corte (el llamado "orden" del corte) es indicativo de su mayor o menor probabilidad: un corte de orden elevado requiere que fallen simultáneamente diversos componentes, por lo que—en principio—debería ser menos probable que un corte de orden inferior. Análogamente, el corte con menor orden define cualitativamente la fiabilidad del sistema.

En el caso del ejemplo se han obtenido cinco cortes, y un orden mínimo de dos. Esto es, existe una combinación de tan solo dos componentes que, caso de fallar simultáneamente, provocan el estallido del reactor.

La aparición de los diversos sucesos elementales en los cortes permite también hacer alguna deducción acerca de su importancia relativa. En efecto, un suceso es más importante (su contribución al suceso de cabecera es mayor) cuanto:

- Mayor número de cortes contengan el suceso en cuestión.
- Menor sea el orden de los cortes donde aparezca el suceso.
- En el caso estudiado, por ejemplo, puede afirmarse que:
  - El fallo del disco de ruptura aparece en todos los cortes. Se trata, por tanto, de un fallo crítico: si no se produce, no se puede dar jamás el estallido del reactor.
  - El fallo del ordenador de control aparece en el único corte de segundo orden. Por tanto, el fallo de este ordenador requiere tan solo la contribución simultánea del fallo del disco de ruptura para originar el estallido. Así pues, será un fallo con mayor importancia que los restantes.
- Los fallos de los instrumentos (sensores y válvulas) aparecen tan solo en cortes de tercer orden. En principio, se trata por tanto de fallos menos importantes que los anteriores.

Nótese que el análisis anterior es puramente cualitativo. Sus resultados podrían ser alterados en función de los valores cuantitativos de las diferentes probabilidades. Además, estas reglas no permiten establecer prioridades entre fallos que aparecen en el mismo número de cortes del mismo orden (como es el caso de los fallos de caudalímetro y sonda de temperatura, por ejemplo). En el apartado siguiente se establecerán métodos cuantitativos más precisos.

CUANTIFICACIÓN DE ÁRBOLES DE FALLOS

En general, resulta deseable cuantificar la probabilidad del evento de cabecera a partir de las probabilidades de los eventos elementales. Para ello debe, en primer lugar, determinarse las probabilidades de cada uno de los eventos elementales. Pueden utilizarse para ello algunas de las bases de datos sobre fallos de componentes habituales. Evidentemente, debe ejercitarse un cuidado importante a la hora de seleccionar la base de datos que resulte representativa del sistema que se estudia, de sus modos de fallo, etc. Estas consideraciones exceden el alcance del presente artículo.

Dado que los eventos elementales son independientes entre sí, se puede aplicar la siguiente ecuación del cálculo de probabilidades para calcular la probabilidad de un corte mínimo de árbol:

$$P_{(A1 \otimes A2 \otimes \ldots \otimes An)} = P_{A1} \times P_{A2} \times \ldots \times P_{An}$$

Es decir, la probabilidad del corte mínimo de árbol es, simplemente, el producto de las probabilidades de cada uno de sus eventos elementales.

El cálculo de la probabilidad del evento de cabecera es algo más complejo. En el caso más sencillo posible (solo dos cortes de árbol), puede aplicarse la siguiente expresión:

$$P_{(C1 \oplus C2)} = P_{C1} + P_{C2} - P_{C1} \times P_{C2}$$

Es decir, la probabilidad de que se produzca el corte C1 o el C2 es la suma de las probabilidades de ambos menos la probabilidad de que se produzcan ambos simultáneamente.

En un caso con tres cortes de árbol la expresión adecuada sería:

$$P_{(C1 \oplus C2 \oplus C3)} = P_{C1} + P_{C2} + P_{C3} - P_{C1} \times P_{C2} - P_{C1} \times P_{C3} - P_{C2} \times P_{C3} + 2 \times P_{C1} \times P_{C2} \times P_{C3}$$

Y las expresiones se van complicando a medida que aumenta el orden del corte de árbol. En la práctica, los programas disponibles para la cuantificación de árboles de fallos utilizan diversos procedimientos numéricos para aproximar la solución hasta el nivel de precisión requerido.

En el caso del ejemplo, se han utilizado las siguientes probabilidades de los sucesos elementales (se indican también en la zona superior derecha de cada suceso en la figura 6):

Tabla 2. Probabilidades de los sucesos elementales

Código	Nombre	Probabilidad
E1	Fallo del caudalímetro FIC	0,03
E2	Fallo del ordenador de control	0,0001
E3	Fallo de la válvula V1 (abre excesivamente)	0,025
E4	Fallo de la sonda de temperatura TIC	0,02
E5	Fallo de la válvula V2 (cierra excesivamente)	0,015
E6	Fallo de disco de ruptura (no abre)	0,01

La tabla 3 muestra las probabilidades de cada uno de los cortes mínimos de árbol (se invita al lector a comprobarlas).

Tabla 3. Probabilidades de cada uno de los cortes mínimos de árbol

Corte	Probabilidad
E1 ⊗ E4 ⊗ E6	$6{,}00 \times 10^{-6}$
E1 ⊗ E5 ⊗ E6	$4{,}50 \times 10^{-6}$
E2 ⊗ E6	$1{,}00 \times 10^{-6}$
E3 ⊗ E4 ⊗ E6	$5{,}00 \times 10^{-6}$
E3 ⊗ E5 ⊗ E6	$3{,}75 \times 10^{-6}$

Finalmente, la probabilidad del evento de cabecera es $1{,}98 \times 10^{-5}$. Nótese que esta probabilidad es distinta de las dos siguientes que, erróneamente, se utilizan en algunas ocasiones:

- La simple suma de las probabilidades de los cortes mínimos de árbol, que en este ejemplo arrojaría un resultado de 2,03 X 10^{-5}.

- La utilización de lo que podríamos denominar "álgebra de probabilidades rudimentaria", consistente en sustituir "Y" por "multiplicación", "O" por "adición" y operar sin ninguna otra precaución. En este caso, los valores obtenidos para los eventos intermedios y cabecera serían:

Tabla 4. Probabilidades calculadas erróneamente de los sucesos intermedios y de cabecera

Código	Procedimiento de cálculo	Probabilidad
C11	E1 + E2 + E3	0,0551
C12	E4 + E2 + E5	0,0351
C1	C11 X C12	0,00193
C2	E6	0,01
C	C1 X C2	1,93 X 10^{-5}

Es conveniente destacar que la probabilidad del evento de cabecera, correctamente calculado es siempre:

- Menor o igual que la suma de probabilidades de los cortes mínimos de árbol. La igualdad se da únicamente cuando los cortes de árbol no tienen sucesos elementales comunes entre ellos.

- Mayor o igual que lo que hemos llamado álgebra rudimentaria. La igualdad se da únicamente cuando cada suceso elemental aparece una sola vez en el árbol.

La conclusión es, obviamente, que los cálculos deben efectuarse de forma correcta, por personal debidamente formado y competente, requiriéndose, en general, la utilización de herramientas informáticas. Estas herramientas de cálculo utilizan métodos numéricos tales como Monte-Carlo y otros, cuya descripción excede ampliamente el propósito del presente artículo.

EL ANÁLISIS DE IMPORTANCIA COMO HERRAMIENTA DE GESTIÓN

El análisis de importancia permite determinar cuáles de entre los sucesos elementales son más importantes (en varios sentidos) para originar el suceso de cabecera.

A continuación se muestra un análisis empleando tres medidas estadísticas comunes.

Importancia de Fussell-Vesely

Se define la importancia de Fussell-Vesely (IFV) de un suceso elemental como la probabilidad de que éste haya contribuido al suceso de cabecera, caso de haberse producido éste. Formalmente, puede calcularse como:

$$IFV_i = \frac{\sum P_{Ci}}{P_C}$$

Donde IFV_i es la importancia del suceso elemental E_i, P_C es la probabilidad del suceso de cabecera y P_{Ci} es la probabilidad de un corte de árbol donde interviene el suceso elemental E_i. El sumatorio se extiende a todos los cortes de árbol.

Como se deduce de su definición y fórmula, la importancia de un suceso es un número comprendido entre 0 y 1 (dado que es una probabilidad). Cuanto mayor es la importancia, más probable es que el suceso de cabecera se produzca a consecuencia del suceso elemental en cuestión (solo o acompañado por otros). En el extremo, si la IFV de un suceso es 1, esto significa que el suceso de cabecera no puede producirse si no se produce el suceso elemental. De la misma forma, si la IFV de un suceso es 0, esto significa que este suceso es irrelevante respecto a la ocurrencia del suceso de cabecera.

Las IFV de los diferentes sucesos elementales en el caso del ejemplo son:

Tabla 5. Importancia (IFV) de los sucesos elementales

Código	Nombre	Probabilidad	IFV
E1	Fallo del caudalímetro FIC	0,03	0,52
E2	Fallo del ordenador de control	0,0001	0,05
E3	Fallo de la válvula V1 (abre excesivamente)	0,025	0,44
E4	Fallo de la sonda de temperatura TIC	0,02	0,55
E5	Fallo de la válvula V2 (cierra excesivamente)	0,015	0,41
E6	Fallo de disco de ruptura (no abre)	0,01	1,00

De estos resultados puede deducirse que:

- Para alcanzar el suceso de cabecera es imprescindible que se produzca el fallo del disco de ruptura (E6), dado que la IFV para este suceso es de 1. Este efecto era ya conocido, teniendo en

cuenta que E6 aparece en todos los cortes de árbol.

- Por contra, el fallo del ordenador de control (E2) tiene una importancia pequeña (5%, aproximadamente), por lo que es poco probable que contribuya al suceso de cabecera. Este efecto era también conocido, teniendo en cuenta que el corte de árbol en el que aparece E2 es el que tiene menor probabilidad.

Evidentemente, casos más complejos, con mayor número de eventos elementales y relaciones más complejas entre ellos permitirían obtener conclusiones adicionales.

Risk Achievement Worth (RAW)

El RAW de un suceso elemental es una medida de cuál sería la probabilidad del suceso de cabecera si el suceso elemental en cuestión ya se hubiera producido; dicho en otras palabras, si su probabilidad fuese 1 en lugar del valor que corresponda. Formalmente, puede calcularse como:

$$RAW_i = 1 + IFV_i \left(\frac{1}{P_{Ei}} - 1\right)$$

Donde P_{Ei} es la probabilidad del suceso elemental E_i.

El RAW de un suceso es un valor siempre mayor o igual que uno, que constituye una medida del perjuicio que podría causarse a la fiabilidad de un sistema si se deteriora el componente afectado por el suceso. Es útil, por tanto, para gestionar estrategias de mantenimiento. En el extremo, si el RAW de un suceso es uno, esto significa que no se producirá alteración alguna de la probabilidad del suceso de cabecera, aunque el suceso elemental en cuestión se dé por producido. En el otro extremo, si el RAW de un suceso es muy grande, esto significa que si se produce este suceso, es casi inevitable el suceso de cabecera.

Los RAW de los diferentes sucesos en el caso del ejemplo son:

Tabla 6. Importancia (IFV y RAW) de los sucesos elementales

Código	Nombre	Probabilidad	IFV	RAW
E1	Fallo del caudalímetro FIC	0,03	0,52	18
E2	Fallo del ordenador de control	0,0001	0,05	505
E3	Fallo de la válvula V1 (abre excesivamente)	0,025	0,44	18
E4	Fallo de la sonda de temperatura TIC	0,02	0,55	28
E5	Fallo de la válvula V2 (cierra excesivamente)	0,015	0,41	28
E6	Fallo de disco de ruptura (no abre)	0,01	1,00	100

De estos resultados puede deducirse que:

- Caso de fallar el ordenador de control (E2), la probabilidad de estallido del reactor aumentaría notablemente.
- El fallo del disco de ruptura (E6) causaría un aumento inferior de la probabilidad de estallido.
- El resto de los sucesos, caso de darse, provocarían aumentos menos significativos de la probabilidad de estallido.

A la vista de estos resultados, para evitar el aumento de la probabilidad de estallido, cabría concentrar los recursos de mantenimiento en prevenir el fallo del ordenador de control y, en segunda instancia, del disco de ruptura. Nótese que se trata de los dos elementos con la probabilidad de fallo más baja del sistema estudiado. Por contra, otros componentes con probabilidades de fallo más elevadas (como, por ejemplo, las válvulas) tienen una RAW significativamente más baja, por lo que, caso de encontrarse falladas, la probabilidad del suceso de cabecera no aumenta significativamente. Como puede comprobarse, incluso con un ejemplo tan simple como el analizado, el RAW permite obtener conclusiones no tan simples a priori.

Risk Reduction Worth (RRW)

El RRW de un suceso elemental es una medida de cuál sería la probabilidad del suceso de cabecera si el suceso elemental en cuestión no se produjera nunca; dicho en otras palabras, si su probabilidad fuese 0 en lugar del valor que corresponda. Se calcula mediante:

$$RRW_i = \frac{1}{1 - IFV_i}$$

El RRW de un suceso es un valor mayor o igual que uno, que constituye una medida del beneficio que podría causarse a la fiabilidad de un sistema si se mejora el componente afectado por el suceso. Es útil, por tanto, para decidir estrategias de diseño o de sustitución por equipos o componentes más fiables. En el extremo, si el RRW de un suceso es uno, esto significa que no se producirá alteración alguna de la probabilidad del suceso de cabecera, aunque el suceso elemental en cuestión se dé por producido. En el otro extremo, si el RRW de un suceso es muy grande, esto significa que, si se impide este suceso, es casi imposible que se produzca el suceso de cabecera.

Los RRW de los diferentes sucesos en el caso del ejemplo son los mostrados en la tabla 7.

De estos resultados puede deducirse que:

- Si se evita el fallo del disco de ruptura (E6), se impide completamente el estallido del reactor. Obviamente, este es un resultado que ya se había deducido anteriormente, sin más que observar que el evento citado aparece en todos los cortes de árbol. Por lo tanto, si se desea modificar el diseño para aumentar la seguridad, la medida más eficaz sería redundar el disco de ruptura.
- El fallo del ordenador de control (E2) tiene un valor de RRW sensiblemente igual a la unidad, lo que significa que mejorando su fiabilidad prácticamente no se reduciría la probabilidad de estallido del reactor. Por lo tanto, no tiene ningún sentido invertir en un ordenador más fiable para mejorar la seguridad del sistema.
- Los fallos de caudalímetro y sonda de temperatura tienen valores similares, del orden de 2, por lo que su mejora de fiabilidad aportaría una discreta reducción a la probabilidad del evento de cabecera.

De nuevo, incluso en un caso tan simple como el del ejemplo, se obtienen resultados no evidentes a priori y que, por cierto, están en contra de la tendencia reciente a implantar sistemas de seguridad instrumentada, a menudo a costes muy elevados.

RESUMEN Y CONCLUSIONES

El análisis mediante árboles de fallos constituye una herramienta potente para la identificación de los sucesos elementales que contribuyen a un suceso no deseado (cabecera), y de las interrelaciones entre ellos. Incluso sin cuantificar numéricamente, permite identificar equipos críticos para evitar el suceso de cabecera. Así pues, un árbol de fallos contiene información altamente valiosa sobre las secuencias de eventos que conducen a un suceso no deseado.

En caso de disponer de frecuencias de ocurrencia de los sucesos elementales, no solamente se puede cuantificar el árbol, y determinar la probabilidad del evento de cabecera, sino también calcular diversas medidas de la importancia de cada suceso elemental. Las medidas de importancia pueden ser de gran ayuda a la hora de determinar mejoras en el diseño, u optimización del mantenimiento.

Tabla 7. Importancia (IFV, RAW y RRW) de los sucesos elementales

Código	Nombre	Probabilidad	IFV	RAW	RRW
E1	Fallo del caudalímetro FIC	0,03	0,52	18	2,126
E2	Fallo del ordenador de control	0,0001	0,05	505	1,053
E3	Fallo de la válvula V1 (abre excesivamente)	0,025	0,44	18	1,790
E4	Fallo de la sonda de temperatura TIC	0,02	0,55	28	2,247
E5	Fallo de la válvula V2 (cierra excesivamente)	0,015	0,41	28	1,713
E6	Fallo de disco de ruptura (no abre)	0,01	1,00	100	∞

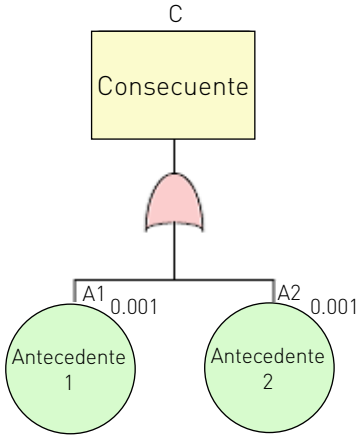
ANEXOS

PUERTAS LÓGICAS

En la construcción de árboles de fallos los distintos eventos se conectan mediante puertas lógicas, que definen las relaciones entre ellos. Se utilizan fundamentalmente dos tipos de puertas lógicas: "O" e "Y".

El suceso que está unido a dos antecedentes mediante una puerta lógica "O" se producirá si suceden uno cualquiera de los antecedentes, tal como muestra la siguiente tabla:

Antecedente 1	Antecedente 2	Consecuente
Sí	Sí	Sí
Sí	No	Sí
No	Sí	Sí
No	No	No



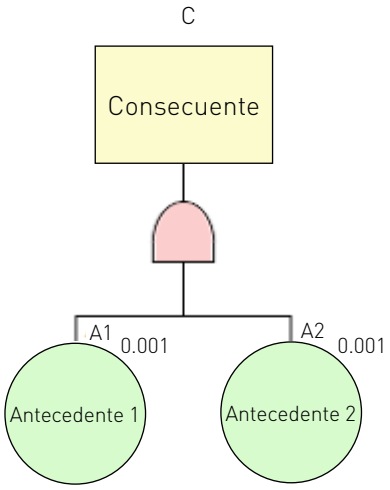
En el caso de una puerta lógica "Y", el suceso consecuente se producirá si y solo si se producen todos los antecedentes relacionados con él a través de la puerta, tal como indica la tabla siguiente:

Antecedente 1	Antecedente 2	Consecuente
Sí	Sí	Sí
Sí	No	No
No	Sí	No
No	No	No

FALLOS Y MODOS DE FALLO

Se considera que un sistema, equipo o componente está en "fallo" si no es capaz de llevar a cabo la misión para la que ha sido diseñado. A menudo los sistemas, equipos o componentes pueden fallar de más de un modo. Así, por ejemplo, el disco de ruptura del ejemplo tiene, como mínimo, los siguientes modos de fallo:

- El disco no se abre a pesar de alcanzarse la presión interior para la que ha sido diseñado.
- El disco se abre a pesar de que la presión interior del reactor es inferior a la de diseño del disco.



Obviamente, es importante precisar el modo de fallo a que se hace referencia en cada caso, dado que su probabilidad será distinta.

Tipos de fallos

Durante la realización de árboles de fallos se puede distinguir entre dos tipos principales de fallos:

Fallo en servicio, o en misión. El equipo o componente del que se estudia el fallo se encuentra permanentemente en operación, de tal forma que su fallo es inmediatamente percibido. Una vez se detecta el fallo, el equipo o componente se repara o sustituye también inmediatamente. La probabilidad de fallo de un componente con frecuencia de fallo λ durante un tiempo de misión o servicio T es:

$$P_f = 1 - \exp(-\lambda T)$$

Cuando el producto λT es significativamente menor que 1 (lo cual es bastante habitual, ya que las frecuencias de fallo acostumbran a ser bajas), la probabilidad de fallo en servicio puede aproximarse mediante:

$$P_f \approx \lambda T$$

Fallo en demanda. Es característico de un equipo o componente del que no se conoce cuál es su estado (operativo o no), durante la operación normal de la planta. Este estado únicamente se conoce cuando se "demanda" su operación o bien durante una prueba. Un resultado negativo de la prueba (componente en estado no operativo) comporta su sustitución o reparación inmediata.

La probabilidad de fallo en demanda de un componente con frecuencia de fallo λ con un intervalo entre pruebas T es:

$$P_f = \frac{\lambda T - 1 + \exp(-\lambda T)}{\lambda T}$$

Obviamente, ambos tipos de fallos constituyen una simplificación de la realidad, que obvian cuestiones tales como la posibilidad de un estado de funcionamiento parcial, o bien el tiempo de reparación. Estos factores pueden tenerse en cuenta mediante otro tipo de técnicas, tales como los diagramas de Markov.

DEKRA Insight

ARTURO TRUJILLO

Arturo Trujillo tiene más de treinta años de experiencia en el análisis y prevención de riesgos en las industrias de proceso, principalmente en los sectores oil & gas, químico y petroquímico. Su experiencia abarca los análisis de riesgos de proceso (PHA, tales como HAZID, HAZOP, What-if...), los análisis de consecuencias, análisis cuantitativos de riesgos, estudios de asignación SIL/LOPA y planes de autoprotección y emergencia, tanto interiores como exteriores.

Consultoría

ATEX (Atmósferas Explosivas)

- Directiva 1999/92/CE: Elaboración y mantenimiento del Documento de Protección contra Explosiones / Clasificación de áreas ATEX / Procedimientos, instrucciones y permisos de trabajo / Inspección de instalaciones
- Directiva 2014/34/UE: certificación ATEX de equipos
- Formación y certificación de personas (IsmATEX)
- Certificación de talleres de reparación de equipos ATEX (SaqrATEX)
- Prevención de riesgos electrostáticos : auditorías, mediciones en campo, soluciones a medida
- Propuesta y diseño de medidas de mitigación

Identificación y evaluación de riesgos de proceso

- Análisis de riesgos: HAZOP, What-if, HAZID, FMEA, etc
- Análisis cuantitativo de riesgos (ACR)
- Cálculo y simulación de consecuencias
- Asignación SIL, LOPA
- Fichas de datos de seguridad, etiquetas
- Transporte de mercancías peligrosas

Gestión de riesgos de proceso

- Programas de mejora de la gestión de seguridad de procesos (PSM)
- Auditorías de sistemas de gestión y de la cultura de seguridad de procesos
- Verificación SIL
- Estudios de fiabilidad, disponibilidad y mantenimiento (RAM)
- Programas de inspección basada en el riesgo (Risk based inspection, RBI)
- Optimización de sistemas de inertización
- Investigación de incidentes
- Gestión de emergencias
- Planes de emergencia
- Seguridad de maquinaria
- Transporte de mercancías peligrosas

Seveso

- Notificación de accidentes graves
- Sistema de gestión de la seguridad
- Política de prevención de accidentes graves
- Información básica para la administración
- Plan de autoprotección (o plan de emergencia interior)
- Informe de transporte
- Análisis cuantitativo de riesgo

Seguridad de reacciones químicas

- Identificación y evaluación de riesgos en reacciones químicas
- Desarrollo y optimización de procesos químicos
- Dimensionamiento de venteos de emergencia

Ensayos de laboratorio

Laboratorios acreditados BPL (Buenas Prácticas de Laboratorio)

Ensayos de inflamabilidad

- Propiedades ATEX
- Explosividad de polvos
- Explosividad de líquidos, gases y vapores

Estabilidad térmica

- Caracterización de reacciones químicas exotérmicas
- Autocalentamiento y estabilidad de polvos
- Calorimetrías DSC, RC1, ARC, DEWAR

Ensayos reglamentarios (FDS/REACH/CLP/GHS)

- Ensayos para fichas de datos de seguridad (FDS)
- Ensayos de clasificación UN para el transporte de mercancías peligrosas
- Ensayos fisicoquímicos
- Ensayos toxicológicos
- Ensayos ecotoxicológicos

Propiedades electrostáticas

- Cargabilidad, tiempo de relajación y resistividad de polvos
- Conductividad de líquidos, películas y envases
- Resistividad de suelos, calzado y guantes
- Mediciones in situ (conductividad y resistividad)

To contact us:

> France : info-fr@chilworthglobal.com
> Netherlands : info-nl@chilworthglobal.com
> India : info-in@chilworthglobal.com
> Italy : info-it@chilworthglobal.com
> Germany : exam-info@dekra.com
> Spain : info-es@chilworthglobal.com
> UK : info-uk@chilworthglobal.com
> USA : safety-usa@chilworthglobal.com
> China : info-cn@chilworthglobal.com
> Wallonia : info-be@chilworthglobal.com