XVII Congreso de Confiabilidad

25 y 26 de noviembre de 2015. Parque Científico y Tecnológico de Bizkaia. Zamudio (Bizkaia)

MODELAR LA FIABILIDAD DE SISTEMAS USANDO ÁRBOLES DE FALLO ESTÁTICOS Y DINÁMICO

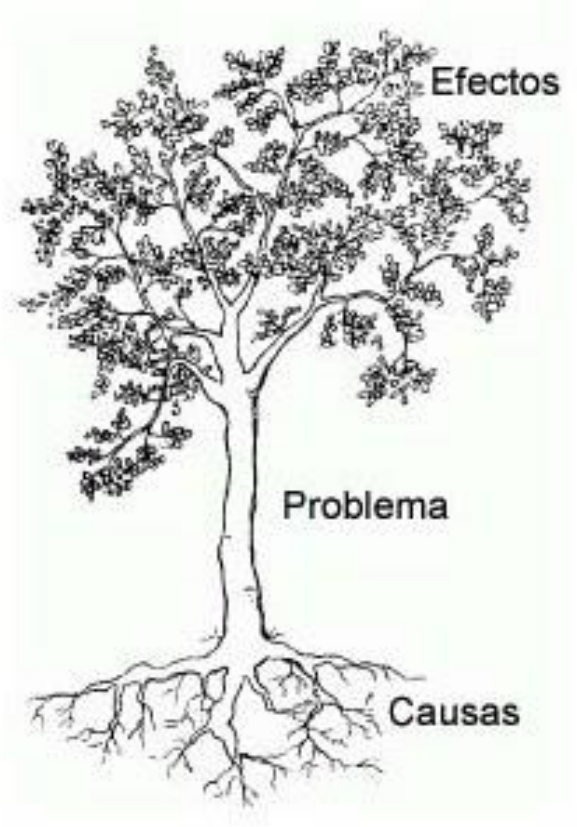
Marta López

Ingeniera de RAMS

INNOVATING SOLUTIONS

INTRODUCCIÓN

¿Qué es un árbol de fallos?



Técnica analítica-deductiva

- Se parte de la definición un evento indeseado del sistema
- Se evalúan los eventos básicos y la circunstancias que pueden dar lugar a ese evento

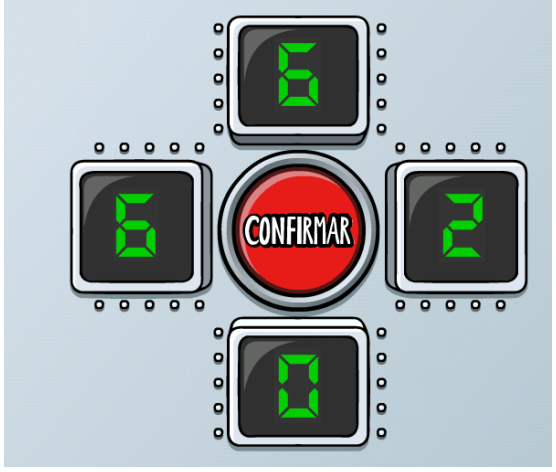
Evento indeseado:

Fallo de un sistema

INTRODUCCIÓN

¿Qué conseguimos con un árbol de fallos?

1. Identificar **causas**
2. Identificar **debilidades** y posibles **mitigaciones**.
3. Evaluar la **fiabilidad** o **seguridad**.
4. Identificar efectos de los **errores humanos**
5. Identificar el **impacto** de **cambios** en un sistema
6. Optimizar las **pruebas del sistema** y el **mantenimiento**

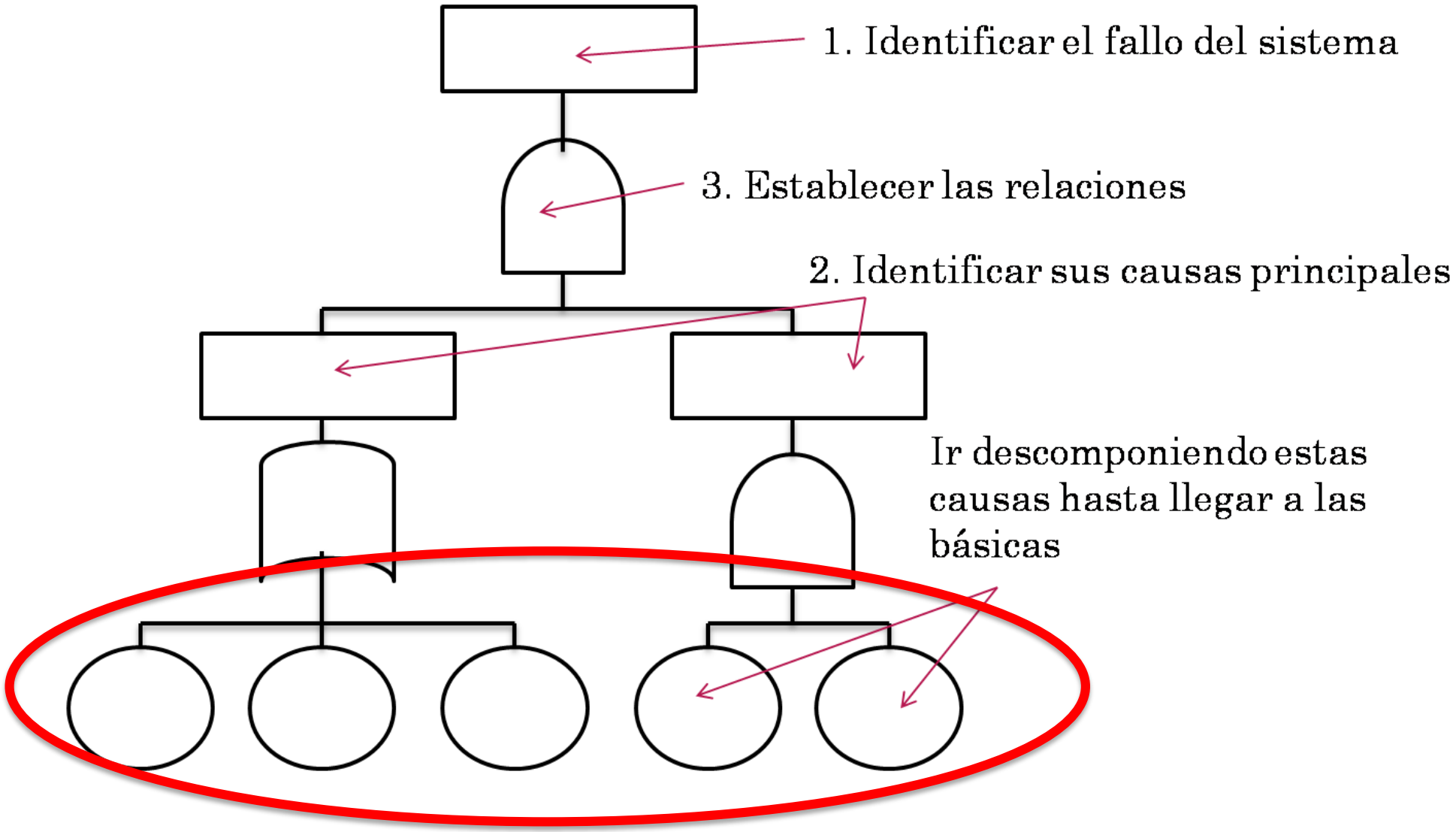


¿La clave?
Modelizar de forma realista el comportamiento del sistema

CONTENIDO

1. Modelización de eventos básicos
2. Modelización de relaciones
   a) Puertas clásicas en un FTA
   b) Puertas para relaciones secuenciales
   c) Condiciones
3. Resolución de FTAs mediante cadenas de Markov.
4. Conclusiones
5. El futuro

MODELIZACIÓN DE EVENTOS

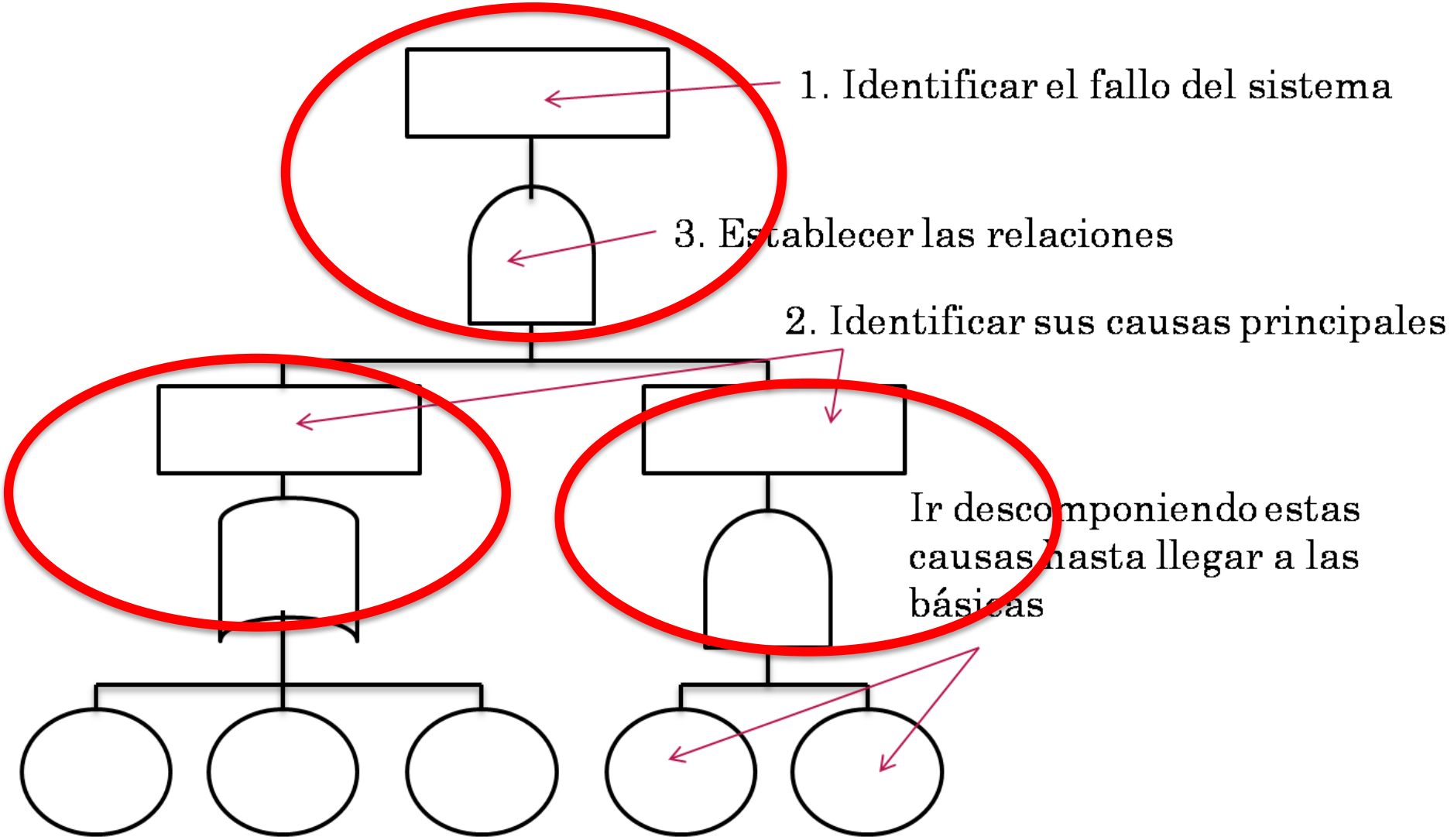


MODELIZACIÓN DE EVENTOS

Eventos básicos

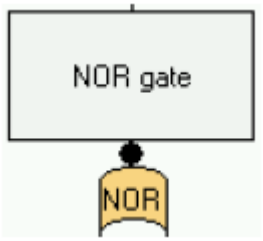
- **Componentes reparable**: tras un fallo es posible llevar a cabo una reparación y devolver al componente a un estado operacional. En este caso se puede conocer la probabilidad de fallo y el tiempo medio de reparación (MTTR, Mean Time to Restore) .
- **Componente no- reparable**: tras un fallo no es posible llevar a cabo una reparación y el componente tiene que ser sustituido. En este caso se puede conocer la probabilidad de fallo y el tiempo de sustitución (que será el valor asociado al MTTR).

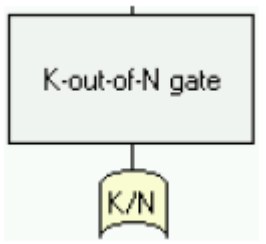
MODELIZACIÓN DE RELACIONES



MODELIZACIÓN DE RELACIONES

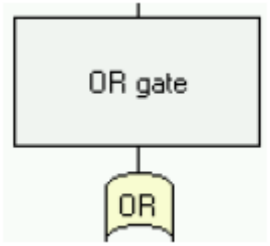
a) Puertas clásicas del FTA

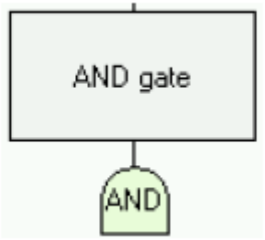


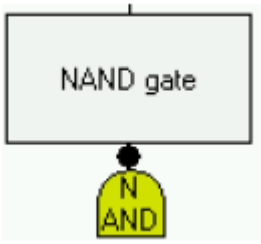


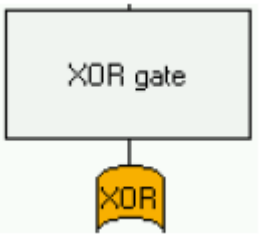
PUERTAS LÓGICAS

- OR, AND, NAND, NOR, XOR…









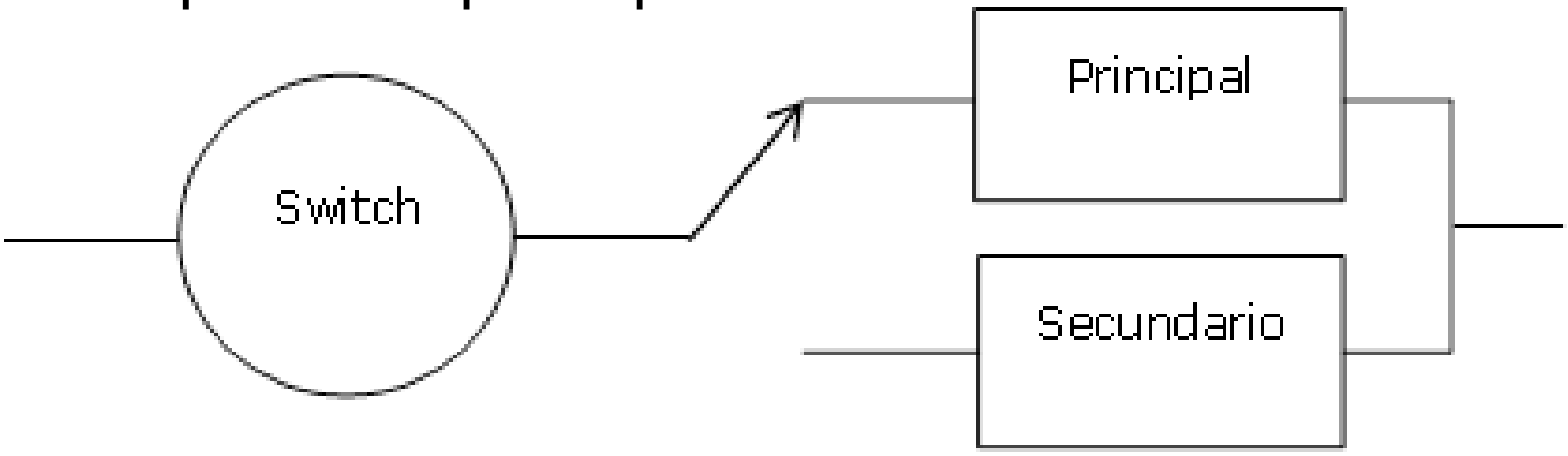
Estas puertas permiten **modelizar la relación entre eventos**

No son apropiadas para modelizar el orden en el que tienen que ocurrir los eventos básicos para que se produzca el fallo.

MODELIZACIÓN DE RELACIONES

b) Relaciones secuenciales: *Priority Gate*

- Un **componente principal** que está dando un servicio
- Un **componente de repuesto**, que se activa si el principal falla.
- Un ***switch***, que realiza el cambio cuando el componente principal falla.

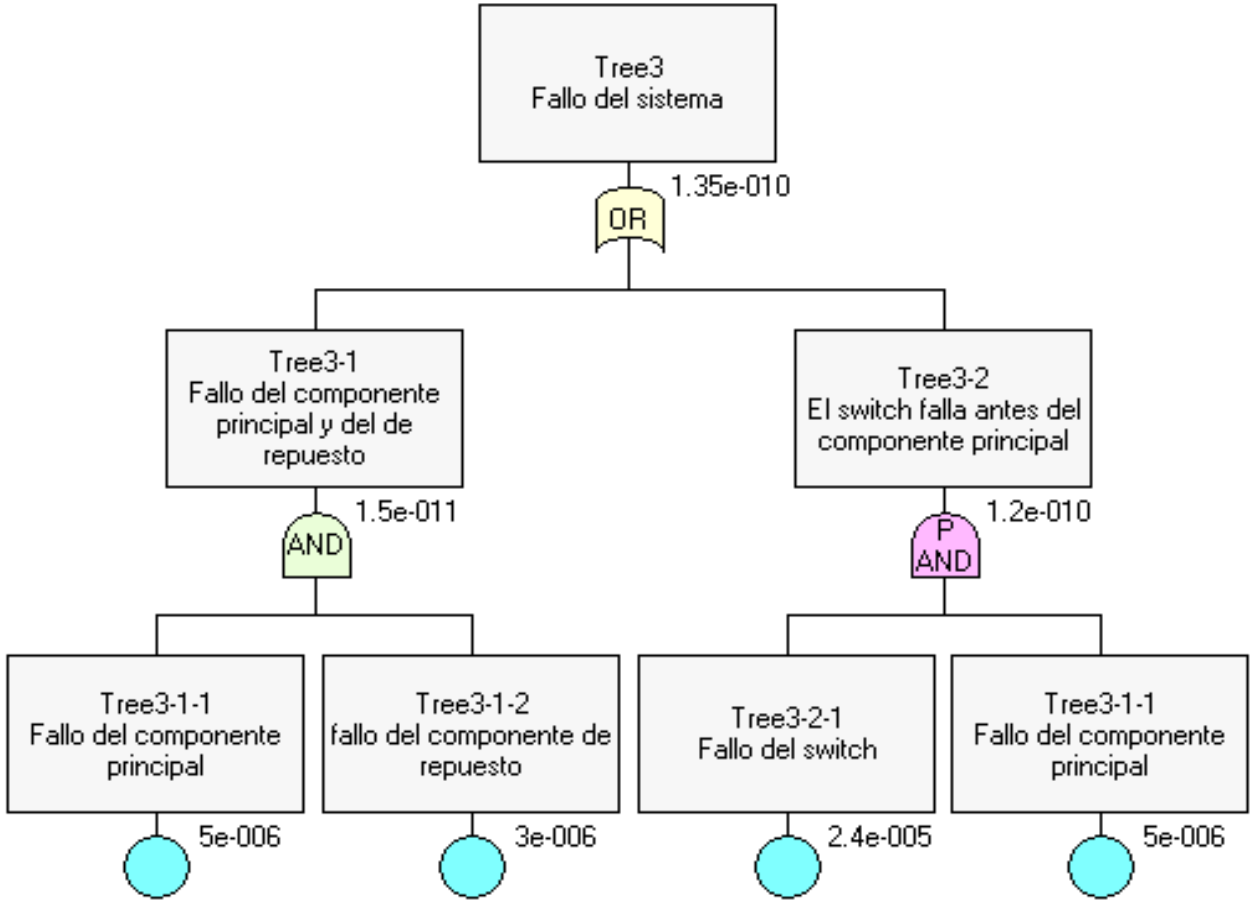


MODELIZACIÓN DE RELACIONES

b) Relaciones secuenciales: *Priority Gate*

Posibles fallos:

- Fallan el componente principal y secundario
- Fallan el switch y el componente principal, en ese orden

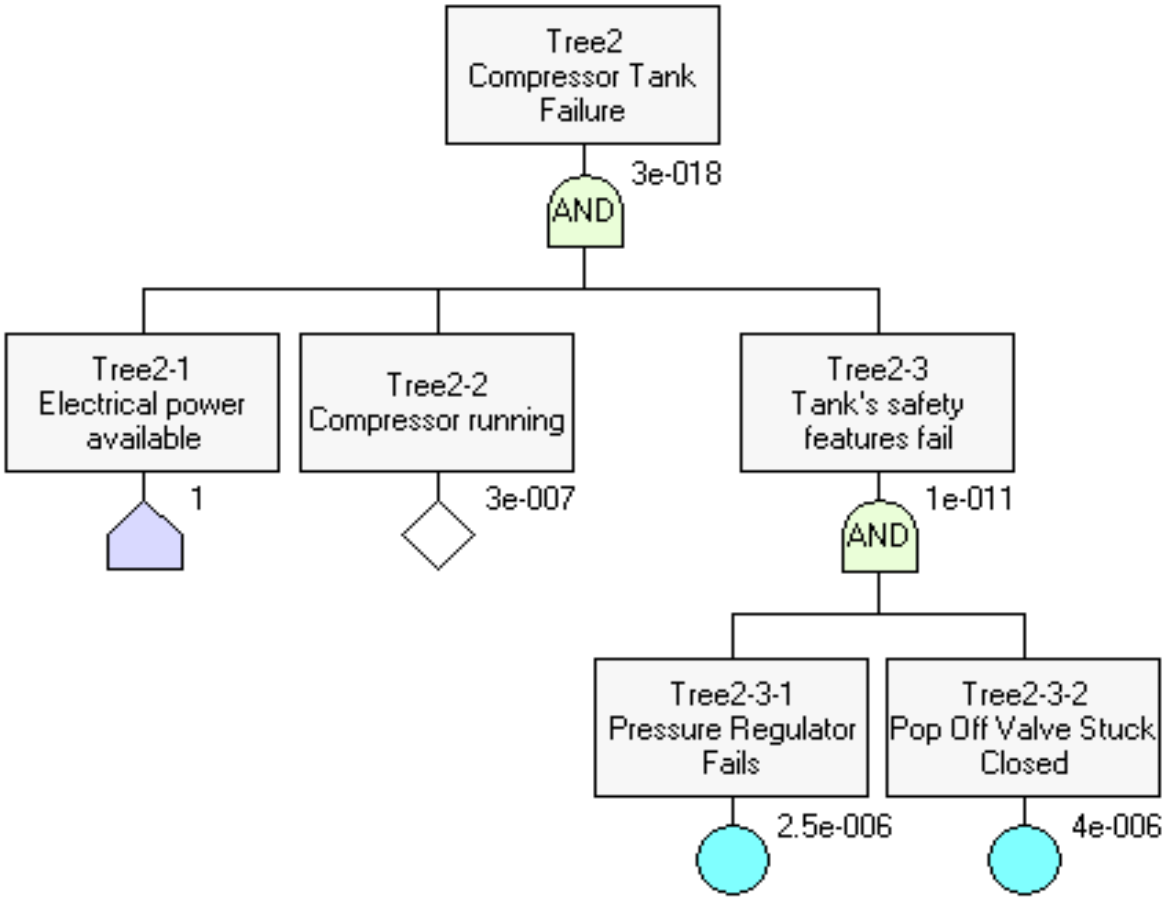


MODELIZACIÓN DE RELACIONES

c) Condiciones de entorno y fases de operación

EVENTOS HOUSE

- Activación de condiciones.
- Deshabilitar o habilitar ramas del árbol de fallos.
- Eventos desencadenantes, externos o fases de operación.



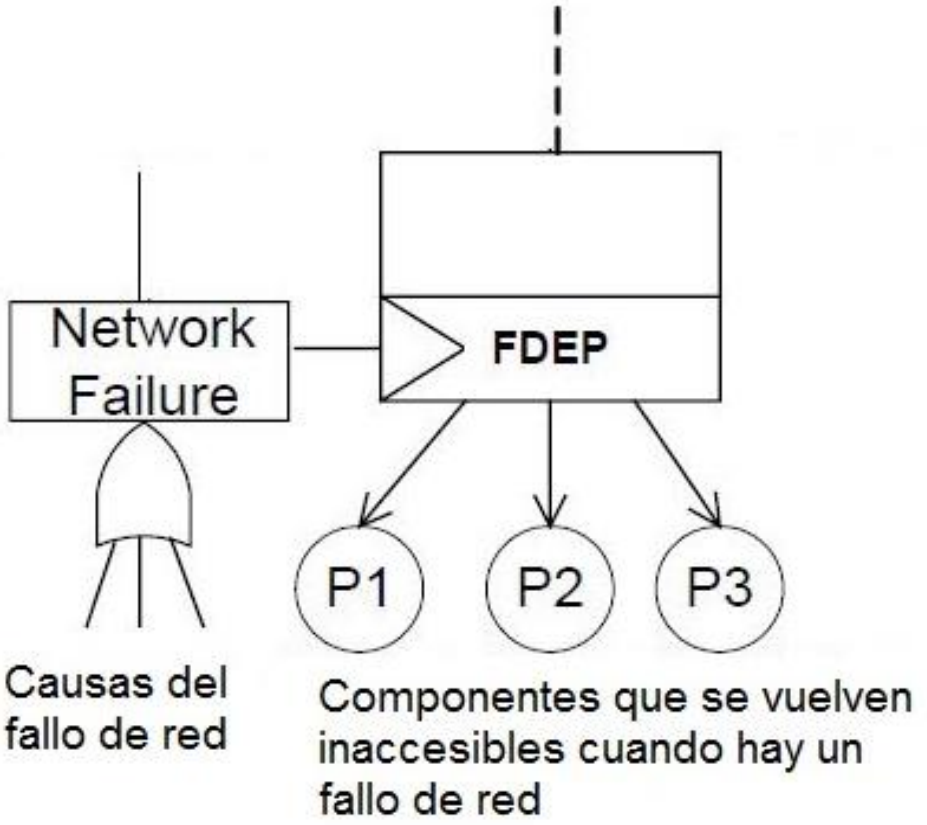
MODELIZACIÓN DE RELACIONES

c) Relaciones secuenciales: *Functional Dependency Gate*

Un **evento desencadenante** y uno o varios **eventos básicos dependientes**.

- Ejemplo:

  Un fallo en la red de comunicaciones de un sistema hace que perdamos otros componentes (P1, P2 y P3)



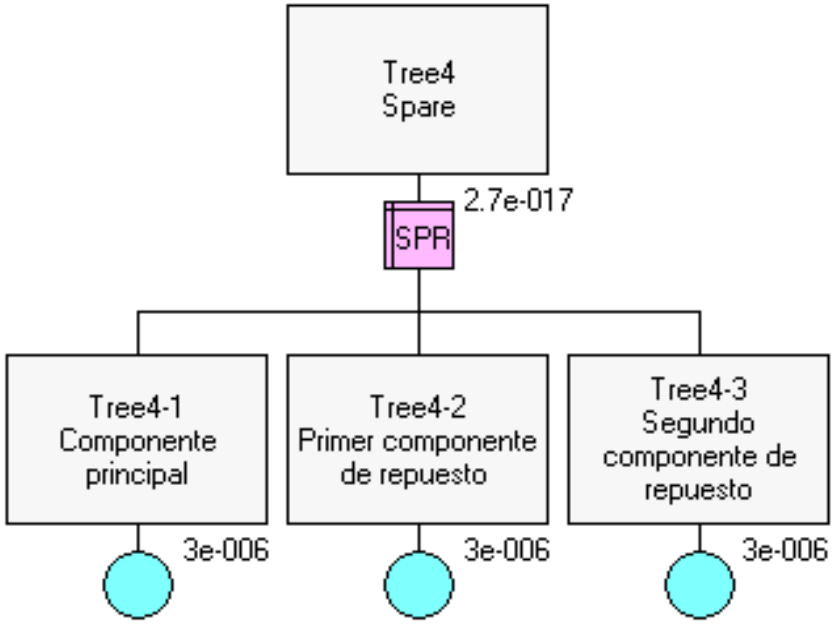
MODELIZACIÓN DE RELACIONES

c) Relaciones secuenciales: *Spare Gate*

Eventos básicos ordenados:

- Componente principal
- Componentes de repuesto

Factor **dormancy**:
normalmente entre 0 y 1.
Multiplica la tasa de fallo del comp. de repuesto → Tasa de fallo del comp. de repuesto mientras no está actuando como el principal.



RESOLUCIÓN CUANTITATIVA DE UN ÁRBOL DE FALLOS CON CADENAS DE MARKOV

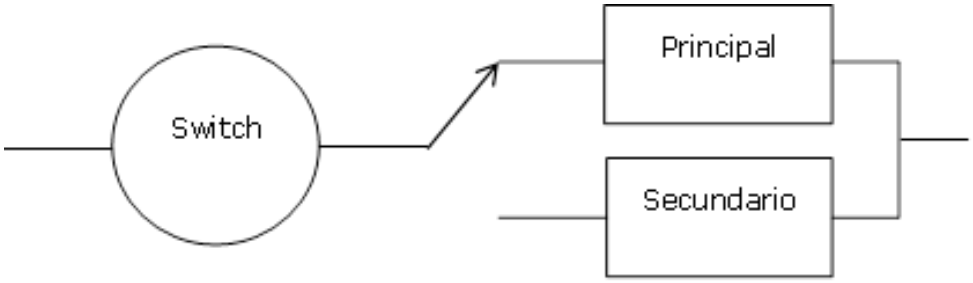
CADENAS DE MARKOV

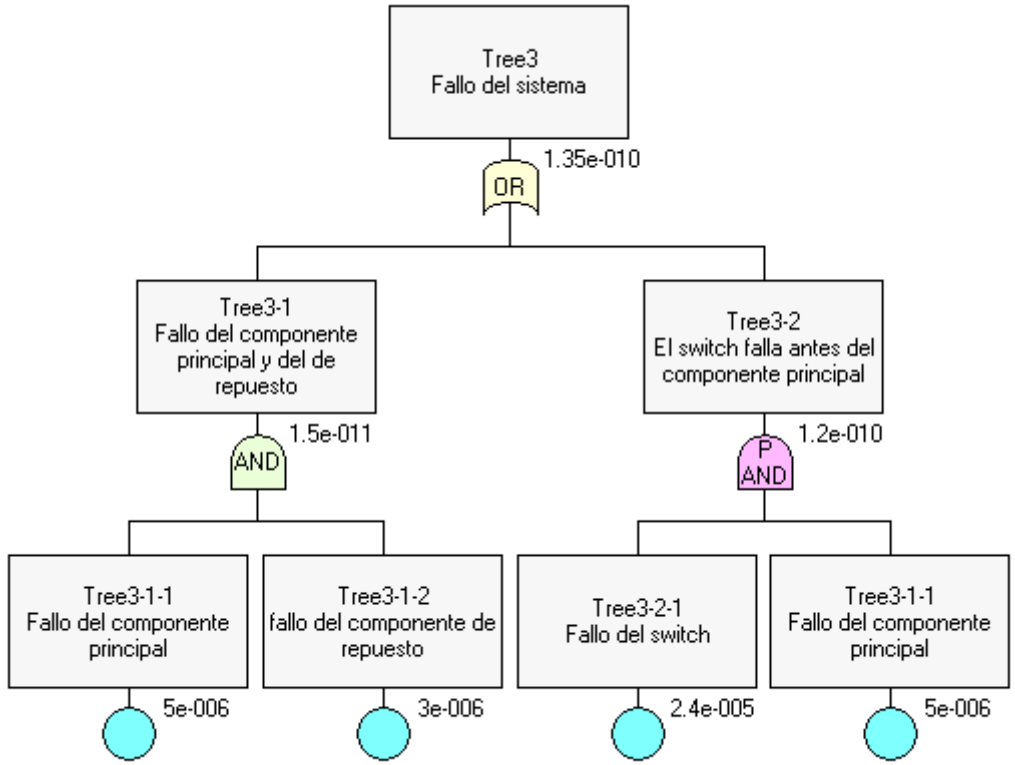
- Identificación de los posibles estados en los que puede encontrarse el sistema (E1 E2 E3 E4…..En)
- La probabilidad de que se cambie de estado de un tiempo al próximo (matriz de transición)
- El estado inicial en el que se encuentra el sistema.

¿Probabilidad de que el sistema se encuentre en un estado e instante determinado?

Solución a la cadena de Markov.

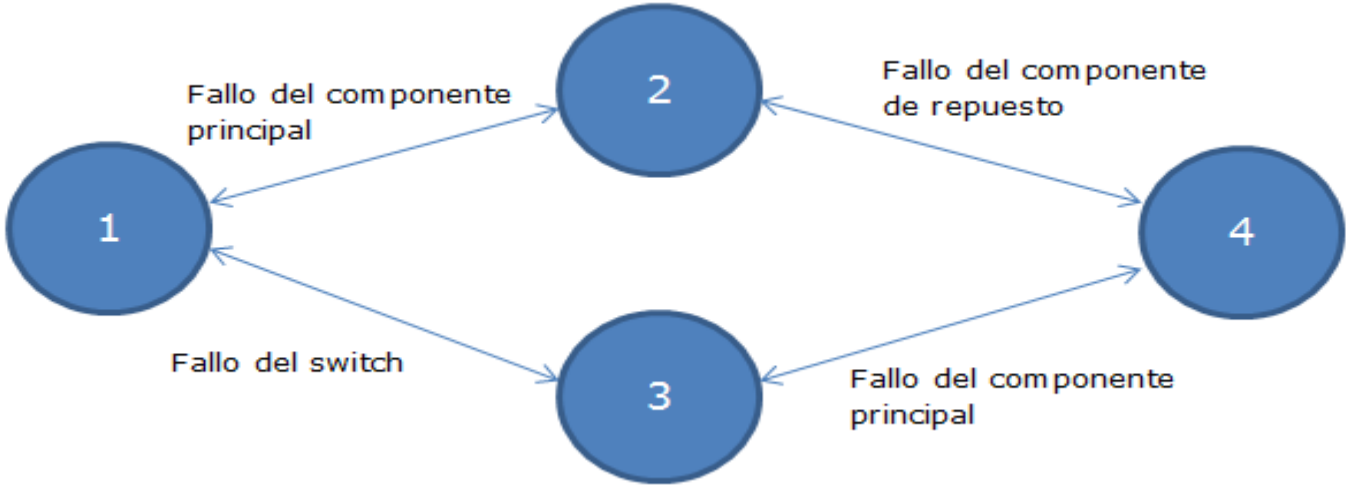
RESOLUCIÓN CUANTITATIVA DE UN ÁRBOL DE FALLOS CON CADENAS DE MARKOV





RESOLUCIÓN CUANTITATIVA DE UN ÁRBOL DE FALLOS CON CADENAS DE MARKOV

- **Estado 1:** ningún componente del sistema ha fallado.
- **Estado 2:** el componente principal ha fallado pero se ha efectuado el cambio y el componente de repuesto está funcionando correctamente.
- **Estado 3:** el componente principal funciona correctamente pero el switch ha fallado.
- **Estado 4:** fallo del sistema, no se puede dar el servicio



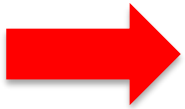
CONCLUSIONES

En esta ponencia **analizamos** la **capacidad** de **modelización** del comportamiento de un sistema mediante un **árbol de fallo**.

- Modelización de los eventos básicos:
  - Reparables
  - No reparables
- Modelización de las relaciones entre eventos:
  - Puertas clásicas del FTA
  - Condiciones
  - Puertas *Priority AND*, *Functional dependency* y *Spare*.
- Resolución de FTAs dinámico.

FUTURAS LÍNEAS DE INVESTIGACIÓN

- **Objetivo**: acercarnos más a la realidad del sistema
- Las hipótesis sobre las distribuciones que siguen los eventos básicos a veces resultan no ser reales, y en muchos casos se suele optar por simplificar utilizando distribuciones exponenciales con tasas de fallo constante.



Realizar simulaciones para obtener datos reales

Con ello conseguimos:

Distribución estadística del fallo de los eventos básicos

Distribución estadística del fallo del evento final de alto nivel

¡Gracias!

Marta López
RAMS Team

INNOVATING SOLUTIONS