



Documentación

NTP 417: Análisis cuantitativo de riesgos: fiabilidad de componentes e implicaciones en el mantenimiento preventivo

Analyse quantitative des risques: Fiabilité de composants et implication dans le maintenance préventive

Quantitative risk analysis: Reliability of components and implication in maintenance preventive

Redactores:

Antonio Cejalvo Lapeña
Ingeniero Industrial

Josep Enric Domingo Biosca
Ldo. en Ciencias Químicas

CENTRO NACIONAL DE CONDICIONES DE TRABAJO

Introducción

La notable evolución y complejidad de determinadas instalaciones en la industria de proceso, exige cada vez más la utilización de técnicas de evaluación de riesgos más potentes, que permitan realizar un análisis riguroso de las instalaciones, aportando algo más que la simple identificación de deficiencias o la detección de desviaciones sobre estándares reglamentarios establecidos.

Para la realización de un análisis cuantitativo de riesgos es necesario obtener la frecuencia-probabilidad de que se produzca un determinado accidente, que conjuntamente con el nivel de daño producido definirá el riesgo de la instalación.

La determinación rigurosa de la frecuencia-probabilidad de un accidente o suceso no deseado en una instalación, se realiza mediante la construcción de un árbol de fallos y errores, que permita obtener dicha frecuencia de ocurrencia a partir de las probabilidades de fallo o indisponibilidades de los equipos que integran el sistema.

La modelización del sistema mediante el árbol de fallos o errores y el análisis cualitativo y cuantitativo del mismo están tratados en la **NTP-333 "Análisis probabilístico de riesgos: Metodología del Árbol del fallos y errores"**, a la que se remite al lector antes de abordar el presente documento.

Esta Nota Técnica de Prevención recoge los modos de fallo de los componentes y las expresiones matemáticas necesarias para el cálculo de sus probabilidades en función de sus tasas de fallo y especificaciones técnicas de operación (tiempo de operación, intervalo de mantenimiento, etc).

Una de las aplicaciones más importante de este tipo de análisis de riesgos consiste en la

determinación de los equipos y funciones más críticas para la seguridad del sistema analizado y la planificación de actuaciones preventivas sobre las mismas, tanto en el diseño de la instalación como en las estrategias de mantenimiento preventivo, con el objeto final de aumentar el nivel de seguridad.

Datos necesarios

Para obtener las indisponibilidades de los sucesos básicos que componen un determinado árbol de fallos es necesario conocer y disponer ciertos parámetros de funcionamiento e intrínsecos de los componentes o equipos (válvulas, bombas, etc) que forman el sistema a analizar.

- Estos parámetros están almacenados unos en bases de datos de fiabilidad de componentes y otros en las especificaciones de operación y registros de averías de la planta.
- Los parámetros que a continuación se definen serán utilizados para el cálculo de las indisponibilidades de los sucesos básicos mediante las expresiones matemáticas que procedan para cada modo de fallo.
- Tasa de fallos (λ): Esta determinada por el número de fallos que ocurren en un equipo dividido por el tiempo transcurrido.
- Tasa de fallos en operación (λ_o): Esta determinada por el número de fallos que tiene un equipo cuando está en operación dividido por el tiempo de operación en el que ocurren los fallos.
- Tasa de fallos en espera (λ_s): Esta determinada por el número de fallos que tiene un equipo cuando está en espera dividido por el tiempo de espera en el que ocurren los fallos.
- Indisponibilidad (q): Es el parámetro que en términos probabilísticos define la no disponibilidad de un equipo en un cierto instante de tiempo.
- Indisponibilidad por demanda (q_d): Es el número de fallos que tiene un equipo en la demanda de actuación dividido por el número de demandas efectuadas.
- Tiempo de operación (T_o): Es el tiempo en que un equipo está en funcionamiento o en operación.
- Tiempo entre pruebas (T_{ep}): Es el intervalo de tiempo entre revisiones periódicas de un equipo.
- Tiempo de prueba (T_p): Es el tiempo medio que dura la prueba o revisión de un equipo.
- Tiempo de reparación (T_r): Es el tiempo medio de reparación de un equipo que se ha detectado fallado.

Modos de fallo y modelos de indisponibilidad

Los equipos pueden manifestar sus fallos en tres intervalos de tiempo: mientras están en espera, cuando se demanda su actuación o cuando están en operación o funcionamiento.

La función indisponibilidad, definida por la ecuación (1) se particulariza para cada modo de fallo, adquiriendo expresiones matemáticas diferentes:

$$q(t) = 1 - e^{-\int_0^t \lambda(t) dt} \quad (1)$$

Fallo en espera

Se produce en componentes que están en espera para entrar en operación y estando en este estado fallan. Ejemplos de este tipo de componentes son las válvulas de seguridad, las bombas de refrigeración, redundantes o no, pero que no estén refrigerando en ese periodo, los grupos electrógenos, las alarmas, etc.

Los mecanismos por los que estos componentes fallan son dependientes del tiempo, por corrosión o suciedad, envejecimiento, etc y la tasa de fallos se ajusta a una distribución exponencial

$$\lambda(t) = \lambda_s$$

por lo que la indisponibilidad puntual adquiere la expresión:

$$q(t) = 1 - e^{-\lambda_s t} \quad (2)$$

Estos componentes pueden ser probados periódicamente o no, siendo la indisponibilidad media distinta en cada caso.

- Componentes en espera sometidos a pruebas periódicas: la indisponibilidad media en el intervalo entre pruebas T_{ep} es:

$$q = 1 + \frac{1}{\lambda_s T_{ep}} \left[e^{-\lambda_s T_{ep}} - 1 \right] \quad (3)$$

- Componentes en espera no sometidos a pruebas periódicas: la indisponibilidad media en el tiempo que le queda al componente es:

$$q = 1 + \frac{e^{-\lambda_s T_{vp}} - e^{-\lambda_s T_v}}{\lambda_s (T_{vp} - T_v)} \quad (4)$$

donde T_{vp} y T_v son el tiempo de vida previsto del componente y el tiempo que lleva en funcionamiento, respectivamente.

Indisponibilidad por pruebas

Asociada a componentes en espera que son probados o revisados periódicamente con un intervalo T_{ep} y en los que las revisiones les hace estar indisponibles durante el tiempo de pruebas T_p .

$$q = \frac{T_p}{T_{ep}}$$

Indisponibilidad por mantenimiento preventivo

Asociada a componentes a los que se realiza mantenimiento preventivo con un ciclo de duración T_m , dejándolos indisponibles durante el tiempo de reparación T_r .

$$q = \frac{T_r}{T_m}$$

Fallo en demanda

Se da en componentes que fallan cuando se les demanda un cambio de estado, por ejemplo cuando el componente está funcionando y se le demanda que pare o cuando el componente está en espera y se le demanda que entre en operación, fallando en el arranque. Se le asocia la distribución estadística binomial, ya que la demanda solo puede tomar dos valores, éxito o fracaso:

$$q = q_d = \frac{x}{n}$$

donde x y n son el número de fallos en demanda y el número de demandas efectuadas, respectivamente.

Fallo en operación

Se da en componentes que fallan durante el tiempo de operación T_o . La tasa de fallos se ajusta a la distribución exponencial:

$$\lambda(t) = \lambda_o$$

Por lo que la probabilidad de que un componente en operación falle antes de que finalice el tiempo de operación esta determinada por:

$$q = 1 - e^{-\lambda_o T_o}$$

Fallo humano

Son fallos producidos en componentes debido a un error humano en su operación. Este modo de fallo se encuentra tratado de forma sucinta en las Notas Técnicas de Prevención [360](#) y [377](#).

Análisis de un sistema de refrigeración

En este apartado se presenta un caso práctico de la aplicación de los datos de fiabilidad de componentes. La aplicación de esta metodología puede ser tanto para el análisis de seguridad de las instalaciones, como para mejorar su mantenimiento preventivo.

Se realiza el análisis de la disponibilidad del sistema de refrigeración de un reactor

discontinuo ("batch"), representado, esquemáticamente en la figura 1. Este sistema, además de ser un ejemplo poco complejo y relativamente fácil de analizar, corresponde a una instalación muy extendida en la industria química de proceso y en particular en las PYMES del sector químico, por ejemplo en la industria de química fina.

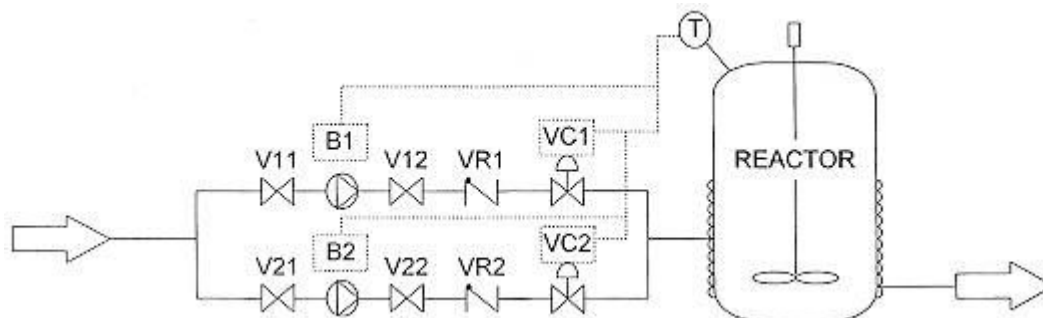


Fig. 1: Esquema del sistema de refrigeración

La instalación de refrigeración está formada, básicamente por dos tramos iguales y cada tramo consta de:

- 1 bomba centrífuga para impulsar el agua (B1/B2).
- 2 válvulas de accionamiento manual para aislar la bomba (V11/V21 y V12/V22).
- 1 válvula de retención para evitar que se produzca flujo inverso (VR1/VR2).
- 1 válvula de control, gobernada por un controlador de temperatura del reactor.

Elaboración del árbol de fallos

En el análisis de fiabilidad del sistema de refrigeración se ha empleado la metodología de árbol de fallos y errores humanos (véase **NTP-333**). El paso previo a la elaboración del árbol en sí, es la identificación del suceso no deseado cuya probabilidad se requiere obtener y los sucesos y circunstancias que deben concurrir para llegar al mismo. Esta etapa previa puede ser realizada por medio de:

- Un análisis histórico de accidentes en instalaciones similares, aportando experiencias similares.
- Un análisis sistemático, empleando metodologías como el análisis funcional de operabilidad (HAZOP) (véase **NTP-238**), el análisis modal de fallos y efectos (FMEA), etc.
- La experiencia del personal de la planta y del analista.

En la figura 2 se presenta el árbol de fallos utilizado para analizar la indisponibilidad del sistema. En el presente caso la indisponibilidad estudiada es la falta de refrigeración en el reactor (suceso no deseado o Top event).

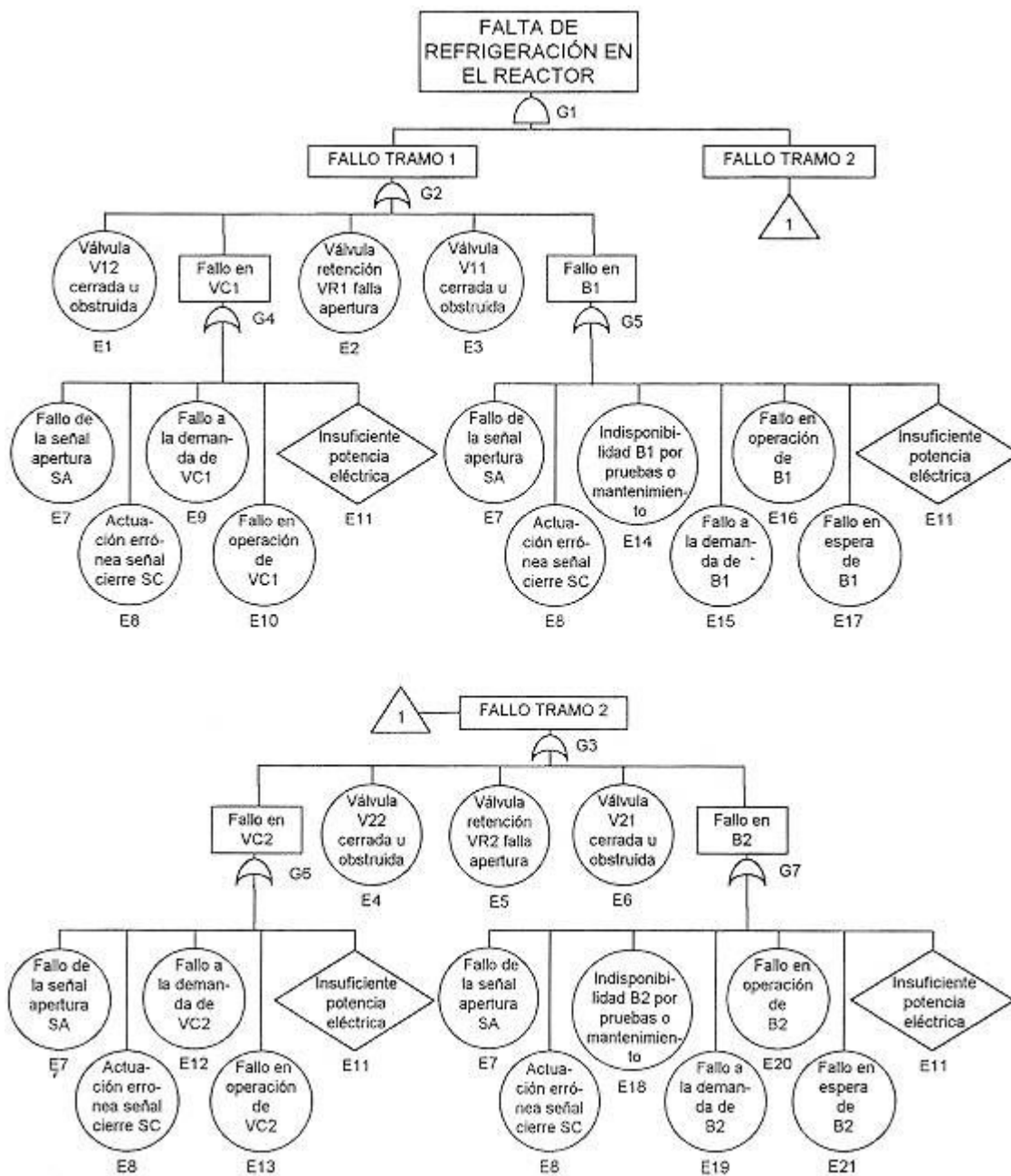


Fig. 2: Árbol de fallos y errores para evaluar la indisponibilidad por falta de refrigeración en el reactor

Los sucesos intermedios que inciden directamente al TOP son: fallo en el tramo 1 y fallo en el tramo 2. Como se ha indicado anteriormente, los dos tramos son idénticos, por lo que, sólo se comenta uno, obviamente tal duplicidad aminora significativamente la indisponibilidad total. Los sucesos considerados para analizar el posible fallo en el tramo son:

- Válvula manual V11 cerrada erróneamente u obstruida.
- Válvula de retención VR1 falla en la apertura.
- Válvula manual V12 cerrada erróneamente u obstruida.
- Fallo en la válvula de control VC1.
- Fallo en la bomba B1.

Los sucesos considerados por los que la válvula de control dejará de operar correctamente son, básicamente:

- Fallo del controlador de temperatura del reactor:
 - Fallo de la señal de apertura SA.
 - Actuación de señal de cierre SC.
- Fallo a la demanda.
- Fallo en operación.
- Fallo del suministro eléctrico.

El segundo suceso y el tercero son modos de fallo de la válvula.

Los sucesos considerados por los que la bomba dejará de operar correctamente o no estará disponible son, básicamente:

- Indisponibilidad de la bomba por pruebas o por mantenimiento.
- Fallo a la demanda.
- Fallo en operación.
- Fallo en espera.
- Fallo del suministro eléctrico.
- Fallo del controlador de temperatura del reactor:
 - Fallo de la señal de apertura SA.
 - Actuación de señal de cierre SC.

Los cuatro primeros sucesos son modos de fallo de la bomba.

El fallo del suministro eléctrico no se ha desglosado en más sucesos básicos, recibiendo el nombre de suceso no desarrollado. A este recurso se recurre cuando no se tiene más información para desglosar un suceso intermedio, su desarrollo no aporta más información o sus consecuencias son despreciables. En este caso, no es objeto del análisis y no aporta más información.

El suceso anterior y los sucesos básicos derivados de los fallos del controlador de temperatura del reactor, en la metodología de árbol de fallos, se pueden considerar como "fallos del modo común", ya que dichos fallos también son sucesos que puedan afectar a las válvula de control.

Análisis cualitativo y cuantitativo del árbol de fallos

El análisis cualitativo del árbol de fallos consiste en identificar las combinaciones mínimas de sucesos básicos que hacen que se produzca el suceso no deseado, también denominado en la terminología de árboles de fallos, conjunto mínimo de fallos (de la nomenclatura anglosajona, minimal cut set).

Para la determinación de los mismos se aplica la lógica del álgebra de Boole, suponiendo que los sucesos básicos son independientes.

Con el listado de los diferentes conjuntos mínimos de fallos, se tiene una clasificación de los caminos o combinaciones de sucesos que pueden producir el suceso no deseado. Pero si lo que se pretende es hacer una clasificación por importancia o magnitud (de más a menos importancia) deberíamos de asignar valores a cada suceso básico, realizando un análisis cuantitativo.

La indisponibilidad de un conjunto mínimo de fallos viene dado por el producto de las indisponibilidades de los sucesos básicos. A su vez, la indisponibilidad total del suceso no deseado es la suma de las indisponibilidades de los conjuntos mínimos de fallos, como límite superior.

La indisponibilidad de cada suceso básico se calcula con las expresiones matemáticas descritas en el apartado "Modos de fallo y modelos de indisponibilidad" de esta NTP y a partir de las tasas de fallos de los componentes y de una serie de tiempos de funcionamiento del sistema (T_o , T_{ep} , T_p , etc).

Las tasas de fallos pueden ser extraídas de bancos de datos de fiabilidad de reconocido prestigio internacional o de la experiencia de la planta basada en registros de fallos o averías, en concreto para el presente caso se han empleado los valores publicados por CCPs (Center for Chemical Process Safety) del AIChE (American Institute of Chemical Engineers) y los tiempos, determinados en las especificaciones de operación del sistema, se han establecido los siguientes:

- Tiempo de operación: 1,25 h (tiempo durante el cual el sistema de refrigeración debe funcionar correctamente, para cada proceso batch)
- Tiempo entre pruebas de las bombas: 2000 h.
- Tiempo en pruebas o mantenimiento de las bombas: 5 h.

Realizando el análisis cualitativo y cuantitativo del presente caso (tabla 1), siguiendo la metodología descrita en la **NTP-333**, se ha obtenido:

- 84 conjuntos mínimo de fallos:
 - 3 de orden 1.
 - 81 de orden 2.
- Indisponibilidad total del sistema: $8,2 \cdot 10^{-4}$ procesos-1 (tabla 2), esto quiere decir que de 1220 batch (o veces que se realice la operación), probablemente en una de ellas se producirá una falta de refrigeración del reactor.

Tabla 1: Indisponibilidad de los sucesos básicos

Identificación	Descripción del suceso básico	Tasa de fallo	Indisponibilidad	Factor error
E1	Válvula manual V12 erróneamente cerrada u obstruida	$2,91 \cdot 10^{-4} \text{ d}^{-1}$	$2,91 \cdot 10^{-4}$	7
E2	Válvula de retención VR1 falla a la apertura	$1,45 \cdot 10^{-4} \text{ d}^{-1}$	$1,45 \cdot 10^{-4}$	1
E3	Válvula manual V11 erróneamente cerrada u obstruida	$2,91 \cdot 10^{-4} \text{ d}^{-1}$	$2,91 \cdot 10^{-4}$	7
E4	Válvula manual V22 erróneamente cerrada u obstruida	$2,91 \cdot 10^{-4} \text{ d}^{-1}$	$2,91 \cdot 10^{-4}$	7
E5	Válvula de retención VR2 falla a la apertura	$1,45 \cdot 10^{-4} \text{ d}^{-1}$	$1,45 \cdot 10^{-4}$	1
E6	Válvula manual V21 erróneamente cerrada u obstruida	$2,91 \cdot 10^{-4} \text{ d}^{-1}$	$2,91 \cdot 10^{-4}$	7
E7	Fallo de la señal de apertura SA del controlador de temperatura	$3,4 \cdot 10^{-6} \text{ h}^{-1}$	$4,26 \cdot 10^{-6}$	12
E8	Actuación errónea de la señal de cierre SC del controlador de temperatura	$1,16 \cdot 10^{-6} \text{ h}^{-1}$	$1,45 \cdot 10^{-6}$	7
E9	Fallo de la válvula VC1 a la demanda	$5,58 \cdot 10^{-3} \text{ d}^{-1}$	$5,58 \cdot 10^{-3}$	10
E10	Fallo de la válvula VC1 en operación	$1,36 \cdot 10^{-6} \text{ h}^{-1}$	$1,70 \cdot 10^{-6}$	4
E11	Insuficiente potencia eléctrica	$6,26 \cdot 10^{-6} \text{ h}^{-1}$	$7,81 \cdot 10^{-6}$	10
E12	Fallo de la válvula VC2 a la demanda	$5,58 \cdot 10^{-3} \text{ d}^{-1}$	$5,58 \cdot 10^{-3}$	10
E13	Fallo de la válvula VC2 en operación	$1,36 \cdot 10^{-6} \text{ h}^{-1}$	$1,70 \cdot 10^{-6}$	4
E14	Indisponibilidad de la bomba 1 por pruebas o mantenimiento	---	$2,5 \cdot 10^{-3}$	10
E15	Fallo de la bomba 1 a la demanda	$9,30 \cdot 10^{-3} \text{ d}^{-1}$	$9,30 \cdot 10^{-3}$	30
E16	Fallo de la bomba 1 en operación	$1,04 \cdot 10^{-4} \text{ h}^{-1}$	$1,30 \cdot 10^{-4}$	24
E17	Fallo de la bomba 1 en espera	$9,30 \cdot 10^{-6} \text{ h}^{-1}$	$9,24 \cdot 10^{-3}$	30
E18	Indisponibilidad de la bomba 2 por pruebas o mantenimiento	---	$2,5 \cdot 10^{-3}$	10
E19	Fallo de la boma 2 a la demanda	$9,30 \cdot 10^{-3} \text{ d}^{-1}$	$9,30 \cdot 10^{-3}$	30
E20	Fallo de la boma 2 en operación	$1,04 \cdot 10^{-4} \text{ h}^{-1}$	$1,30 \cdot 10^{-4}$	24
E21	Fallo de la bomba 2 en espera	$9,30 \cdot 10^{-6} \text{ h}^{-1}$	$9,24 \cdot 10^{-3}$	30

* Factor error: parámetro estadístico que indica la dispersión de los datos

Tabla 2: Relación de conjuntos mínimos de fallos más significativos

	Conjunto mínimo de fallos	Indisponibilidad
Orden 1	E11	$7,81 \cdot 10^{-6}$
	E7	$4,25 \cdot 10^{-6}$
	E8	$1,45 \cdot 10^{-6}$
Orden 2	E15 E19	$8,65 \cdot 10^{-5}$
	E15 E21	$8,59 \cdot 10^{-5}$
	E17 E19	$8,59 \cdot 10^{-5}$
	E17 E21	$8,54 \cdot 10^{-5}$
	E15 E12	$5,19 \cdot 10^{-5}$
	E9 E19	$5,19 \cdot 10^{-5}$
	E17 E12	$5,16 \cdot 10^{-5}$
	E9 E21	$3,11 \cdot 10^{-5}$
	E15 E18	$2,33 \cdot 10^{-5}$
	E14 E19	$2,33 \cdot 10^{-5}$
	E17 E18	$2,31 \cdot 10^{-5}$
	E14 E21	$2,31 \cdot 10^{-5}$
	E10 E19	$1,58 \cdot 10^{-5}$
	E10 E21	$1,58 \cdot 10^{-5}$
	E14 E12	$1,40 \cdot 10^{-5}$
E9 E18	$1,40 \cdot 10^{-5}$	
E10 E12	$9,49 \cdot 10^{-6}$	

Indisponibilidad del sistema = \sum Indisponibilidad del conjunto mínimo de fallos

Indisponibilidad del sistema = $8,2 \cdot 10^{-4}$ proceso⁻¹

Análisis de importancia

En todo análisis de seguridad, es esencial identificar aquellos equipos y modos de fallos que tienen un mayor impacto en la seguridad del sistema analizado, es lo que constituye un "Análisis de importancia" del sistema. Este tipo de análisis permitirá centrar estudios posteriores en aquellos equipos o situaciones que han propiciado los sucesos básicos más importantes, a la vez que marca las pautas a seguir para adoptar las medidas preventivas más eficaces, que obviamente serán sobre aquellos equipos que muestren medidas de importancia más significativas.

La importancia de los sucesos básicos puede calcularse a través de diferentes medidas existentes, que realizan el análisis desde diferentes puntos de vista. En este documento se han considerado tres de las medidas más utilizadas.

- Medida de importancia RAW (Risk Achievement Worth):** se define como el cociente entre la suma de las probabilidades de los conjuntos mínimos de fallo donde aparece el componente, asumiendo para éste una probabilidad de fallo de 1 (fallo seguro), y la probabilidad total del suceso no deseado. Proporciona la degradación del sistema en caso de ocurrir el suceso básico. La ordenación obtenida está basada en la disposición estructural de los sucesos básicos en el árbol de fallos, sin tener en cuenta explícitamente los valores reales de las indisponibilidades de los sucesos.
- Medida de importancia RRW (Risk Reduction Worth):** se define como el cociente entre la probabilidad total del suceso TOP y la suma de las probabilidades de todos los conjuntos mínimos, asumiendo para el componente una tasa de fallo nula. Esta medida proporciona los sucesos básicos que más contribuyen al riesgo. Identifica aquellos sucesos básicos que si fueran perfectamente fiables, con indisponibilidad nula, conducirían a una reducción más importante del riesgo del sistema.

- c. **Medida de importancia de Fussell-Vesely:** se define este factor respecto de un componente, como el cociente entre la suma de las probabilidades de todos los conjuntos mínimos que contienen a este componente y la probabilidad total (o suma de la probabilidad de todos los conjuntos mínimos). En esta medida influye tanto la indisponibilidad del componente como su posición estructural en el árbol de fallos.

En el caso práctico del apartado anterior, los resultados obtenidos para las tres medidas de importancia se muestran en las tablas 3, 4 y 5 y se representan en los gráficos 1, 2 y 3, respectivamente.

- a. Medida RAW: esta medida revela la importancia de asegurar las señales eléctricas SA y SC de actuación de las válvulas de control (VC1 y VC 2) y de las bombas (B1 y B2), así como el suministro eléctrico.
- b. Medidas RRW y Fussell-Vesely: estas medidas proporcionan la misma ordenación de sucesos básicos y revelan la importancia de reducir la probabilidad de los modos de fallo de las bombas (B1 y B2) en demanda y en espera.

Tabla 3: Clasificación de los sucesos básicos más relevantes según medida de importancia RAW

Identificación	Descripción del suceso básico	Valor RAW
E8	Actuación errónea de la señal de cierre SC del controlador de temperatura.	1227,61
E7	Fallo de la señal de apertura SA del controlador de temperatura.	1227,6
E11	Insuficiencia potencia eléctrica.	1227,59
E13	Fallo de la válvula VC2 en operación.	36,79
E20	Fallo de la bomba 2 en operación.	36,78
E5	Válvula de retención VR2 falla a la apertura.	36,78
E6	Válvula manual V21 erróneamente cerrada u obstruida.	36,78

Clasificación de los sucesos básicos más relevantes según medida de importancia RAW

Gráfico 1 Representación de los sucesos básicos más relevantes en función de la medida de importancia RAW

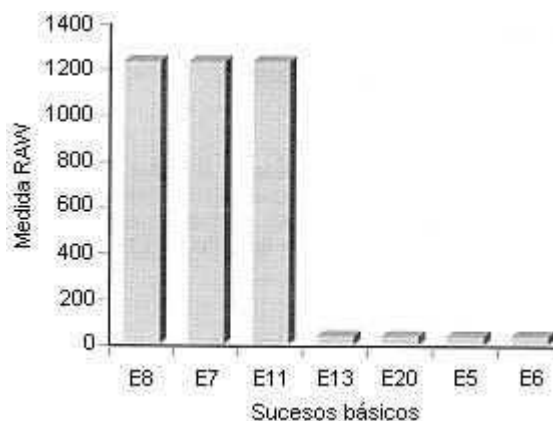


Tabla 4: Clasificación de los sucesos básicos más relevantes según medida de importancia RRW

Gráfico 2 Representación de los sucesos básicos más relevantes en función de la medida de importancia RAW

Identificación	Descripción del suceso básico	Valor RAW
E19	Fallo de la bomba 2 en demanda.	0,667
E21	Fallo de la bomba 2 en espera.	0,669
E15	Fallo de la bomba 1 en demanda.	0,687
E17	Fallo de la bomba 1 en espera.	0,689
E12	Fallo de la válvula VC2 a la demanda.	0,8
E9	Fallo de la válvula VC1 a la demanda.	0,812
E18	Indisponibilidad de la bomba 2 por pruebas o mantenimiento.	0,911

Clasificación de los sucesos básicos más relevantes según medida de importancia RRW

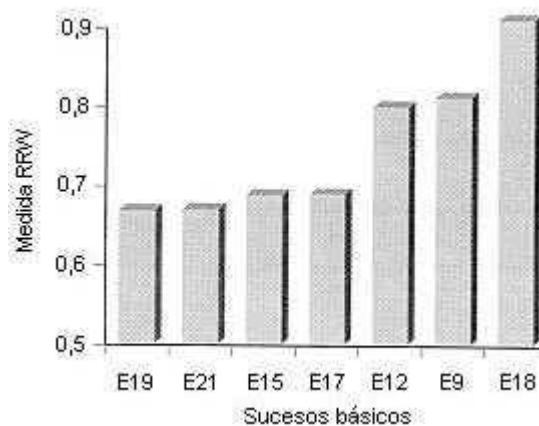
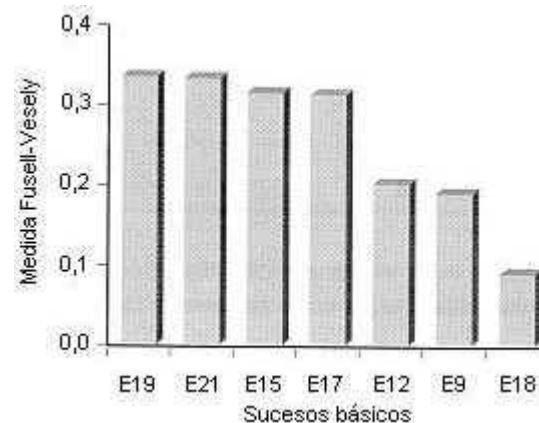


Tabla 5: Clasificación de los sucesos básicos más relevantes según medida de importancia Fussell-Vesely

Identificación	Descripción del suceso básico	Valor RAW
E19	Fallo de la bomba 2 en demanda.	0,333
E21	Fallo de la bomba 2 en espera.	0,331
E15	Fallo de la bomba 1 en demanda.	0,313
E17	Fallo de la bomba 1 en espera.	0,311
E12	Fallo de la válvula VC2 a la demanda.	0,2
E9	Fallo de la válvula VC1 a la demanda.	0,188
E18	Indisponibilidad de la bomba 2 por pruebas o mantenimiento.	0,089

Clasificación de los sucesos básicos más relevantes según medida de importancia Fussell-Vesely

Gráfico 3 Representación de los sucesos básicos más relevantes en función de la medida de importancia Fussell-Vesely



Medidas de reducción de la indisponibilidad. Intervalo óptimo entre pruebas

Las medidas existentes para aumentar la fiabilidad (o disminuir la indisponibilidad) de un sistema o reducir la probabilidad de fallo, pueden ser básicamente de dos tipos.

En primer lugar, modificar la estructura del árbol de fallos: a través de cambios en la instalación, que fundamentalmente pueden consistir en la incorporación de redundancias en aquellos elementos o funciones que se hayan identificado como críticas o imprescindibles para la seguridad del sistema, como en el caso del suministro eléctrico y señales de actuación del ejemplo anterior, que proporcionan los valores superiores en la medida de importancia RAW.

En segundo lugar, disminuir la indisponibilidad de los sucesos básicos: tal y como se ha visto en el punto "Modos de fallo y modelos de indisponibilidad" de esta NTP, la indisponibilidad de cada suceso básico se ha calculado mediante unas expresiones matemáticas para cada modo de fallo, que tienen como variables las tasas de fallos intrínsecas de los componentes (λ_s, λ_o) y las condiciones de operación y mantenimiento del sistema (T_{ep}, T_p, T_o, T_r).

Por ello, la reducción de las indisponibilidades de los sucesos básicos puede ser lograda

mediante la elección de componentes con tasas de fallos bajas y adoptando adecuadas estrategias de mantenimiento preventivo.

En el caso práctico analizado, las medidas de importancia RRW y Fussell-Vesely han revelado la importancia de reducir la indisponibilidad de las bombas instaladas, a las cuales se les realiza pruebas periódicas.

Intervalo óptimo entre pruebas

La indisponibilidad de la bomba esta determinada por:

$$q = q_{espera} + q_{pruebas} + q_{demanda} + q_{operación}$$

$$q = 1 + \frac{1}{\lambda T_{ep}} \left[e^{-\lambda_s T_{ep}} - 1 \right] + \frac{T_p}{T_{ep}} + q_d + 1 - e^{-\lambda_o T_o}$$

El intervalo óptimo entre pruebas se puede obtener derivando la función anterior respecto al tiempo entre pruebas e igualando la derivada a cero:

$$T_{\text{óptimo}} \approx \sqrt{\frac{2T_p}{\lambda_e}}$$

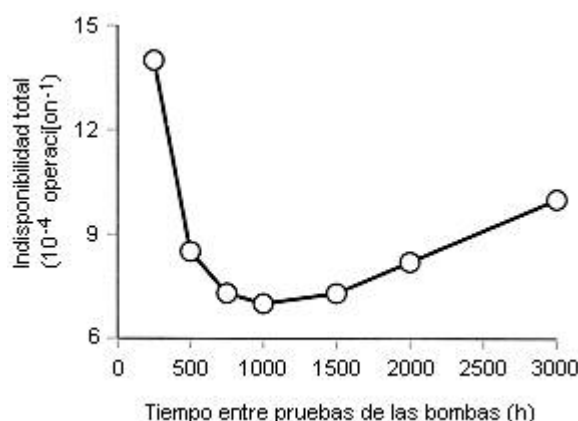
Que en el caso práctico realizado anteriormente proporciona un valor de 1.036 horas.

Para verificar este resultado se ha calculado la indisponibilidad total del suceso no deseado para distintos tiempos entre pruebas de las bombas; los resultados se presentan en la tabla 6 y se representan en el gráfico 4, de donde se desprende que el mínimo valor de la indisponibilidad total se obtiene para un tiempo entre pruebas próximo a 1.000 horas, corroborándose el cálculo matemático del tiempo óptimo realizado anteriormente.

Tabla 6: Los valores indisponibilidad total en función del tiempo entre pruebas de las bombas

Tiempo entre pruebas (h)	Indisponibilidad total (operación ⁻¹)
250	1,4 10 ⁻³
500	8,5 10 ⁻⁴
750	7,3 10 ⁻⁴
1000	7,0 10 ⁻⁴
1500	7,3 10 ⁻⁴
2000	8,2 10 ⁻⁴

Gráfico 4: Representación de los valores indisponibilidad total en función del tiempo entre pruebas de las bombas



Bibliografía

(1) AMERICAN INSTITUTE OF CHEMICAL ENGINEERS
Guidelines for process Equipment Reliability Data - 1989.

(2) BESTRATÉN, MANUEL

NTP-238 Los análisis de peligros y de operabilidad en instalaciones de proceso - 1989.

(3) DIRECCIÓN GENERAL DE PROTECCIÓN CIVIL - MINISTERIO DEL INTERIOR
Guía Técnica. Métodos cuantitativos para el análisis de riesgos - 1994.

(4) HAUPTMANN, ULRICH
Análisis de Árboles de Fallos.

(5) LEES, FRANK P.
Loss Prevention in the Process Industries - 1980.

(6) PIQUE, TOMAS Y CEJALVO, ANTONIO
NTP-333 Análisis probabilístico de riesgos: Metodología del "Árbol de fallos y errores" - 1994.

Advertencia

© INSHT