

# Introducción a la confiabilidad

- En resumen para asegurar un alto grado de confiabilidad humana en situaciones de emergencia, cuartos de control, así como en la cabina de un piloto de avión o en una planta de procesamiento de químicos, los sistemas deben ser diseñados en concordancia con buenas prácticas seguras para las personas.
- Además es importante que todos los procedimientos para cada situación debe ser anticipada, claramente leíble, y finalmente debe ser ensayada por el operador de forma periódica, en simulacros de emergencia, preferiblemente con simuladores que modelen situaciones reales.

# Introducción a la confiabilidad

- A menudo podremos caracterizar el comportamiento humano bajo situaciones de emergencia y sugerir acciones (medidas) que mejoren la confiabilidad humana.
- Es realmente difícil en cambio obtener de manera cuantitativa datos relacionados con la probabilidad de falla, como fue dicho tales situaciones ocurren de manera infrecuente y menudo no son correctamente documentadas.
- Aún más difícil es obtener una respuesta realista de un simulacro del experimento, cuando los sujetos que son sometidos a prueba, saben que es un simulacro y no una situación de la vida real.

# Métodos de Análisis

- Probablemente la tarea más importante para reducir o eliminar la probabilidad de accidentes, es identificar los mecanismos por los cuales estos se producen.
- La habilidad de lograr identificarlos a tiempo requiere que el análisis posea un entendimiento y comprensión del sistema bajo estudio, tanto como funciona, como la limitación de sus componentes.
- Incluso el más experto analista está en riesgo de obviar modos de falla críticos, sin embargo, el análisis puede ser llevado de forma sistemática evitando estos riesgos.

# Métodos de Análisis

- A continuación se describirán tres metodologías que son las más empleadas para un análisis seguro y sistemático:
  - Métodos de Falla.
  - Árbol de Fallas.
  - Árbol de eventos.

# Modo de Fallas y Análisis de Efectos (FMEA)

- Es una de las metodologías más ampliamente utilizadas para describir los posibles modos de fallo de los componentes que conforman un sistema y analizar las consecuencias y características de cada modo de falla en el sistema como un todo.
- El método es primordialmente cualitativo en esencia, sin embargo se estiman algunas probabilidades de falla a menudo.
- Hay muchas variantes del FMEA y una de ellas se ejemplifica en la figura siguiente:

### Modo de Falla y Análisis de Efectos

1. Subsistema: \_\_\_\_\_ 2.DWG #: \_\_\_\_\_ 3. Elaborado por: \_\_\_\_\_ 4. Fecha: \_\_\_\_\_

Componente	Modos de Falla	Causa de la Falla	Posibles Efectos	Probabilidad de ocurrencia	Nivel de riesgo	Acciones para reducir la tasa de fallo o efectos
Carcasa del motor	Ruptura	a. Pobre construcción b. Materiales defectuosos c. Daño durante la manipulación. d. Sobre-presurización	Destrucción del misil	0.0006	Critica	Control meticuloso del proceso de fabricación que garantice un correcto acabado de cada una de las partes del misil bajo los estándares apropiados. Alto control de calidad de los materiales empleados para eliminar defectos. Inspecciones y pruebas de presión de todos las carcasas. Proporcionar un adecuado ambiente durante el transporte del motor.
Grano propelente	a. Agrietamientos b. Vacíos c. Proceso de unión	a. Estrés anormal de cura. b. Baja temperatura excesiva. c. Efectos del tiempo.	Tasa de calentamiento excesiva, sobre-presurización; ruptura de la carcasa del motor en operación normal.	0.0001	Critica	Producción controlada con rigurosidad. Almacenamiento y operación únicamente en los límites prescritos. Formulación compatible para combatir los efectos del envejecimiento por tiempo.
Alineador	a. Separación de la carcasa del motor b. Separación del motor de granos o aislamiento	a. Inadecuada limpieza del motor después de la fabricación. b. Uso de materiales incompatibles con la unión. c. Fallas en el proceso de adecuado de unión.	Tasa de calentamiento excesiva; Sobre-presurización; Ruptura de la carcasa durante la operación.	0.0001	Critica	Estricta vigilancia en los procesos de mantenimiento y limpieza. Estricta inspección post limpieza de la carcasa del motor que garantice que todos los contaminantes fueron eliminados.

# FMEA versión mejorada

- En una versión ampliada del FMEA la información mostrada en la figura podría ser categorizada en 4 niveles de falla:
  - a) Despreciable: No tiene efecto en el funcionamiento.
  - b) Marginal: Podría reducir la funcionalidad del sistema.
  - c) Crítico: Degrada por completo el funcionamiento del sistema.
  - d) Catastrófico: Podría causar consecuencias severas como lesiones o muertes.
- Otras columnas se podrían añadir al FMEA. Por ejemplo, una lista de métodos para la detección de cada falla, o bien una lista de previsiones compensatorias para cada modo de falla podría sugerirse, para enfatizar la relativa gravedad de los modos.
- La prioridad del FMEA es enfatizar en los fenómenos físicos básicos que podrían ocasionar que un componente falle

# Árbol de eventos

- En muchos escenarios de accidentes, el evento que lo ocasiona (Hablando del componente que falló) podría presentar un amplio espectro de posibilidades del porque falló, iniciando por los despreciables hasta llegar a los catastróficos.
- Las consecuencias podrían ser determinadas por la secuencia de acontecimientos que llevó al accidente, considerando los componentes o subsistemas que fallaron y que originaron el problema, particularmente los dispositivos de seguridad o protección y los errores humanos cometidos en respuesta al evento que lo ocasionó.
- En este tipo de situaciones podría ser de utilidad un método inferencial o inductivo, que se inicia preguntándose: ¿Qué pasa si, el evento inicial ocurre? Luego se analiza cada posible consecuencia del evento que resultaría de asumir una falla o un éxito de los componentes y las personas afectadas como consecuencia del accidente.



# Árbol de eventos

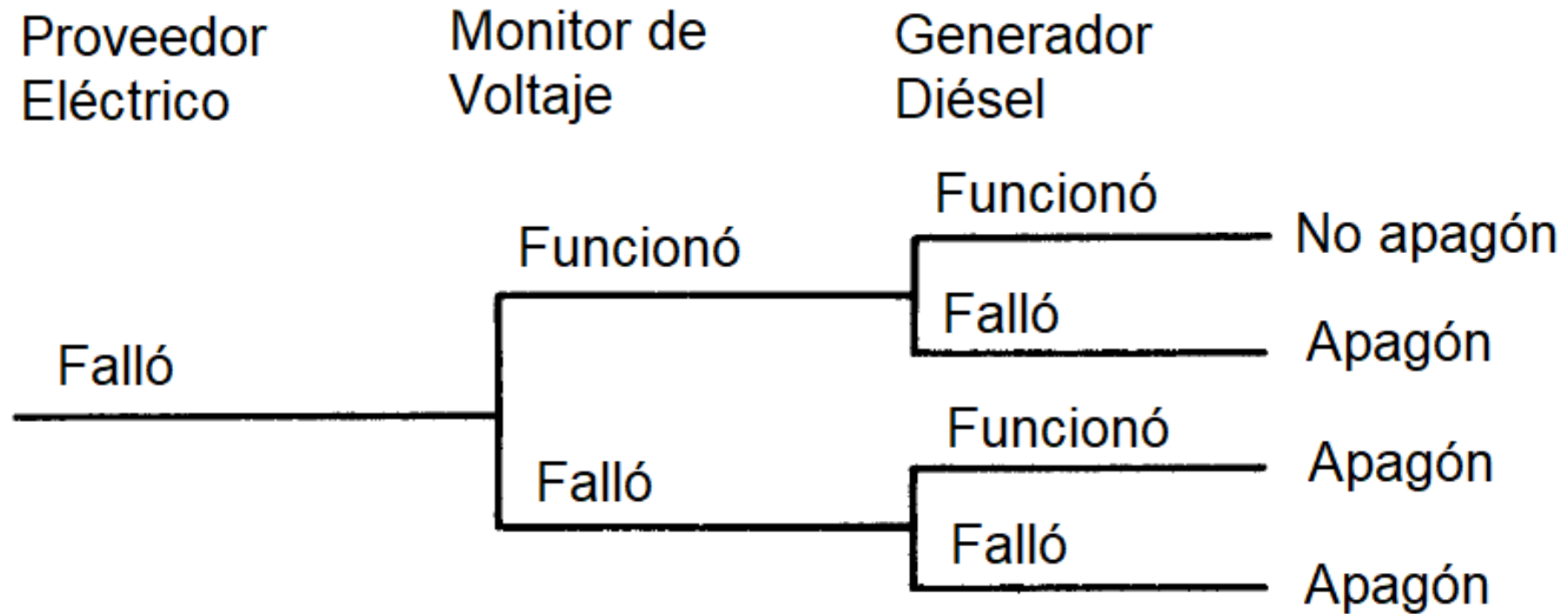
- Luego de que las consecuencias son establecidas se puede intentar colocar probabilidades en cada evento si fuese necesario un análisis cuantitativo.
- El árbol de eventos es una variante o adaptación particular de la forma generalizada de los “**decision tree**” utilizados en finanzas y economía.

A continuación se describe una situación real que puede ser empleada a modo de ejemplo:

# Ejemplo: Proveedor del servicio eléctrico del hospital

- Suponga que se requiere examinar los efectos de una falla en el suministro de un proveedor eléctrico de un hospital, con el propósito de estimar la probabilidad de un apagón en el hospital, asociado con otras consecuencias que podrían ser fatales.
- Para simplificar se asumirá que el sistema será analizado en términos de 3 componentes.
  1. El proveedor eléctrico (Jasec, ICE, FyL).
  2. Generador a Diésel que suministra electricidad en caso de falta por el proveedor.
  3. Un sistema de monitoreo de voltaje que supervisa el suministro del proveedor para enviar la señal de activación al sistema de emergencia para activar el generador a Diésel.

# Diagrama de Árbol de eventos del ejemplo



# Detalles del diagrama de Árbol de eventos

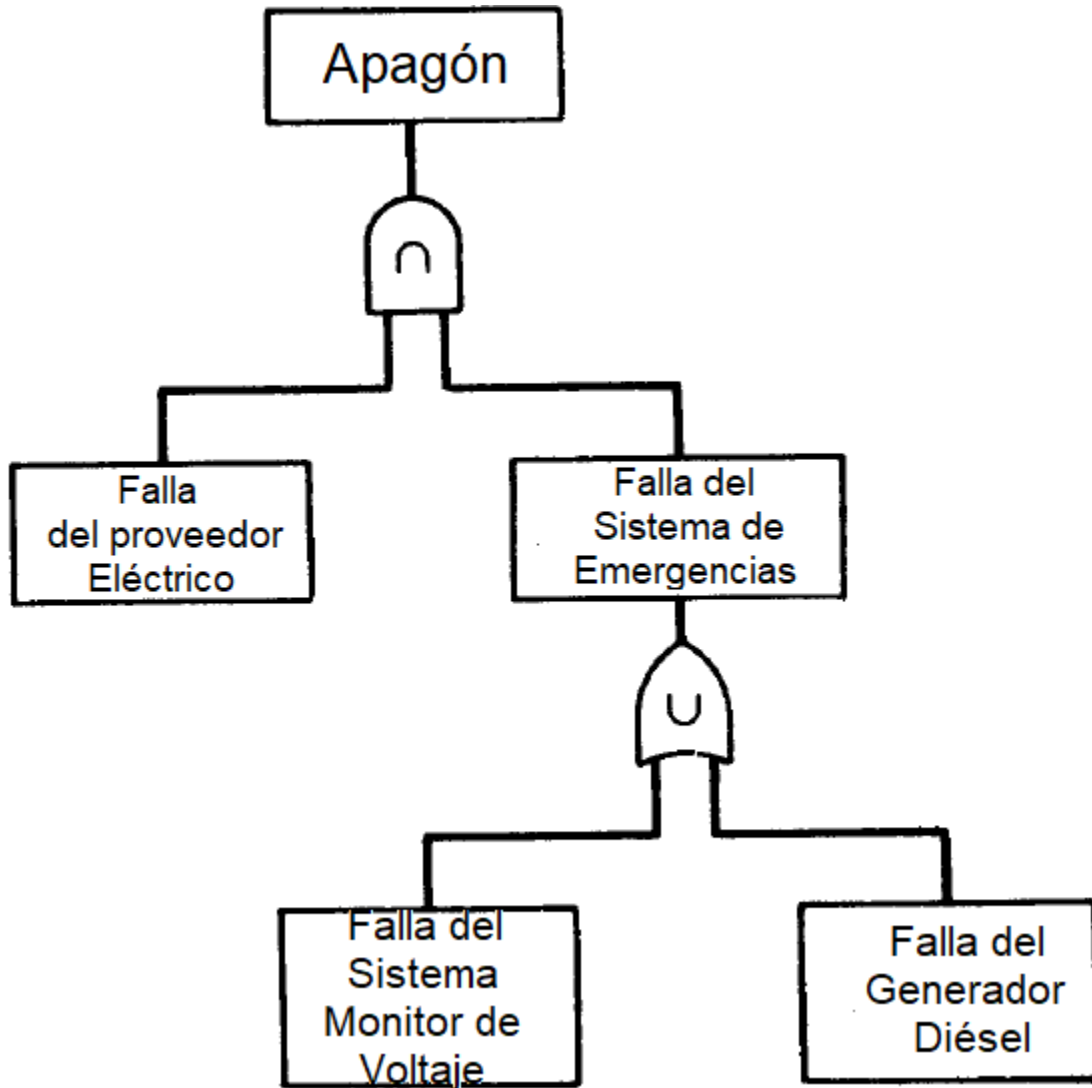
- El árbol podría simplificarse aún más si se considera que el monitor de voltaje no envía la señal de activación al sistema de emergencia y dado esto, el generador diésel jamás podría operar, cuya probabilidad asociada a esta secuencia es cero.
- Se pueden determinar algunas probabilidades de izquierda a derecha, asociadas a la probabilidad de cada evento en el árbol.
- Sea  $P(i)$  = Probabilidad del evento inicial.
- Sea  $P(v)$  = Probabilidad de falla del monitor.
- Sea  $P(g)$  = Probabilidad de falla del Generador a Diésel.

$$P(F) = P(i)P(v) + P(i)(1 - P(v))P(g)$$

# Árbol de fallas

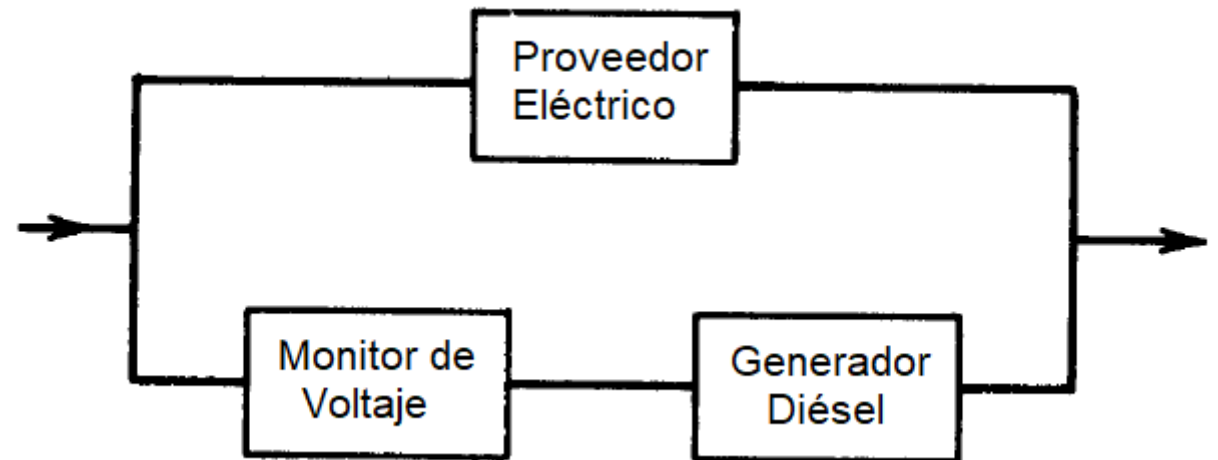
- El análisis por árbol de fallas es un método deductivo para determinar las potenciales causas de accidentes, o de forma generalizada estimar las probabilidades de que los sistema fallen.
- En sentido estricto el análisis por árbol de fallas puede ser visto como una alternativa al uso de diagrama de bloques de confiabilidad, al determinar la confiabilidad del sistema en términos de los componentes correspondientes.
- El análisis por árbol de fallas se centra en encontrar las causas de eventos indeseados, en relación con un evento principal, mientras el árbol de fallas se dibuja con el evento principal en lo más alto.
- Luego se procede a agregar los eventos hacia abajo que incrementarán los detalles, causas o raíz que originó el evento principal.
- Los eventos principales en el tope del diagrama usualmente corresponden a fallas de mayor trascendencia y que generan las mayores consecuencias, produciendo graves riesgos de seguridad o significativas pérdidas económicas.

# Árbol de Fallas del ejemplo

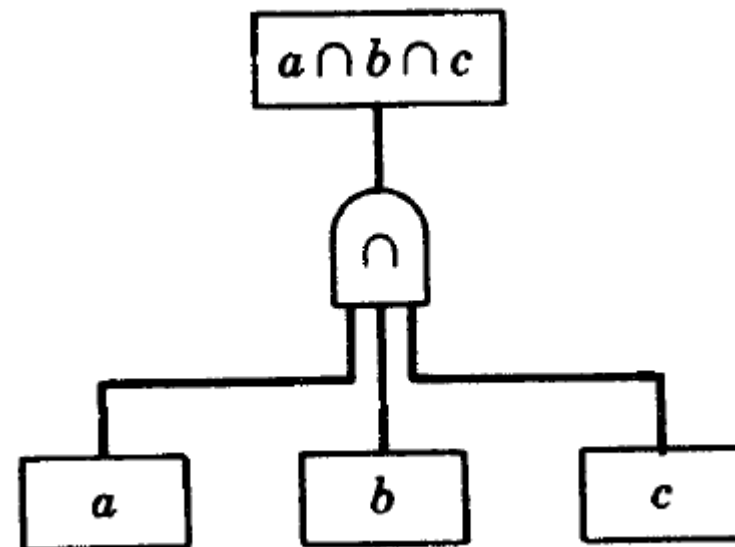
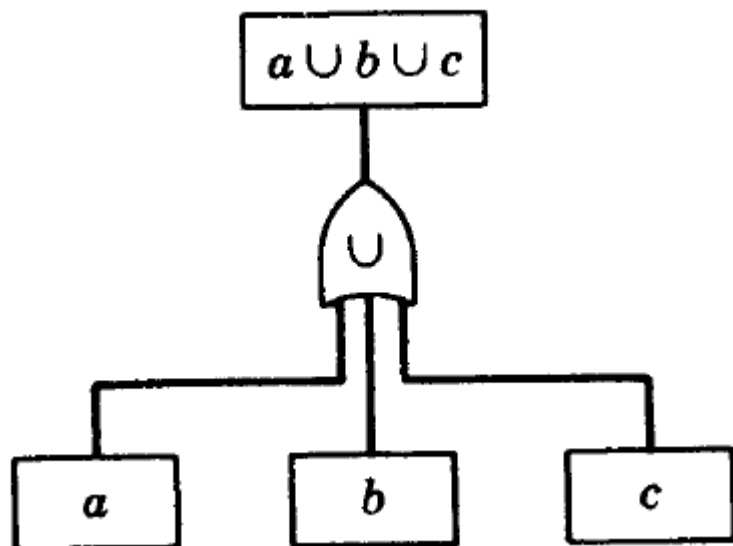


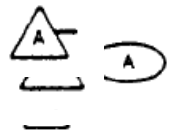
Como puede observarse el diagrama de fallas consiste en bloques con los eventos y estructuras lógicas AND y OR.

## Diagrama de confiabilidad



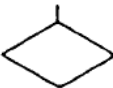



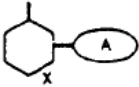




# Nomenclatura



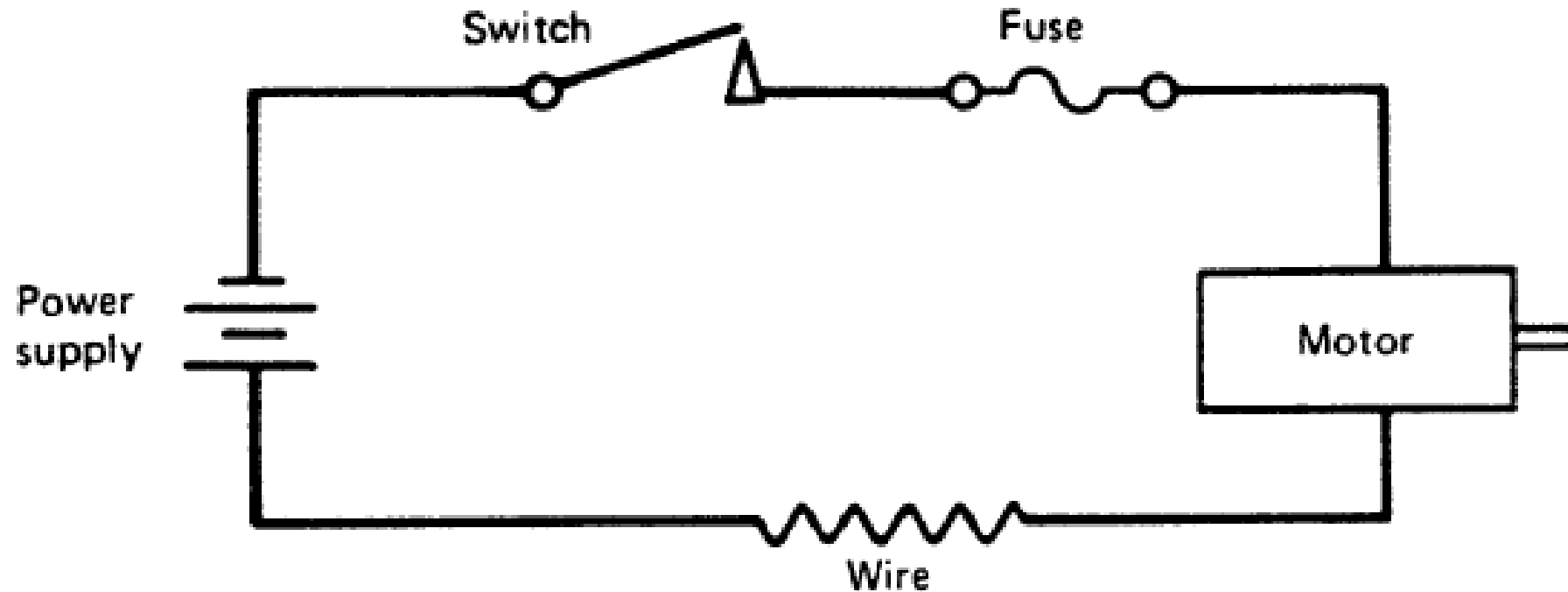


# Nomenclatura

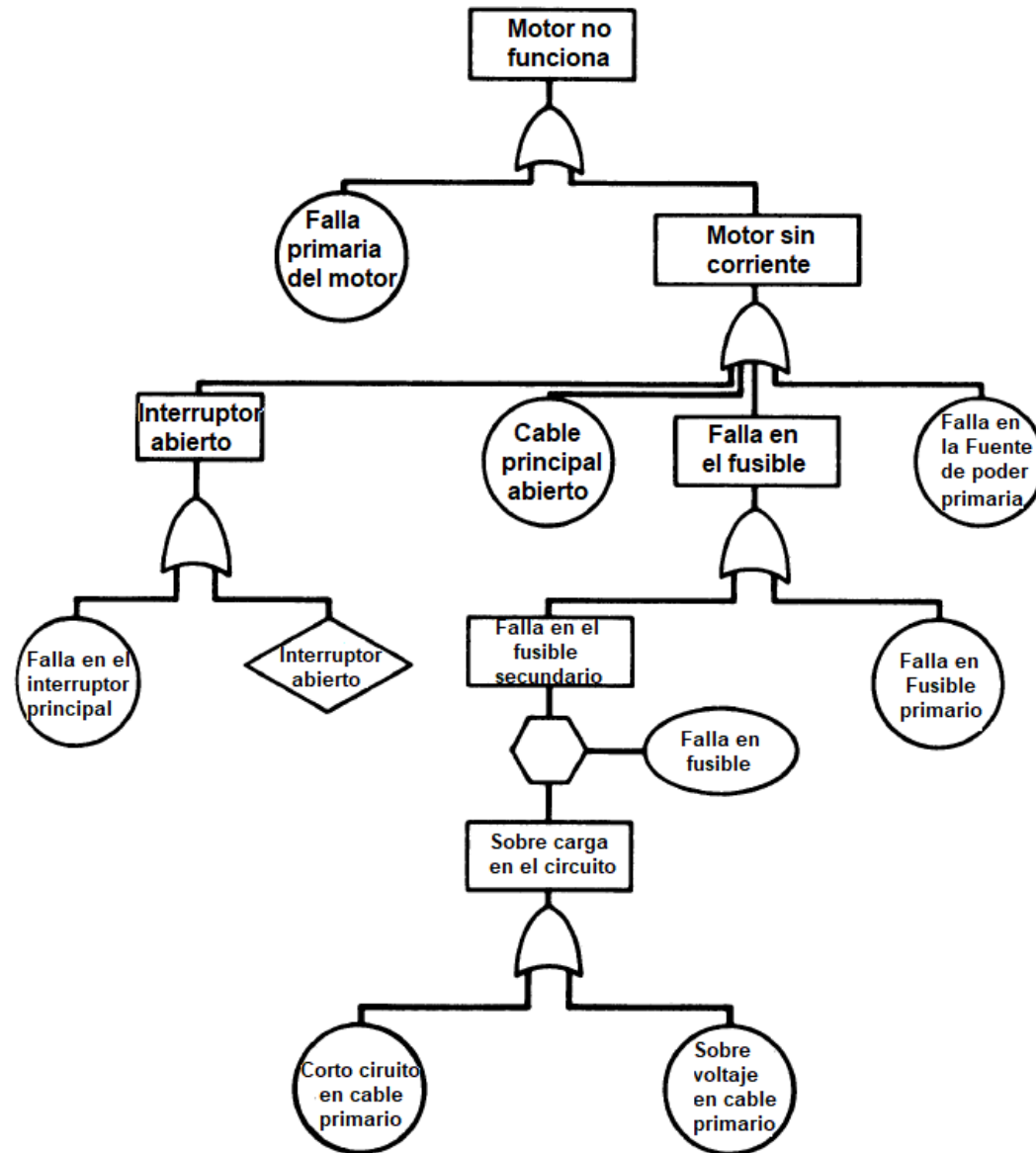
Símbolo	Nombre	Descripción
	Rectángulo	Evento de falla; usualmente es resultado de la combinación lógica de otros eventos
	Círculo	Evento primario de falla independiente
	Diamante	Evento de Falla no desarrollado en su totalidad, sus causas son desconocidas, solo es asumido por el evento primario de falla
	Casa	Normalmente es un evento básico, no es un evento de falla
	Compuerta OR	Operación unión de eventos; Su salida proporciona un evento válido si una de sus dos entradas lo es.
	Compuerta AND	Operación intersección de dos eventos; Su salida solo es válida solo si sus dos entradas lo son
	Compuerta INHIBIDORA	La salida solo es válida si X lo es y la condición A está presente. Funciona parecido a una compuerta AND y es utilizada para eventos secundarios.
	Triángulo de entrada	Proporciona una herramienta para evitar repetir secciones de un árbol de fallas o para transferir los resultados de un árbol de fallas a otra página. Usualmente se encuentra en la parte baja del diagrama de árbol.
	Triángulo de salida	Evita repetir secciones del árbol de fallas y se ubica en la parte alta del árbol de fallas para indicar que esa sección es un sub-árbol de otro evento.



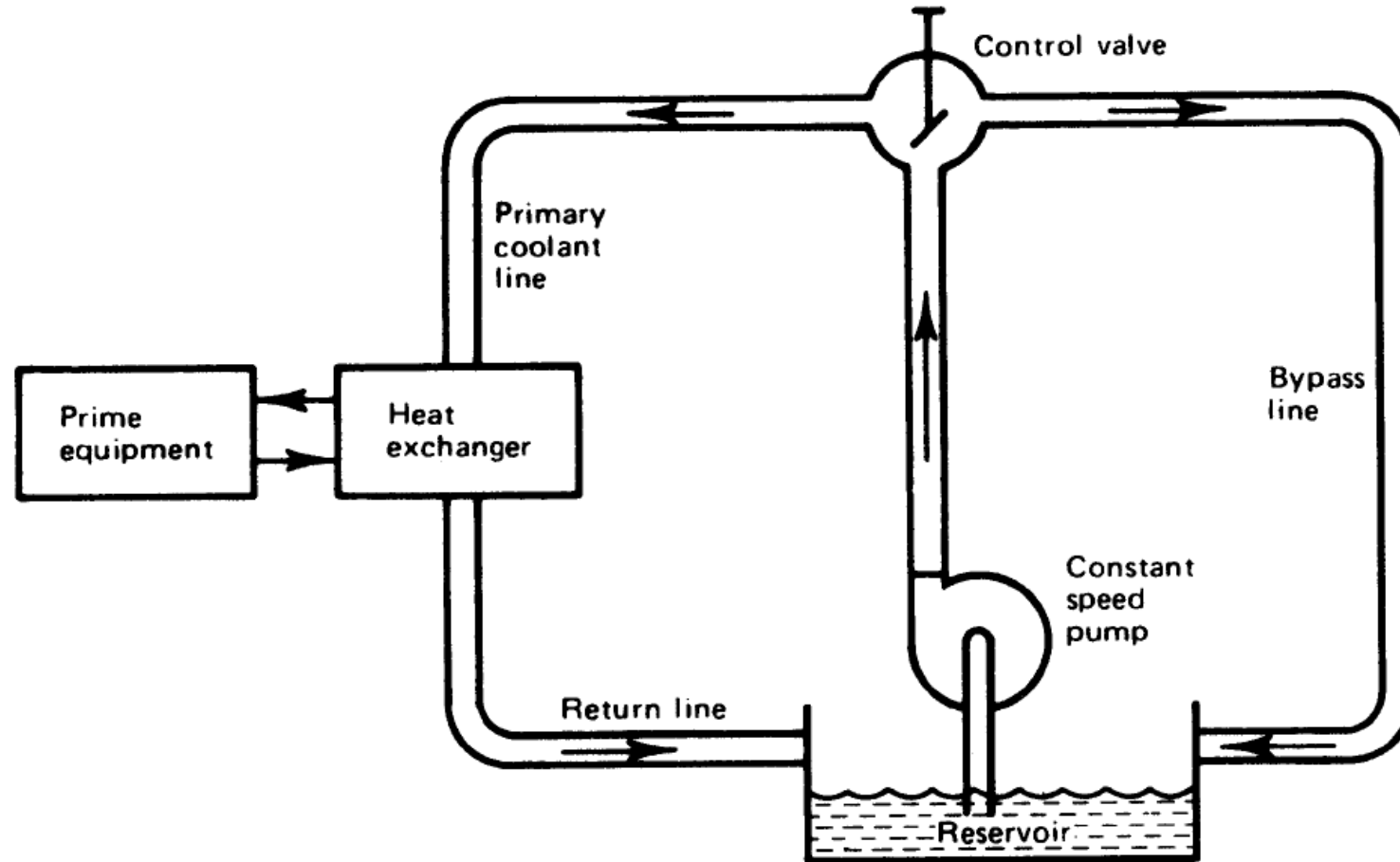
Ejemplo: El evento principal es el fallo del motor al operar



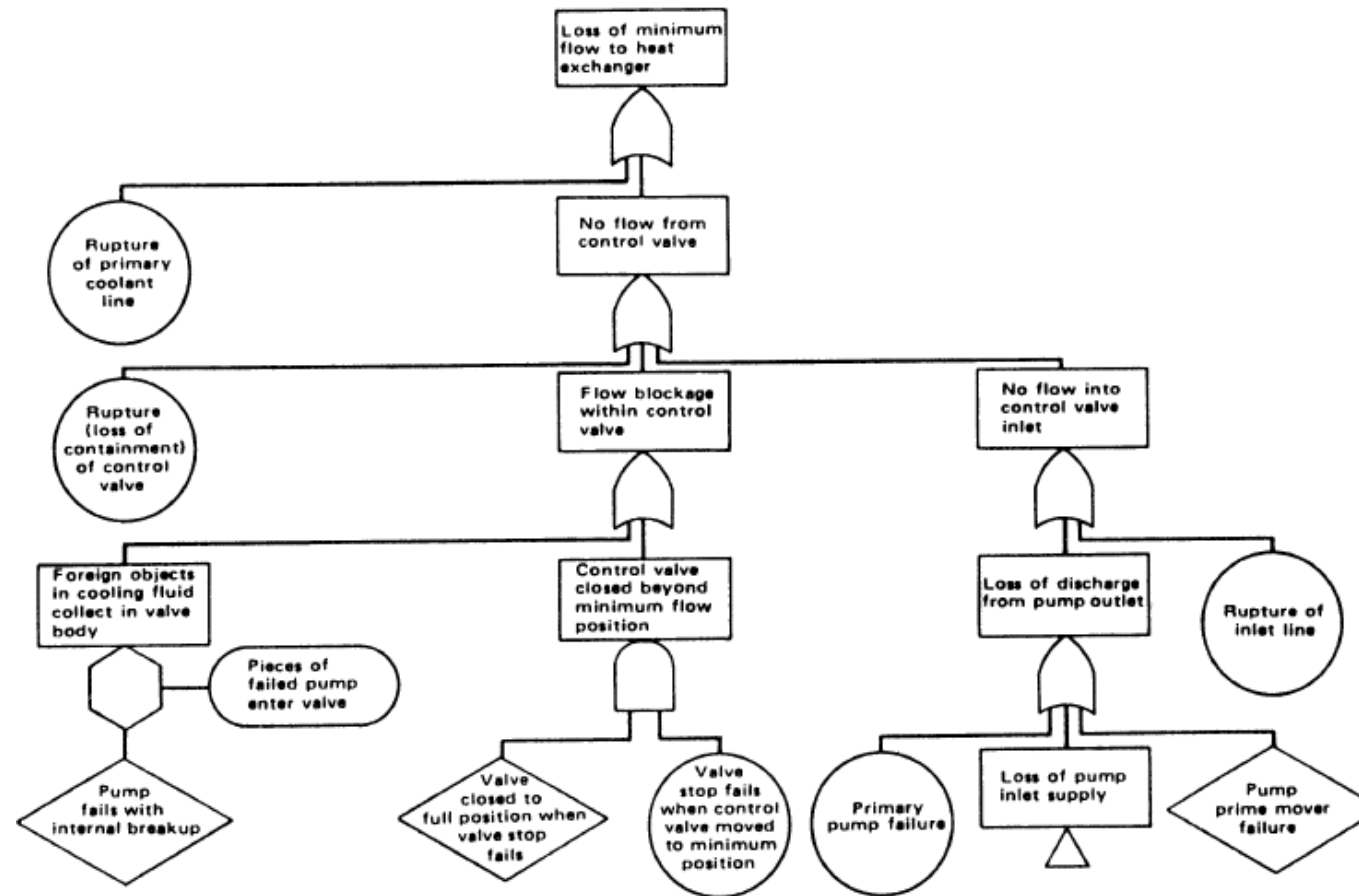
# Diagrama de árbol del ejemplo



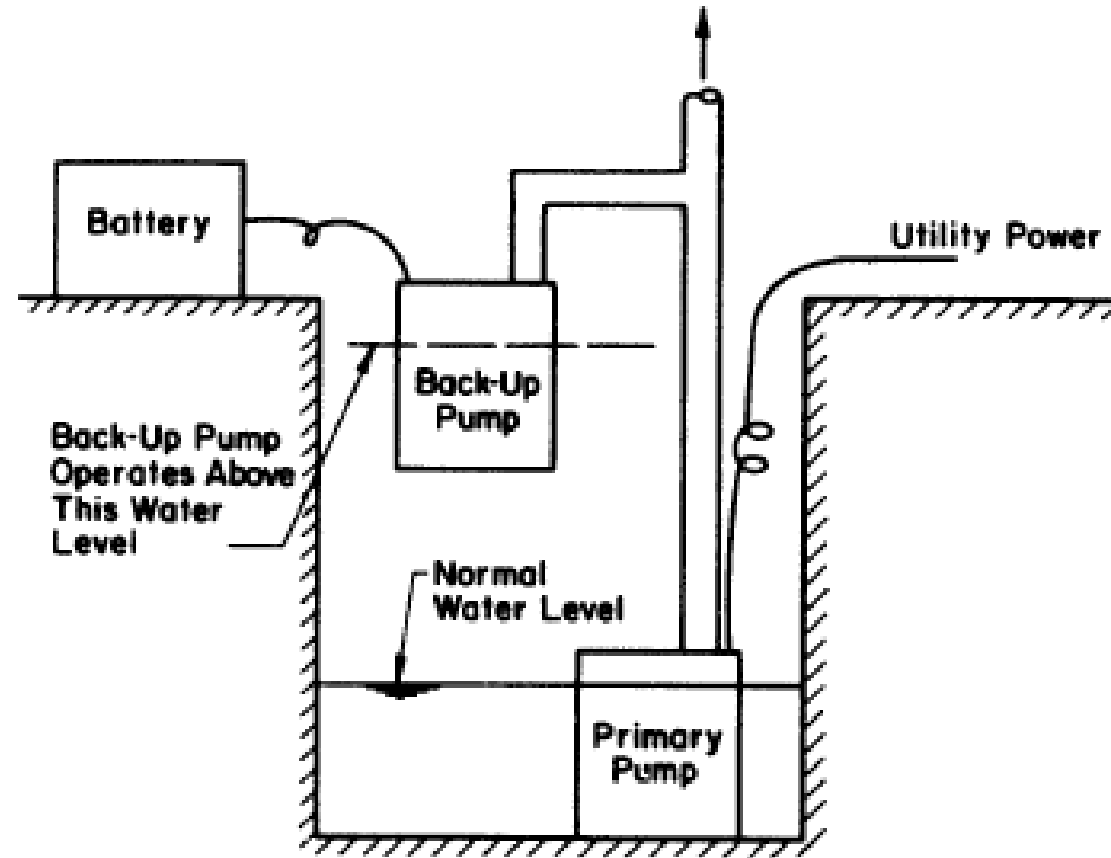
Ejercicio: Evento principal es la pérdida del flujo mínimo en el intercambiador de calor



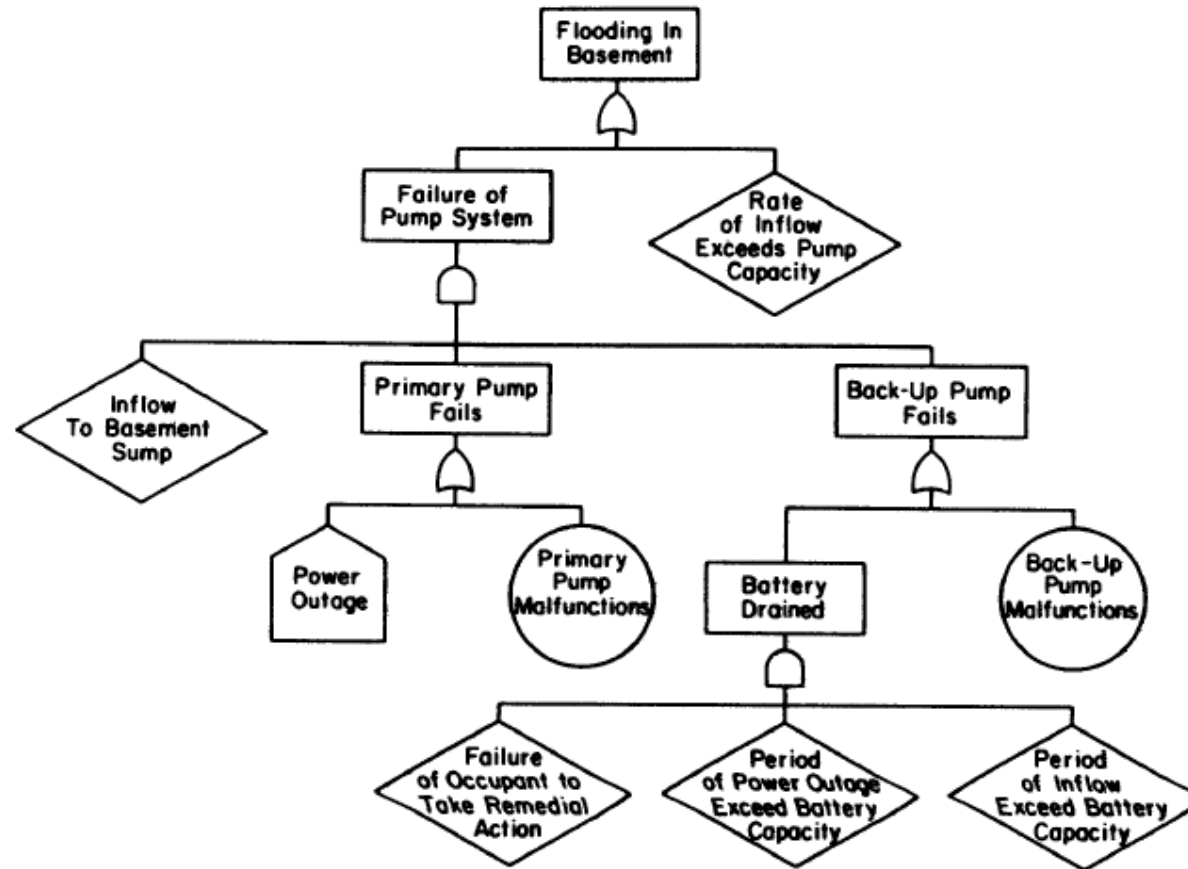
# Ejercicio: Diagrama de árbol del ejercicio



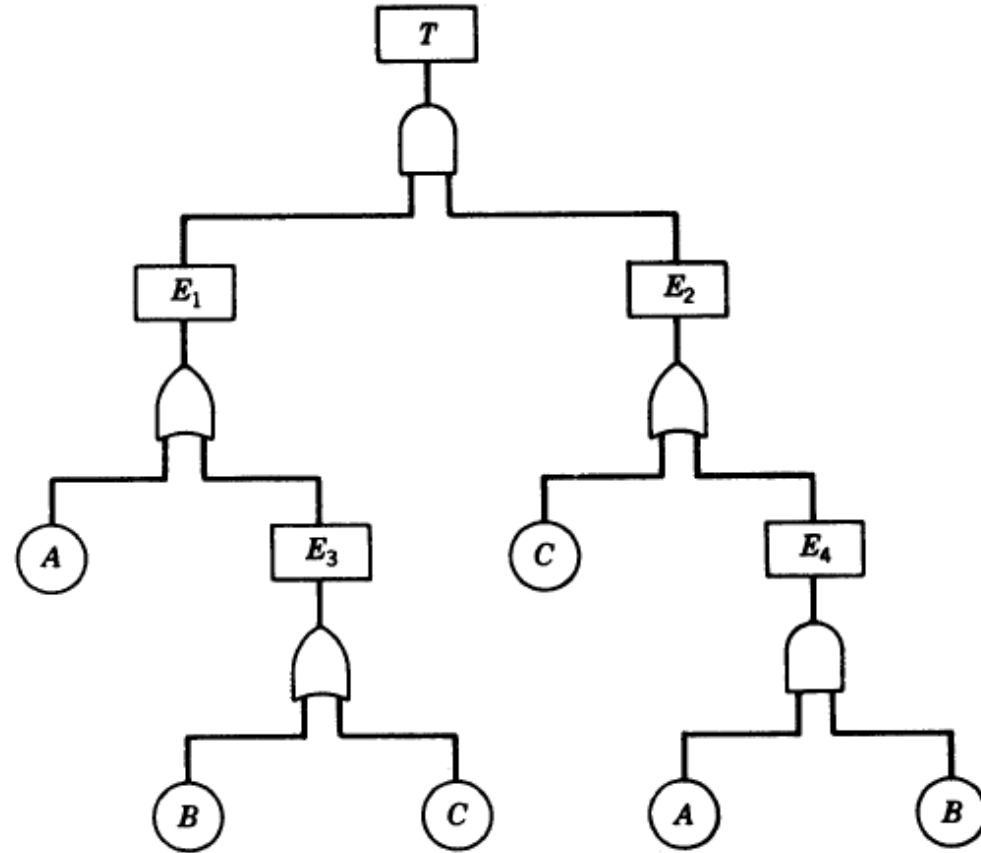
Ejemplo: Este sistema posee redundancia proporcionada por la batería y la segunda bomba. Escriba el árbol de fallas por un sótano protegido por este sistema



# Diagrama para el ejemplo



# Evaluación cualitativa



Top-down

$$T = E_1 \cap E_2$$

$$E_1 = A \cup E_3; \quad E_2 = C \cup E_4$$

$$T = (A \cup E_3) \cap (C \cup E_4).$$

$$E_3 = B \cup C; \quad E_4 = A \cap B.$$

$$T = [A \cup (B \cup C)] \cap [C \cup (A \cap B)].$$

Bottom-up

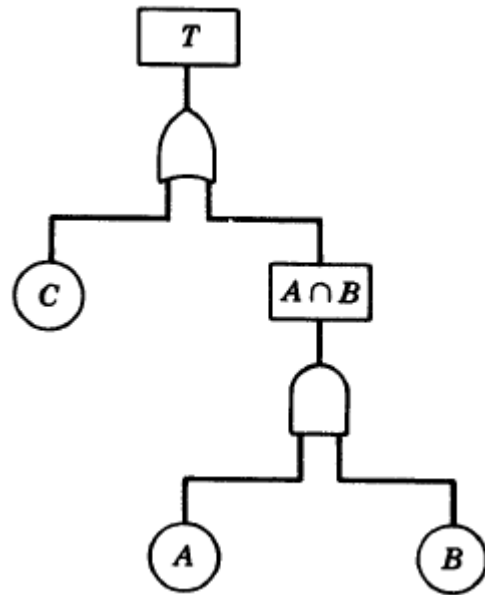
$$E_3 = B \cup C; \quad E_4 = A \cap B.$$

$$E_1 = A \cup E_3; \quad E_2 = C \cup E_4.$$

$$E_1 = A \cup (B \cup C)$$

$$E_2 = C \cup (A \cap B).$$

# Evaluación cuantitativa



## *Probability Relationships*

$$P\{T\} = P\{C\} + P\{B \cap A\} - P\{A \cap B \cap C\},$$

$$P\{T\} = P\{C\} + P\{A\}P\{B\} - P\{A\}P\{B\}P\{C\}.$$

$$P\{X \cup Y\} \approx P\{X\} + P\{Y\},$$

$$P\{T\} \approx P\{C\} + P\{A\}P\{B\}.$$



# Importancia

$$I_{M_i} = \frac{P\{M_i\}}{P\{T\}}$$

$$I_{X_i} = \frac{1}{P\{T\}} \sum_{X_i \in M_i} P\{M_i\}.$$