DISEÑO, SIMULACIÓN, OPTIMIZACIÓN Y SEGURIDAD DE PROCESOS

PARTE V

ÁRBOLES DE FALLAS

Dr. Nicolás José Scenna
Dr. Néstor Hugo Rodríguez
Dr. Juan Ignacio Manassaldi

ANÁLISIS DE ÁRBOL DE FALLAS

(Fault Tree Analysis - FTA)

COMPONENTES DE UN ÁRBOL DE FALLAS

La estructura de un árbol de fallas es la siguiente: la falla o accidente que se quiere analizar aparece en el tope de un diagrama y consiste del ***evento tope***, este luego se vincula con otros eventos básicos (como en un árbol jerárquico) con otros ***eventos de falla*** (el evento tope se va desagregando en ***eventos básicos***) por medio de ***compuertas lógicas***. La ventaja principal del árbol de fallas es que el análisis está solo restringido (concentrado) a un evento particular. La construcción de un árbol de fallas provee al analista un mejor entendimiento de las fuentes potenciales de falla, y por ende un medio para repensar el diseño y la operación de un sistema y, de esta forma, eliminar las potenciales causas de falla. Cuando el árbol de fallas está completo, éste sirve para analizar qué combinación de fallas de componentes, errores operacionales u otras fallas pueden causar el evento tope. Finalmente el árbol de fallas se puede emplear para calcular la ***probabilidad de falla bajo demanda***, la ***no-confiabilidad*** y la ***indisponibilidad*** del sistema en cuestión.

SIMBOLOGÍA PARA ÁRBOLES DE FALLA

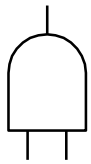
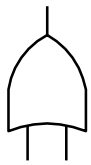
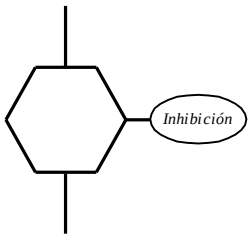
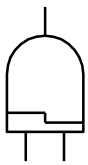
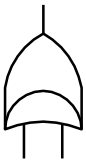
Símbolos de las compuertas

Las compuertas conectan los eventos de acuerdo con las relaciones causales. ***Una compuerta puede tener uno o más eventos de entrada pero sólo un evento de salida.***

El evento de salida de una compuerta *AND* ocurre si todos los eventos de salida ocurren simultáneamente. Por otro lado los eventos de salida de una compuerta *OR* ocurren si cualquiera de los eventos de salida ocurre. Las relaciones causales expresadas por una compuerta *AND* y por una compuerta *OR* son determinísticas, porque la ocurrencia del evento de salida está completamente controlada por el evento de entrada. Un ejemplo de una relación causal no determinística es el siguiente: ***una persona es chocada por un automóvil*** y ***la persona muere***, la relación causal entre estos dos eventos no es determinística porque no siempre una persona muere si es chocada por un automóvil.

La compuerta ***inhibición*** se emplea para representar relaciones causales probabilísticas. El evento de la parte inferior se denomina el ***evento de entrada***, mientras que el evento del costado es el ***evento condicional***. El evento condicional toma la forma de un

evento condicionado al evento de entrada. El evento de salida ocurre si ambos, el evento de entrada y el condicional, ocurren. La compuerta *AND* con prioridad requiere que los eventos de entrada ocurran en el orden que aparecen de izquierda a derecha, para que el evento de salida ocurra. A continuación, se presenta una figura con los símbolos de las compuertas y su significado.

SÍMBOLO	*COMPUERTA*	*SIGNIFICADO*
	**AND**	El evento de salida ocurre si todos los eventos de entrada ocurren.
	**OR**	El evento de salida ocurre si cualquiera de los eventos de entrada ocurre.
	**INHIBICIÓN**	El evento de salida ocurre cuando ocurre el evento de entrada y se satisface la condición de inhibición.
	**AND CON PRIORIDAD**	El evento de salida ocurre si todos los eventos de entrada ocurren en el orden de izquierda a derecha.
	**OR EXCLUSIVA**	El evento de salida ocurre si uno, pero no ambos de los eventos de entrada ocurre.
	**RETARDO**	El evento de salida ocurre cuando el evento de entrada ha ocurrido y ha expirado el tiempo de retardo especificado.

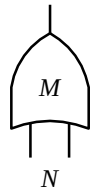
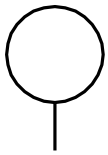
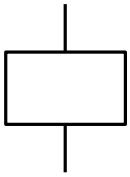
SÍMBOLO	COMPUERTA	SIGNIFICADO
	***M* DE *N***	El evento de salida ocurre si *M* de los *N* eventos de entrada ocurren.

Tabla 1: Operadores lógicos

Símbolos de los eventos

En un árbol de fallas, un rectángulo indica un evento de falla resultante de una combinación de más eventos básicos actuando a través de compuertas lógicas. Los círculos indican un componente de falla básico y representa el límite de resolución de un árbol de fallas (este evento no se descompone). Para poder evaluar un árbol de fallas, el círculo representa un evento del que se dispone información de su confiabilidad. Los eventos casa (***house event***) son eventos que se emplean para representar la ocurrencia o no del mismo. Es decir, el evento es habilitado (***encendido***) para que ocurra o no (***apagado***), esto va de acuerdo con las necesidades de evaluación que se tengan. Inclusive se pueden suspender todas la relaciones causales debajo de una compuerta *AND* por medio de la inhabilitación o ***apagado*** de un evento casa que es una entrada a la compuerta. Los eventos triángulo sirven de transferencia dentro de un árbol. Se emplean para árboles de fallas muy grandes que necesitan varias hojas de papel para su descripción y también para evitar la repetición de secciones de un árbol de fallas, de reemplazar una rama que se repite en alguna otra parte del árbol. En la siguiente gráfica se presentan los símbolos que corresponden a los distintos eventos.

SÍMBOLO	EVENTOS	SIGNIFICADO
	**EVENTO BÁSICO**	Falla de un componente que no requiere mayor desarrollo. Un evento básico es el menor nivel de desarrollo de un FT.
	**EVENTO INTERMEDIO**	Un evento de falla que resulta de la interacción de otros eventos de falla que son desarrollados por las compuertas lógicas mencionadas anteriormente.

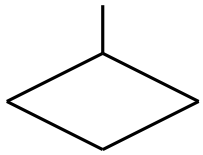
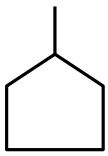
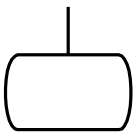
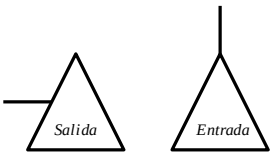
	**EVENTO NO DESARROLLADO**	Evento de falla que no se examina en mayor grado porque la información es insuficiente o un mayor desarrollo va más allá del objeto de estudio.
	**EVENTO CASA O EXTERNO**	Una condición o un evento que se asume existe como parte del escenario en que se desarrolla el árbol de fallas. Puede o no ocurrir.
	**EVENTO CONDICIONAL**	Evento utilizado como una compuerta de inhibición.
	**SÍMBOLOS DE TRANSFERENCIA DE ENTRADA/SALIDA**	El símbolo de *transferencia de entrada* indica que el FT se desarrolla más en el correspondiente símbolo de *transferencia de salida* (por ej., otra página). Los símbolos son rotulados usando números o códigos para asegurar que puedan ser diferenciados. Se utilizan para evitar la repetición de secuencias lógicas dentro de un FT.

Tabla 2: Eventos

EVENTOS

Definiciones

Los eventos básicos y eventos de falla que representan las fallas de los equipos y las personas (de aquí en adelante, nos referiremos a personas y equipos como ***componentes***) se pueden dividir en ***desperfectos*** y ***fallas***. Un ***desperfecto*** de un componente es un mal funcionamiento del mismo que requiere que sea reparado antes de poder funcionar nuevamente en forma correcta. Por ejemplo, la rotura del sello de una bomba será clasificada como un desperfecto de un componente. Una ***falla*** de un componente es un mal funcionamiento que se solucionará asimismo una vez que las condiciones que causaban el mal funcionamiento sean corregidas.

Análisis de los eventos

Existen dos formas de analizar las relaciones causales: hacia adelante (***forward)*** ó hacia atrás ***(backward)***. El análisis hacia adelante comienza con un conjunto de fallas y

procede hacia adelante buscando las posibles consecuencias de los eventos. El análisis hacia atrás comienza con un accidente o falla del sistema y va hacia atrás buscando las posibles causas del accidente. Este último es el más empleado por los árboles de fallas. La estrategia en el análisis hacia atrás es la de identificar las relaciones causales que llevan a una falla en el sistema. Un evento tope puede ser solo alguno de todos los posibles accidentes sobre el sistema. El árbol de fallas por si mismo no identifica los eventos posibles que pueden ocurrir en el sistema. Un sistema grande o complejo puede estar compuesto por múltiples eventos topes y árboles de fallas.

INTERRELACIÓN DE COMPONENTES Y TOPOGRAFÍA DEL SISTEMA

Un ***sistema*** consiste de componentes tales como equipos, accesorios, materiales, plantas y personal, está rodeado por un ambiente social y físico, y sufre de envejecimiento. Los riesgos son causados por uno o un conjunto de componentes generando eventos de falla. El ambiente, el personal y el envejecimiento pueden afectar al sistema sólo a través de los componentes del sistema. Cada componente de un sistema está relacionado con otro de una manera específica, componentes iguales pueden tener diferentes características en sistemas diferentes. Por lo tanto, para la construcción de los árboles de fallas se debe clarificar la interrelación de los componentes y la topografía del sistema.

TIPOS DE FALLAS

Características de las fallas de los componentes

Las fallas de los componentes son fundamentales en las relaciones causales. Ellos se clasifican en: ***fallas (o desperfectos) primarias***, ***fallas secundarias*** y ***fallas de comandos***.

- ***Falla primaria:*** Ocurre en condiciones ambientales y bajo una carga para las cuales el componente estaba diseñado para funcionar. Las fallas primarias son causadas, fundamentalmente por: diseños, fabricación o construcción defectuosas; también son fallas primarias aquellas correspondientes al desgaste y/o envejecimiento del componente. También pueden deberse a desgastes anticipados o mal mantenimiento. No se pueden atribuir a condiciones o fuerzas exteriores. Ejemplo: ruptura del tanque por fatiga del metal. Esto es, son fallas relacionadas con el funcionamiento.
- ***Falla secundaria:*** Ocurre en condiciones ambientales y bajo una carga para la cual el componente no fue diseñado. Por ejemplo, un recipiente a presión falla porque estuvo

trabajando a una presión mayor a la de diseño. Como se indica la falla no es propia del recipiente sino que se debió a la excesiva carga o ambiente desfavorable. Estas fallas ocurren de manera aleatoria y se caracterizan por una frecuencia de falla constante. No son responsabilidad del equipo que falló sino que se pueden atribuir a condiciones o fuerzas exteriores. Otros ejemplos: ***el fusible se rompió por una corriente excesiva***, ***el terremoto quebró el tanque***.

- ***Falla de comando o control:*** ocurre cuando un componente cumple su función en un instante equivocado, o en una localización distinta de la que estaba prevista. La falla no es atribuible al componente sino a la señal que recibe (o no recibe). En general, no se requiere una reparación para corregir la falla. Ejemplo: un recipiente bajo presión puede perder presión por medio de una apertura errónea de una válvula de alivio, aún cuando no se registró una presión excesiva.

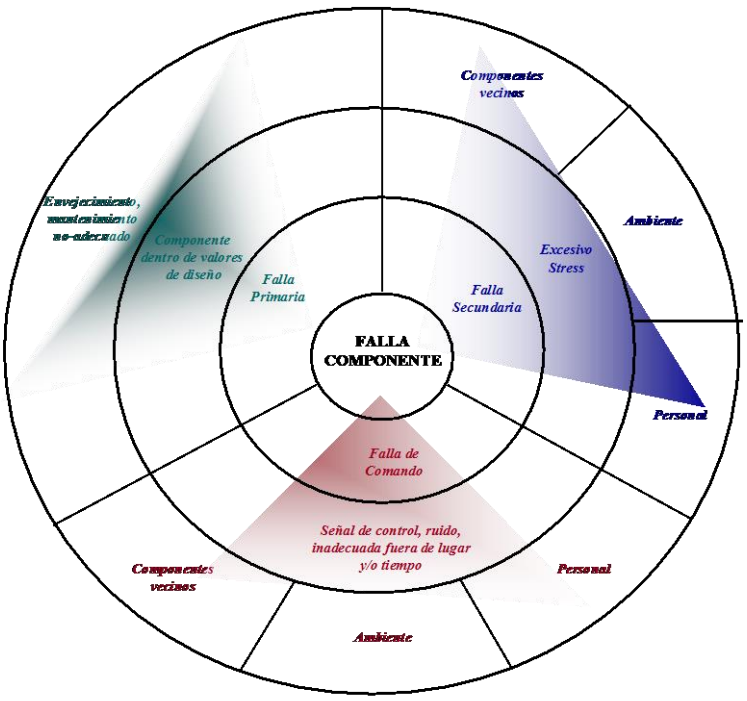


Figura 1: fallas de componente

Falla de componentes

Normalmente en un árbol de fallas, las fallas primarias están en los extremos de las ***ramas*** del árbol, mientras que las fallas secundarias y de comando son eventos intermedios, unidos a los anteriores y entre sí mediante compuertas lógicas. Otras fallas no relacionadas en principio con el componente, como sucesos externos y errores humanos, suelen ocupar también niveles primarios.

Fallas activas y pasivas

Los componentes son diseñados como ***pasivos*** o ***activos***.

Los ***componentes pasivos*** incluyen cosas tales como: cañerías, cables, soldaduras y cerrojos. Ellos funcionan de un modo más o menos estático, algunas veces actuando como transmisores de energía o fluidos. Transmisores de cargas mecánicas, como columnas o elementos de una estructura, y conectores como soldaduras, bridas, etc., son considerados elementos pasivos. Un componente pasivo puede considerarse como un mecanismo de transmisión de la salida de un elemento activo a la entrada de otro elemento activo.

Los ***componentes activos*** contribuyen al funcionamiento del sistema de una manera dinámica, alterando de algún modo el comportamiento del sistema. Por ejemplo, las bombas y las válvulas modifican el flujo del fluido; los relays, los conectores, amplificadores, rectificadores y los chips de una computadora modifican las señales eléctricas; los motores, embragues y otros dispositivos modifican la transmisión de las cargas mecánicas.

La principal razón para distinguir entre los componentes activos y pasivos es que las frecuencias de falla son normalmente más altas para los componentes activos que para los pasivos.

MÉTODO PARA EL ANÁLISIS

Hay cuatro pasos que un analista debe realizar para poder llevar a cabo un FTA:

1. ***Definición del problema***
2. ***Construcción del árbol de fallas***
3. ***Análisis cualitativo y cuantitativo del modelo de FT***
4. ***Documentación de los resultados***

Definición del problema

Para definir el problema se deben seleccionar (1) un ***evento tope*** y (2) las ***condiciones***

de contorno para el análisis. Estas condiciones de contorno incluyen:

▪ Límites físicos del sistema	▪ Eventos no permitidos
▪ Nivel de resolución	▪ Condiciones existentes
▪ Condiciones iniciales	▪ Otras suposiciones

Tabla 3: Condiciones de contorno

- ***Evento tope:*** La definición del evento tope es uno de los aspectos más importantes del primer paso. El evento tope es el accidente (o evento no deseado) que es el sujeto del FTA (este evento normalmente se identifica a través de previas evaluaciones de riesgos). Los eventos topes se deben definir precisamente para el sistema o la planta que se está evaluando, debido a que los análisis muy amplios y los eventos pobremente definidos normalmente conducen a análisis ineficientes. Por ejemplo: un evento tope de ***incendio en la planta*** es demasiado general para un FTA. En cambio, un evento tope apropiado sería ***disparo de la reacción en un reactor de oxidación del proceso durante la operación normal***. Este descripción del evento está bien definida y bien determinada ya que nos dice el: ***qué, dónde*** y ***cuándo***. El ***qué*** (disparo de la reacción) nos dice el tipo de accidente, el ***dónde*** (reactor de oxidación del proceso) nos dice el equipo del sistema o proceso involucrado en el accidente, y el ***cuándo*** (durante la operación normal) nos dice la configuración de la totalidad del proceso.
- ***Condiciones de contorno:*** En los ***límites físicos del sistema*** se tienen en cuenta los equipos, las interfaces de los equipos con otros procesos, y los sistemas de soporte/servicio que se incluirán en el FTA. Junto con los límites físicos del sistema, el analista deberá especificar el ***nivel de resolución*** para los eventos del FT (cantidad de detalles que se incluirán en el FT). Por ejemplo: una válvula motorizada puede ser incluida como una pieza de un equipo, o puede describirse como varios elementos (ej., cuerpo de la válvula, elementos internos, motorización). Esta descomposición podría también incluir: el suministro de energía, llave de arranque, y la necesidad de un operador para manipular la válvula. Un factor que debe considerarse en la decisión del nivel de resolución es la cantidad de información detallada de fallas disponible para el analista, quizás a partir de un FMEA o estudio de seguridad previos.

  Otra condición de contorno es la ***configuración inicial de equipo*** o las ***condiciones***

iniciales de operación. Esta información establece la configuración del sistema y los equipos que se incluyen en el FTA. El analista especifica: que válvulas están abiertas, cuales cerradas, que bombas están encendidas, cuales apagadas, etc., para todos los equipos dentro de los límites físicos del sistema. Estas condiciones de contorno describen al sistema en su estado normal, no fallado.

Los ***eventos no permitidos*** son, para los propósitos de un FTA, eventos que se consideran increíbles o que, por alguna otra razón, no van a ser considerados en el análisis. Por ejemplo, fallas en los cables podrían ser excluidas del análisis de un instrumento del sistema. Las ***condiciones existentes*** son (también para las condiciones del FTA) eventos o condiciones que seguramente pueden ocurrir. Generalmente, los eventos no permitidos y los existentes no aparecen en el árbol de fallas final, pero se deben considerar sus efectos en el desarrollo de otros eventos de falla a medida que se construye el árbol de fallas. El analista debe especificar ***otras suposiciones*** tanto como sea necesario para definir el sistema para el FTA. Por ejemplo: el analista puede asumir que el sistema está trabajando a un 50% de la capacidad normal. Después que la definición del problema está completada y que las condiciones de contorno están establecidas, estas ***otras suposiciones*** deberán clarificar incertidumbres que queden acerca del estado del sistema.

Construcción del árbol de fallas

La construcción del árbol de fallas comienza con el evento tope y procede, nivel por nivel, hasta determinar todas las causas básicas (eventos básicos) que contribuyen a cada uno de los eventos de falla. El analista comienza con el evento tope y, para el siguiente nivel, utiliza un razonamiento deductivo causa/efecto para determinar las causas inmediatas, necesarias y suficientes que dan como resultado el evento tope. Normalmente, estas no son causas básicas, pero son fallas intermedias que requieren desarrollo adicional. Si el analista puede determinar inmediatamente las causas básicas del evento tope, el problema es muy simple como para un FTA y puede ser evaluado por otros métodos (como un FMEA).

Si cualquiera de las causas inmediatas al evento tope resulta directamente en éste, éstas se conectan con el evento tope a través de una compuerta lógica *OR*. En cambio, si se requiere que se cumplan todas las causas inmediatas para que ocurra el evento tope, éstas se conectan con el mismo a través de una compuerta lógica *AND*. Cada uno de los eventos intermedios se trata de la misma forma que el evento tope. Para cada evento intermedio, las causas son determinadas y mostradas en el FT (***fault tree***) con las compuertas lógicas

apropiadas. El analista continua este procedimiento hasta que todos los eventos básicos intermedios han sido desarrollados hasta sus causas de falla.

En la siguiente tabla se citan diversas reglas básicas que se han desarrollado para proporcionar consistencia e integridad al proceso de construcción de un árbol de fallas. Las mismas intentan enfatizar la importancia de construir un árbol de fallas de manera sistemática y metódica.

REGLAS PARA LA CONSTRUCCIÓN DE ÁRBOLES DE FALLAS	
Afirmaciones del evento de falla	Escriba las afirmaciones que están contenidas en los compartimentos de eventos y redondéelas como malos funcionamientos. Formule una precisa descripción del componente y su modo de falla. Para una completa descripción del evento de falla es necesario hacer estas afirmaciones tan preciso como sea posible. Las partes "Dónde" y "Qué" especifican el equipo y su estado fallado relevante. La condición "Porqué" describe el estado del sistema con respecto al equipo, diciendo porque el estado del equipo se considera como una falla. Las afirmaciones deben ser lo más completas posibles; el analista debe resistir la tentación de abreviarlas durante la construcción del árbol de fallas.
Evaluación del evento de falla	Cuando se evalúa un evento de falla, haga la pregunta: ¿ Puede ser esta falla un desperfecto de un equipo ?. Si la respuesta es "Sí", clasifique el evento de falla como una "*Falla del estado del equipo*". Si la respuesta es "No", clasifique la falla como una "*Falla del estado del sistema*". Esta clasificación ayuda al desarrollo posterior de los eventos de falla. Si el evento es una falla del estado del equipo, agregar una compuerta *OR* al evento de falla y buscar las fallas primarias, secundarias y de comando que pudieron originar el evento. Si el evento de falla es una falla del estado del sistema, busque las causas del evento de falla.
No considera milagros	Si el funcionamiento normal de los equipos propaga un secuencia de falla, considere que el equipo funciona normalmente. Nunca considere que desperfectos totalmente milagrosos e inesperados interrumpan o eviten la ocurrencia de un accidente.
Completar cada compuerta	Todas las entradas a una compuerta deben estar completamente definidas antes de comenzar el estudio de cualquier otra compuerta. Para modelos simples, el árbol de fallas debe ser completado en niveles, y cada nivel debe ser completado antes de comenzar con el próximo nivel. Sin embargo, analistas experimentados encontrarán difícil de manejar esta regla cuando desarrollen árboles de fallas largos y complejos.
No use compuerta a compuerta	Las compuertas de entrada deben ser definidas adecuadamente, esto es, las compuertas no deben estar conectadas directamente a otras compuertas. El recorte del desarrollo de los árboles de falla acarrea confusiones, debido a que las compuertas de salida no están especificadas.

Tabla 4: Reglas de construcción de árboles de fallas

Ejemplo: En las siguientes figuras, y a modo de ejemplo, se presentan los diagramas de dos procesos y a continuación sendos árboles de fallas simplificados cada uno correspondiente a dichos procesos.

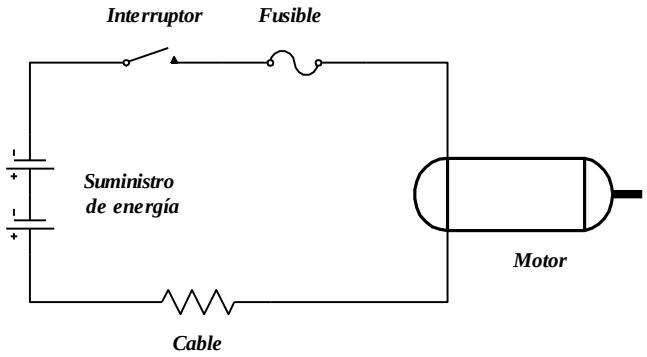


Figura 2: Circuito de comando del motor eléctrico.

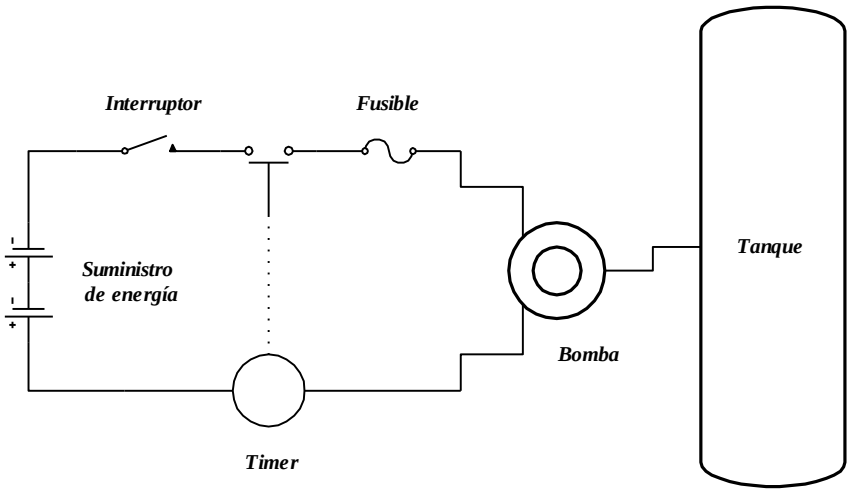


Figura 3: Diagrama esquemático del sistema de bombeo.

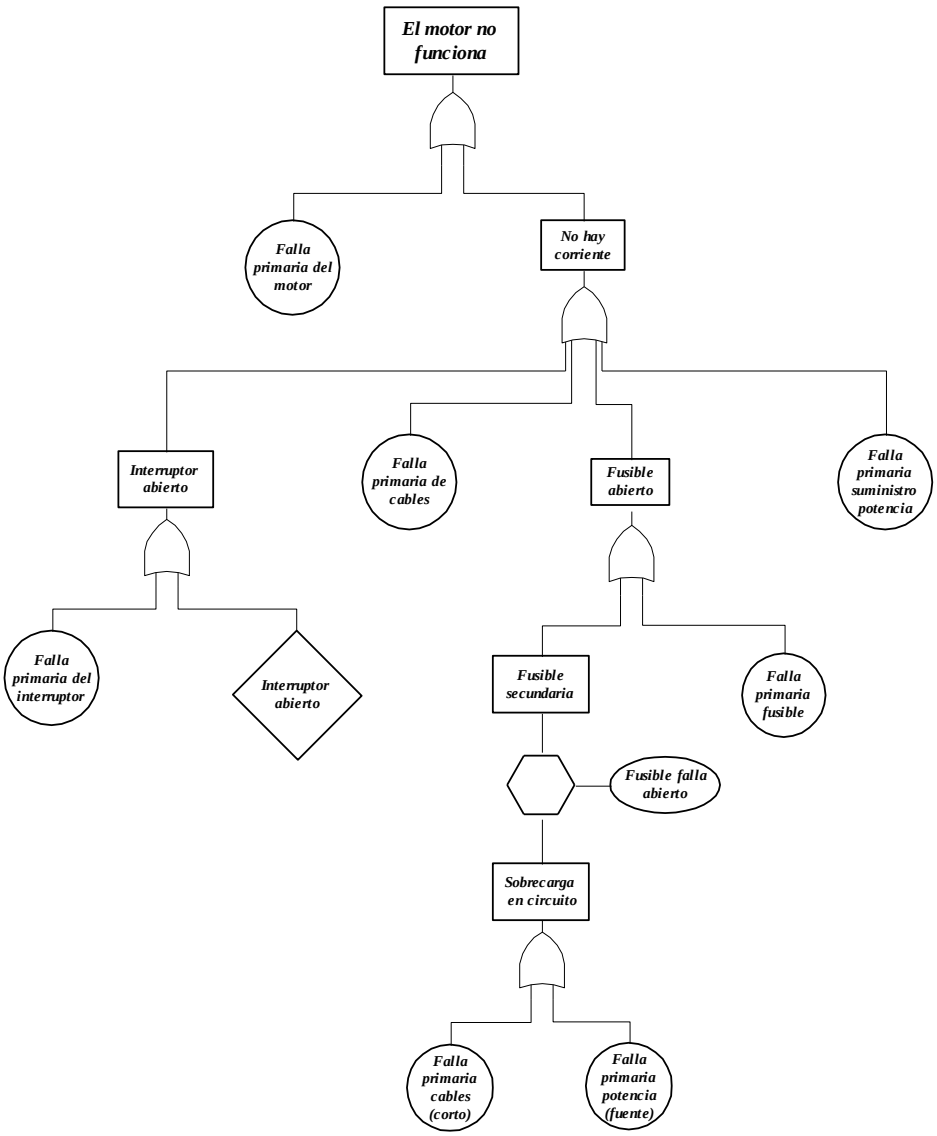


Figura 4: Árbol de falla del circuito eléctrico de un motor.

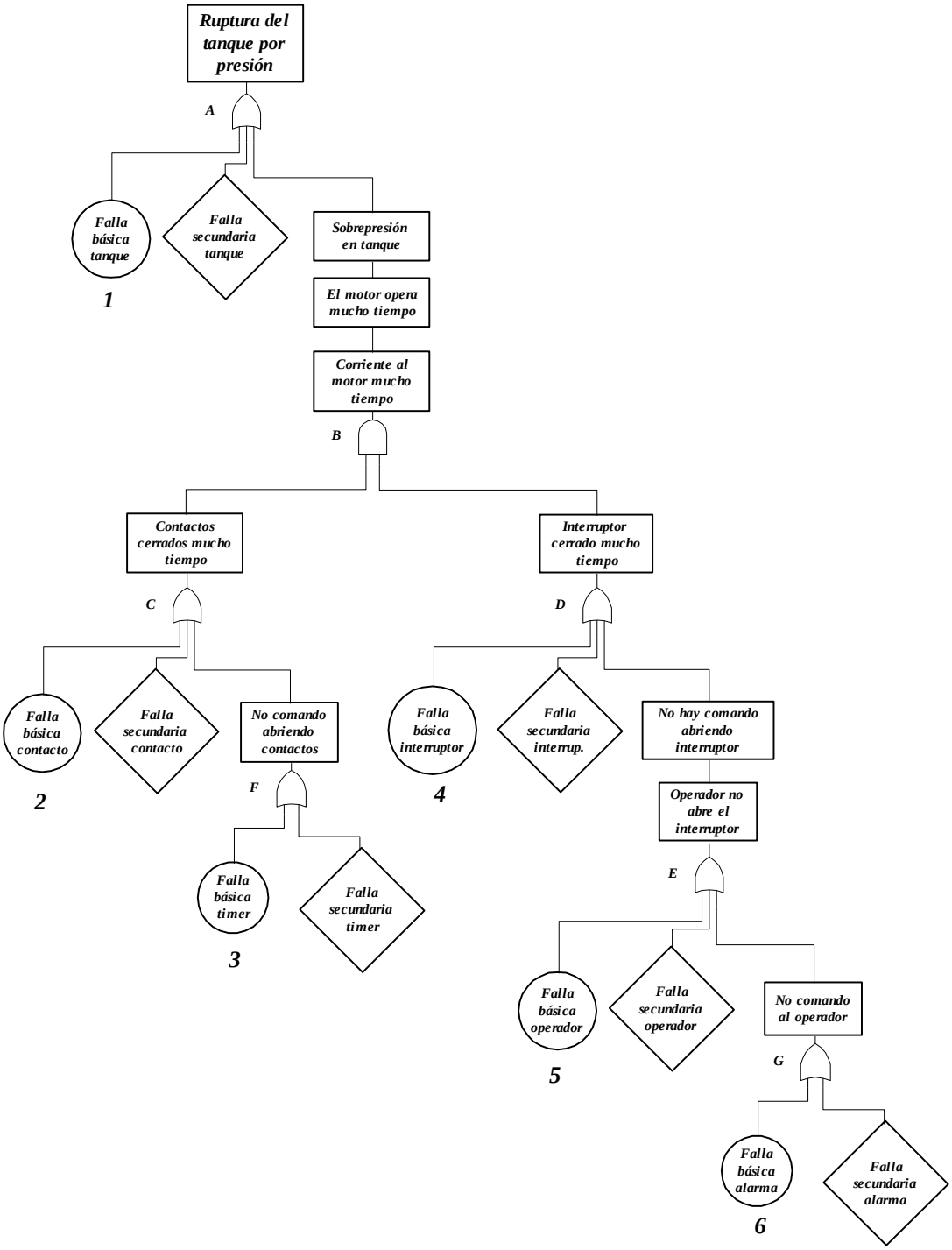


Figura 5: Árbol de fallas del sistema de bombeo.

Evaluación de árboles de fallas

La evaluación de los árboles de fallas se realiza en dos etapas. En primer lugar, una expresión lógica se construye para el evento tope en términos de combinaciones (uniones e intersecciones) de los eventos básicos. Esto se considera como un análisis cualitativo. Luego estas expresiones se emplean para dar la probabilidad del evento tope en término de las probabilidades de los eventos primarios. Esto se considera como el análisis cuantitativo. Esto significa que conociendo las probabilidades de los eventos primarios podemos conocer las probabilidades del evento tope. Para realizar estas simplificaciones las reglas del álgebra de Boole son muy útiles. Ellas permiten simplificar las expresiones lógicas para el árbol de fallas y por lo tanto expresar en una fórmula la probabilidad que el evento tope ocurra en términos de las probabilidades de falla de los eventos básicos. En la siguiente tabla se citan algunas de las reglas Booleanas de uso frecuente en la evaluación de árboles de fallas:

REGLAS BOOLEANAS DE USO FRECUENTE EN LA EVALUACIÓN DE ÁRBOLES DE FALLAS		
Conmutativa	$AB = BA$ $A + B = B + A$	
Asociativa	$A(BC) = (AB)C$ $A + (B + C) = (A + B) + C$	
Distributiva	$A(B + C) = AB + AC$ $A + BC = (A + B)(A + C)$	
Otras	$AA = A$ $A(A + B) = A$ $AA^* = 0$ $0A = 0$ $1A = A$ $(A^*)^* = A$	$A + A = A$ $A + AB = A$ $A + A^* = 1$ $0 + A = A$ $1 + A = 1$

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*".

Tabla 5: Reglas lógicas

Evaluación cualitativa directa

Supongamos que se quiere evaluar el árbol de fallas de la siguiente figura:

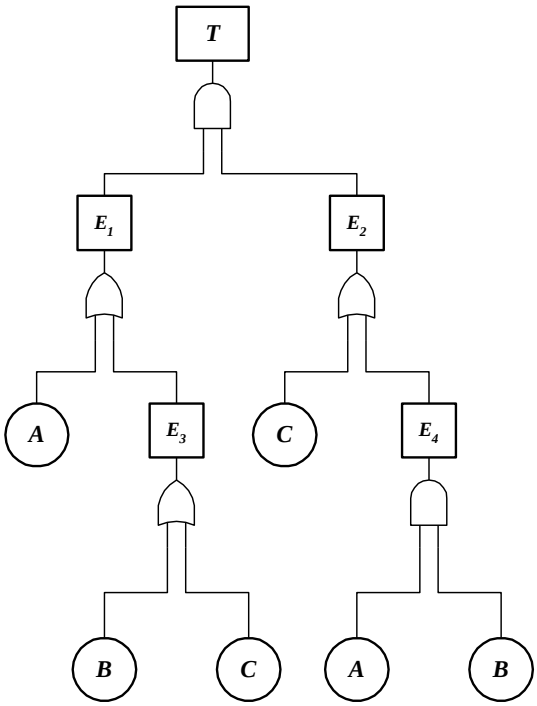


Figura 6: árbol de fallas genérico

En esta figura los eventos primarios son identificados por las letras desde la *A* hasta la *C*. Notar que los elementos primarios pueden darse en más de una rama del árbol. El evento tope se identifica por la letra *T* y los eventos intermedios como E_i.

Metodología Top-Down

En esta metodología comenzamos por el evento tope y trabajamos hacia abajo a través de los niveles del árbol, reemplazando las compuertas por los símbolos correspondientes *OR* y *AND*. Esto es:

$$T = E_1 E_2$$

y también

$$E_1 = A + E_3 \ \wedge \ E_2 = C + E_4$$

$$E_3 = B + C \ \wedge \ E_4 = A B$$

entonces nuestro resultado final es:

$$T = \left(A + \left(B + C\right)\right)\left(C + \left(A B\right)\right)$$

Este mismo resultado se puede obtener trabajando desde abajo hacia arriba (queda

como ejercicio de la clase).

Para muchos árboles de fallas, particularmente aquellos con una ó más fallas primarias que ocurren en más de una rama del árbol, se pueden emplear las reglas del álgebra de Boole para simplificar la expresión lógica que corresponde al evento tope. En nuestro ejemplo primero vamos a aplicar la ley conmutativa para escribir:

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

entonces:

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

aplicando la ley distributiva obtenemos:

$$T=AC+BC+CC+AAB+BAB+ABC$$

Por la ley asociativa tenemos que:

$$CC=C$$
$$AAB=AB$$
$$BAB=BA$$
$$C\subset AC\ y\ BC$$

entonces como:

$$AB=BA$$

llegamos a que:

$$T=C+(AB)$$

Esta expresión nos dice que en el árbol de fallas bajo consideración el evento tope ocurre por la falla del evento básico C o por la falla de ambos elementos A y B.

El árbol de fallas original se puede reducir al siguiente:

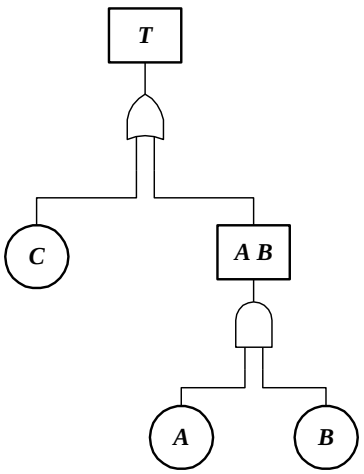


Figura 7: Reducción del árbol de fallas

Evaluación cuantitativa directa

La suposición usual que se hace con lo eventos básicos B_1, B_2, …, B_n es que son independientes, esto es que la ocurrencia de un evento dado no es afectada por la ocurrencia de otros eventos básicos. Entonces, para eventos básicos independientes, la probabilidad de existencia simultánea se expresa de la siguiente manera:

$$Pr(B_1\ B_2\ ...B_n) = Pr(B_1)Pr(B_2)...Pr(B_n)$$

Considerando ahora el siguiente árbol que consiste de una compuerta *AND*, y que la ocurrencia del evento de salida consiste de la existencia simultánea de todos los eventos de entrada.

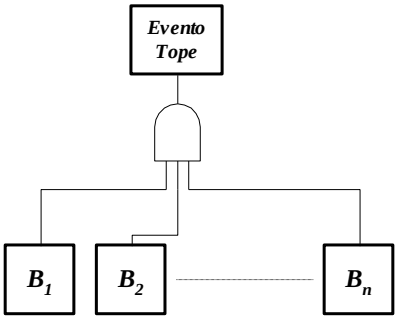


Figura 8: Árbol de Falla con compuerta AND

Esto significa que la indisponibilidad del sistema a un tiempo *t*, dada por la ocurrencia del evento de salida es :

$$Q_s(t) = Pr(B_1\ B_2\ ...B_n) = Pr(B_1)Pr(B_2)...Pr(B_n)$$

Para una compuerta *AND* con dos eventos de entrada esto se reduce a:

$$Q_s(t) = Pr(B_1\ B_2) = Pr(B_1)Pr(B_2)$$

Si tuviéramos el sistema representado en la siguiente figura con una compuerta *OR* conectando el evento tope con los eventos básicos, esto implica que el evento tope ocurre si y solo si uno de los n eventos básicos ocurre.

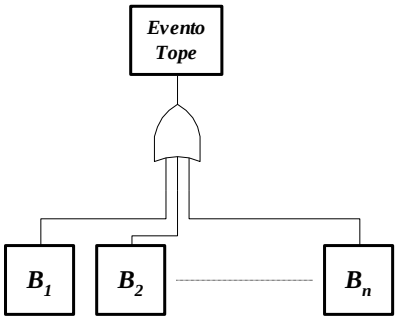


Figura 9: Árbol de Falla con compuerta OR

La disponibilidad e indisponibilidad del sistema están dadas por:

$$A_s(t) = Pr(\overline{B}_1\ \overline{B}_2\ ...\overline{B}_n)$$

$$Q_s(t) = Pr(B_1 + B_2 + ... + B_n)$$

donde $\overline{B}_i$ = ***complemento del evento*** B_i, y significa la no ocurrencia del evento *i* al tiempo *t*. La independencia de los eventos básicos B_1, B_2, …, B_n implica la independencia de los eventos complementarios $\overline{B}_1$, $\overline{B}_2$, ..., $\overline{B}_n$. Las ecuaciones anteriores se pueden reescribir de la siguiente manera:

$$A_s(t) = Pr(\overline{B}_1\ \overline{B}_2\ ...\overline{B}_n) = [1 - Pr(B_1)][1 - Pr(B_2)]...[1 - Pr(B_n)]$$

$$Q_s(t) = 1 - A_s(t) = 1 - \{[1 - Pr(B_1)][1 - Pr(B_2)]...[1 - Pr(B_n)]\}$$

Si *n* = 2:

$$Q_s(t) = Pr(B_1) + Pr(B_2) - Pr(B_1)Pr(B_2)$$

Si *n* = 3:

$$Q_s(t) = Pr(B_1) + Pr(B_2) + Pr(B_3) - Pr(B_1)Pr(B_2) - Pr(B_2)Pr(B_3) - Pr(B_1)Pr(B_3) + Pr(B_1)Pr(B_2)Pr(B_3)$$

o más generalmente:

$$Q_s(t) = \sum_{i=1}^{m} Pr(B_i) - \sum_{i=2}^{m}\sum_{j=1}^{i-1} Pr(B_i)Pr(B_j) + \sum_{i=3}^{m}\sum_{j=2}^{i-1}\sum_{k=1}^{j-1} Pr(B_i)Pr(B_j)Pr(B_k) + ... + (-1)^{m-1}[Pr(B_1)Pr(B_2)...Pr(B_m)]$$

Por lo general los productos son mucho menores que los sumandos y se desprecian en la evaluación a partir de un cierto índice (cuatro por ejemplo).

Evaluación cualitativa por medio de conjuntos de corte (cut sets) y conjuntos de caminos (path sets)

Las ***fallas en los sistemas*** pueden ocurrir de muchas maneras diferentes. Cada forma única es un ***modo de falla del sistema*** e involucra simples o múltiples fallas de los componentes del mismo. Para reducir las posibilidades de fallas del sistema, primero debemos identificar los modos de falla y luego eliminar los que ocurren de modo más frecuente y/o los más probables.

Para un dado árbol de fallas el concepto de ***conjunto de corte (cut set)*** define

claramente los modos de falla de un sistema.

Conjuntos de corte (cut sets)

Un ***conjunto de corte*** es un conjunto de eventos básicos tal que si todos ellos ocurren la ocurrencia del evento tope está garantizada. Por ejemplo, para el árbol de la figura de la página 85 si ocurren los eventos 2 y 4 simultáneamente, el evento tope ocurre, por lo tanto el conjunto de eventos {2,4} es un ***conjunto de corte*** ó ***cut set***. En esa misma figura {1} y {3,5} también son conjuntos de corte.

Conjuntos de caminos (path sets)

Un ***conjunto de caminos*** es el concepto dual de un ***conjunto de corte***. Este es un conjunto de eventos básicos que si ninguno de los eventos en el conjunto ocurre el evento tope se garantiza que no ocurre. Para el árbol de fallas de la página 85, si los eventos 1, 2 y 3 no ocurren, el evento tope no puede suceder. Por lo tanto si el tanque, los contactos y el ***timer*** son normales el tanque no se rompe. Esto implica que el conjunto {1,2,3} es un ***conjunto de caminos***. Otro conjunto de caminos de un árbol de fallas es {1,4,5,6}.

Conjuntos de corte y conjuntos de caminos mínimos

Un sistema grande tiene un gran número de modos de falla, un sistema con 40-90 componentes puede llegar a tener cientos de miles de ***conjuntos de corte***. Para estos casos es necesario llegar a reducir los modos de falla para simplificar el análisis. Se requieren sólo los modos de falla que son generales, en el sentido que si eliminamos estos modos de falla, esto resultará en la eliminación de gran parte de los modos de falla del sistema. Un ***conjunto de corte mínimo (Minimal Cut Set - MCS)*** es uno tal que si un elemento se remueve del conjunto, los demás eventos colectivamente ***no son más un conjunto de corte***. Un conjunto de corte que incluye otros conjuntos ***no es un conjunto de corte mínimo***. El concepto de conjunto de corte mínimo nos permite reducir el número de conjuntos de corte y el número de eventos básicos involucrados en cada ***conjunto de corte***. Lo que simplifica el análisis. El árbol de fallas de la figura I tiene 7 conjuntos de corte mínimos: {1}, {2,4}, {2,5}, {2,6}, {3,4}, {3,5}, {3,6}. El ***conjunto de corte*** {1,2,4} no es un conjunto mínimo porque incluye: {1} y {2,4}.

Un ***conjunto de caminos mínimo (Minimal Path Set - MPS)*** es uno tal que si se

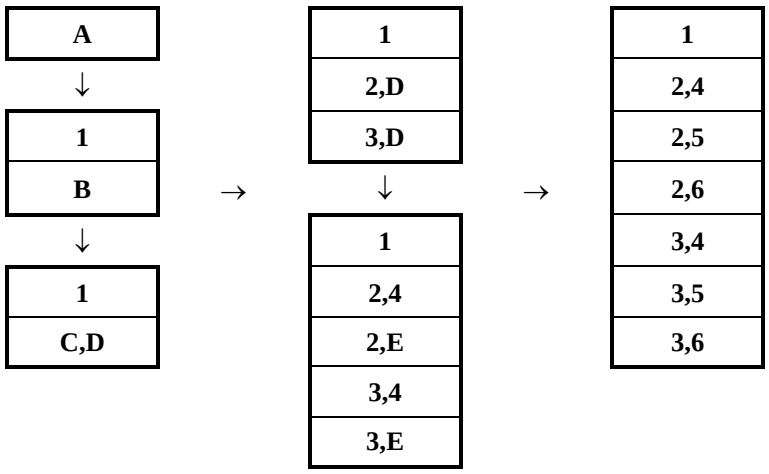
remueve cualquier evento básico del set los restantes elementos colectivamente no son más un ***path set***. El árbol de la figura I tiene dos conjuntos de caminos mínimos: {1,2,3} y {1,4,5,6}. Si {1,2,3} no falla, ni tampoco {1,4,5,6} el tanque opera normalmente.

Algoritmo de identificación de un MCS

Una compuerta *OR* incrementa el número de ***conjuntos de corte***, mientras que una compuerta *AND* incrementa el número de eventos en un ***conjunto de corte***, de acuerdo con esto se puede establecer el siguiente algoritmo:

1. ***Identifique las compuertas con un nombre.***
2. ***Identifique (numere) cada evento básico.***
3. ***Ubique la primera compuerta después del evento tope en la primera fila y columna de una matriz.***
4. ***Itere de un modo top-down haciendo las siguientes operaciones:***
   - Reemplace las compuertas *OR* por un arreglo vertical compuesto por las entradas a la compuerta e incremente los ***conjuntos de corte***.
   - Reemplace las compuertas *AND* por arreglos horizontales de las entradas e incremente la medida del ***conjunto de corte***.
5. ***Cuando todas las compuertas han sido reemplazadas por los eventos básicos obtenga los conjuntos de corte mínimos removiendo todos los supersets (conjuntos que incluyen algún otro conjunto).***

Siguiendo el árbol de la figura I donde las compuertas y los eventos se encuentran identificados y aplicando el algoritmo escrito podemos tener la siguiente secuencia:



Entonces tenemos los siguientes conjuntos de corte: {1}, {2,4}, {2,5}, {2,6}, {3,4}, {3,5} y {3,6}. Todos son mínimos dado que ***no incluyen ningún otro conjunto de corte mínimo.***

Si nuestro resultado hubiera sido:

1,2,G
1,2,3,G
1,2,K

deberíamos haber eliminado 1,2,3,G dado que incluye a 1,2,G, nuestro resultado sería :

1,2,G
1,2,K

Si un evento aparece más de una vez en un arreglo horizontal, este debería ser agregado en un solo:

{1,2,3,2,H} ➔ {1,2,3,H}

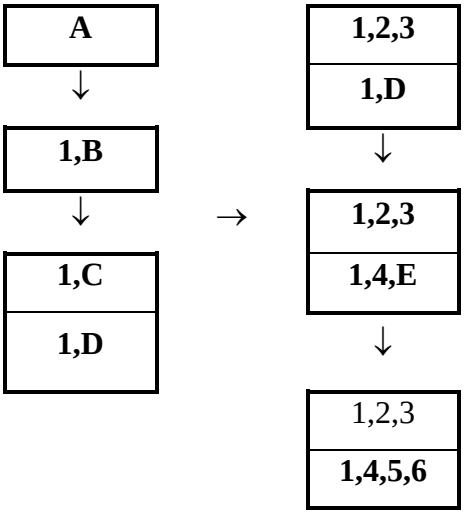
Algoritmo de identificación de los MPS

Para la generación de los ***conjuntos de caminos*** debemos tener en cuenta que una compuerta *AND* incrementa la cantidad de ***conjuntos de caminos***, y que una compuerta *OR* agranda la medida del ***conjunto de caminos*** (a la inversa de lo que ocurre en la generación de un conjunto de corte). El algoritmo se ejecuta de la siguiente manera:

1. ***Identifique las compuertas con un nombre.***
2. ***Identifique (numere) cada evento básico.***
3. ***Ubique la primera compuerta después del evento tope en la primera fila y columna de una matriz.***
4. ***Itere de un modo top-down haciendo las siguientes operaciones:***
   - ***Reemplace las compuertas AND por un arreglo vertical compuesto por las entradas a la compuerta e incremente los conjuntos de caminos.***
   - ***Reemplace las compuertas OR por arreglos horizontales de las entradas a la compuerta e incremente la medida del conjunto de caminos.***

Cuando todas las compuertas han sido reemplazadas por los eventos básicos obtenga los ***conjuntos de caminos mínimos*** removiendo todos los ***supersets*** (conjuntos que incluyen

algún otro conjunto).



Tenemos entonces dos ***conjuntos de caminos***: {1,2,3} y {1,4,5,6}.

Evaluación cuantitativa por medio de los conjuntos de corte

La siguiente figura representa el árbol de fallas compuesto por los ***conjuntos de corte mínimos*** que es equivalente al árbol de fallas original.

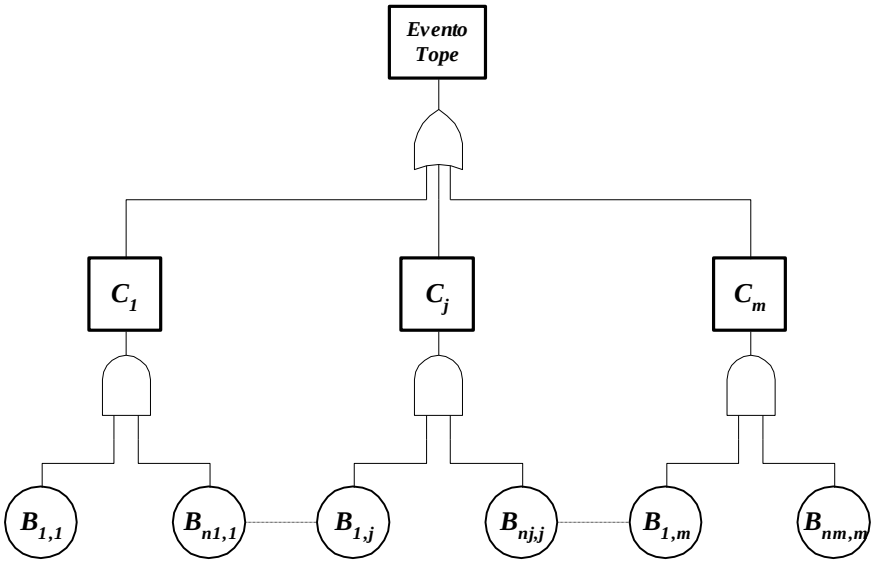


Figura 10: Representación de un árbol de falla por los conjuntos mínimos

donde :

$\{B_{1,1}, B_{2,1}, \ldots, B_{n1,1}\}$ → *conjunto de corte 1 representado por el evento* C_1

$\{B_{1,j}, B_{2,j}, \ldots, B_{nj,j}\}$ → *conjunto de corte j representado por el evento* C_j

$\{B_{1,m}, B_{2,m}, \ldots, B_{nm,m}\} \rightarrow$ ***conjunto de corte m representado por la evento*** C_m

El evento tope ocurre si y solo si todos los eventos básicos de un ***conjunto de corte mínimo*** ocurren simultáneamente. De los resultados expuestos es evidente el cálculo de la probabilidad de ocurrencia del evento tope por cualquiera de los ***conjuntos de corte mínimos***. La probabilidad de ocurrencia del evento tope está dada por:

$$Pr(Evento\ Tope) = 1 - \{[1 - Pr(C_1)][1 - Pr(C_2)]...[1 - Pr(C_m)]\}$$

de acuerdo con lo expresado anteriormente (en la evaluación cuantitativa directa):

$$Pr(Evento\ Tope) = \sum_{i=1}^{m} Pr(C_i) - \sum_{i=2}^{m}\sum_{j=1}^{i-1} Pr(C_i)Pr(C_j) + \sum_{i=3}^{m}\sum_{j=2}^{i-1}\sum_{k=1}^{j-1} Pr(C_i)Pr(C_j)Pr(C_k) + ... + (-1)^{m-1}[Pr(C_1)Pr(C_2)...Pr(C_m)]$$

Para poder evaluar esta expresión se debe evaluar la probabilidad de ocurrencia de ***conjuntos de corte individuales***, con lo cual:

$$Pr(C_j) = Pr(B_{1,j}\ B_{2,j}\ ...B_{nj,j}) = Pr(B_{1,j})Pr(B_{2,j})...Pr(B_{nj.j})$$

Por lo general en este tipo de evaluaciones no es necesario calcular todos lo términos que hacen a la ocurrencia del evento tope, sino que como muchos de ellos tienen valores despreciables frente a los otros, solo será necesario calcular los dos, a lo sumo tres, primeros términos de cada ***conjunto de corte***, como se expresara anteriormente

Jerarquización de conjuntos mínimos

La ***jerarquización*** de los ***conjuntos de corte mínimos*** identificados suele ser uno de los pasos finales de un análisis FTA.

Para una ***evaluación cualitativa*** se considera la ***jerarquización*** dentro del grupo de conjuntos de tamaño determinado, teniendo en cuenta el tipo de eventos involucrados. La regla en este caso es:

1ero.) ***Errores humanos.***

2do.) ***Errores debidos a fallas de equipos activos*** (que están en funcionamiento activo).

3ero.) ***Errores debidos a fallas de equipos pasivos*** (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 mínimos de tamaño 2 (dos eventos), uno que involucre un error humano y otro de un equipo (pasivo o activo) será más importante que, por ejemplo, otro que involucre dos errores de equipos activos.

Esta ***jerarquización*** 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 eventos más probables se establece tomando como base, sobre todo, la experiencia del personal que maneja la planta.

Importancia de los cut sets

Conocer los ***conjuntos de corte*** para un árbol de fallas particular puede brindar una comprensión importante acerca de los puntos débiles de un sistema complejo, aún cuando no es posible calcular la probabilidad de ocurrencia de un ***conjunto de corte*** o del evento tope porque no se tienen suficientes datos probabilísticos. Tres consideraciones cualitativas pueden ser útiles: el ranking de los ***conjuntos de corte mínimos*** de acuerdo con el número de fallas primarias requeridas, la importancia de las fallas de los componentes individuales en la ocurrencia de los ***conjuntos de corte mínimos*** y la susceptibilidad de un determinado ***conjunto de corte*** o modo de falla común. Los ***conjuntos de corte mínimos*** son ***categorizados*** normalmente como singles, dobles, triples, etc., de acuerdo con el número de fallas primarias que posee el ***conjunto de corte***. El énfasis se pone en la eliminación de los ***conjuntos de corte*** que tienen el menor número de fallas, dado que éstos, por lo general, se espera que tengan la mayor contribución a la falla del sistema. De hecho, un criterio de diseño común dice que la falla de ningún componente simple debe causar la falla del sistema, es equivalente a decir que todos los ***conjuntos de corte mínimos*** simples deben ser eliminados del árbol de fallas, cosa que no siempre es posible sin modificar el diseño de manera significativa

Otra aplicación de la información de los ***conjuntos de corte*** está en la evaluación cualitativa de la importancia de un componente particular. Suponga que deseamos evaluar el efecto que tiene sobre el sistema el mejorar la confiabilidad de un componente particular, o si la falla de un componente en particular será considerable sobre el sistema total. Si el componente aparece en uno o más de los ***conjuntos de corte*** de orden bajo (por ejemplo simples o dobles) su confiabilidad probablemente tendrá un efecto pronunciado. Por otra parte, si se tiene un ***conjunto de corte mínimo*** con varias fallas, su importancia será menor.

Documentación de los resultados

El paso final en la realización de un FTA es documentar los resultados del estudio. El analista de riesgo debe proporcionar una ***descripción del sistema analizado*****, una** ***discusión sobre la definición del problema*****, una** ***lista de suposiciones*****, los** ***modelos de árboles de fallas que fueron desarrollados*****, una** ***lista de los conjuntos de corte mínimos*****, y una** ***evaluación de la significancia de los MCS***. Además se debe incluir cualquier ***recomendación*** que surja del FTA realizado.

RESULTADOS ESPERADOS DEL ANÁLISIS

El producto final de un FTA cualitativo es la lista de MCS del sistema jerarquizados. El modelo de FT se utiliza generalmente como una herramienta muy efectiva de comunicación con los encargados de tomar las decisiones técnicas y no técnicas. El equipo, en función del número y tipo de fallas de los MCS, recomendará las mejoras necesarias para hacer menos probable el evento tope.

ANEXO: EJEMPLO CUANTITATIVO DE ÁRBOL DE FALLAS.

Se demostrará con un ejemplo de fuga en un tanque (Ozog 1985)

Paso 1. Descripción del sistema. El P&ID para el sistema de tanques de almacenamiento se muestra en la Figura 11. El tanque de almacenamiento (T-I) está diseñado para contener un líquido inflamable bajo una ligera presión positiva de nitrógeno. Un sistema de control (PICA-I) controla la presión. Además, el tanque está equipado con una válvula de alivio para hacer frente a emergencias. El líquido se alimenta al tanque desde camiones cisterna. Una bomba (P-I) suministra el líquido inflamable al proceso.

Paso 2. Identificación de riesgos. Ozog (1985) utilizó HAZOP para identificar el peligro más grave como una liberación importante de inflamables del tanque. Este incidente es el evento superior que se desarrollará en el árbol de fallas.

Paso 3. Construcción del Árbol de Fallas. Con base en el conocimiento del sistema y los eventos iniciadores en el estudio HAZOP, el árbol se construye manualmente. Cada evento está etiquetado secuencialmente con una B para evento básico o no desarrollado, M para evento intermedio y T para evento superior. El procedimiento comienza en el evento superior, liberación importante de inflamables, y determina los posibles eventos que podrían conducir a este incidente como:

Ml: Derrame durante descarga de camión

M2: Rotura del tanque por evento externo

B1: Se rompe el drenaje del tanque

M3: Ruptura del tanque por implosión

M4: Rotura del tanque por sobrepresión

Los eventos M1, M2, MS y M4 requieren mayor desarrollo. Sin embargo, existen datos históricos y de confiabilidad adecuados para el Evento Bl que permiten tratarlo como un evento básico. El análisis avanza hacia abajo, un nivel a la vez, hasta que todos los mecanismos de falla hayan sido investigados a la profundidad adecuada. Los eventos básicos y los eventos no desarrollados están simbolizados por círculos y diamantes, respectivamente. No se considera necesario ni posible un mayor desarrollo de los acontecimientos no desarrollados.

El árbol de fallas final (Figura 12) es esencialmente idéntico al presentado por Ozog (1985). Sin embargo, se han agregado varios cuadros de eventos intermedios para mayor claridad.

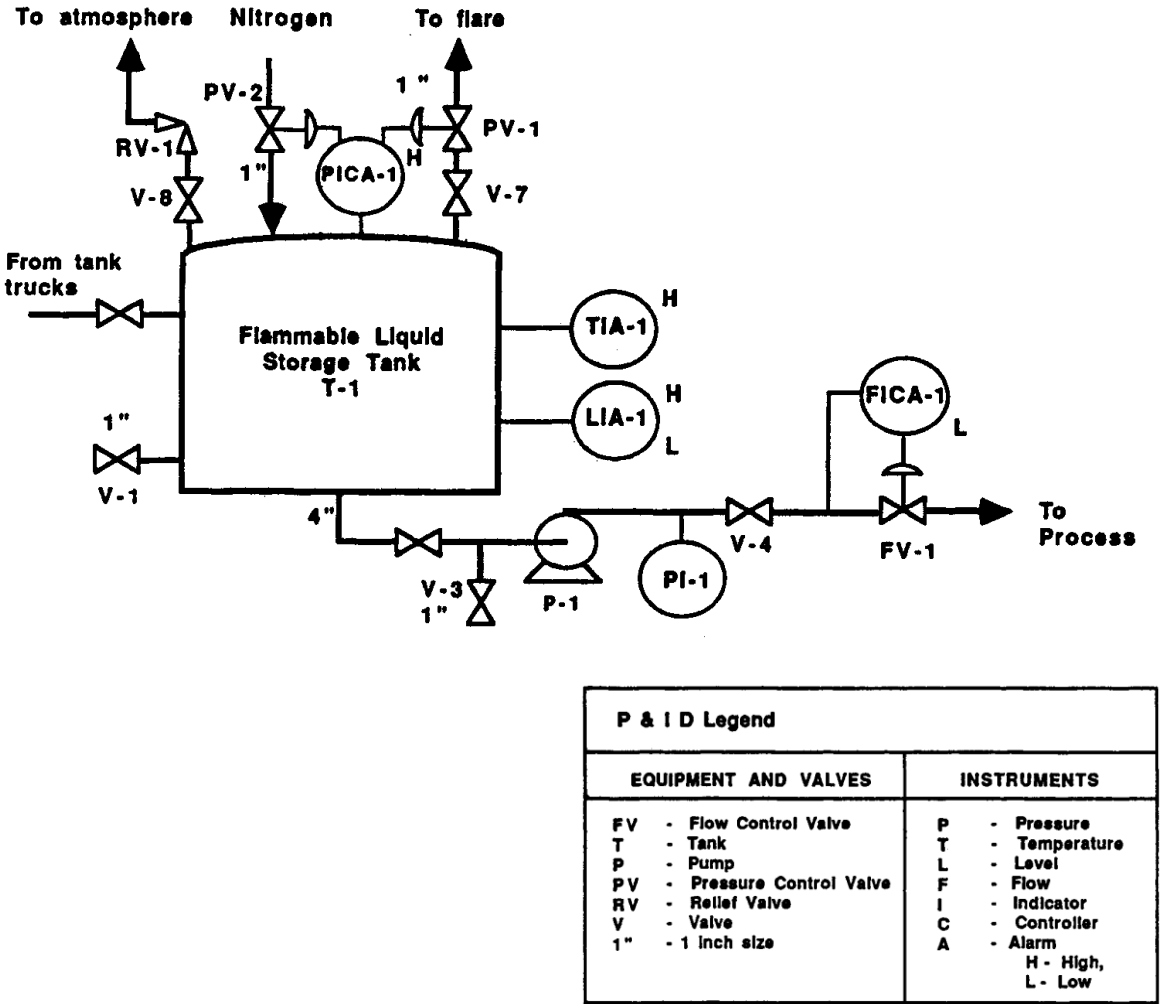


Figura 11: P&ID del Tanque

Paso 4. Examen Cualitativo de la Estructura. La clasificación cualitativa se realiza mejor utilizando el análisis de conjunto de corte mínimo (Apéndice D-CPQRA) para este problema. Sin embargo, la inspección por sí sola muestra los cinco mecanismos principales que conducen a una liberación importante de inflamables. Por ejemplo, los eventos individuales B1, B3, B4, B5 y B6 conducen al evento superior. En este ejemplo, la clasificación cualitativa tiene un beneficio limitado ya que se desea un valor de frecuencia para CPQRA.

En este paso, el analista debe revisar los conjuntos de cortes mínimos para asegurarse de que representen accidentes reales y posibles. Un conjunto de corte mínimo que no causará el evento superior es una indicación de un error en la construcción del árbol de fallas o en la determinación de los conjuntos de corte mínimo.

Paso 5. Evaluación Cuantitativa del Árbol de Fallas. Para este ejemplo, se emplea el método de análisis puerta por puerta para cuantificar el árbol de fallas de la Figura 12. El árbol debe escanearse cuidadosamente en busca de eventos repetidos, ya que pueden provocar

errores numéricos. No hay eventos repetidos. El analista debe ingresar un valor numérico para la frecuencia (por año) o la probabilidad (adimensional) en cada evento base (las Secciones 5.5 y 5.6 enumeran las fuentes de datos comunes).

El cálculo comienza en la parte inferior del árbol y continúa hacia arriba hasta el evento superior. Se presenta un cálculo para la rama más a la izquierda del árbol hasta el evento Ml, derrame durante la descarga del camión. Para mayor claridad, en este ejemplo sólo se utiliza una cifra significativa.

La compuerta más baja es M9, sobrellenado del tanque y liberación vía RV-I. Las dos entradas a esta puerta AND son probabilidades.

$$P(M9) = P(B15) \times P(B16)$$
$$= (1\times10^{-2}) \times (1\times10^{-2}) = 1\times10^{-4}$$

Al mismo nivel que M9 se encuentra la Puerta MlO, rotura del tanque por reacción. Hay cuatro entradas para esta puerta AND, todas probabilidades, y la fórmula de la Tabla 3.3 puede generalizarse como:

$$P(M10) = P(B17) \times P(B18) \times P(B19) \times P(B20)$$
$$= (1\times10^{-3}) \times (1\times10^{-2}) \times (1\times10^{-1}) \times (1\times10^{-1}) = 1\times10^{-7}$$

Las puertas M9 y M1O son entradas a la puerta M5, derrame importante del tanque. Hay dos probabilidades de entrar por la puerta OR:

$$P(M5) = 1 - [1 - P(B9)][1 - P(M10)] \cong P(M9) + P(M10)$$
$$\cong (1\times10^{-4}) + (1\times10^{-7}) \cong 1\times10^{-4}$$

La puerta Ml es un brazo de eventos intermedio y es una puerta AND con dos entradas, una frecuencia y una probabilidad.

$$P(M1) = F(B2) \times P(M5)$$
$$= 300 \times año^{-1} \times (1\times10^{-4}) = 3\times10^{-2} \times año^{-1}$$

De manera similar, se pueden calcular todas las demás frecuencias y probabilidades, hasta el evento superior. La frecuencia máxima de eventos (T), liberación importante de materiales inflamables, es de 3 x 10^{-2} $años^{-1}$ en una liberación cada 30 años.

Las frecuencias de los cinco eventos intermedios principales que conducen a esto son

Ml: Derrame durante la descarga del camión 3x10^{-2} $año^{-1}$

M2: Ruptura del tanque debido a un evento externo 3x10^{-5} $años^{-1}$

Bl: Interrupción del drenaje del tanque $1x10^{-4}$ $años^{-1}$

M3: Ruptura del tanque por implosión $2x10^{-3}$ $años^{-1}$

M4: Rotura del tanque por sobrepresión $2x10^{-5}$ $años^{-1}$

Desde la evaluación cuantitativa, las fallas debidas a Ml y M3 contribuyen más al evento superior; La frecuencia y las medidas correctivas serían más productivas en estas áreas.

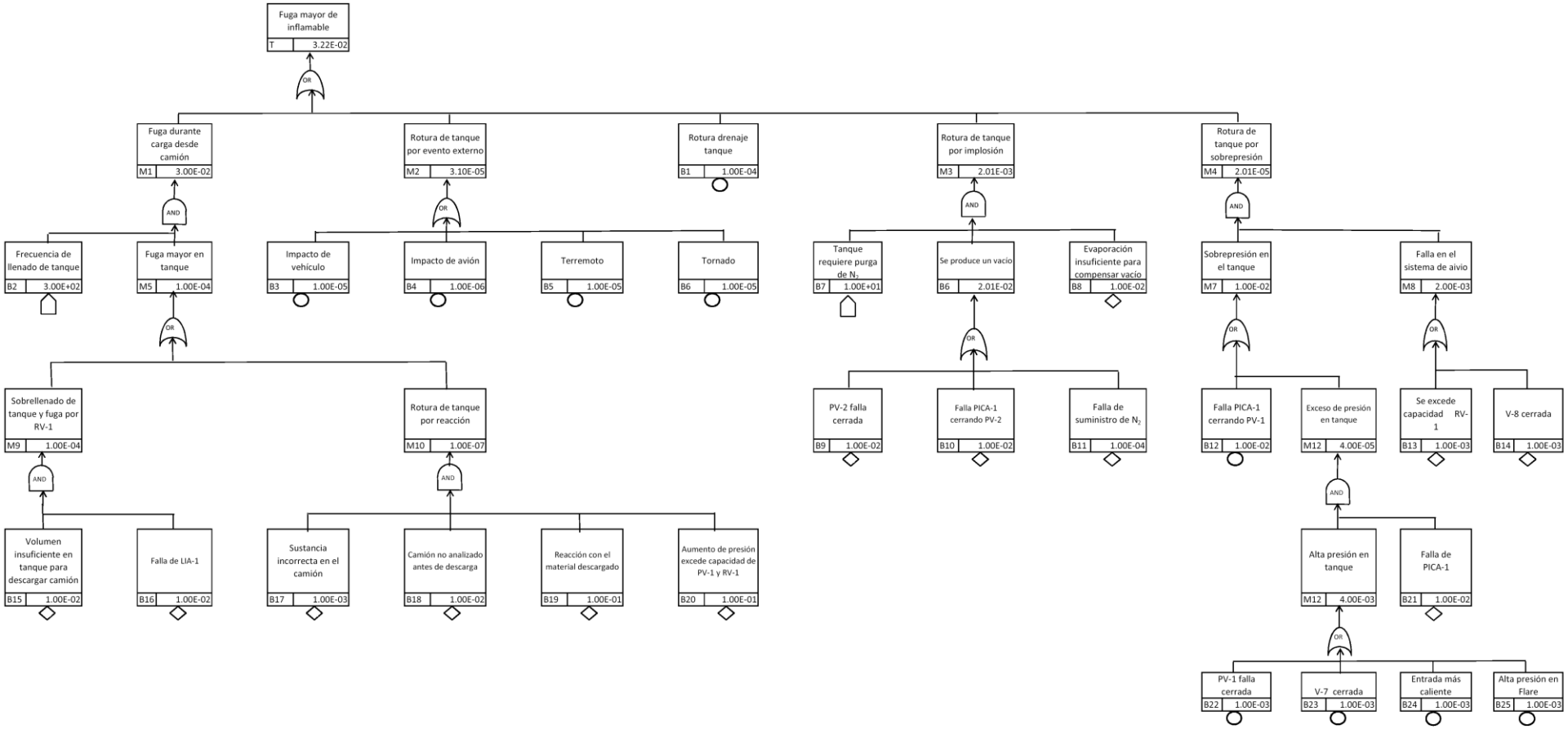


Figura 12: Árbol de fallas completo