22. INSTITUTO NACIONAL DE SEGURIDAD E HIGIENE EN EL TRABAJO: *Fichas Internacionales de Seguridad Química* (traducción de las «International Safety Cards», publicadas por la Comisión de las Comunidades Europeas). INSHT. Madrid (1992).
23. NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION: *Base de datos del programa ALOHA 4.0.* NOAA. Seattle, Washington (1988).
24. BODHURTHA, F. P.: *Industrial Explosion Prevention and Protection.* Mc Graw-Hill. Nueva York (1980).

CAPÍTULO

6

Evaluación cuantitativa de riesgos

«A menudo resultaba imposible imaginar cómo podían fallar unos excelentes componentes electrónicos que habían sido sujetos a la más rigurosa comprobación previa; sin embargo, fallaban.»

2001, una odisea espacial, cap. XXII, Arthur C. Clarke.

«Señor caballero, los caballeros andantes han de acometer las aventuras que prometen esperanzas de salir bien dellas, y no aquellas que de todo en todo la quitan; porque la valentía que se entra en la juridición de la temeridad, más tiene de locura que de fortaleza.»

El ingenioso hidalgo Don Quijote de la Mancha,
segunda parte, cap. XVII, Miguel de Cervantes Saavedra.

Introducción

En este capítulo se tratan brevemente los métodos que permiten cuantificar la probabilidad de que tenga lugar un determinado tipo de accidente. No basta con identificar todos los posibles tipos de accidentes, sus causas y sus cadenas de evolución. Tampoco es suficiente poder predecir los efectos de un accidente, supuesto un determinado conjunto de circunstancias. El analista de riesgos necesita, además, ser capaz de estimar la frecuencia prevista para el accidente, o bien la probabilidad de que el accidente tenga lugar en un período de tiempo determinado. Esto le permitirá evaluar la esperanza matemática de pérdidas (EMP), como el producto de la magnitud de unos efectos determinados y la probabilidad que tengan lugar durante la vida útil de la instalación. La EMP es el indicador que va a permitir establecer la comparación entre el nivel de peligrosidad de accidentes potenciales.

Así, supongamos que nuestros métodos de estimación de consecuencias revelan que un accidente determinado *(A)* es capaz de producir unas pérdidas económicas totales de 10.000 millones de pesetas (considerando los daños materiales directos, pérdidas por interrupción de la

producción, indemnizaciones, corrección de daños medioambientales, etc.), con una frecuencia estimada de 10^{-4} años^{-1}, es decir, una vez cada diez mil años. Un segundo accidente *(B)*, en caso de que ocurriera, daría lugar a unas pérdidas económicas totales de unos 50 millones de pesetas, con una frecuencia estimada de 0,1 años, una vez cada diez años. Supongamos que en ninguno de los dos casos se esperan víctimas humanas y que la vida útil de la planta se estima en unos veinticinco años. En el caso *A*, la esperanza matemática de pérdidas durante la vida de la planta se cifra en 25 millones de pesetas, mientras que en el caso *B* sería de 125 millones. Es decir, a pesar de que cuando ocurre el accidente *B* el daño económico es 200 veces menor, la esperanza matemática de pérdidas es 5 veces mayor, y desde este punto de vista el accidente *B* es más serio y requiere una mayor prioridad a la hora de arbitrar mecanismos de seguridad que reduzcan su frecuencia estimada.

Como se verá en este capítulo, lo anteriormente expuesto no es estrictamente cierto, y el impacto previsto para los accidentes de gran magnitud suele requerir correcciones adicionales (además del hecho de que es poco realista suponer que un accidente capaz de causar 10.000 millones en pérdidas económicas no represente ningún peligro para las personas). Sin embargo, el indicador EMP, con las correcciones que se estimen necesarias, resulta útil para establecer escalas de peligrosidad y prioridades de inversión en seguridad. Para poder llegar a establecer un valor, siquiera aproximado, para la EMP de un accidente determinado, es necesario conocer los rudimentos de la evaluación cuantitativa de probabilidades. A lo largo de este capítulo se irán exponiendo las bases del procedimiento para la estimación de valores de la EMP. En la tabla 6.1 se proporcionan las definiciones de los principales términos utilizados (1), (2), (3).

Fiabilidad de equipos

Distribuciones de probabilidad

Los equipos que se utilizan en cualquier industria, y en la industria química en particular, constan de una serie de componentes que se disponen de acuerdo a un diseño previo. Las posibilidades de fallo para una instalación son infinitas. Puede haber existido un fallo en la concepción inicial de la misma o en su diseño, o el equipo puede utilizarse

Tabla 6.1. Definición de los términos utilizados en la evaluación cuantitativa del riesgo

Disponibilidad («Availability»), *(A):* Es la probabilidad de que un equipo esté disponible para comenzar una tarea cuando se le requiere. Pueden distinguirse distintos tipos de disponibilidad: Disponibilidad en estado estacionario, disponibilidad instantánea, disponibilidad hasta un tiempo dado.

Error humano («Human Error»): Cualquier acción de diseñadores, operadores o supervisores que pueda contribuir a/o resultar en accidentes.

Fallo («Failure»): Funcionamiento de un equipo o componente fuera de las tolerancias especificadas.

Fiabilidad de un equipo («Equipment Reliability»), *(R):* Es la probabilidad de que, bajo unas condiciones determinadas, el equipo realice sus funciones dentro de las tolerancias esperadas, durante un intervalo de tiempo determinado.

Fiabilidad humana («Human Reliability»): Es la probabilidad de que una persona realice con éxito una tarea determinada, bajo unas condiciones dadas.

Intervalo de confianza («Confidence Interval»): Es el intervalo de valores de una variable para el que existe una probabilidad determinada (p. ej., 95 por 100) de que el valor de la variable se encuentre dentro de dicho intervalo.

Intervalo entre revisiones («Test Interval»), *(T):* Los sistemas de protección deben verificarse a intervalos regulares. *T* es el tiempo entre dos revisiones periódicas.

Modalidad de fallo («Failure Mode»): Es la manera en que un sistema deja de realizar su función. El modo de fallo no debe confundirse con la causa del fallo. Así, un modo de fallo para un compresor podría ser no arrancar al producirse la demanda, mientras que la causa del fallo podría ser una interrupción en el suministro de energía eléctrica. Las modalidades de fallo se dividen en tres grupos, de acuerdo con su severidad: *i) Catastrófico,* cuando el fallo es súbito y afecta a funciones esenciales del equipo. *ii) De degradación,* cuando el fallo es gradual o parcial. *iii) Incipiente,* cuando el fallo consiste en una imperfección en el funcionamiento del equipo que puede resultar en un fallo catastrófico o de degradación a menos que se tomen acciones correctivas.

Probabilidad de fallo («Failure Probability»): La probabilidad de que un sistema falle al ocurrir una demanda, o también la probabilidad de que un sistema falle en un intervalo de tiempo determinado.

Tasa de demanda («Demand Rate»), *(D):* La frecuencia (número de ocasiones por año) en que se requiere la actuación de un sistema de protección, como, por ejemplo, la apertura de una válvula de alivio o la parada de emergencia activada por una alarma de temperatura.

Tasa o frecuencia de fallos («Failure Rate»), *(μ):* La frecuencia con que se producen fallos en un sistema. Puede expresarse como frecuencia estricta (número de ocasiones por año), o como frecuencia sobre demanda (número de fallos dividido

Tabla 6.1. (Continuación)

por el número total de demandas). Siempre que sea posible, los sistemas de protección deben diseñarse con la condición de «fallo seguro». En este caso, al fallar el sistema debe quedar en situación conservadora desde el punto de vista de la seguridad. Así, por ejemplo, una válvula de control en un sistema de refrigeración puede diseñarse de manera que al inactivarse por un fallo de corriente quede en posición de máxima apertura.

Tasa de peligro («Hazard Rate»), *(H):* La frecuencia (número de ocasiones por año) en que una situación peligrosa se materializa (por ejemplo, el número de veces por año en que una mezcla reaccionante alcanza la temperatura de autoignición, o el número de veces por año en que rebasa la presión de diseño de un recipiente). No es la frecuencia con que ocurre un accidente, ya que, por ejemplo, el hecho de que la presión de diseño sea rebasada no implica necesariamente la ruptura del recipiente.

Tiempo medio para la reparación («Mean Time to Repair»), (TMR): Es la media estadística de la distribución de tiempos de reparación. Puede estimarse como la suma de los tiempos de reparación durante un período determinado dividida por el número total de fallos durante ese período.

Tiempo medio entre fallos («Mean Time Between Failures»), *(TMEF):* Es el tiempo promedio entre dos fallos sucesivos. Puede estimarse como el cociente entre el tiempo total de operación para una población de componentes y el número total de fallos, incluyendo en el tiempo total de operación el correspondiente a aquellos componentes que no fallaron.

Tiempo medio hasta el fallo («Mean Time to Failure»), *(TMHF):* El parámetro TMEF sólo tiene sentido cuando se aplica a una población de componentes reparables. Cuando los sistemas no se reparan, se utiliza el parámetro *TMHF,* que es la medida de la distribución de tiempos hasta el primer fallo.

Tiempo muerto fraccional («Fractional Dead Time»), *(TMF):* Es la fracción de tiempo que un sistema se encuentra no disponible (en fallo o en reparación). $TMF = 1 - A$.

Verosimilitud («Likelyhood») *(V):* Es una medida de la probabilidad o de la frecuencia esperadas para un evento determinado. Puede expresarse directamente como frecuencia (número de eventos esperados por año), como probabilidad de que el suceso tenga lugar durante un tiempo determinado, o como probabilidad condicional (por ejemplo, la probabilidad de que exista una fuente de ignición presente en el caso de que se haya producido la ruptura de la tubería que transporta una mezcla inflamable).

en condiciones distintas de aquellas para las que fue diseñado. Puede haber existido un defecto indetectado en la etapa de construcción, o bien la instalación puede ser utilizada indebidamente o sin el necesario

mantenimiento. También pueden producirse fallos por causas externas (fallo en el suministro eléctrico, rotura por impacto de un vehículo, etcétera), o simplemente alguno de los componentes puede haber llegado al límite de desgaste que es capaz de soportar para seguir funcionando correctamente, etc. La Ingeniería de la Fiabilidad *(Reliability Engineering)* es la rama de la ingeniería que trata de la relación de la fiabilidad de un equipo con el correcto funcionamiento de sus componentes. Sus fundamentos se desarrollaron para fines militares a partir de la Segunda Guerra Mundial, extendiéndose posteriormente a la industria aerospacial, nuclear y electrónica en general, y posteriormente al resto de industrias (4).

En ocasiones el fallo puede deberse directamente a errores humanos. Ya se han citado algunos, como mal diseño o falta de mantenimiento. En realidad, cualquier fallo es en última instancia un fallo humano, puesto que todo equipo ha sido concebido, instalado y utilizado por seres humanos, pero cuando se habla de fallo humano como causa de un accidente suele entenderse que el fallo está relacionado con una acción errónea directamente relacionada con el accidente. De los fallos humanos nos ocuparemos más adelante en este capítulo y también en el capítulo 8.

Los fallos de un equipo ocurren como resultado de una interacción compleja de sus componentes individuales y las circunstancias de la operación del mismo. La predicción de los fallos de un equipo se realiza habitualmente de manera empírica, recogiendo datos de funcionamiento de un número representativo de equipos durante un tiempo suficientemente prolongado, y ajustando estadísticamente los fallos observados a una determinada distribución de probabilidad. La probabilidad de que un componente, que funciona satisfactoriamente a $t = 0$, tenga un tiempo de vida menor o igual que t (es decir, falle en el intervalo desde 0 hasta t), viene dada por la *función probabilidad de fallo, P(t).* El complementario de esta función se denomina *función fiabilidad, R(t),* de forma que

$$R(t) = 1 - P(t) \qquad [6.1]$$

También es muy importante la *función densidad de fallos,* que se define como

$$f(t) = \frac{dP(t)}{dt} \qquad [6.2]$$

El producto $f(t)dt$ proporciona la probabilidad de que el sistema falle entre t y $t + dt$, supuesto que ha funcionado hasta el tiempo t. Análogamente, la probabilidad de que el sistema falle entre dos tiempos cualesquiera t_1 y t_2 viene dada por:

$$P(t_1,t_2) = \int_{t_1}^{t_2} f(t)dt \qquad [6.3]$$

La tasa de fallos instantánea en una población de equipos o de componentes puede expresarse como

$$\mu(t) = -\frac{1}{N}\frac{dN(t)}{dt} \qquad [6.4]$$

donde N es el número de componentes que permanecen en funcionamiento a tiempo t y $\mu(t)$ es la tasa instantánea de fallos a tiempo t, con unidades de fallos por componente y por unidad de tiempo. La integración de la ecuación [6.4] entre 0 y t lleva a

$$N = N_0 \exp\left[-\int_0^t \mu(t)dt\right] \qquad [6.5]$$

donde N_0 es el número inicial de componentes funcionando a tiempo cero. Por tanto, la fiabilidad se define como

$$R(t) = \exp\left[-\int_0^t \mu(t)dt\right] \qquad [6.6]$$

En el caso de que la tasa de fallos sea constante, la ecuación [6.5] se convierte en

$$N = N_0 \exp(-\mu t) \qquad [6.7]$$

La ecuación [6.7] corresponde a un tipo especial de distribución de probabilidad denominada *distribución exponencial*, que se caracteriza por un valor de μ constante. De acuerdo con las ecuaciones anteriores, la fiabilidad, probabilidad de fallo y densidad de fallos para una distribución exponencial vienen dadas por:

$$R(t) = e^{-\mu t} \qquad [6.8]$$

$$P(t) = 1 - e^{-\mu t} \qquad [6.9]$$

$$f(t) = \mu\, e^{-\mu t} \qquad [6.10]$$

A partir de la ecuación anterior es inmediato hallar el tiempo medio hasta el primer fallo como el primer momento de la función densidad de fallos

$$TMHF = \int_0^\infty t\, f(t)dt = 1/\mu \qquad [6.11]$$

Ejemplo 6.1:

Un sistema posee una tasa de fallos instantánea constante. Representar la variación con el tiempo de las funciones fiabilidad, probabilidad de fallo y densidad de fallos para tasas de fallo de 0,01 y 0,05 fallos/hora, respectivamente.

Las ecuaciones a aplicar son las [6.8] a [6.10]. Sustituyendo los valores de μ se obtienen en función del tiempo las curvas de la figura 6.1. La fiabilidad (en este caso, la probabilidad de que el equipo no falle durante el intervalo de 0 a t) cae rápidamente con el tiempo (las tasas de fallos son bastante elevadas), y la disminución es tanto más rápida cuanto mayor es el valor de μ. La función probabilidad de fallo sigue un comportamiento complementario. Por último, el área bajo la curva de la función densidad de fallos en ambos casos es próxima a 1 (sería exactamente 1 si la representación de la figura 6.1 se extendiera a tiempo infinito). El valor inicial de densidad de fallos es cinco veces mayor para $\mu = 0{,}05$, pero la disminución es más amortiguada en el caso $\mu = 0{,}01$, lo que compensa este efecto.

Hasta ahora se ha discutido el caso de una distribución de probabilidad de fallos exponencial, que corresponde a una tasa de fallos constante. Sin embargo, la tasa de fallos $\mu(t)$ por lo general varía con el tiempo. De hecho, la curva de variación de la tasa de fallos con el tiempo para la mayor parte de los componentes y/o equipos tiene la forma característica de la figura 6.2, por lo que las curvas de tasa de fallos frente a tiempo suelen denominarse «curvas bañera». La forma

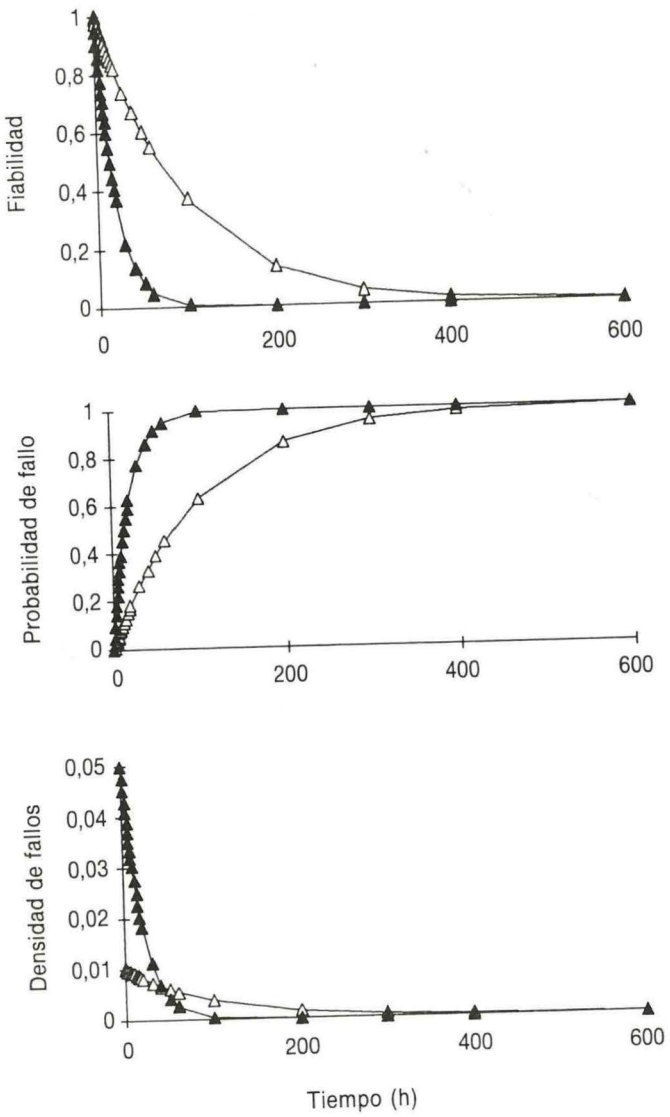

Figura 6.1. *Variación de las funciones fiabilidad, probabilidad de fallo y densidad de fallos con el tiempo de operación. Los triángulos blancos y negros corresponden, respectivamente, a tasas de fallo de 0,01 y 0,05 fallos/hora.*

de la curva proviene de las tres diferentes etapas en la vida útil de un equipo. En la etapa inicial, correspondiente a la zona I de la figura, se producen los fallos tempranos, debidos a defectos de fabricación, instalación incorrecta, etc. También, donde ello sea posible, pueden producirse fallos debidos a que el operador está en la etapa de aprendizaje de uso del equipo, y comete fallos en su utilización. Los equipos que traspasan la etapa I tienen una probabilidad razonable de estar bien construidos e instalados, y el operador se ha familiarizado con su uso. En la etapa II, la tasa de fallos es prácticamente constante, causada en gran medida por fluctuaciones aleatorias en la carga que soporta el equipo, que pueden exceder la resistencia de alguno de sus componentes. Finalmente, el aumento rápido de la tasa de fallos en la etapa III es consecuencia del desgaste del equipo.

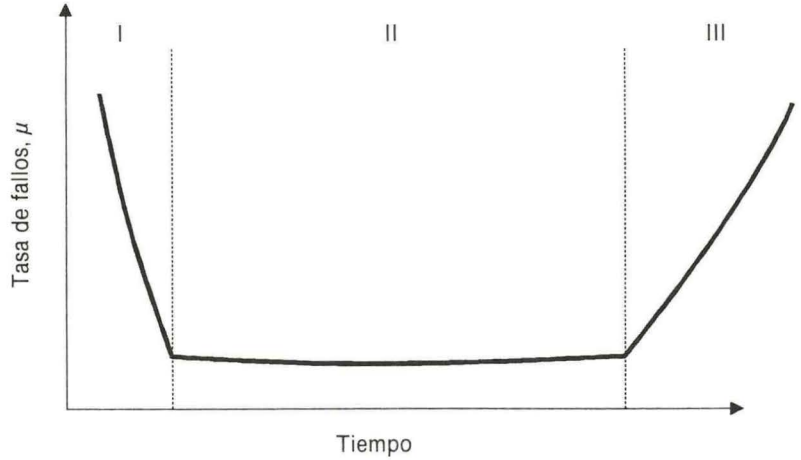

Figura 6.2. *Curva típica de tasa de fallos frente a tiempo.*

La curva de la figura 6.2 representa un caso típico en el que la tasa de fallos es dependiente del tiempo. En otras ocasiones se encuentran elementos cuya tasa de fallos depende de la demanda a la que están sometidos. Así, la probabilidad de que un alambre de cobre se rompa al ser sometido a flexión depende del número de flexiones que se ha realizado previamente a la ruptura. La tasa de fallos suele referirse a la demanda al tratar de aquellos elementos que normalmente están inactivos, y sólo actúan durante un corto intervalo de tiempo, en el cual se

produce la demanda. Éste sería, por ejemplo, el caso de un interruptor de corriente eléctrica.

La hipótesis de tasa de fallos constante implícita en el uso de la distribución exponencial es razonable para muchos equipos industriales, ya que a menudo existe un período de rodaje previo al empleo normalizado, y también es frecuente que los equipos se sustituyan por otros al cabo de un cierto tiempo de funcionamiento. Por tanto, aunque algunos autores expresan reservas en la aplicación de este principio a equipos mecánicos (4), en muchos casos cabe esperar una tasa de fallos más o menos constante a lo largo de la vida activa del elemento. De hecho, la distribución exponencial se ha utilizado con éxito para estudios sobre el riesgo de las centrales nucleares, o de numerosas instalaciones químicas (5). A pesar de ello, existen muchas otras distribuciones que se utilizan en estudios de fiabilidad. La *distribución de Poisson* pertenece al grupo de las distribuciones discretas de probabilidad, y tiene las propiedades siguientes:

i) El número de sucesos que ocurren en un intervalo de tiempo es independiente del número que ocurre en cualquier otro intervalo disjunto (el proceso de Poisson «no tiene memoria»). *ii)* La probabilidad de que un suceso sencillo ocurra en un intervalo de tiempo muy corto es proporcional al tamaño del intervalo, y no depende del número de sucesos que ocurren fuera de ese intervalo. *iii)* Es despreciable la probabilidad de que más de un suceso ocurra en ese intervalo de tiempo tan corto.

De acuerdo con las anteriores propiedades, la probabilidad de que ocurra un número determinado de sucesos (fallos) x en un tiempo t cuando la tasa promedio de sucesos es μ viene dada por (6):

$$P(x, \mu t) = \frac{e^{-\mu t}}{x!} (\mu t)^x \qquad [6.12]$$

Haciendo $x = 0$ en la ecuación anterior se obtiene la fiabilidad, es decir, la probabilidad de cero fallos en el intervalo de 0 a t. Bajo estas condiciones la ecuación [6.12] coincide con la ecucación [6.8].

Cuando la tasa de fallos no es constante suele usarse la *distribución de Weibull*, introducida por el físico sueco del mismo nombre en 1939. Esta distribución es útil como generalización de la distribución exponencial, ya que su flexibilidad le permite manejar tasas de fallo variables con el tiempo. En la distribución de Weibull la tasa de fallos viene dada por (5):

$$\mu(t) = \upsilon\alpha(\upsilon t)^{\alpha-1} \qquad [6.13]$$

donde υ y α son parámetros positivos. $1/\upsilon$ se denomina *vida característica* del elemento, mientras que α es el llamado *factor de forma.* Cuando α es menor que 1 se obtiene una tasa de fallos decreciente, correspondiente al comportamiento durante el período de rodaje que se muestra en la figura 6.2. Cuando α es igual a 1, la distribución tiene una tasa de fallos constante con el tiempo, y vuelve a coincidir con la distribución exponencial. Finalmente, si α es mayor que 1, se obtiene el comportamiento dado por la zona III de la figura 6.2, que corresponde a fallos causados principalmente por el envejecimiento del componente (4). La fiabilidad para el caso de sistemas que siguen la distribución de Weibull se obtiene combinando las ecuaciones [6.6] y [6.13]:

$$R(t) = \exp\left(-(\upsilon t)^{\alpha}\right) \qquad [6.14]$$

De acuerdo con lo anteriormente expuesto, el tiempo medio hasta fallo para un sistema que sigue la distribución de Weibull será (5):

$$TMHF = \int_0^{\infty} \exp\left(-(\upsilon t)^{\alpha}\right) dt \qquad [6.15]$$

Entre las distribuciones vistas, la distribución exponencial suele aplicarse si no se dispone de otra información, lo cual a menudo es el caso en análisis de riesgos, y existen numerosos análisis basados en esta distribución. La de Poisson es una distribución discreta, cuyo uso es apropiado cuando un suceso puede ocurrir en cualquier instante de tiempo, es decir, el número de fallos ocurrido en un intervalo de tiempo arbitrario no indica nada acerca del número de fallos que se producirá en otro intervalo distinto. Finalmente, la distribución de Weibull es capaz de proporcionar una gran flexibilidad al tratamiento de datos, siempre que se disponga de bastantes medidas como para obtener con la suficiente fiabilidad sus parámetros característicos.

Aparte de las anteriores, existen muchas otras distribuciones de probabilidad de fallo que pueden usarse. Por supuesto, la *distribución normal* es bien conocida y se utiliza ampliamente, en especial para describir tipos de fallo debidos a desgaste, variaciones en las dimensiones de piezas realizadas por procesos automáticos, fallos debidos a fenómenos físicos y naturales, etc. La *distribución log-normal* implica la distribución normal de los logaritmos de los valores de la variable aleatoria. Esta

distribución es la preferida cuando las desviaciones respecto del valor medio son en proporciones o porcentajes más que en valores absolutos como ocurre en la distribución normal, y se usa en aplicaciones como estudios de fatiga de metales, vida de aislamientos eléctricos, ajustes de datos sobre tiempos de reparación y numerosos casos de fallos de procesos continuos (7). Otras distribuciones habituales en estudios de fiabilidad son las *Binomial, Multinomial* o *Geométrica* (discretas) y las *Rayleigh, Gamma, Rectangular, Pareto* y de *valores extremos* (continuas).

La identificación de la distribución que mejor representa los datos observados no es, en la mayor parte de los casos, un paso obvio, y requiere considerable experiencia por parte del analista. No obstante, en la actualidad se han desarrollado considerablemente las técnicas numéricas para el ajuste estadístico, lo que permite una mayor eficacia en la discriminación de modelos y en la estimación de sus parámetros. En la figura 6.3 se han representado esquemáticamente los pasos a seguir para la selección de la distribución y el cálculo de sus parámetros característicos.

Un paso previo a la determinación de la distribución probabilística de fallos para un componente determinado es la recogida de datos de fallos realizada sobre una población representativa. Los datos disponibles pueden ser específicos de planta o genéricos. Los datos específicos de planta se recogen directamente por los operarios, anotando los fallos de un equipo determinado, y las condiciones en que se producen. A este respecto existen formularios normalizados (7) en los que se señalan datos de identificación completa del equipo, fecha y hora del fallo, descripción del tipo de fallo y las circunstancias del mismo, método de detección del fallo, estado del equipo (parado, a plena carga, al 80 por 100, etc.) y de la planta (operación normal, arranque, etc.) al producirse el fallo, efectos sobre otros equipos y detalles sobre la reparación. Toda esta información resulta de gran utilidad para poder construir una base de datos adecuada. El inconveniente de la utilización de datos específicos es que, afortunadamente, los equipos que se utilizan suelen tener una fiabilidad alta, por lo que casi nunca se dispone de suficientes datos sobre fallos de un equipo concreto, lo que dificulta y a veces imposibilita el análisis estadístico de los mismos.

Cuando no es posible utilizar datos específicos se acude a datos genéricos, que incluyen todas las plantas de la empresa, o si esto no es suficiente, datos de otras plantas de la industria de proceso y datos de

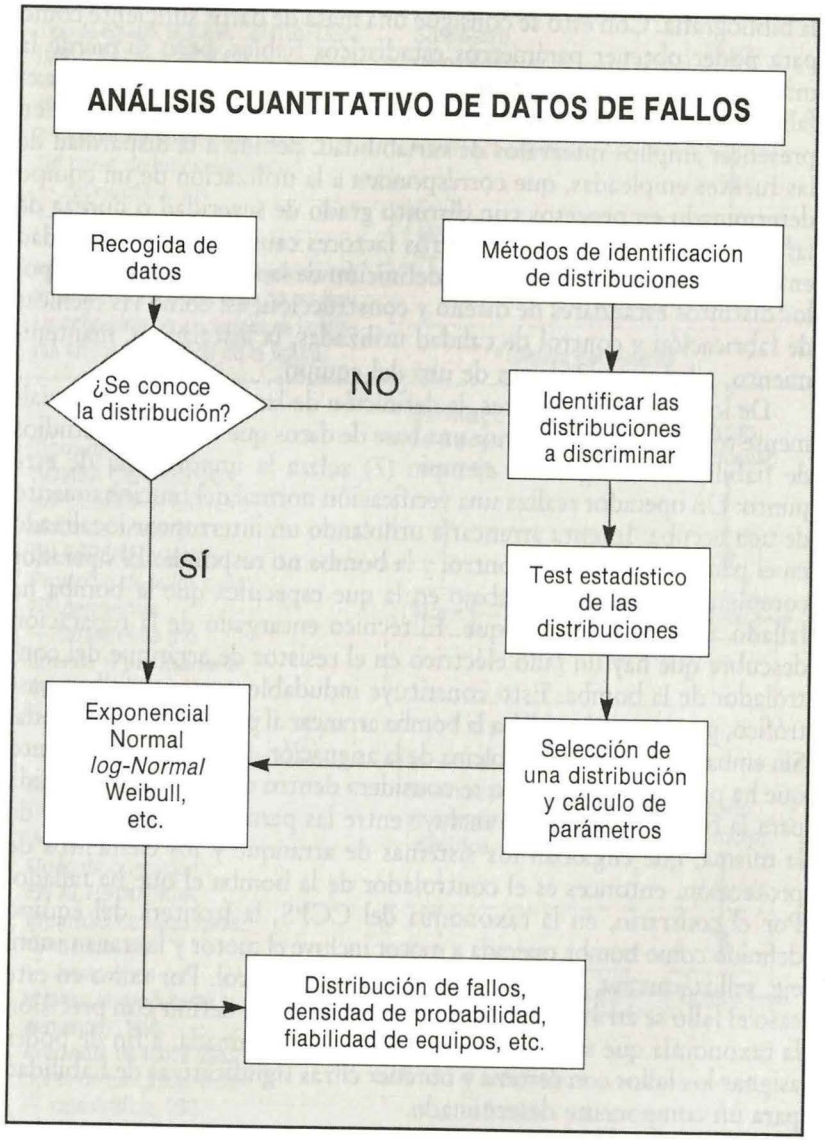

Figura 6.3. *Esquema para la selección de un modelo de distribución de probabilidades de fallos. (Adaptado de la referencia 3.)*

la bibliografía. Con esto se consigue una masa de datos suficiente como para poder obtener parámetros estadísticos fiables, pero se pierde la información específica en cuanto a las condiciones en que se produce el fallo del equipo. Así resulta que los datos de la bibliografía suelen presentar amplios intervalos de variabilidad, debido a la disparidad de las fuentes empleadas, que corresponden a la utilización de un equipo determinado en procesos con distinto grado de severidad o dureza de las condiciones de operación. Otros factores causantes de variabilidad en los datos de fallos incluyen la definición de las fronteras del equipo, los distintos estándares de diseño y construcción, así como las técnicas de fabricación y control de calidad utilizadas, la instalación, mantenimiento, edad y condiciones de uso del equipo.

De los factores anteriores, la definición de las fronteras es especialmente relevante para construir una base de datos que sea útil en estudios de fiabilidad. El siguiente ejemplo (7) aclara la importancia de este punto: Un operador realiza una verificación normal del funcionamiento de una bomba. Intenta arrancarla utilizando un interruptor localizado en el panel del cuarto de control y la bomba no responde. El operador completa una orden de trabajo en la que especifica que la bomba ha fallado al intentar el arranque. El técnico encargado de la reparación descubre que hay un fallo eléctrico en el resistor de arranque del controlador de la bomba. Esto constituye indudablemente un fallo catastrófico, puesto que impidió a la bomba arrancar al producirse la demanda. Sin embargo, persiste el problema de la asignación del fallo. Si el elemento que ha producido el fallo no se considera dentro de la frontera definida para la bomba, sino que se incluye entre las partes del controlador de la misma, que engloban los sistemas de arranque y los elementos de protección, entonces es el controlador de la bomba el que ha fallado. Por el contrario, en la taxonomía del CCPS, la frontera del equipo definido como bomba operada a motor incluye el motor y la transmisión, eje, sellos, carcasa, impulsor y elementos de control. Por tanto en este caso el fallo se atribuye a la bomba. Es importante definir con precisión la taxonomía que se utiliza en una fuente determinada, a fin de poder asignar los fallos con certeza y obtener cifras significativas de fiabilidad para un componente determinado.

En la figura 6.4 se muestran varios ejemplos de datos de fiabilidad, tomados de la recopilación del CCPS (7) para los que además de las cifras de fallos se indican las fronteras que se han considerado para cada equipo. Puede observarse que en la figura 6.4a, para un mismo equipo

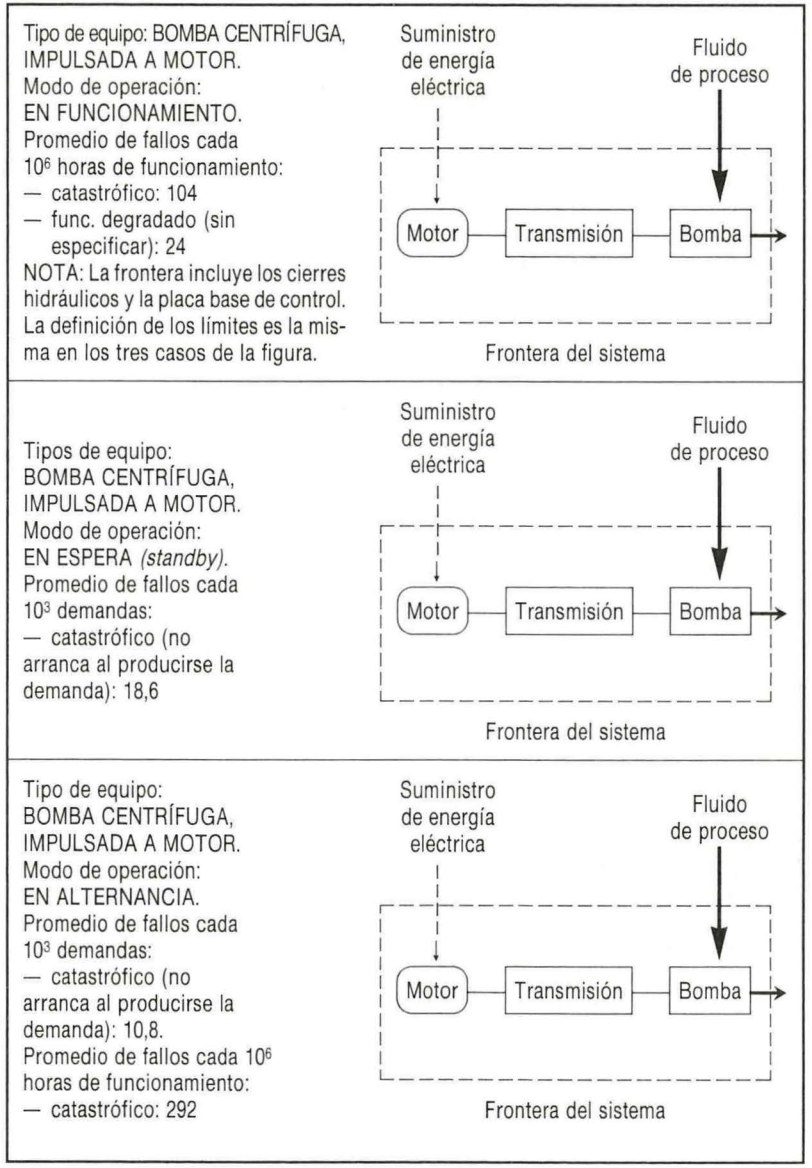

Figura 6.4a. *Datos de frecuencia de fallos en algunos equipos de proceso. (Tomados de la referencia 7.)*

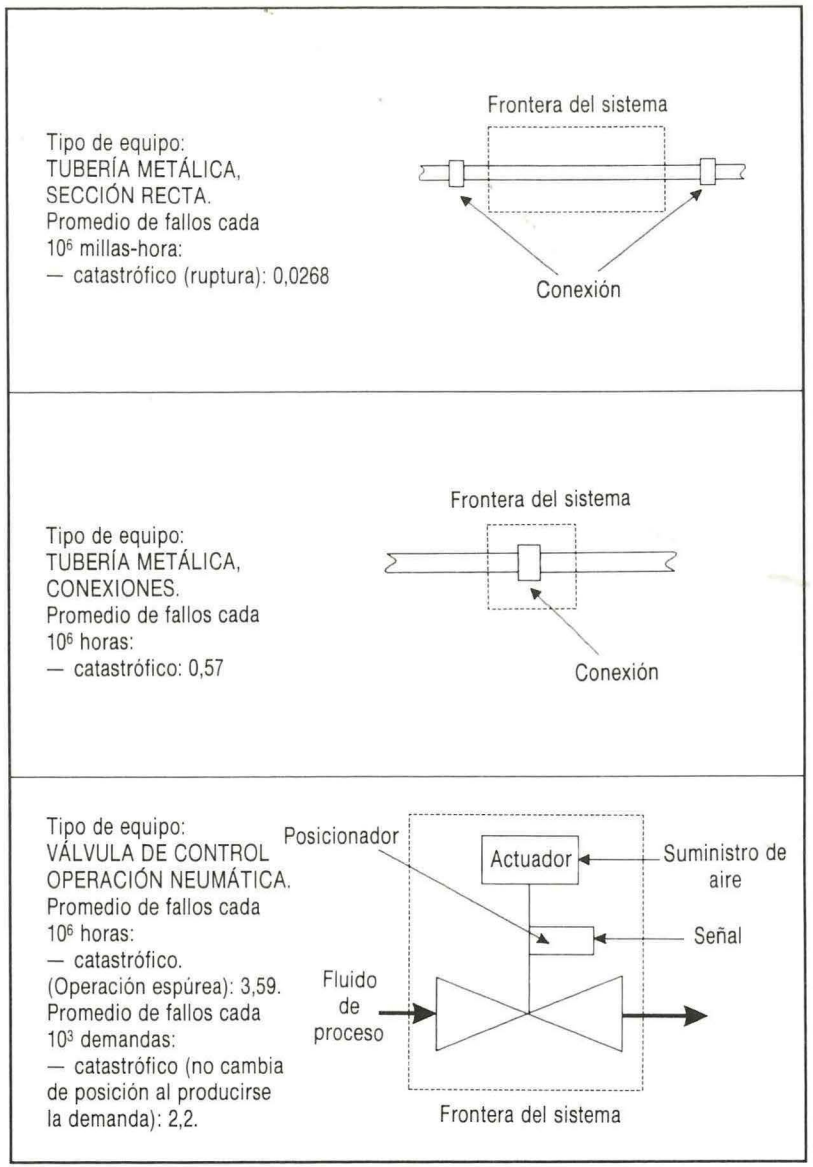

Figura 6.4b. *Datos de frecuencia de fallos en algunos equipos de proceso. (Tomados de la referencia 7.)*

(bomba centrífuga operada por un motor eléctrico) la frecuencia de fallos es considerablemente distinta dependiendo del modo de operación que se utilice. Esto es lógico, ya que los modos de fallo y las causas de los mismos son distintos. Así, por ejemplo, es frecuente que en operaciones de cierta importancia para un proceso se asignen dos bombas para realizar la misma tarea, una de las cuales está funcionando de manera continua, mientras que la otra (de repuesto) está en espera. La probabilidad de que la bomba en funcionamiento deje de funcionar en un intervalo de tiempo determinado es diferente de la probabilidad de que la que está en espera no arranque cuando se le requiere (8). En el primer caso, las causas del fallo pueden incluir factores como sobrecalentamiento que no ocurrirían en la bomba parada antes de su puesta en marcha, mientras que la bomba en espera puede tener fallos con causa propia, como sería, por ejemplo, un defecto en el contactor de arranque.

En la figura 6.4 no se indica el nivel de severidad de los procesos en los que se obtuvieron los datos que se muestran, lo que, como se ha señalado anteriormente, es consecuencia del hecho de que se han recogido datos genéricos. Sin embargo, el nivel de severidad del proceso influye fuertemente en la tasa de fallos, por lo que debe tenerse en cuenta siempre que sea posible. A menudo se han sugerido factores de ajuste, por los que habría que multiplicar la tasa de fallos para adecuarla a condiciones más severas. Se recomiendan incrementos del 7 por 100 (factores de 1,07) para instrumentos en general, y válvulas de control en las siguientes condiciones (3): operación bajo temperaturas extremas, humedad alta, suciedad en el medio de trabajo, localización inadecuada por exposición a posibles daños por causas mecánicas o inaccesible para inspección periódica. Por atmósfera corrosiva se sugiere un factor de 1,21. Para otros agentes dañinos se sugieren distintos factores para instrumentación en general y válvulas de control (indicadas entre paréntesis). Así, por corrosión el factor sugerido es de 1,07 (1,14), por erosión de 1,14 (1,28), por posibilidad de ensuciamiento/taponamiento de 1,07 (1,14), por flujo pulsante de 1,14 (1,07) y por vibración de 1,42 (1,21).

Ejemplo 6.2:

Una importante compañía química se plantea un estudio de fiabilidad sobre un tipo particular de válvula de control operada a motor, de amplio uso en las plantas de proceso continuo de esta empresa. Se dispone de datos recogidos durante un período de cinco años sobre 158 válvulas activas de proceso, totalizando 4,8 millones de horas de trabajo. Durante este período se ha contabilizado un total de 11 fallos catastróficos en funcionamiento por operación espúrea (la frontera del sistema incluye en este caso el motor, además de la válvula en sí). Estimar las probabilidades de este tipo de fallo para el equipo considerado.

Si se supone una tasa de fallos constante se obtienen 2,3 fallos por cada 10^6 horas de funcionamiento ($2{,}3 \times 10^{-6}$ fallos por válvula-hora). Los datos genéricos para este equipo indicarían (7) una tasa de fallos media de 1,36 fallos por cada millón de horas en funcionamiento, por lo que el valor de 2,3 fallos podría ser indicativo de defectos en mantenimiento, o de una severidad de proceso superior a la media.

Para estimar los límites de confianza de la tasa de fallos se utilizan las siguientes expresiones (3):

$$L.S. = \frac{(x+1)\,F_1}{(n-x)+(x+1)F_1} \qquad [6.16]$$

$$L.I. = \frac{x}{(n-x+1)F_2 + x} \qquad [6.17]$$

donde *L.S.* y *L.I.* son respectivamente los límites superior e inferior del intervalo de confianza de la estimación, x es el número de fallos observados y n el tamaño de muestra. En este caso el tamaño de la muestra es de 4,8 millones de válvulas-hora. F_1 y F_2 son los valores de la distribución F para un nivel de probabilidad determinado, con grados de libertad (f_1, f_2) y (f_3, f_4) respectivamente, que se definen como:

$$f_1 = 2\,(x+1)$$
$$f_2 = 2\,(n-x) \qquad [6.18]$$

Ejemplo 6.2 (continuación):

$$f_3 = 2\,(n-x+1)$$
$$f_4 = 2x \qquad [6.18]$$

Los valores F_1 y F_2 se obtienen de tablas estadísticas convencionales (por ejemplo, referencia 6). De acuerdo con las ecuaciones [6.18], se obtienen los valores siguientes: $f_1 = 24$, $f_2 = f_3 = 9{,}6 \times 10^6$, $f_4 = 22$, es decir, los valores de f_2 y f_3 corresponderían a infinitos grados de libertad a los efectos de las tablas de probabilidad de la distribución F. En esas condiciones, de las tablas estadísticas se obtiene para un 95 por 100 de confianza valores de F_1 y F_2 de 1,52 y 1,78, respectivamente. A partir de las ecuaciones [6.16] y [6.17], los límites del intervalo de confianza son $3{,}8 \times 10^{-6}$ y $1{,}3 \times 10^{-6}$, es decir, al nivel de confianza del 95 por 100 el intervalo se sitúa entre 1,3 (límite inferior) y 3,8 (límite superior) fallos por cada millón de horas de trabajo. Para un nivel de confianza del 99 por 100 el intervalo iría de 1 a 4,5 fallos por cada millón de horas de funcionamiento.

Fiabilidad y disponibilidad de sistemas de protección

Un sistema de protección es un dispositivo que se instala para evitar la materialización de un peligro. Ejemplos de sistemas de protección son un dispositivo de alivio de presión, una alarma de alta temperatura o un sistema de parada de emergencia. Puesto que los sistemas de protección tienen como finalidad reducir la probabilidad de accidentes, es especialmente importante asegurarse de su fiabilidad. La fiabilidad de sistemas complejos requiere un estudio detallado, que no se aborda aquí. En otros textos (1), (3), (4), (5), (9), (10) se desarrolla el tema con mayor amplitud.

La mayor parte de los sistemas de protección funcionan sólo de vez en cuando. Esto quiere decir que es posible que un sistema de protección haya fallado (por ejemplo, que una válvula de alivio esté bloqueada en cierre), y que el fallo no se haga patente hasta que no se produzca una demanda sobre el sistema. Este tipo de fallos se denominan *fallos ocultos,* y son extremadamente importantes desde el punto de vista de la segu-

ridad. En otros casos, el operador tiene conocimiento del fallo en el momento de producirse éste, y, por lo tanto, puede tomar acciones correctoras antes de que se produzca la demanda. Este tipo de fallos se denominan *fallos evidentes;* un ejemplo de los mismos sería la apertura de un disco de ruptura a una presión inferior a la de consigna, debido al debilitamiento del mismo por causa de ataque químico.

Si un sistema de protección nunca se comprueba, eventualmente se degradará y fallará, con una probabilidad de fallo que aumentará con el tiempo. La única manera de reducir la probabilidad de que ocurran fallos ocultos es realizar inspecciones frecuentes sobre los sistemas de protección. Cuando se descubre un fallo, hay que realizar una reparación, y durante el tiempo que dura la misma el sistema tampoco se encuentra disponible. Como se indica en la tabla 6.1, el *TMF* es la fracción de tiempo que un sistema se encuentra incapacitado, ya sea en fallo o en reparación.

Para que se dé una situación peligrosa tiene que ocurrir que se produzca la demanda y que el sistema se encuentre inactivo, es decir, en «tiempo muerto». *Para el caso en el que tanto el tiempo muerto fraccional como la tasa de demanda son bajos* (la situación más corriente en los sistemas de protección), la tasa de peligro H definida en la tabla 6.1 puede calcularse como el producto de la tasa de demanda por la probabilidad de que el sistema se encuentre incapacitado, es decir

$$H = D \times TMF \qquad [6.19]$$

Un equipo sin sistema de protección es equivalente a un sistema de protección permanentemente incapacitado ($TMF = 1$), en cuyo caso la tasa de peligro es igual a la tasa de demanda. Supongamos que el tiempo que se tarda en reparar un sistema es pequeño comparado con el tiempo entre comprobaciones, o bien que, inmediatamente que se descubre el fallo durante una inspección, el sistema es sustituido por otro mientras la reparación tiene lugar. Si el intervalo entre pruebas es T, el tiempo muerto fraccional viene dado por

$$TMF = \frac{1}{T}\int_0^T P(t)dt \qquad [6.20]$$

Por tanto, para conocer el tiempo muerto fraccional es necesario haber determinado previamente la distribución de la probabilidad de

fallo. En el caso de que la probabilidad de fallo siga una distribución exponencial de las ecuaciones [6.9] y [6.20] se sigue que

$$TMF = 1 - \frac{1}{\mu T}(1 - e^{-\mu T}) \qquad [6.21]$$

Desarrollando el término $e^{-\mu T}$ en serie de Taylor y despreciando los términos de la expansión a partir del tercero se obtiene que

$$TMF \approx \frac{1}{2}\mu T \qquad [6.22]$$

que es una aproximación válida cuando $\mu T \leq 0{,}1$. La ecuación [6.22] es casi una expresión «intuitiva» para la estimación del tiempo muerto fraccional. En efecto, consideremos el diagrama de la figura 6.5. El sistema de protección, inicialmente activo, puede quedar inactivo como consecuencia de un fallo. La condición del sistema sólo se pone de manifiesto cuando se procede a la revisión, o cuando se produce una demanda. En el ejemplo del diagrama, las revisiones se llevan a cabo cada tres semanas. El primer fallo se produce a las dos semanas de instalar el equipo, pero como no se produce ninguna demanda, el fallo queda sin descubrir hasta la primera revisión, que ocurre a las tres semanas (nótese que esta condición es poco realista; un equipo recién instalado, especialmente un sistema de protección, debería llevar consigo revisiones con más frecuencia, hasta rebasar el período I de la curva de fallos). Tras la primera revisión el equipo se repara, y durante las segundas tres semanas no sufre fallos, de modo que en la segunda

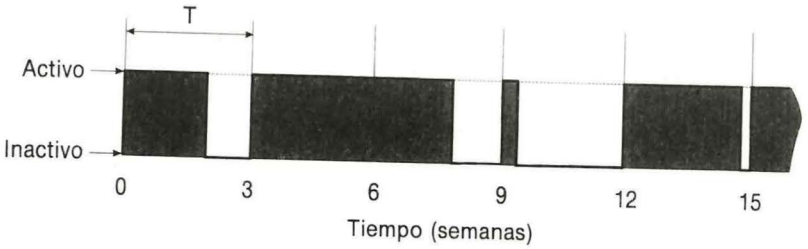

Figura 6.5. *Diagrama de estado de un componente para fallos no revelados.*

revisión se comprueba que funciona correctamente. El siguiente fallo se produce cerca de las ocho semanas, y no se descubre hasta la revisión de las nueve semanas, y así sucesivamente. Aunque unos fallos ocurrirán en una etapa temprana del período entre revisiones y otros en una etapa tardía, el fallo, si tiene lugar, ocurrirá como promedio a mitad del período entre reparaciones. En este caso el tiempo muerto fraccional puede estimarse como el producto de la tasa de fallos por la mitad del tiempo entre revisiones (ecuación 6.22). Por tanto, si el sistema falla en promedio una vez por año y el período entre revisiones es de tres semanas, el tiempo muerto fraccional será de 1,5 semanas por año, es decir, 0,0288. Como se desprende de la ecuación [6.20], la expresión [6.22] sería exacta si la distribución de probabilidad de fallo fuese $P(t) = \mu t$, es decir, si la probabilidad de fallo fuese directamente proporcional al tiempo transcurrido (de ahí su carácter «intuitivo»). La ecuación [6.21], correspondiente a la distribución exponencial, tiene mayor generalidad.

Por otro lado, la ecuación [6.19] es, como se ha indicado, válida si tanto D como TMF son bajos. En caso contrario, debe ser sustituida por (2):

$$H = \mu\,(1 - e^{-DT/2}) \qquad [6.23]$$

Las predicciones de H obtenidas a partir de las ecuaciones [6.19] y [6.23] coinciden para bajos valores del producto DT (las divergencias para $DT \leq 0{,}4$ son menores del 10 por 100), pero pueden diferir notablemente para valores superiores. De hecho, cuando DT alcanza valores muy altos la ecuación anterior establece que H tiende a μ, es decir, la tasa de peligro se aproxima a la tasa de fallos del sistema, ya que a valores muy altos de la demanda (o a valores muy altos del intervalo de tiempo entre revisiones) será probable la producción de una demanda simultáneamente con el fallo de un sistema de protección.

Las ecuaciones [6.21] y [6.22] proporcionan estimaciones del TMF, debido al fallo individual de un componente, para unas condiciones determinadas. Evidentemente, dichas ecuaciones pueden corregirse para tener en cuenta el tiempo muerto debido a la revisión en sí y a las reparaciones, así como la probabilidad de una reparación defectuosa (3). Así, el valor total del tiempo muerto fraccional se calcula como una suma de los tiempos muertos debidos al fallo del componente que se ha discutido con anterioridad, más las contribuciones al TMF debidas a la duración de la revisión y/o reparación, los TMF adicionales que proceden

de errores humanos en la revisión o reparación del sistema, y los que se deben a fallos de causa común, que se tratan más adelante.

Ejemplo 6.3:

Un sistema tiene una tasa de fallos de 0,5 años^{-1}. Suponiendo que puede aplicarse una distribución exponencial de probabilidad, calcular cuál será la tasa de peligro si las revisiones se verifican: a) *trimestralmente, y* b) *anualmente, sabiendo que el sistema soporta en promedio una demanda semestral.* c) *¿Cuál debe ser el intervalo entre revisiones para que la tasa de peligro disminuya hasta 0,005 años^{-1}?*

a) El producto DT es mayor que 0,4 tanto en este apartado como en el *b)*, por lo que la tasa de peligro viene dada por la ecuación [6.23] en lugar de la [6.19], aunque en este caso el error sería pequeño. Sustituyendo $D = 2$ años^{-1}, $\mu = 0{,}5$ años^{-1} y $T = 0{,}25$ años en la ecuación [6.23] se obtiene $H = 0{,}11$ años^{-1}, una vez cada 9,1 años (con la ecuación [6.19] se hubiera obtenido $H = 0{,}12$, la diferencia es del orden del 10 por 100).

b) De manera análoga, se obtiene $H = 0{,}32$ años^{-1} (una vez cada 3,1 años), mientras que la ecuación [6.19] hubiera dado para H un resultado un 30 por 100 mayor. Puede verse que la disminución de la frecuencia de revisión de una por trimestre a una por año triplica la tasa de peligro.

c) Las tasas de peligro obtenidas en los apartados anteriores son elevadas. Si se quiere reducir la tasa de peligro hasta un valor de $H = 0{,}005$ años^{-1} (una vez cada doscientos años), la ecuación [6.23] (o la [6.19], ya que en este caso DT es considerablemente más bajo) establece que $T = 0{,}01$ años, es decir, se requieren revisiones aproximadamente dos veces por semana.

Asociación de sistemas

En el ejemplo anterior se ha puesto de manifiesto que es posible reducir la tasa de peligro mediante la disminución del intervalo entre revisiones. Como hemos visto, para valores de T bajos, el TMF varía

de manera prácticamente proporcional a T. Evidentemente, existe un límite de tipo práctico en la reducción del tiempo muerto fraccional que puede lograrse aumentando la frecuencia de las revisiones. Por otro lado, aun en el caso de reparaciones de corta duración, la suposición de que el tiempo de reparación es despreciable frente a T deja de ser cierta para valores muy altos de la frecuencia de revisiones.

Otra forma de reducir la tasa de peligro consiste en duplicar y a veces multiplicar equipos esenciales. Esto puede hacerse de dos maneras: la *redundancia* consiste en el uso de varios equipos idénticos, cada uno de los cuales es capaz de llevar a cabo la función requerida. El término *diversidad* se aplica a la utilización de varios equipos diferentes, cada uno de los cuales puede realizar la función requerida. Tiene como objeto el disminuir la probabilidad de fallo por causa común, que puede afectar a los equipos redundantes.

Las dos formas más simples de asociación de equipos de protección son la *asociación en serie* y la *asociación en paralelo,* que se muestran conceptualmente en la figura 6.6. La asociación en serie es la que tiene lugar cuando, para que funcione el sistema de protección, tienen que funcionar *todos* los equipos asociados. Por tanto, no se instala para aumentar matemáticamente la fiabilidad del sistema, sino porque existen razones de tipo físico que lo aconsejan. El ejemplo típico es el de un sistema de alivio de presión que consiste en un disco de ruptura en

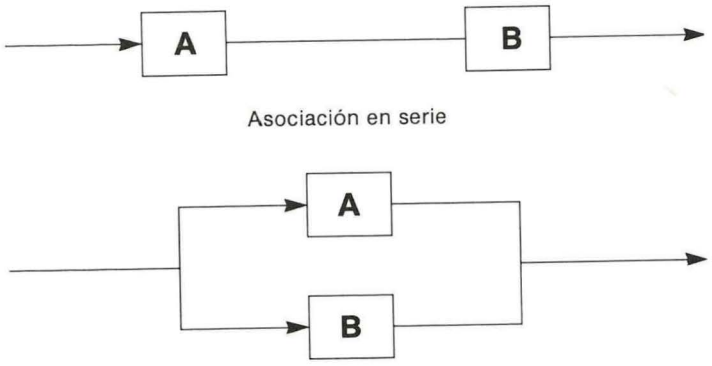

Figura 6.6. *Asociación de sistemas de protección.*

serie con una válvula de seguridad. Para que el alivio de presión se produzca adecuadamente, tanto el disco de ruptura como la válvula de seguridad tienen que abrirse a sus respectivas presiones de consigna. Por tanto, matemáticamente, parece que la probabilidad de que la asociación falle debería ser mayor que la de que fallen cualquiera de sus componentes por separado. A pesar de ello esta asociación se utiliza, por ejemplo, cuando el fluido de proceso puede causar corrosión en la válvula de seguridad. En este caso, la función del disco de ruptura es la protección de la válvula de seguridad, y esta acción mejora considerablemente la fiabilidad individual de la válvula de seguridad. Así, la fiabilidad del sistema disco de ruptura/válvula de seguridad es mayor que la de una válvula de seguridad expuesta a corrosión por parte del fluido de proceso.

En cuanto a la asociación de sistemas de protección en paralelo, siempre aumenta la seguridad, y es típica de sistemas redundantes. Un sistema en paralelo funcionará si funciona *cualquiera* de sus componentes. Siguiendo con el ejemplo anterior, si el disco de ruptura falla, ocasiona el fallo del sistema de protección. Para evitarlo puede colocarse un segundo sistema disco de ruptura/válvula de seguridad en paralelo con el primero, o bien un segundo disco de ruptura, con una presión de consigna ligeramente más alta. Para que ahora falle el sistema de protección deben fallar *ambos* discos de ruptura. Puesto que la probabilidad de fallo de ambos es mucho menor, la redundancia ha permitido aumentar grandemente la fiabilidad del sistema.

El uso de la redundancia como sistema para aumentar la fiabilidad de un sistema de protección tiene, sin embargo, sus límites. Consideremos un reactor en el que existe la posibilidad de una reacción fuera de control. Supongamos que se ha instalado una alarma de temperatura que, cuando ésta rebasa cierto límite, inicia automáticamente la parada de emergencia del sistema. Evidentemente, el sistema de emergencia descansa en la lectura de un sensor de temperatura (por ejemplo, un termopar), que puede ser considerado un elemento crítico para la protección del reactor, por lo que en la mayoría de los casos se consideraría inaceptable confiar la acción del sistema de protección a la lectura de un solo elemento. En este caso podemos instalar un segundo sensor, de manera que si cualquiera de los dos sensores registra un aumento de temperatura por encima del valor establecido, se dispara la acción de emergencia. Así, aunque uno de los sensores funcione incorrectamente y proporcione lecturas de temperatura por debajo del valor real, lo más

probable es que el segundo sensor proporcione lecturas correctas y active el sistema de emergencia.

Los termopares son relativamente baratos de manera que se podría plantear un nivel mucho mayor de redundancia con la instalación de, digamos, una docena de sensores, de forma que cuando cualquiera de ellos registre la lectura prefijada se active la parada de emergencia. Esto disminuiría hasta valores despreciables la probabilidad de que no se active la parada de emergencia por fallo de un termopar, ya que, aunque todos los sensores menos uno diesen lecturas incorrectas por defecto, el sistema funcionaría. A cambio se tendría un sistema con frecuentes «paradas indebidas por fallo seguro» de los sensores de temperatura. Cada vez que uno de ellos registrase un fallo de lectura por exceso el sistema se dispararía, lo que también es inaceptable, no sólo por el coste económico de la parada y el arranque posterior, sino porque es muy probable que las frecuentes interrupciones del estado estacionario de la operación den como resultado una operación insegura. Para evitar este tipo de situaciones es frecuente el uso de los «sistemas votantes», en los que se requiere que exista un número mínimo de señales (por ejemplo, 2 sensores de 3, 2 de 4, etc.) con valores por encima del nivel que activa la alarma.

El cálculo del tiempo muerto fraccional en sistemas simples con redundancia o diversidad se realiza siguiendo los principios generales ya expuestos. Por ejemplo, si en un sistema se instala diversidad en paralelo con dos elementos de protección cuyas tasas de fallo son μ_1 y μ_2 (por ejemplo, un disco de ruptura y una válvula de seguridad o dos discos de ruptura diferentes), la probabilidad de fallo del sistema de protección será la de que fallen ambos componentes (ya que deben fallar ambos para que el sistema quede desprotegido). Si se consideran probabilidades de fallo independientes y dadas por una distribución exponencial, entonces a partir de la ecuación [6.9] para cada uno de los componentes.

$$P_i(t) = 1 - e^{-\mu_i t} \qquad [6.24]$$

Para valores bajos del producto $\mu_i t$, las probabilidades de fallo pueden aproximarse por $P_i(t) = \mu_i t$, y aplicando la ecuación [6.20], el tiempo muerto fraccional del sistema de protección viene dado por

$$TMF = \frac{1}{T}\int_0^T (\mu_1 t)\,(\mu_2 t)dt = \mu_1\mu_2\,\frac{T^2}{3} \qquad [6.25]$$

o bien igual a $(1/3)\mu^2T^2$ en el caso de que en lugar de diversidad exista redundancia y los sistemas 1 y 2 sean idénticos. En general, para el fallo de n sistemas de protección redundantes (cuyas revisiones ocurren al mismo tiempo), el tiempo muerto fraccional viene dado por (3):

$$TMF = \left[\frac{n!}{r!(n-r)!}\right]\frac{1}{(r+1)}\,\mu^r T^r \qquad [6.26]$$

donde n es el número de equipos o componentes redundantes, $r = n - m + 1$, y m es el número de sistemas que deben funcionar correctamente para que el sistema quede protegido. Así, en un sistema con tres componentes redundantes donde basta con que funcione uno para que el sistema esté protegido, el TMF viene dado por $(1/4)\,\mu^3T^3$, mientras que si se requiere el funcionamiento de al menos dos componentes de los tres instalados (sistema votante), el TMF será μ^2T^2.

Fallos de causa común

En la exposición anterior se ha considerado que los fallos que un componente determinado puede sufrir son independientes en cuanto a su probabilidad, de los de otros componentes. Así, si se consideran dos discos de ruptura en paralelo se supone que sus probabilidades de fallo no están relacionadas. Sin embargo, consideremos el caso de que ambos discos de ruptura hayan sido fabricados por la misma empresa y aproximadamente en la misma época. Supongamos también que en ese período se produce accidentalmente un fallo en la composición de los materiales utilizados que no es detectado en el control de calidad. Como consecuencia, los discos de ruptura no se abren a la presión a la que deberían hacerlo. Si consideramos aisladamente la probabilidad P de un fallo de fabricación en un disco de ruptura que le impida abrirse a la presión de consigna veremos que es baja, ya que estos dispositivos sufren un control de fabricación riguroso. Por tanto, con un disco redundante deberíamos estar adecuadamente protegidos, ya que la probabilidad de que los dos discos que hemos instalado hayan sufrido fallos *independientes* en el proceso de fabricación (P^2) es muy baja. Sin embargo, en el caso que hemos considerado existe una causa común para ambos fallos, lo que eleva extraordinariamente la probabilidad de su concurrencia.

Hauptmanns (5) cita la siguiente clasificación para el análisis de fallos de causa común:

— Fallos de dos o más componentes similares o idénticos debidos a una causa común.
— Fallos de dos o más componentes similares o idénticos que se producen como consecuencia de un fallo único inicial (fallos secundarios).
— Fallos de dos o más componentes o sistemas similares o idénticos que se deben a dependencias funcionales, como, por ejemplo, la dependencia de un sistema auxiliar común (aire de instrumentos, suministro eléctrico, agua de refrigeración, etc.), o un error humano que afecta a varios sistemas a la vez. Este tipo de fallos suele detectarse con cierta facilidad al realizar un análisis de árbol de fallos o un análisis HAZOP (ver capítulo 2), mientras que los dos primeros grupos pueden pasar inadvertidos con mayor frecuencia.

Las causas del fallo común pueden ser variadas incluyendo defectos de diseño, fabricación o instalación de los componentes, defectos de mantenimiento (por ejemplo, una calibración periódica de sensores que se efectúa erróneamente), operación incorrecta (parámetros de operación/control inapropiados, operación en condiciones extremas de temperatura, humedad, vibración, etc.), o sucesos externos (incendio, sabojate, terremoto, etc.).

Estimación cuantitativa de riesgos utilizando el análisis de árbol de fallos

En el capítulo 2 se introdujo el análisis de árbol de fallos (FTA), como técnica de identificación y cuantificación de riesgos, se explicaron los símbolos básicos y se discutieron algunos ejemplos de aplicación del análisis a casos sencillos. En realidad, el análisis FTA puede llegar a complicarse bastante cuando se aplica a sistemas reales de la industria química, por lo que su utilización requiere experiencia previa. Un tratamiento extenso de la construcción de árboles de fallos o de los métodos de resolución existentes queda fuera del alcance de este libro, donde nos limitaremos a una breve ampliación de lo ya visto en cuanto a las bases de la aplicación del método. Quienes requieran una mayor profundidad en la exposición pueden dirigirse a textos más especializados (5), (9), (10), (11), (12).

Un árbol de fallos es una representación lógica de las secuencias de acontecimientos que pueden llevar a un suceso arbitrariamente elegido como «suceso culminante». Cuando todas las secuencias razonables se han identificado y el árbol está bien construido, el análisis FTA es posiblemente la herramienta más poderosa para la cuantificación de riesgos. Por otro lado, las situaciones a analizar a menudo son complejas, lo que puede llevar a errores en la construcción y aplicación del árbol de fallos. Los errores de análisis más frecuentes son de naturaleza cualitativa, y suelen provenir de las siguientes causas (3):

— El sistema al que se aplica el análisis no se comprende bien por parte de los analistas (comprensión del funcionamiento físico del sistema, de sus mecanismos de fallo, etc.). Esto lleva frecuentemente a omitir secuencias de sucesos importantes (debe recordarse siempre que no existe ningún método que garantice que todos los casos razonables se han tomado en cuenta) o a construir secuencias erróneas.
— Se producen fallos lógicos en la descripción de los fallos del sistema, lo que lleva a evaluaciones cuantitativas incorrectas.
— Los fenómenos de fallos por causa común no se comprenden bien, o se tienen en cuenta incorrectamente.

El árbol de fallos consiste en varios niveles de sucesos, conectados por puertas lógicas, habitualmente puertas *Y* o puertas O. Las citadas conexiones lógicas suelen representarse utilizando el álgebra de Boole. Las reglas de más frecuente aplicación al análisis de árbol de fallos se muestran en la tabla 6.2. Al construir un árbol de fallos los sucesos suelen identificarse con letras y/o números. La negación de un suceso (suceso complementario) se representa con la letra de ese suceso y un asterisco, o bien con una barra encima.

En cuanto a *fallos de equipos* se distinguen tres clases que pueden describirse usando el análisis FTA (13):

— *Fallos primarios,* son aquellos que ocurren cuando se opera en las condiciones para las que el equipo teóricamente ha sido diseñado. Son atribuibles al equipo, y no a condiciones externas. Un ejemplo es el caso del recipiente que no soporta la presión de trabajo, aunque ésta no ha superado la presión de diseño.

Tabla 6.2. Reglas booleanas de uso frecuente en el análisis de árboles de fallos

Commutativa:

$$AB = BA$$
$$A + B = B + A$$

Asociativa:

$$A(BC) = (AB)C$$
$$A + (B + C) = (A + B) + C$$

Distributiva:

$$A(B + C) = AB + AC$$
$$A + BC = (A + B)(A + C)$$

Otras:

$AA = A$	$A + A = A$
$A(A + B) = A$	$A + AB = A$
$AA^* = 0$	$A + A^* = 1$
$0A = 0$	$0 + A = A$
$1A = A$	$1 + A = 1$
$(A^*)^* = A$	

NOTA: En la nomenclatura empleada, AB corresponde a «Suceso A y Suceso B», A^* es el complementario del Suceso A, $A + B$ corresponde a «Suceso A o Suceso B», etc.

— *Fallos secundarios,* son los que se producen en condiciones para las que el equipo no ha sido diseñado. Por ejemplo, un recipiente explosiona porque una perturbación externa hace que la presión en su interior exceda a la de diseño. El fallo no es atribuible al equipo, sino a las perturbaciones excesivas en las condiciones de operación.

— *Fallos de control,* son aquellos en los que el equipo cumple su función, pero en un instante equivocado, o en una localización distinta de la que estaba prevista. El fallo tampoco es atribuible al equipo, sino a la señal que recibe (o no recibe). Por ejemplo, si una alarma de alta temperatura falla y no señala una temperatura por encima del nivel de alarma (fallo de control) es porque el sensor de temperatura ha fallado previamente (fallo primario).

En un árbol de fallos normalmente los fallos primarios están en los extremos de las «ramas» del árbol, mientras que los fallos secundarios y de control son eventos intermedios, unidos a los anteriores y entre sí mediante puertas lógicas. Otros fallos no relacionados en principio con el equipo, como sucesos externos y errores humanos, suelen ocupar también niveles primarios.

Un árbol de fallos siempre puede describirse con una expresión equivalente del álgebra de Boole. Así, para una puerta O con dos entradas A y B, la salida tiene un valor igual a $A + B - AB$, y si las entradas son A, B y C, la salida es $A + B + C - AB - AC - BC + ABC$. Como se ha indicado en el capítulo 2, cuando las frecuencias o probabilidades asignadas a los sucesos A, B, etc., son bajas, es habitual despreciar los términos producto, y expresar la salida como la suma de los términos individuales.

Una parte importante del análisis FTA es la identificación de las agrupaciones de sucesos que pueden dar origen al evento culminante. Estas agrupaciones se denominan «conjuntos de separación» (*cut sets*). Por lo general, los conjuntos de separación identificados son susceptibles de manipulación con el fin de simplificarlos, reduciéndolos a una serie equivalente con un número menor de conjuntos que se denominan «conjuntos mínimos» (*minimal cut sets*). Un conjunto mínimo es aquel que no contiene otros conjuntos. Frecuentemente la reducción se lleva a cabo utilizando programas de cálculo, pero también puede realizarse de forma manual en casos relativamente sencillos, como se muestra en el ejemplo siguiente tomado del trabajo de Schreiber (14).

Ejemplo 6.4:

Tras el estudio de un sistema se ha elaborado el árbol de fallos que se muestra en la figura 6.7a. Obtener la expresión booleana que representa el árbol de fallos, obtener la expresión reducida y representar el árbol de fallos equivalente.

En la figura puede verse que el mismo suceso (B) aparece en distintas ramas del árbol que se unen en una puerta Y. Cuando esto sucede, es necesario reestructurar el árbol, de manera que los fallos comunes puedan tratarse adecuadamente. De lo contrario, las evaluaciones que se deriven del árbol pueden contener fallos importantes.

Ejemplo 6.4 (continuación):

De acuerdo con las reglas ya expuestas podemos escribir:

$T = [(A + B)\ C][DB + (B + E)]$

$T = [AC + BC][B + E]$, ya que DB + B = B.

$T = ABC + ACE + BCB + BCE$

$T = ACB + ACE + BC + BCE$, ya que $BC \cap B = BC$.

Puesto que $ACB \subset BC$ y $BCE \subset BC$, podemos escribir

$T = ACE + BC = C\ [AE + B]$

El árbol de fallos reducido que corresponde a esta expresión se muestra en la figura 6.7b, en la que ya no aparece ningún suceso común en las diferentes ramas. Los conjuntos mínimos para este caso son las agrupaciones de sucesos (*A*, *C*, *E*) y (*B*, C), respectivamente.

Jerarquización de conjuntos mínimos

La jerarquización de los conjuntos mínimos identificados suele ser el paso final en el análisis FTA. Para una jerarquización *cualitativa* basta considerar dos tipos de factores (13):

i) importancia estructural, basada en el número de sucesos básicos en cada uno de los conjuntos mínimos. Desde este punto de vista, un conjunto unitario (un solo suceso) es más importante que uno que contenga dos, y éste que otro que incluya tres, etc. La base consiste en que, a igualdad de otras condiciones, un camino hacia el evento culminante que involucre un solo acontecimiento es más probable que otro que implique dos, éste que otro que implique tres, y así sucesivamente.

ii) El segundo factor considera la jerarquización dentro del grupo de conjuntos de un tamaño determinado, teniendo en cuenta el tipo de sucesos involucrados. La regla en este caso es: Primero errores humanos, segundo errores debidos a fallos de equipos activos (que están en funcionamiento activo) y tercero errores debidos a fallos de equipos pasivos

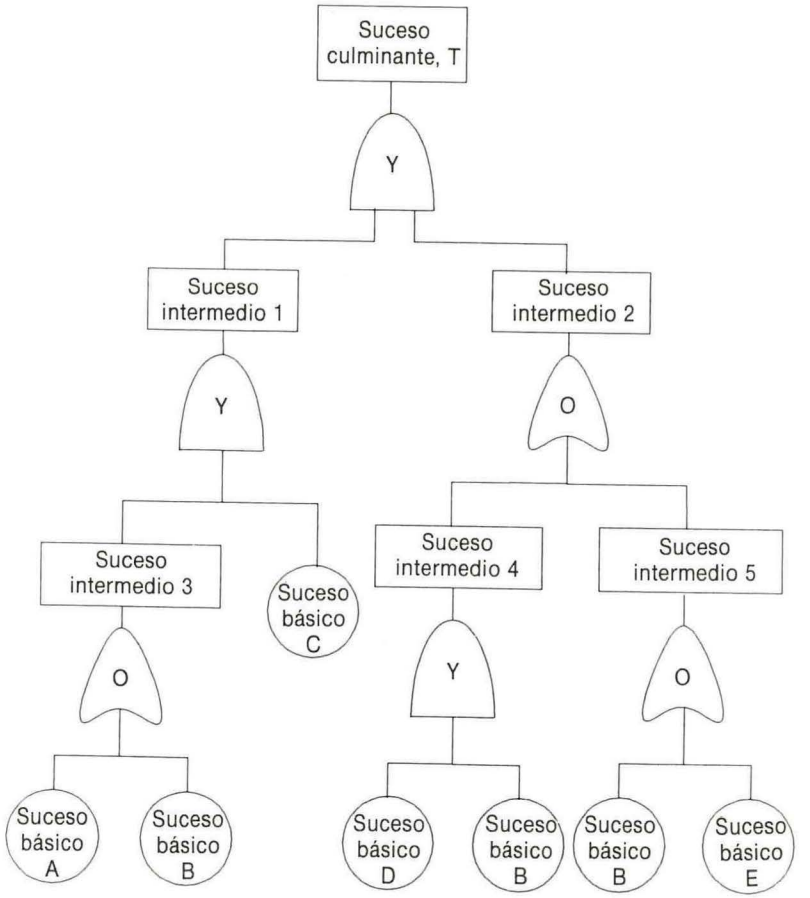

Figura 6.7a. *Diagrama inicial de árbol de fallos para el ejemplo 6.4.*

(estáticos, como una tubería o un tanque de almacenamiento). De nuevo, esta jerarquización se basa en la consideración de que un error humano es más probable que el de un equipo activo, y el de éste más probable que el de uno pasivo. Así, dentro de los conjuntos mínimo de tamaño 2 (dos sucesos), uno que involucre un error humano y otro de un equipo (activo o pasivo) será más importante que, por ejemplo, otro que involucre dos errores de equipos activos.

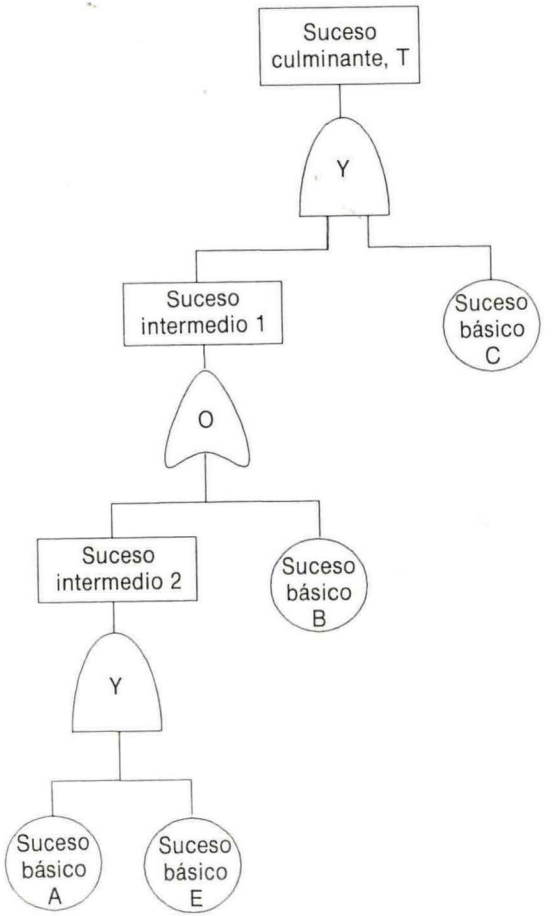

Figura 6.7b. *Diagrama del árbol de fallos reducido para el ejemplo 6.4.*

Por supuesto, la jerarquización anterior sólo proporciona una orientación de tipo general y puede modificarse en casos particulares, dependiendo del tipo y calidad del equipo involucrado, la política de mantenimiento, el entrenamiento de los operadores, etc. Al final, la jerarquía de sucesos más probables se establece tomando como base, sobre todo, la experiencia del personal que maneja la planta. Además, hay que tener en cuenta que las probabilidades y frecuencias de fallo difieren gran-

demente de unos equipos (activos o pasivos) a otros, como se puede ver en los ejemplos mostrados en la figura 6.4, por lo que también habrá que realizar una jerarquización *cuantitativa* de los conjuntos mínimos.

El siguiente ejemplo, tomado de la bibliografía (13), muestra el desarrollo de un árbol de fallos, así como la obtención y jerarquización de los conjuntos mínimos correspondientes, para un caso concreto que involucra un reactor continuo en el que existe la posibilidad de reacción fuera de control.

Ejemplo 6.5:

Una reacción con problemas importantes de estabilidad se está llevando a cabo en el reactor que se muestra en la figura 6.8. El sistema es sensible a pequeños aumentos de temperatura, y, por lo tanto, se ha provisto de un sistema de extinción de la reacción (quench) *para protegerlo en caso de pérdida de control de la reacción. La temperatura del reactor es continuamente monitorizada por dos sensores de temperatura* T1 *y* T2. *La válvula que abre el paso al fluido de extinción se activa automáticamente cuando* T1 *detecta un aumento determinado de temperatura. Independientemente,* T2 *activa una alarma en la sala de control para alertar al operador sobre la posible pérdida de control de la reacción. Cuando la alarma suena, el operador debe apretar el botón que cierra la válvula* V-1, *cortando el paso a la alimentación. Asimismo, en el caso de que el sensor* T1 *falle, al oír la alarma el operador también está instruido para oprimir el botón que abre la válvula del fluido de extinción. Tanto si la válvula* V-2 *abre como si la* V-1 *cierra, un cruzamiento de señales* (interlock) *activa una parada de emergencia estable, sin daño para el sistema. Realizar un análisis de árbol de fallos para este sistema, teniendo como evento culminante «daño al reactor debido a una temperatura excesiva».*

NOTA: En las consideraciones previas a la realización del análisis FTA el equipo de analistas acuerda no tomar en consideración sucesos como fallo de suministro eléctrico, fallos en los botones de apertura y cierre de las válvulas o fallos del cableado eléctrico, que se tendrán en cuenta en otros análisis posteriores. Asimismo, el análisis se limita al equipo incluido en los límites del

Ejemplo 6.5 (continuación):

digrama de la figura 6.8, sin considerar sistemas corriente arriba o corriente abajo del mismo. El estado normal del sistema es con la válvula V-*1 abierta y* V-*2 cerrada.*

El árbol de fallos (ver figura 6.9) se comienza de la forma habitual, buscando los acontecimientos que, de manera directa, pueden dar origen al suceso culminante T. En este caso se requiere que no se produzca la descarga del agente de extinción y además que la válvula V-1 no se cierre a tiempo, ya que en los supuestos del análisis cualquiera de las dos acciones impediría el evento culminante. A partir de aquí se continúa desarrollando cada una de las ramas del árbol como se indica en la figura. Nótese que el suceso A se ha identificado con un rombo, indicando que no se desarrolla más, aunque podría hacerse (obviamente puede haber muchas causas razonables para que el tanque del fluido de extinción se encuentre vacío).

La expresión que representa el árbol de fallos es:

$$T = (A + B + C[D + E + H])(F + G + E + H)$$

Operando y simplificando, teniendo en cuenta que $CHH = CH$, $CEE = CE$, $CDH \subset CD$, $CEG \subset CE$, etc., se tiene que

$$T = AE + AF + AG + AH + BE + BF + BG + BH + CE + CH + CDF + CDG$$

Por tanto, puede establecerse la siguiente jerarquización cualitativa:

Teniendo en cuenta la importancia estructural distinguimos conjuntos binarios: AE, AF, AG, AH, BE, BF, BG, BH, CE, CH y conjuntos terciarios: CDF, CDG. Dentro de cada uno de estos grupos podemos establecer una jerarquía atendiendo al tipo de fallo. Así, para los binarios el orden será (suponiendo que el suceso no desarrollado A se debe a un fallo humano):

AG (dos fallos humanos), AH (fallo humano y fallo del sensor de temperatura, que es un equipo activo), $AF = AE = BG$

Ejemplo 6.5 (continuación):

(en los tres casos se conjuga un fallo humano y un fallo de un equipo activo), $CH = BH = CE = BE = BF$ (fallo en dos equipos activos). Nótese que si se hubiera supuesto que el suceso no desarrollado A fuese clasificable como un fallo pasivo (por ejemplo, si la causa de que el tanque esté vacío fuera una perforación en el tanque, equipo pasivo), la jerarquización cambiaría considerablemente.

Para los terciarios:

CDG (dos fallos humanos, un fallo de equipo activo), CDF (un fallo humano, dos fallos de equipos activos).

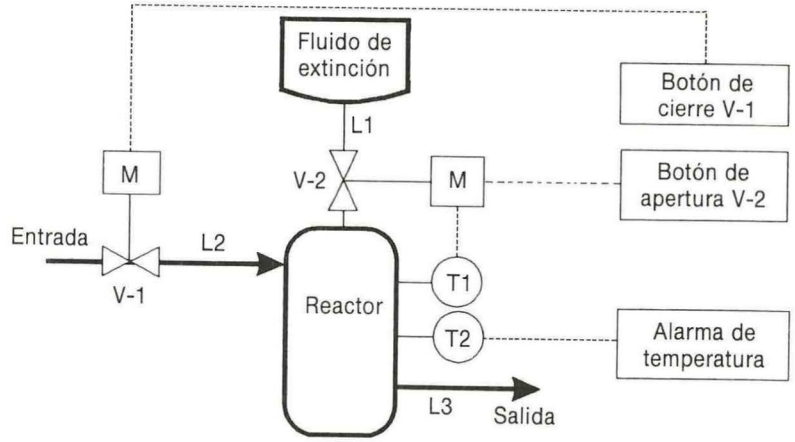

Figura 6.8. *Esquema del reactor utilizado en el ejemplo 6.5.*

Errores humanos y fiabilidad humana

En la sección anterior se ha hecho referencia repetidas veces a los *fallos humanos* o *errores humanos* sin definirlos y sin entrar en consideraciones sobre sus características o los factores que influyen en la frecuencia con que se producen. Sin embargo, su importancia desde el

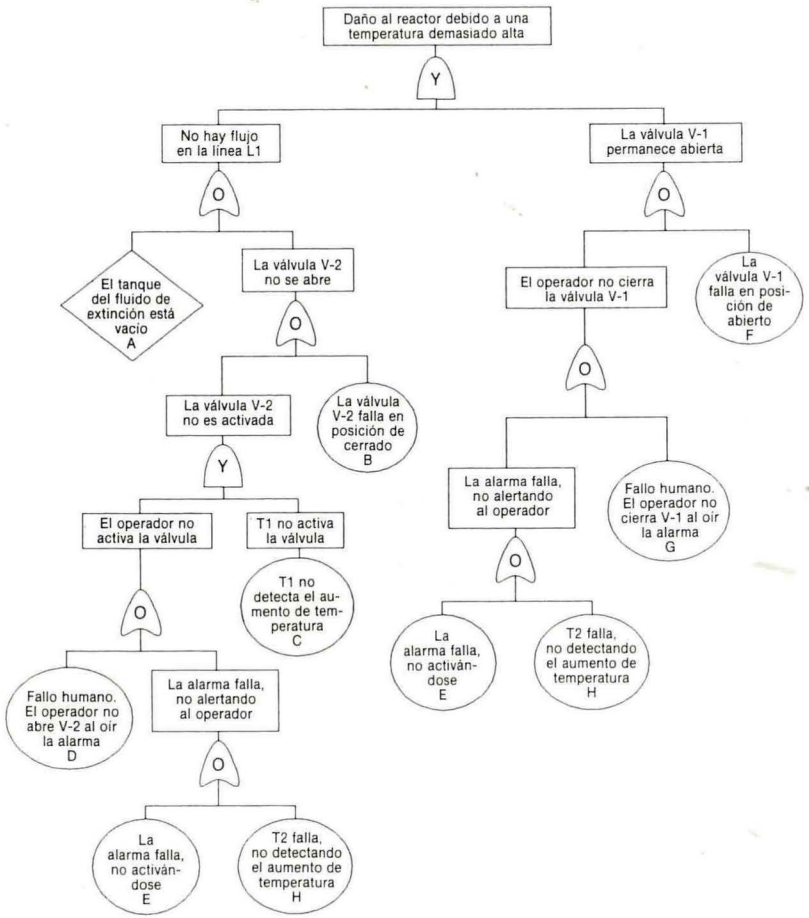

Figura 6.9. *Árbol de fallos para el ejemplo 6.5.*

punto de vista de la seguridad es enorme, estimándose que son directamente responsables de más de la mitad de los incidentes y accidentes industriales de los que existe registro (15). Por tanto, resulta útil realizar aquí algunas reflexiones sobre la naturaleza de los fallos humanos y sobre los métodos que suelen emplearse para estimar la frecuencia o probabilidad con que pueden tener lugar.

De manera similar al fallo de un componente, un error humano suele definirse como una acción, realizada por una persona, que rebasa los límites de aceptabilidad definidos para un sistema. La acción puede ser simple (accionar el botón de arranque de una bomba) o compleja (realizar un análisis de la respuesta del sistema y tomar una decisión basada en el mismo).

Como ya se ha señalado, desde un punto de vista general puede considerarse que todos los accidentes son causados por fallos humanos, ya que si un equipo falla es debido a un diseño inadecuado, a un fallo de construcción, a una instalación incorrecta, a su uso en condiciones inapropiadas, a un mantenimiento incorrecto, etc. Centrando el análisis únicamente en fallos debidos a acciones próximas, realizadas directamente por personas, Kletz (16) proporciona la siguiente clasificación para los errores humanos:

— Errores debidos a una distracción momentánea. En este caso la intención del operador es correcta, pero a pesar de ello la acción es incorrecta. Es el caso del operario que conoce su trabajo y pone atención para realizarlo correctamente, pero, a pesar de ello, de vez en cuando se confunde al oprimir un interruptor o lo hace demasiado tarde, etc.
— Errores que provienen de un adiestramiento insuficiente o de instrucciones deficientes. El operador no sabe qué hacer, o incluso peor, cree que sabe pero no es así, lo que le lleva a cometer errores importantes. Es el caso del operador de un reactor a quien no se le ha instruido adecuadamente sobre el comportamiento del sistema. Un día, la velocidad de la reacción resulta ser demasiado baja y, al inspeccionar el equipo, descubre que durante el arranque del reactor ha olvidado poner en funcionamiento el agitador, lo que le lleva a tomar inmediatamente la decisión de conectarlo, aunque ya se encuentra a la temperatura de reacción. La mezcla súbita de reactantes provoca un aumento brusco de la velocidad de reacción, lo que lleva a la explosión del reactor.
— Errores debidos a falta de capacidades físicas o mentales por parte del operador para hacer frente a una situación determinada. Ejemplos de esto son la válvula manual que se ha atascado de forma que el operador no posee la fuerza suficiente para hacerla funcionar, o el caso del trabajador de la sala de control sobrecargado con la supervisión de demasiados equipos.

— Errores debidos a la falta de motivación, o a la decisión deliberada de no seguir ciertas instrucciones. Evidentemente en algunos casos un acto de este tipo podría clasificarse como sabotaje industrial, pero en otras ocasiones el operario puede creer sinceramente que es mejor no seguir las instrucciones en unas circunstancias determinadas.
— Errores atribuibles a políticas erróneas de la dirección de la compañía. Entrarían dentro de este grupo las políticas laxas en cuanto a permisos de trabajo para «agilizar» las reparaciones, instalación de equipo de menor fiabilidad o reducción de medidas de seguridad para ahorrar costes, sistemas de trabajo que impongan una presión excesiva sobre los operarios, procedimientos de investigación de accidentes/incidentes que ponen el énfasis en la búsqueda de responsables, etc.

No existe una clara delimitación entre los grupos anteriores, y a menudo más de una de las circunstancias mencionadas contribuye a un accidente. Incluso en el caso de los accidentes debidos a distracciones por parte del operario, a menudo podría haberse mejorado el diseño del equipo de forma que tales errores no pudiesen tener lugar. Los siguientes ejemplos, tomados del trabajo del Kletz (16), ilustran esta posibilidad.

Ejemplo 6.6:

Muchos de los accidentes de aviación que han tenido lugar han sido debidos a un fallo humano del piloto, que acciona un mando equivocadamente. Por ejemplo, los reactores actuales están equipados con alerones de aterrizaje, fijados a la parte superior de las alas. Los alerones se levantan después del aterrizaje, a fin de reducir el empuje ascendente. Si por error se levantan antes del aterrizaje se produce un descenso brusco del avión. En un DC-8 el piloto tiene dos alternativas: i) levantar *una palanca antes del aterrizaje para armar los alerones que, una vez armados, se levantan automáticamente tras el aterrizaje, o bien,* ii) *esperar a que se produzca el aterrizaje y* tirar hacia fuera *de la misma palanca.*

Ejemplo 6.6 (continuación):

Un día el piloto tiró hacia fuera *de la palanca antes del aterrizaje. El resultado fue la muerte de 109 personas. La reacción de la Autoridad Federal de Aviación de los Estados Unidos fue sugerir que se pusiera un letrero en el tablero de mandos, junto a la palanca del alerón, con la inscripción «Está prohibido levantar los alerones durante el vuelo.» Igual resultado hubiese dado escribir «Hagan el favor de no estrellar este avión.» El accidente no fue, en última instancia, atribuible al piloto, sino a un diseño defectuoso. Era inevitable que antes o después alguien cometiese un error con la palanca.*

El fabricante del avión no tomó en principio ninguna iniciativa. Sólo después de que dos o quizá tres aviones más hubieran tenido el mismo accidente decidieron instalar un dispositivo que impedía que los alerones de aterrizaje pudieran levantarse antes de que el avión hubiese tocado el suelo.

Ejemplo 6.7:

*El reactor discontinuo de la figura 6.10 se utiliza para llevar a cabo una reacción a presión. Al terminar la reacción, la presión se reducía y el producto se descargaba en un tanque apropiado. Para impedir que la descarga se produjese antes de tiempo, se dispuso un sistema de protección que, mediante un cruzamiento de señales (*interlock*), impedía la apertura de la válvula de descarga mientras la presión manométrica en el interior del reactor fuese superior a 0,3 bares.*

En una de las operaciones del reactor se decidió parar la reacción, que no estaba procediendo adecuadamente, y para ello se comenzó por reducir la presión a través de la válvula de venteo. Por descuido del operador, el actuador remoto de la válvula de descarga se había dejado en posición abierto, y la válvula de drenaje también estaba abierta, de manera que en cuanto la presión descendió por debajo de 0,3 bares se produjo una descarga de los productos inflamables del reactor en el área de trabajo.

Ejemplo 6.7 (continuación):

Evidentemente, en este caso un fallo humano del operador fue la causa directa de la descarga. Sin embargo, el accidente podría haberse impedido con un sistema de protección mejor diseñado. En este caso, un análisis HAZOP hubiera sido muy útil para poner de manifiesto los defectos del sistema.

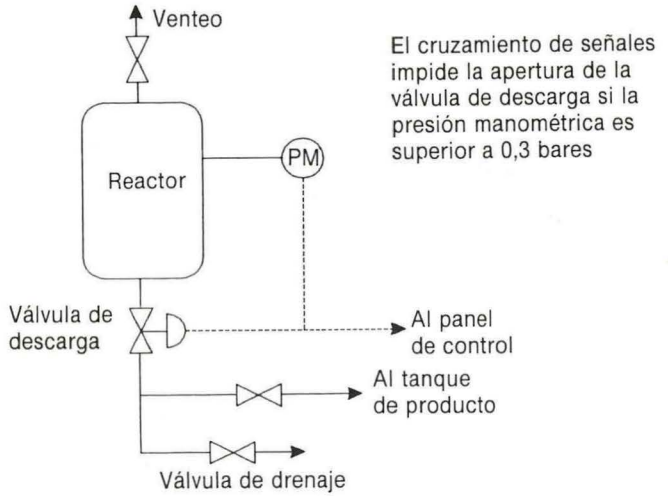

Figura 6.10. *Disposición de las válvulas para el reactor del ejemplo 6.7.*

Los ejemplos anteriores muestran la dificultad de catalogar un accidente dentro de la categoría de fallos humanos, incluso en un caso simple como es el de accidentes debidos a descuidos del operador. A pesar de ello, en determinadas circunstancias (aquellas que corresponden a las situaciones más sencillas, donde el proceso decisión-acción se realiza sobre un número limitado de alternativas) sí existen mediciones que proporcionan una idea aproximada de la probabilidad de fallo. En la tabla 6.3 se presentan, a título de ejemplo, algunas estimaciones tomadas de la bibliografía.

En otras ocasiones se ha seguido una aproximación más estructurada, capaz de individualizar hasta cierto punto las características de cada

Tabla 6.3. Algunas estimaciones de errores humanos para tareas simples. [Seleccionadas entre las recogidas en la referencia (16).]

Probabilidad	Acción del operador
0,04	No observa el indicador, o lo observa pero no emprende ninguna acción, aunque debería hacerlo.
0,03	No percibe la alarma, o la percibe pero no emprende ninguna acción, aunque debería hacerlo.
0,001	No bloquea una tubería, como estaba previsto en una parada planificada.
0,005	No bloquea una tubería, como estaba previsto en una parada de emergencia.
0,0025	Se equivoca al accionar las válvulas cuando se intercambia un conjunto de dos bombas (se para la que está funcionando, se arranca la que estaba en espera).
0,01	Para manual de una bomba sin tomar acciones para bloquear la tubería.
0,003	Error general de comisión (por ejemplo, leer equivocadamente un rótulo y como consecuencia seleccionar el interruptor equivocado).
0,01	Error general de omisión cuando no existe indicación en el cuarto de control del estado del elemento afectado (por ejemplo, olvidar poner otra vez una válvula en la configuración apropiada después de haber realizado trabajos de mantenimiento).
0,003	Error general de omisión cuando el paso omitido está incluido dentro de un procedimiento en lugar de al final, como ocurría en el caso anterior.
0,03	Errores de operaciones aritméticas simples, realizadas manualmente y comprobadas rutinariamente, sin repetir el cálculo en otro papel.
$\cong$ 1,0	El operador no toma la decisión correcta, durante los primeros sesenta segundos en una situación de muy alto estrés.
0,9	El operador no toma la decisión correcta, durante los primeros cinco minutos en una situación de muy alto estrés.
0,1	El operador no toma la decisión correcta, durante los primeros treinta minutos en una situación de alto estrés.

tarea. Es el caso del trabajo de Bello y Columbiori (17), quienes propusieron un método para tener en cuenta los factores que influyen en el proceso que lleva a la comisión de errores. La probabilidad del error se estima en este caso como el producto de los factores $K1$ a $K5$ de la tabla 6.4. Los valores numéricos de la tabla son orientativos, y en ocasiones han de modificarse para atender a circunstancias concretas. Así, por ejemplo, el estrés no siempre es un factor que conduzca al aumento en la probabilidad de error. Swain y Guttman (18) consideran que existe un nivel de estrés óptimo que corresponde a valores de estrés moderados. Por encima de este nivel, la fiabilidad humana disminuye a causa de la acumulación de tensión, pero también lo hace si el nivel se rebaja demasiado, desembocando en una tarea monótona.

En todo caso, la realización de análisis de fiabilidad humana más allá de la asignación de valores puramente orientativos es habitualmente

Tabla 6.4. Parámetros de probabilidad de error utilizados en el método Teseo (17)

TIPO DE ACTIVIDAD	K1
Rutinaria, simple	0,001
Rutinaria, requiere atención	0,01
No rutinaria	0,1
FACTOR DE ESTRÉS TEMPORAL (tareas rutinarias)	**K2**
Tiempo disponible: 2 segundos	10
Tiempo disponible: 10 segundos	1
Tiempo disponible: 20 segundos	0,5
FACTOR DE ESTRÉS TEMPORAL (tareas no rutinarias)	**K2**
Tiempo disponible: 3 segundos	10
Tiempo disponible: 30 segundos	1
Tiempo disponible: 45 segundos	0,3
Tiempo disponible: 60 segundos	0,1
CARACTERÍSTICAS DEL OPERADOR	**K3**
Bien seleccionado y adiestrado, experto	0,5
Conocimiento y adiestramiento promedios	1
Escaso conocimiento, adiestramiento deficiente	3

Tabla 6.4. (Continuación)

FACTOR DE ANSIEDAD EN LA ACTIVIDAD REALIZADA	K4
Situación de grave emergencia	3
Situación de emergencia potencial	2
Situación normal	1
FACTOR ERGONÓMICO EN LA ACTIVIDAD REALIZADA	**K5**
Microclima excelente, muy buena interfase con la planta	0,7
Buen microclima, buena interfase con la planta	1
Microclima aceptable, interfase con la planta aceptable	3
Microclima aceptable, interfase con la planta deficiente	7
Microclima en malas condiciones, interfase con la planta deficiente	10

trabajo para especialistas. El CCPS (3) señala un procedimiento de 12 etapas a seguir por los analistas: *i)* Familiarización con la operación de la planta, controles, etc. *ii)* Examen del árbol de fallos para identificar los fallos humanos que puedan conducir al evento culminante. *iii)* Diálogo con el personal implicado para lograr la familiarización con los procedimientos relevantes. *iv)* Análisis de tareas, que involucra la descomposición de las mismas en acciones discretas. *v)* Expresión de las acciones secuencialmente, como ramas binarias de un árbol de sucesos, con cada rama expresando acierto o fallo del operador. *vi)* Asignación de probabilidades de fallo humano a las acciones anteriores. *vii)* Modificación, en su caso de las probabilidades anteriores por las circunstancias particulares de la operación. *viii)* Modificación, en su caso de las probabilidades anteriores por la dependencia entre las distintas tareas a realizar. *ix)* Cálculo de la probabilidad global de acierto o fallo. *x)* Inclusión de los efectos de factores de recuperación, que tienen en cuenta el hecho de que los operadores pueden darse cuenta de los fallos y corregirlos. *xi)* Realización, en su caso, de un análisis de sensibilidad paramétrica. *xii)* Suministrar la información adecuada al equipo que desarrolla el análisis FTA.

Hay que tener en cuenta además que, en la industria moderna, la automatización ha eliminado gran parte de las tareas humanas de tipo repetitivo, de manera que el papel de los operadores se dirige cada vez más a la supervisión, y a la toma de decisiones a medida que surgen problemas que no se resuelven automáticamente. El análisis en estos

casos involucra el procesado de información en varios niveles: diagnóstico de la situación, evaluación de objetivos, establecimiento de prioridades y planificación.

Cuando un operador se enfrenta a una situación anormal, para la que no hay previsto un tratamiento rutinario, está desarrollando, en un tiempo a menudo fuertemente limitado, un procedimiento para tratar dicha situación. Dependiendo de su conocimiento de las respuestas del sistema tomará decisiones y emprenderá acciones más o menos acertadas, que son en realidad *experimentos* en tiempo real. A la vista del resultado de los mismos persistirá en el curso de operación iniciado o intentará otras alternativas. De esta manera, los errores son, inevitablemente, parte del mecanismo de aprendizaje cuando se confrontan situaciones nuevas, y ciertas acciones que cuando se juzgan en retrospectiva se clasifican como errores, son en realidad intentos razonables de obtener información acerca del estado de los acontecimientos y su posible evolución. Así, según Rasmussen (19), en situaciones complejas sería más apropiado considerar a los errores humanos como «experimentos sin éxito en un ambiente hostil», y concentrar los esfuerzos de diseño en el desarrollo de sistemas capaces de tolerar el error humano. En este tipo de sistemas los errores deben producir resultados observables, y la respuesta del sistema debe ser tal que los errores puedan corregirse antes de que se produzcan consecuencias inaceptables. En otras palabras, no es posible cambiar la naturaleza de las personas para que disminuyan sus errores más allá de cierto límite, pero sí podemos concebir diseños en los que los errores humanos se produzcan con menos frecuencia, o tengan resultados menos perjudiciales. También es necesario asistir al operador en la toma de decisiones en situaciones no programadas. A este respecto se han desarrollado sistemas expertos capaces de llevar a cabo esta misión, indicando al supervisor en la sala de control el aumento del factor de riesgo que ocurre a medida que se van produciendo nuevos acontecimientos, como, por ejemplo, el fallo secuencial o simultáneo de equipos tras el fallo inicial de uno de ellos (20).

Consideración de agentes externos

Además de los fallos del equipo y los fallos humanos, de los que ya se ha hablado, la cuantificación del riesgo (ya sea por análisis FTA o por otro método) debe tomar en cuenta los riesgos debidos a agentes

externos, siempre que éstos sean relevantes. Por agentes externos se entienden todos aquellos que no tienen relación directa con el proceso que se lleva a cabo en la planta, pero que, sin embargo, son capaces de aumentar significativamente la probabilidad de un accidente en la misma. Entre éstos están el impacto de aviones, barcos o vehículos terrestres, las guerras y los ataques terroristas, el sabotaje de las instalaciones, las grandes perturbaciones de causa meteorológica (tormentas, inundaciones, huracanes, etc.), impactos de meteoritos, fuegos propagados desde el exterior, actividad sísmica, actividad volcánica, etc.

Aunque evidentemente la probabilidad de tales eventos es, por lo general, muy pequeña, tienen el potencial suficiente para causar accidentes importantes o al menos para iniciarlos, a menudo debido a fallos de causa común. El analista de riesgos debe, por tanto, decidir cuáles de ellos se incluyen en el análisis y cuáles no, justificando su decisión en ambos casos.

En general, el diseño de una instalación industrial se realiza de manera que resista un cierto nivel de los fenómenos anteriores. Así, el CCPS (3) cita como requisitos de diseño en los Estados Unidos para instalaciones de GLP que éstas sean capaces de resistir movimientos sísmicos con probabilidades anuales de hasta 10^{-4}, la peor inundación registrada en un período de cien años o la combinación más crítica intensidad del viento-duración que tenga una probabilidad de hasta 10^{-4}. En nuestro país, las normas y reglamentos aplicables imponen condiciones sobre resistencias al fuego, cimentación, calefacción para impedir la formación de hielo, etc., dependiendo del tipo de instalación (véase, por ejemplo, el Reglamento sobre Almacenamiento de Productos Químicos, el Reglamento sobre Gases Licuados del Petróleo, etc.).

La cuantificación de la probabilidad de los eventos externos es difícil, por la amplia variabilidad que existe dependiendo de la localización y características de los mismos. Así, la probabilidad de impacto de aeronaves varía a medida que nos acercamos a un aeropuerto, la de terremotos depende del nivel de actividad seísmica de una zona y la de guerras o ataques terroristas puede evolucionar considerablemente al variar la situación política en un país determinado. No obstante, existen estimaciones disponibles, a menudo con la precisión suficiente como para decidir la inclusión o no de un agente externo particular dentro del análisis de riesgos. Se dispone de estadísticas que proporcionan la probabilidad de impacto de aeronaves sobre un área determinada, re-

gistros meteorológicos con el historial de viento, temperaturas, precipitaciones, etc., así como estudios geológicos e historial de actividad sísmica (y volcánica en su caso), para la mayor parte de las localizaciones de interés industrial. A modo de orientación, las cifras de probabilidad que se citan para el impacto de un avión en una planta a lo largo de un año son del orden de 10^{-6} o 10^{-7}, dependiendo de la localización (2), (4), y para impacto de un meteorito o de un rayo, del orden de 10^{-11} y 10^{-7}, respectivamente.

Incertidumbre en los datos y sensibilidad paramétrica

Cuando se realiza una búsqueda de datos sobre frecuencia de fallos para evaluar la fiabilidad de un equipo determinado se intenta, dentro de lo posible, seleccionar datos de componentes similares, trabajando en las mismas o parecidas condiciones. A menudo los datos que se encuentran son escasos o tienen gran dispersión, y como consecuencia se obtienen estimaciones de la probabilidad o de la frecuencia de fallos con amplios intervalos de variabilidad para un nivel de confianza determinado.

Este hecho ha sido utilizado en ocasiones como un argumento en contra de la realización de análisis de riesgos cuantitativos, con el argumento de que no vale la pena el esfuerzo, muy considerable, que implica un análisis de cierto rigor, si todo lo que va a obtenerse a cambio en una estimación de probabilidad que además tiene una incertidumbre elevada. Cabe señalar a este respecto que la escasez de datos no es una razón válida para rechazar la aproximación probabilística, sino todo lo contrario, y que, a pesar de la incertidumbre en los datos con que a menudo debe enfrentarse el analista de riesgos, la mayor parte de las estimaciones de fiabilidad de sistemas se encuentran dentro de un factor de 2 con respecto a los valores reales (21). Esto se debe en parte al hecho de que, a menudo, la frecuencia o probabilidad del evento culminante en un árbol de fallos viene determinada fundamentalmente por los valores de la frecuencia o probabilidad de un grupo reducido de sucesos. Esto implica que no se requiere gran exactitud en *todas* las estimaciones de verosimilitud de los diferentes sucesos, sino sólo en un grupo de valores que son los que tienen mayor influencia en el resultado final.

Realizando un *análisis de sensibilidad paramétrica* puede conocerse la influencia que la probabilidad de cada uno de los sucesos tiene en la probabilidad del evento culminante. Esto es interesante no sólo para saber dónde es necesario realizar un esfuerzo especial para aumentar la exactitud de los datos, sino sobre todo para poder concentrar los esfuerzos de reducción de riesgos en las áreas que proporcionan mayor eficacia en la reducción del riesgo global. Se define la sensibilidad paramétrica a la probabilidad de un suceso determinado j como

$$S_j = \Delta P_T / \Delta P_j \qquad [6.27]$$

es decir, como el cociente entre el cambio porcentual en la probabilidad del suceso culminante y el cambio porcentual en la probabilidad del suceso respecto del cual se realiza el estudio de sensibilidad paramétrica.

Ejemplo 6.8:

Determinar la sensibilidad paramétrica del suceso culminante del ejemplo 6.4 respecto de cada uno de los sucesos básicos involucrados, para un nivel de variación del 50 por 100, sabiendo que, para los sucesos A, B, C *y* E *se han estimado, respectivamente, probabilidades de 0,02, 0,0005, 0,02 y 0,0001.*

Según se ha mostrado en el ejemplo 6.4, la expresión booleana que representa el árbol de fallos es

$$T = C[AE + B]$$

por tanto, la probabilidad del evento culminante viene dada por $T = 1{,}004 \times 10^{-5}$. Para calcular la sensibilidad paramétrica suponemos que se aumenta en un determinado porcentaje (en este caso el 50 por 100) la probabilidad de cada uno de los sucesos anteriores, mientras los demás mantienen sus valores originales y calculamos la correspondiente probabilidad para el evento culminante. Las sensibilidades se calculan de acuerdo con la ecuación [6.27]. La siguiente tabla resume los cálculos:

Ejemplo 6.8 (continuación):

Parámetro que cambia	Valor inicial	Valor modificado	Nuevo valor de T	$\Delta P_T(\%)$	S_i
P_A	0,02	0,03	$1{,}006 \times 10^{-5}$	0,2	0,004
P_B	0,0005	0,00075	$1{,}504 \times 10^{-5}$	49,8	0,996
P_C	0,02	0,03	$1{,}506 \times 10^{-5}$	50	1,0
P_E	0,0001	0,00015	$1{,}006 \times 10^{-5}$	0,2	0,004

En este caso se observa que la sensibilidad a los valores de la probabilidad de los sucesos B y C es mucho mayor (unas 250 veces) que a la probabilidad de los sucesos A y E. Este resultado indica que los esfuerzos para mejorar la exactitud de las estimaciones de probabilidad hay que concentrarlos en los sucesos B y C, ya que A y E prácticamente no influyen sobre la probabilidad del suceso culminante (a pesar de que A tiene una probabilidad 40 veces superior a E). De igual manera, resultaría inútil invertir en reducir la probabilidad de A y E (colocando sistemas redundantes, etc.), mientras que sería beneficioso reducir la de B o C, que tienen una influencia directa en T.

Aceptabilidad del riesgo

El resultado final de un análisis de árbol de fallos es un valor de la probabilidad o frecuencia que cabe esperar para el suceso culminante. Este dato se combina con las estimaciones de consecuencias que se han discutido en los capítulos 3 a 5, lo que proporciona un valor para la esperanza matemática de pérdidas. Al final del análisis podemos tener un resultado con una estructura del tipo: «La aplicación del escenario B a la planta en estudio conduce a la explosión del reactor $R3$, con la liberación instantánea de sus contenidos. En estas condiciones existe un 60 por 100 de probabilidad de bajas humanas (el operario del reactor), y se esperan unas pérdidas económicas de aproximadamente 230 millones de pesetas. La frecuencia estimada para el escenario B es de $2{,}3 \times 10^{-3}$ años^{-1}, es decir, una vez cada 435 años.»

En principio los cálculos a efectuar en el análisis de riesgos terminan aquí, una vez establecido el intervalo de confianza para la cifra de frecuencia obtenida. La decisión de si el nivel de riesgo calculado es demasiado alto o si por el contrario puede considerarse aceptable (o más bien *tolerable*) requiere consideraciones que van más allá de los aspectos meramente técnicos. En el capítulo 1 se expusieron algunas de las dificultades que se suelen encontrarse a la hora de fijar niveles de riesgo tolerables. Los principales aspectos en la percepción de la tolerabilidad del riesgo se refieren a si éste es asumido voluntariamente o no por los sujetos pasivos, si los sujetos pasivos reciben beneficios por la asunción del riesgo, si los posibles efectos perjudiciales son inmediatos o retrasados en el tiempo y, en este último caso, si son detectables, si las consecuencias son reversibles o irreversibles y si el riesgo se conoce con precisión.

Puesto que la percepción del riesgo depende en gran parte de factores subjetivos parece imposible establecer niveles de tolerabilidad que puedan tener validez universal. De hecho, la susceptibilidad social hacia los riesgos industriales ha experimentado un fuerte incremento con el tiempo, y en la actualidad varía considerablemente de unos lugares a otros. A pesar de lo anterior, pueden realizarse algunas reflexiones que sirvan como referencia para la comparación de niveles de riesgo.

Riesgos que sólo involucran pérdidas materiales

Ya que es imposible la reducción del riesgo a nivel cero, cualquier empresa industrial debe protegerse contra las pérdidas económicas derivadas de accidentes. La forma más usual de transferencia de riesgo consiste en realizar un seguro. Éste puede ser un seguro tradicional, con una compañía de seguros establecida, o puede ser en la modalidad de auto-seguro. El trabajo de Natale (22) discute estas y otras formas de financiar el riesgo de accidentes. Hay que tener en cuenta no sólo el daño causado al equipo e instalaciones de la planta, sino los costes debidos a la interrupción de la producción y los derivados de la responsabilidad civil, que pueden ser muy cuantiosos, especialmente en los casos en que el accidente involucra daños a personas. Un ejemplo reciente de esta última situación es el accidente de Bhopal, tras el cual la compañía Union Carbide tuvo

que hacer frente a litigios por una demanda total de unos 3.000 millones de dólares.

Cuando sólo están en juego daños materiales, la combinación del concepto de seguro de accidentes y el análisis de riesgos permite establecer un criterio para decidir la tolerabilidad de un riesgo. Un riesgo no es aceptable si existen medios técnicos para reducirlo, cuya implantación sea beneficiosa desde el punto de vista de las primas del seguro necesario para cubrir las pérdidas previstas. Así, si en el estado actual de la instalación el coste de las primas del seguro sería de M pts./año y tras la instalación de las medidas de seguridad se reduce a N pts./año, el nivel de riesgo actual no es aceptable si el coste de las medidas de seguridad es igual o inferior a $(M - N)$ pts./año.

Un concepto similar está basado en el cálculo del coste promedio anual de un accidente. Supongamos que en el caso mencionado al principio de esta sección la probabilidad de pérdidas humanas fuese despreciable y el único peligro fuese la explosión del reactor con daños totales de 230 millones de pesetas, con una frecuencia estimada de una vez cada cuatrocientos treinta y cinco años. El coste promedio anual sería entonces de unas 529.000 pesetas. Supongamos que añadiendo un sistema redundante de seguridad las pérdidas totales se mantienen, pero la frecuencia del accidente se rebaja a una vez cada novecientos ochenta años. El coste anual promedio tras la instalación de las medidas de protección sería de unas 235.000 pesetas. La diferencia, 294.000 pts./año, es el ahorro obtenido tras la implantación de las medidas de seguridad. Por tanto, el riesgo en el nivel actual no es aceptable si el coste de las medidas es inferior a dicha cantidad.

Evidentemente ambos criterios son simplificados, y las cantidades mencionadas pueden corregirse teniendo en cuenta intereses, depreciación de los equipos y costes de mantenimiento de los mismos, descuentos por gastos futuros, bonificaciones adicionales por mejora de la imagen de la compañía, etc., pero proporcionan un orden de magnitud apropiado para centrar el problema. Sin embargo, el principal obstáculo a la instalación de medidas suplementarias de seguridad no radica en los cálculos económicos, que pueden sofisticarse cuanto sea necesario, sino en la inercia de quienes no perciben el coste económico de un accidente potencial como un *coste real,* porque «al fin y al cabo se trata de estimaciones aproximadas de riesgo», «puede que el accidente no ocurra nunca (durante la vida útil de la planta)» y «llevamos cinco años funcionando y no ha ocurrido nada».

Accidentes que involucran pérdidas humanas

Cuando existe una probabilidad significativa de pérdidas humanas la decisión sobre el nivel de riesgo tolerable se complica considerablemente. Kletz (2) sugiere utilizar el índice FAR, que es el número de accidentes mortales en un grupo de 1.000 trabajadores durante toda su vida laboral (aproximadamente 10^8 horas). Si aceptamos un FAR de 4 como representativo de las condiciones de la industria química, entonces el trabajador promedio está expuesto a un FAR de 2 como consecuencia de los riesgos derivados directamente del proceso en el que trabaja (la otra mitad del FAR proviene de la contribución de accidentes comunes a cualquier trabajo como caer por unas escaleras o ser atropellado por una carretilla elevadora). Kletz propone reducir prioritariamente todos aquellos riesgos derivados del proceso que ocasionen que algún trabajador esté expuesto a un valor FAR mayor que 2. Esto implica, como hipótesis de partida, que hemos identificado y evaluado todos los riesgos que concurren sobre todos los trabajadores. Si esto no es así, una actitud conservadora sería reducir cualquier riesgo individual de proceso que dé lugar a un valor FAR mayor que 0,4.

En cuanto a los *riesgos para el público en general,* parece razonable que las personas que no son trabajadores de la planta, y, por tanto, no conocen los riesgos involucrados ni los han aceptado voluntariamente, tengan derecho a que el riesgo añadido que soportan por causa de la instalación industrial sea considerablemente inferior al de aquellos que trabajan en la misma.

De nuevo siguiendo a Kletz (2), la frecuencia de accidentes mortales para el público en general (es decir, de fuera de la planta), a causa de las actividades de una instalación industrial determinada, debe ser inferior a un nivel de 10^{-7} años^{-1}. Se llega a esta cifra a partir de varias consideraciones: por ejemplo, el riesgo *global* de muerte para un hombre joven, considerando todas las causas posibles, es de aproximadamente 10^{-3} años^{-1}. Un riesgo industrial adicional de muerte para el público en general del orden de 10^{-7} años^{-1} supone un aumento de 0,01 por 100 en el riesgo al que ya está expuesto, lo que ciertamente está muy por debajo del nivel de incertidumbre en la estimación del valor de 10^{-3} años^{-1} antes citado. Por otro lado, un valor de 10^{-7} años^{-1} es del orden del que se atribuye a sucesos extremadamente improbables, del tipo de que alguien sea herido por un rayo, o de que se produzcan muertes a personas *sobre el terreno* a causa de que un avión se estrelle, y es cier-

tamente mucho menor que el de otros riesgos que se asumen voluntariamente (por ejemplo, unas 1.000 veces menor que la probabilidad de morir en accidente de circulación o unas 40.000 veces menor que el riesgo asumido voluntariamente por los escaladores).

Ejemplo 6.9:

Aplicar el criterio propuesto por Kletz para determinar si el riesgo de muerte en el caso discutido al principio de esta sección puede considerarse aceptable.

Según se indica al comienzo de esta sección existe un escenario con una frecuencia estimada de $2{,}3 \times 10^{-3}$ años^{-1} en el que existe una posibilidad del 60 por 100 de que se produzca alguna baja humana. Esto nos proporciona una frecuencia estimada de bajas humanas de $1{,}38 \times 10^{-3}$ años^{-1}. Los años laborales considerados en el cálculo del FAR tienen $50 \times 40 = 2.000$ horas, por tanto, la frecuencia estimada expresada en ocasiones/hora sería de $6{,}9 \times 10^{-7}$ horas^{-1}. En 10^8 horas el FAR es de 69, es decir, unas 172 veces mayor que el valor recomendado de 0,4.

Hay que tener en cuenta que al aplicar este criterio debe considerarse siempre al trabajador expuesto al mayor riesgo, no el riesgo promedio de los trabajadores de la planta. Como hace notar Kletz (2), de poco consuelo serviría decir a un operario «no te preocupes, tu riesgo particular es alto, pero el promedio para ti y tus compañeros es aceptable».

Cuestiones y problemas

6.1. *i)* Discutir las ventajas e inconvenientes de utilizar una distribución de Weibull en lugar de una exponencial. *ii)* Suponer que la tasa de fallos de un equipo viene dada por la distribución de Weibull, con $\upsilon = 3 \times 10^{-5}\text{h}^{-1}$ y $\alpha = 1{,}30$. ¿Cuál es la fiabilidad al cabo de 4.000 horas de funcionamiento? *iii)* ¿Cuál sería la tasa de fallos de una distribución exponencial que proporcionase la misma fiabilidad a ese tiempo? *iv)* ¿Cual sería la fiabilidad en los casos *ii)* e *iii)* anteriores para $t = 6.000$ horas? *v)* Reflexionar acerca de las relaciones entre los parámetros de ambas distribuciones.

6.2. La señal de salida de un analizador de gases en línea se utiliza para iniciar la parada de emergencia de un reactor en el caso de que se detecten concentraciones en un nivel determinado. Se ha realizado una fuerte inversión para asegurarse que, una vez recibida la señal, la fiabilidad del sistema de parada sea muy alta. Un estudio del sistema muestra que, de ocurrir un posible fallo en el proceso de parada de emergencia, éste sería debido a un fallo en el analizador de gases. La tasa de fallos catastróficos del analizador (obtenida a partir de datos genéricos) es de 20,8 fallos por cada millón de horas en funcionamiento (considerando que la frontera del equipo incluye también el sistema de toma de muestra). Sin embargo, las condiciones de servicio para el analizador son de una severidad superior a la media, operándose a temperaturas altas y existiendo además una posibilidad importante de corrosión. *i)* Calcular la tasa de fallos corregida, expresándola en años^{-1}. *ii)* Calcular la tasa de peligro para revisiones mensuales y semanales, suponiendo que se alcanzan concentraciones peligrosas una vez al mes.

6.3. Calcular la tasa de peligro para el ejemplo anterior si se instalan dos analizadores en paralelo.

6.4. Un análisis HAZOP del sistema del ejemplo 6.4 ha revelado que el suceso básico *E* (un fallo catastrófico en una válvula de control) también puede dar origen al suceso intermedio 3, por lo que las entradas de la puerta O correspondiente son ahora *A*, *B* y *E*. Obtener la nueva expresión booleana inicial, la expresión reducida y el árbol de fallos equivalente.

6.5. Discutir qué tipo de distribución de probabilidad de fallos sería adecuada para dar cuenta de fallos humanos en tareas simples (por ejemplo abrir y cerrar válvulas en la descarga de un camión cisterna). ¿Cómo podrían caracterizarse los fallos humanos en tareas más complejas? ¿Cómo afectaría la curva de aprendizaje a la tasa de fallos observada?

6.6. El reactor de una planta de oxidación de hidrocarburos tiene un sistema de alivio de presión que utiliza dos válvulas pilotadas en paralelo. Se considera que la tasa de fallos de este tipo de válvulas es de cuatro veces cada 1.000 demandas. Calcular la fiabilidad del sistema para una tasa de demanda de 0,2 veces al mes, suponiendo que se realiza un mantenimiento semestral de las válvulas.

6.7. Se realiza un análisis de árbol de fallos en el sistema del problema anterior, considerándose que la probabilidad de colapso del reactor debido al evento externo más probable (impacto de un avión) es del orden de 5×10^{-7}. Discutir cuántas válvulas de alivio deben instalarse en paralelo

para que la probabilidad del suceso externo sea significativa frente a la probabilidad de explosión del reactor debido a sobrepresión.

6.8. Al discutir la aceptabilidad del riesgo se han propuesto algunos criterios que pueden servir como guía para decidir si un valor es o no aceptable. Discutir si esos criterios podrían ser modificables o no en función de la situación económica: por ejemplo, en tiempos de crisis, cuando muchas empresas están cerrando, es posible que otras empresas vengan a instalarse si se relajan los requerimientos en materia de seguridad, etc.

6.9. Kletz (2) propone la siguiente cuestión: considérese el caso de un accidente *A*, que puede resultar en la muerte de una persona, con una probabilidad de producirse de una vez al año, durante cien años, y el de un accidente *B*, en el que 100 personas pueden perder la vida, que tiene una probabilidad de producirse de una vez cada cien años. En ambos casos el riesgo de pérdida de vidas es el mismo. ¿Debe darse preferencia a la prevención de *B* sobre *A*? ¿Por qué?

6.10. En 1991, la revista *Chemical Engineering Progress* llevó a cabo una encuesta sobre actitudes éticas de los ingenieros químicos [CEP, *87* (4), 62, (1991)], proponiendo dos situaciones hipotéticas a considerar. En uno de los casos, Tom, un joven ingeniero, es ascendido y destinado a una planta donde las medidas de seguridad no son demasiado estrictas. En particular, existe el peligro de una reacción fuera de control en un reactor si la temperatura llega a 180° C. Está previsto un sistema de parada de emergencia, pero es poco fiable, y de hecho ya han tenido lugar varios incidentes peligrosos, llegando a ocurrir un vertido al exterior de parte de la mezcla reaccionante, a causa de un aumento de presión causado por la pérdida de control de la reacción. Existe un peligro real de accidente, con heridas o muerte de los operarios del reactor. Tom pone todo esto en conocimiento de su jefe, adjuntando abundante documentación, y realiza una propuesta de inversión para mejorar la instrumentación del reactor. La respuesta es que no se justifica el gasto en la situación económica de la empresa, aunque Tom no está de acuerdo. En particular, la situación es difícil por la actitud de su jefe inmediato, un hombre próximo a la jubilación que no tiene intención de cambiar las cosas en el tiempo que le queda. Discutir las opciones que Tom puede tomar y que fueron propuestas en la encuesta del Chemical Engineering Progress: *i)* No hacer nada, esperar a que el jefe se retire en tres o cuatro años (es probable que Tom vuelva a ser ascendido entonces) y solucionar los problemas. *ii)* Denunciar la situación al inspector de seguridad (al que se le ha proporcionado una versión falsa de los incidentes ocurridos en la planta), aunque parece claro que esa opción terminará con la carrera de Tom en la empresa. *iii)* Intentar convencer a su jefe, con más datos técnicos. *iv)* Pasar por encima de su jefe, saltándose el conducto reglamentario para hablar directamente con el vicepresidente del grupo. *v)* Buscar otro trabajo.

Bibliografía

1. FRANKEL, E. G.: *Systems Reliability and Risk Analysis* (2.ª edición). Kluwer Academic Publishers. Dordrecht (1988).
2. KLETZ, T.: *Hazop and Hazan. Identifying and Assessing Process Industry Hazards* (3.ª edición). The Institution of Chemical Engineers. Rugby (1992).
3. CCPS (CENTER FOR CHEMICAL PROCESS SAFETY): *Guidelines for Chemical Process Quantitative Risk Analysis*. AIChE. Nueva York (1989).
4. LEES, F. P.: *Loss Prevention in the Process Industries*. Butterworth-Heinemann. Londres (1980).
5. HAUPTMANNS, U.: *Análisis de Árboles de Fallos*. Ediciones Bellaterra. Barcelona (1986).
6. WALPOLE, R. E., y MYERS, R. H.: *Probabilidad y Estadística* (4.ª edición). McGraw-Hill/Interamericana de México. México (1991).
7. CCPS (CENTER FOR CHEMICAL PROCESS SAFETY): *Guidelines for Process Equipment Reliability Data*. AIChE. Nueva York (1989).
8. O'MARA, R. L.; GREENBERG, H. R., y HESSIAN, R. T.: «Quantified Risk Assessment», en *Risk Assessment and Risk Management for the Chemical Process Industry*. GREENBERG, H. R., y CRAMER, J. J. (Eds.). Van Nostrand Reinhold. Nueva York (1991).
9. BILLINGTON, R., y ALLAN, R. N.: *Reliability Evaluation of Engineering Systems: Concepts and Techniques*. Plenum Press. Nueva York (1983).
10. HENLEY, E. J., y KUMAMOTO, H.: *Reliability Engineering and Risk Assessment*. Prentice-Hall. Englewood Cliffs (1981).
11. MC CORMIC, N. J.: *Reliability and Risk Analysis*. Academic Press. Nueva York (1981).
12. FUSSELL, J. B.: «Fault Tree Analysis. Concepts and Techniques», en *Generic Techniques in Systems Reliability Assessment*. HENLEY, E. J., y LYNN, J. W. (Eds.). Noordhoff International Publishing (1976).
13. BATTELLE COLUMBUS DIVISION-AIChE/CCPS: *Guidelines for Hazard Evaluation Procedures*. American Institute of Chemical Engineers. Nueva York (1985).

14. SCHREIBER, A. M.: *Using Event Trees and Fault Trees*. Chemical Engineering, *89* (20), 115 (1982).
15. O'MARA, R. L.: «Calculation of Human Reliability», en *Risk Assessment and Risk Management for the Chemical Process Industry*. GREENBERG, H. R., y CRAMER, J. J. (Eds.). Van Nostrand Reinhold. Nueva York (1991).
16. KLETZ, T.: *An Engineer's View of Human Error* (2.ª edición). The Institution of Chemical Engineers. Rugby (1991).
17. BELLO, G. C., y COLUMBIORI, V.: *Reliability Engineering, 1* (1), 3 (1980).
18. SWAIN, A. D., y GUTTMANN, H. E.: *Handbook of Human Reliability Analysis, with Emphasis on Nuclear Power Plant Applications*. U. S. Nuclear Regulatory Commission, NUREG/CR-1278. Washington, D. C. (1983).
19. RASMUSSEN, J.: «Approaches to the Control of the Effects of Human Error on Chemical Plant Safety», en *Proceedings of the International Symposium on Preventing Major Chemical Accidents*. WOODWARD, J. L. (Ed.), American Institute of Chemical Engineers. Nueva York (1987).
20. ARENDT, J. S.; LORENZO, D. K.; MONTAGUE, D. F., y DYCUS, F. M.: «Ensuring Operator Reliability During Off-normal Conditions Using an Expert System», en *Proceedings of the International Symposium on Preventing Major Chemical Accidents*. WOODWARD, J. L. (Ed.). American Institute of Chemical Engineers. Nueva York (1987).
21. INTERNATIONAL STUDY GROUP ON RISK ANALYSIS-EUROPEAN FEDERATION OF CHEMICAL ENGINEERING: *Risk Analysis in the Process Industries*. Institution of Chemical Engineers. Rugby (1985).
22. NATALE, M. J.: «Risk Financing», en *Risk Assessment and Risk Management for the Chemical Process Industry*. GREENBERG, H. R., y CRAMER, J. J. (Eds.). Van Nostrand Reinhold. Nueva York (1991).

CAPÍTULO

7

Reducción del riesgo en el diseño de plantas químicas

«Súbitamente recordó algo que uno de los diseñadores de la nave le había dicho con ocasión de haber estado discutiendo los sistemas de "Seguridad Total": Podemos diseñar un sistema a prueba de accidentes y estupidez; pero no a prueba de malicia deliberada.»

2001, una odisea espacial, cap. XXVIII, Arthur C. Clarke.

Introducción

Es un lugar común el refrán: «Más vale prevenir que curar», y como ya se ha indicado en este libro, la mejor manera de evitar accidentes de cualquier tipo es eliminar la posibilidad de que tengan lugar. La reducción del riesgo debe comenzar desde la concepción de un nuevo proceso: a través del diseño de plantas intrínsecamente seguras y fácilmente controlables.

Kletz (1) propone seis pasos secuenciales para controlar los riesgos provenientes del manejo de materias peligrosas:

No usarlas (sustitución).
Usar menos cantidad (intensificación).
Usarlas en condiciones que las hagan menos peligrosas (atenuación).
Confinarlas (para que no pueda haber fugas).
Controlar las fugas (bloqueos de emergencia, facilitar la dispersión...).
Defenderse de las consecuencias de las fugas (protección contra incendios, brigadas contra incendios, edificios resistentes a las explosiones...).

La aplicación de estas reglas a lo largo de todas las etapas de un proyecto, desde la investigación y el desarrollo del producto y el proceso, hasta la ingeniería de detalle, pasando por la ingeniería del proceso puede ayudar a minimizar el riesgo que necesariamente, en mayor o menor grado, conlleva una planta química.