Técnicas de Fiabilidad y Safety para Software

IX JICS. 1 y 2 julio 2004,
Madrid

Conceptos RAMS

RAMS: **Reliability, Availability, Maintainability, Safety.**

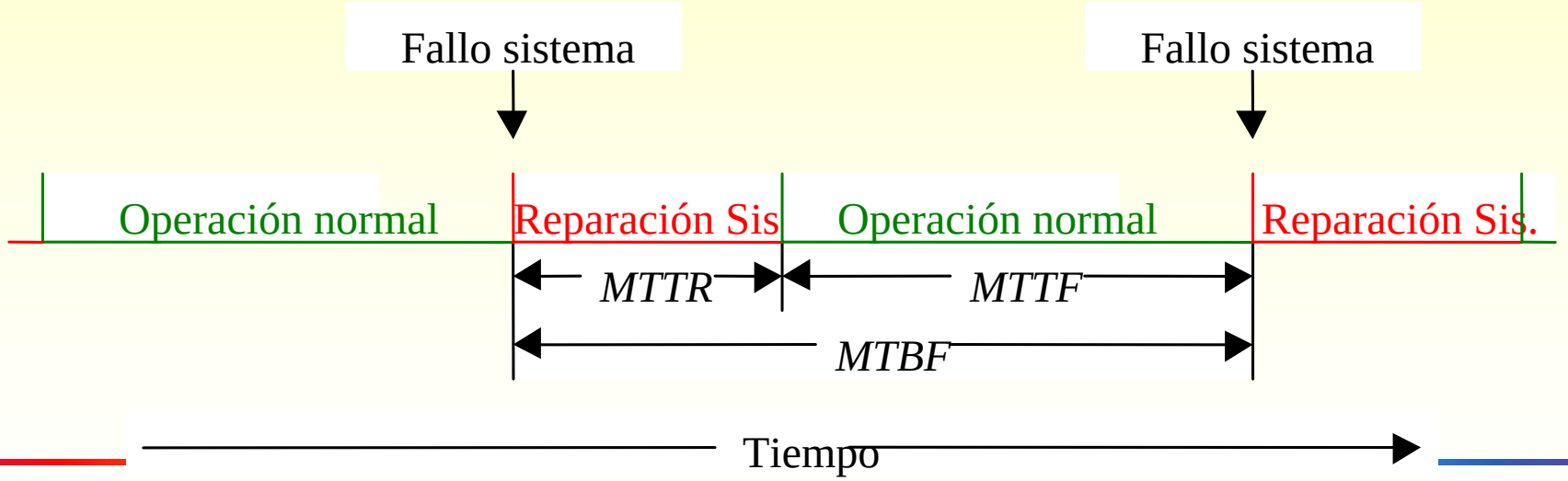
Failure Rate: **Número esperado de Fallos por unidad de tiempo.**

MTBF: **Mean time between failures.**

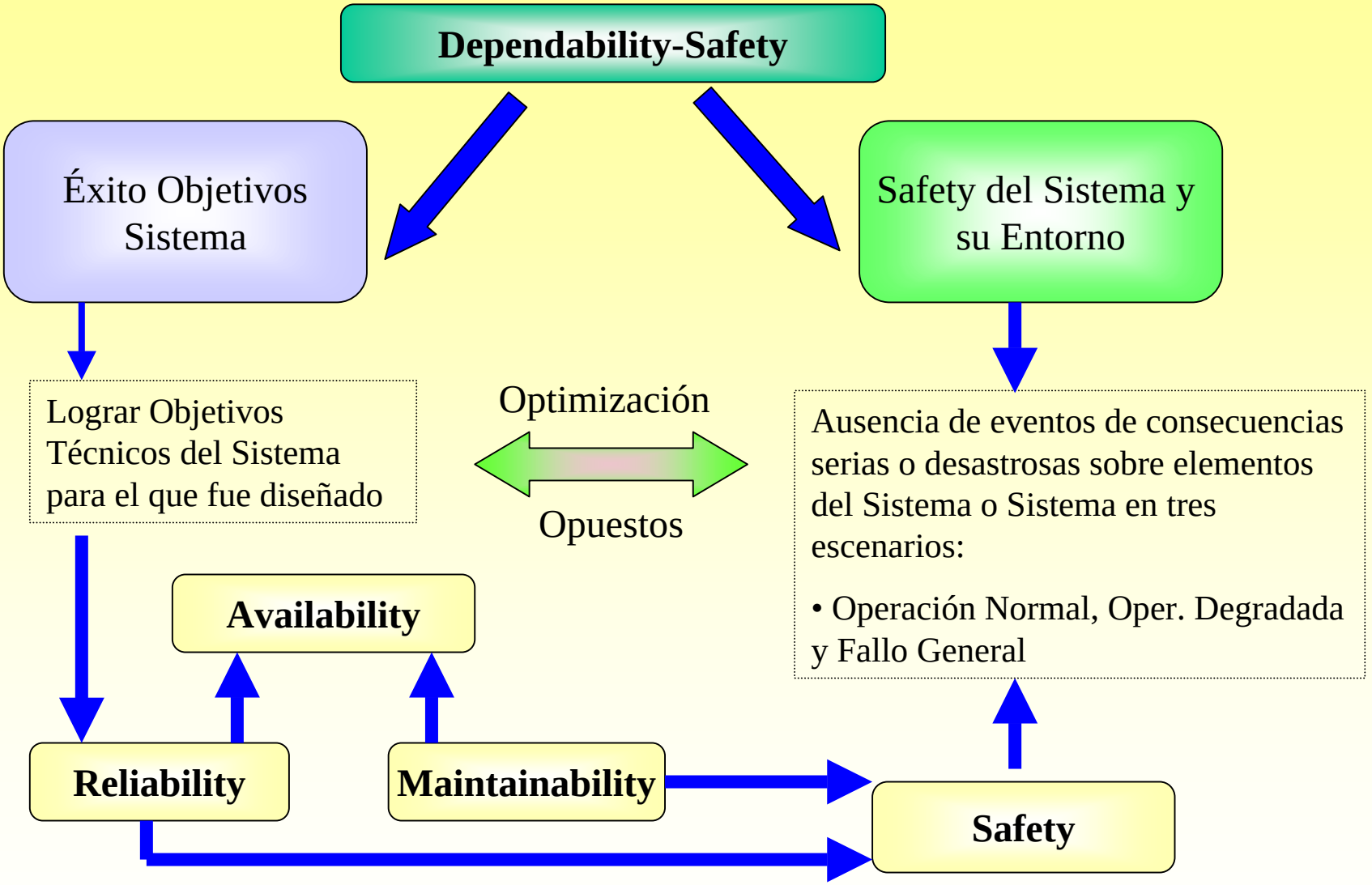
MTTF: **Mean time to failure.**

MTTR: **Mean time to recovery.**

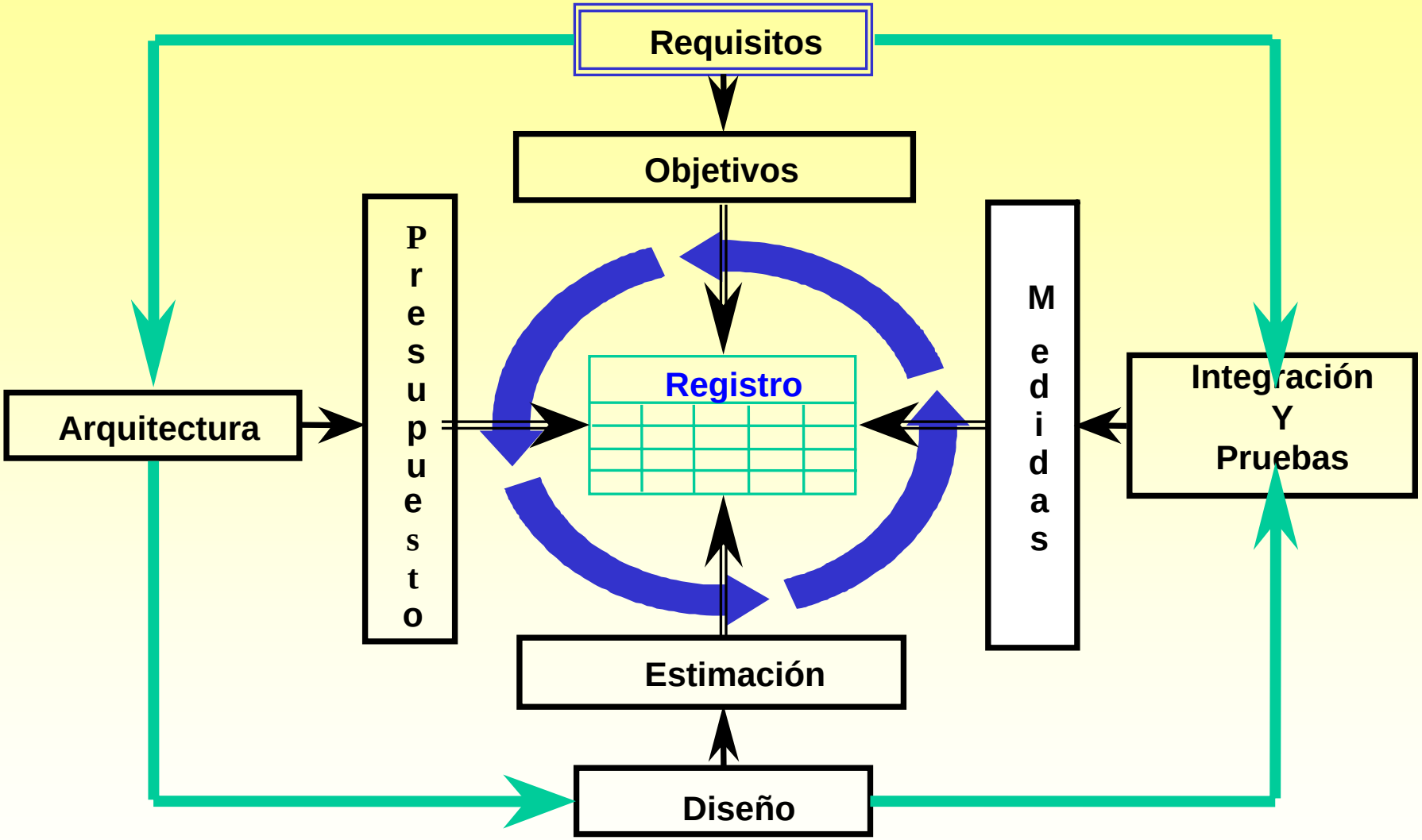
Otros parámetros **: Factor Fault Coverage, Redundancy, Recovery Successful Probability, Fail-over Successful Probability, Fail-over Time, Manual Failure Detection Time**



Confiabilidad (AENOR) : Dependability-Safety



Ciclo Fiabilidad



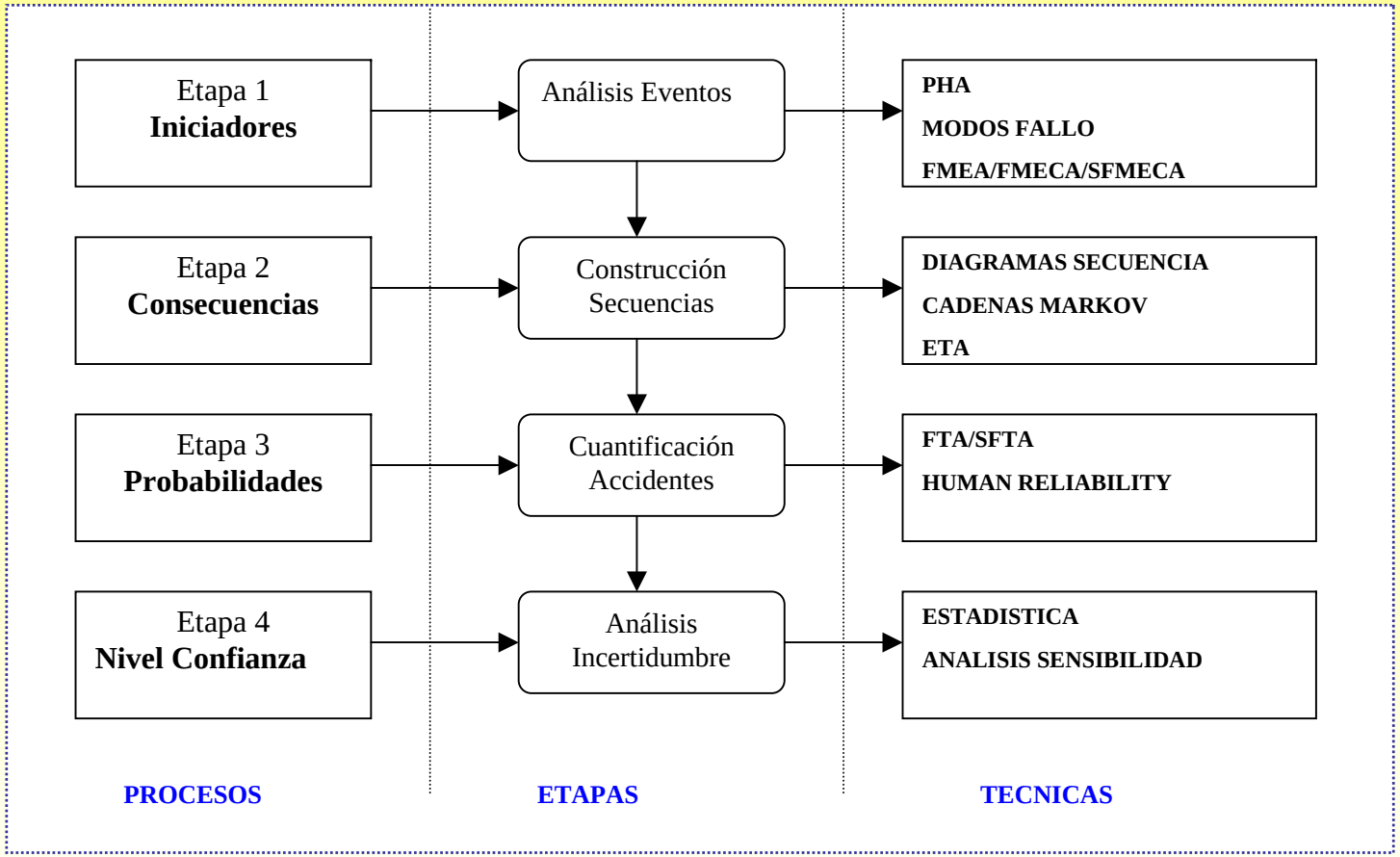
Evaluación Riesgos

ETAPAS:

1. Qué cosas pueden ir mal, iniciadores o eventos que conducen a situaciones de consecuencias adversas.
2. Para cada evento iniciador, detalle de las consecuencias adversas que se generan y severidad asociada a la ocurrencia del evento.
3. Probabilidad y Frecuencia de eventos no deseados y consecuencias.
4. Nivel de confianza del análisis de los puntos anteriores.

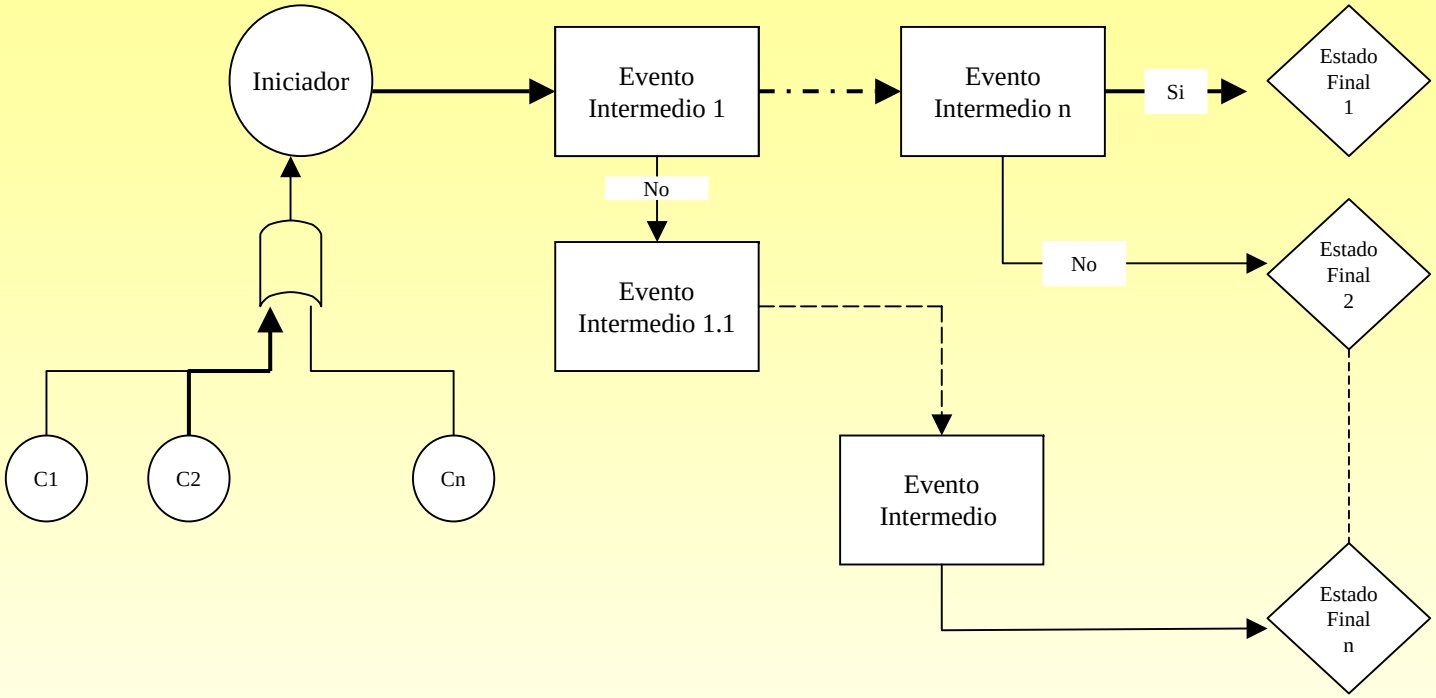
Cada etapa tiene asociada un conjunto de técnicas candidatas idóneas: Functional Analysis (FA), Preliminary Hazard Analysis (PHA), Diagramas de Estado de Markov, Reliability Block Diagrams (RDB), Failure Mode and Effects Criticality Analysis (FMECA) o Fault Tree Análisis (FTA).

Evaluación Riesgos Sistemas Software



Analizar Fiabilidad/Safety para Software es incluir además de los componentes tradicionales del Sistema –eléctricos, mecánicos...- los componentes Software

Secuencia Accidentes y Propagación



Secuencia de propagación de fallos desde componentes hasta el Estado final. Un Modo de Fallo ocurre en el componente C2 derivando en accidente en el estado final 1

Análisis de Fiabilidad/Safety/Disponibilidad

1- Identificar Modos de Fallo del Sw

(Presente Ponencia)

2- Tratamiento de Modos de fallo

Paramétricos y No paramétricos

Datos de fallos es Integración y Pruebas

Datos de fallos de Campo

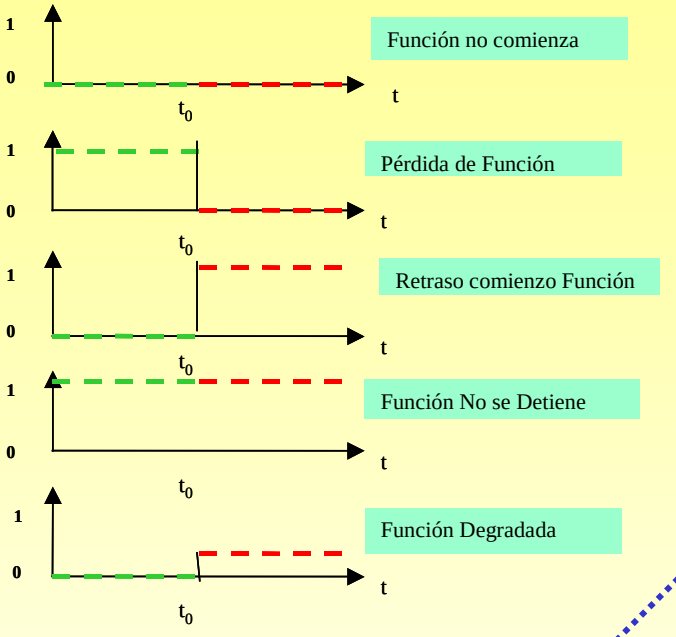
3- Modelos de Fiabilidad, Safety, Disponibilidad

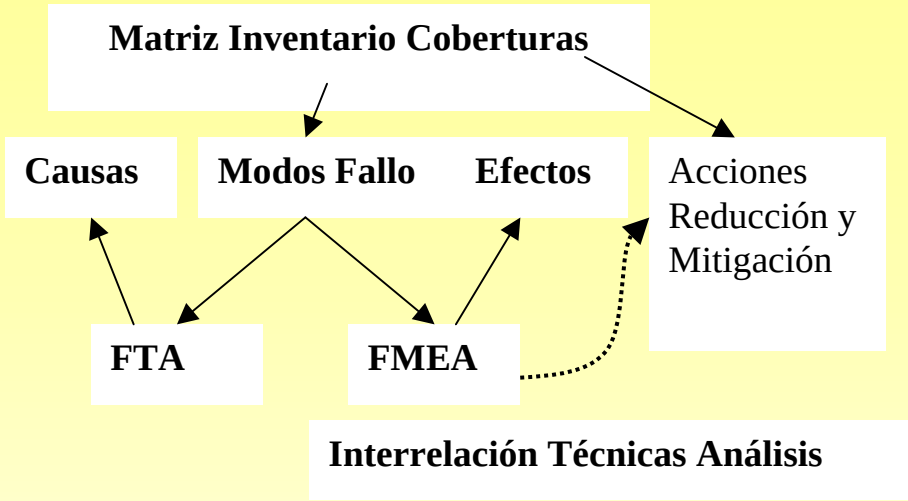
Modelos basados en Fallos

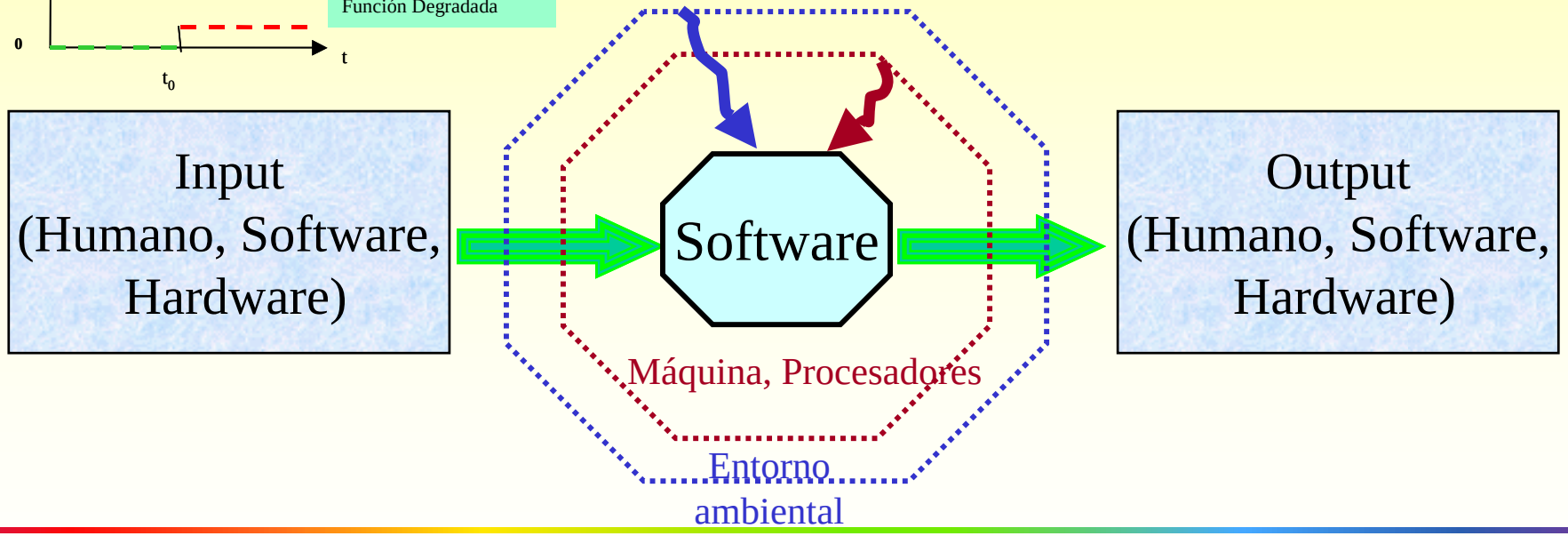
Modelos basados en Defectos

Modelos basados en el Ciclo Vida del Desarrollo

Contexto del Software

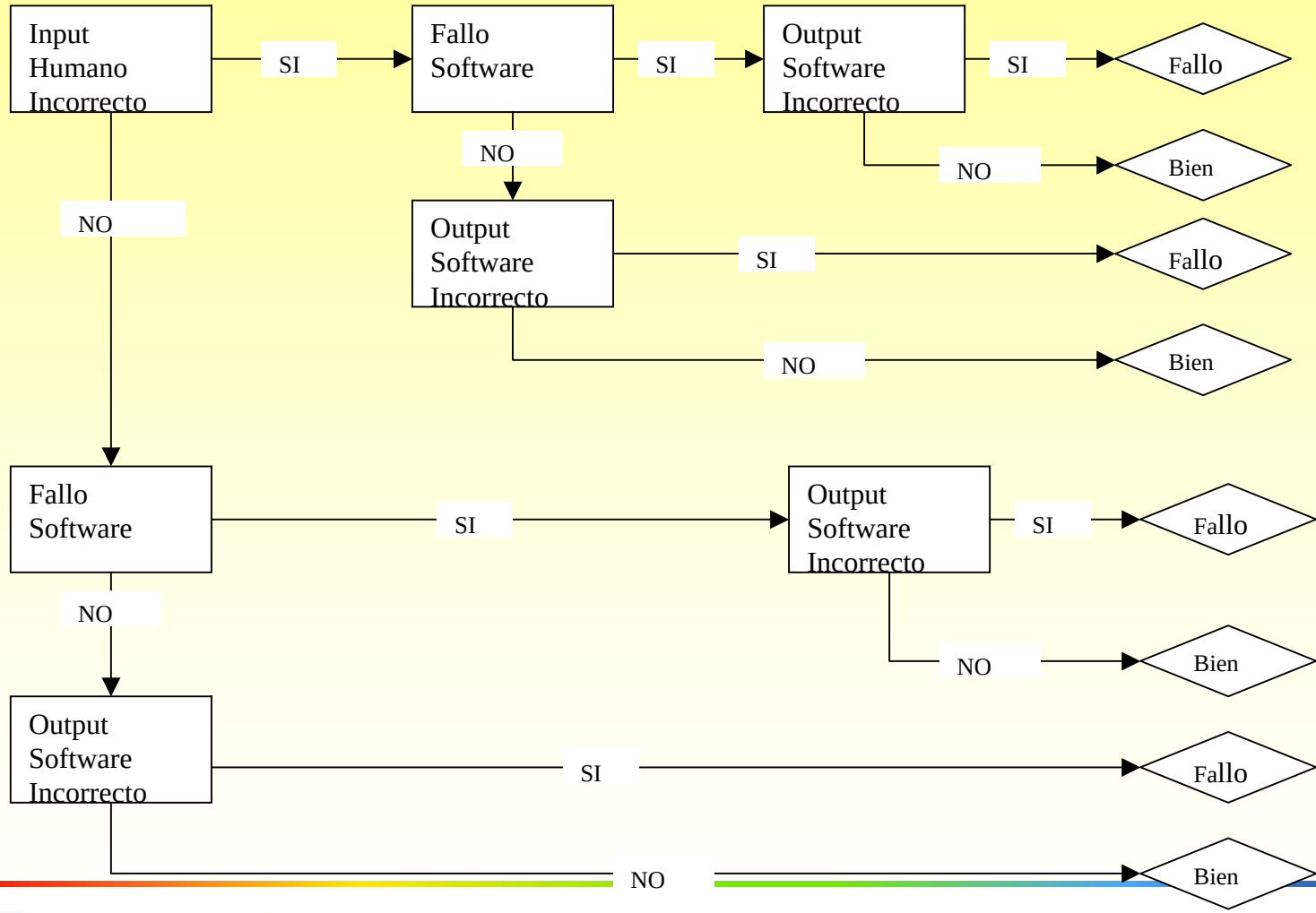






Genérico Interacción Humana / Software

- **Proceso Interacción Humanos y Software : Un humano introduce Input –datos o comandos de control- a un Procesador –interfaz Sw-, el Sw se ejecuta usando los inputs y genera outputs**



D S E

Clasificación Modos de Fallo. Identificación (I)

Tipología Fallo	Característica	Identificación
Funcional	Función : F conjunto de funciones especificadas en Requisitos	• Omisión de una función : $\exists f \in F, f \notin F_i$ siendo F_i las funciones implantadas • Realización incorrecta de una función: $\exists f \in F, f_i \in F_i, f_i \neq f$ siendo f_i la implementación de f • Función implementada no especificada en Requisitos : $\exists f \in F_i, f \notin F$
	Atributo	• Omisión Atributo de Función f : : $\exists a \in A(f), a \notin A_i$ (f) siendo a un atributo y A_i (f) los atributos implantados • Realización Incorrecta de un atributo : $\exists a \in A(f), a_i \in A_i(f), a_i \neq a$ siendo a_i la implementación de a • Atributo implementado no especificado en Requisitos : $\exists a \in A_i(f), a \notin A(f)$
	Interacción entre funciones	• Omisión de una de las funciones en el conjunto S : $\exists f \in S(f), f \notin S_i(f)$ siendo $S_i(f)$ el conjunto de funciones implantadas que reciben el control cuando la función f ha terminado su ejecución • Introducción de una de función no está en el conjunto S : $\exists f \in S_i(f), f \notin S(f)$ • Sustitución de una función del conjunto S por otra : $\exists f \in S(f), f_i \in S_i(f), f_i \neq f$ siendo f_i la implementación de f

Clasificación Modos de Fallo. Identificación (II)

Tipología Fallo	Característica	Identificación
Input/Output (Hardware, Errores Humanos y Software)	Valor : Valor de el input/output : V(Ii, t) = Valor de variable Ii en el instante t	• Valor incorrecto : $V(Ii, t) \neq \forall$, siendo $\forall$ el valor del i-ésimo input en el instante t, según lo especificado en requisitos • .....
	Rango : Límites de inputs/outputs : Rg(Ii, t) = [min V(Ii, t), max V(Ii, t)]	• Fuera de rango : $V(Ii, t) < \mu_I$ o $V(Ii, t) > \mu_S$ siendo μ_I = min V(Ii, t) y μ_S = max V(Ii, t) • ……
	Cantidad ….	• .....
	Tipos	• .....
	Tiempo	• .....
	Frecuencia	• .....
	Duración	• .....
	Carga	• .....
Interacción múltiple	Comunicación, desincronización	• .....
Soporte / Recursos	Procesos : Propiedad y Liberación de Recursos, Tiempos, Deadlock, Lockout	• .....
Soporte/Plataformas Físicas	Soporte físico, CPU, Memoria, Periféricos....	• .....
Entorno / ambientales	Destrucción inmediata	• .....
	Degradación progresiva : Failure rate $\lambda(t)$	• Interferencia electrónica • Interferencia otras señales • Presión barométrica, ingravidez, fuegos, temperaturas, atmósfera salina, humedad, desastre natural

Modos de Fallo	Bases de Datos
Input	No se conocen. Datos a medida
Funciones	ARF Error Dataset, DACS Productivity Database, NASA Ames Error/Fault Dataset
Ouputs	No se conocen. Datos a medida
Soporte, Plataformas	Electronic Parts Reliability Data (RAC), MIL-HDBK-217
Entorno, Ambientales	Electronic Parts Reliability Data (RAC), MIL-HDBK-217

Aplicación Sistema Control Higrometría (I)

Uso de los Modos de Fallo.
Identificación Defectos y Fallos

Característica	Modos Posibles Fallo	Ejemplo Sistema Control Higrometría : SCR
Función	• Omisión de Función • Realización Incorrecta de una Función • Función implantada no especificada en Requisitos	• Sistema no avisa al Operador cuando un Sensor envía siempre mismos datos con trascurso del tiempo. Situación anómala : los datos temporales dinámicos cambian en general • Función de timing del actuador de iniciador de aspersión no especificado en los requisitos. No señala de manera precisa el tiempo de actuación desde que se produce señal Baja o Baja/Baja • Apertura de válvula no Requerida. (Función responde a un único Sensor no al conjunto Sensores del área) • SCR avisa del flujo es de valor promedio. Avisa sin exigirlo en las especificaciones, pero no es de mucho valor este dato

Aplicación Sistema Control Higrometría (II)

Uso de los Modos de Fallo.
Identificación Defectos y Fallos

Característica	Modos Posibles Fallo	Ejemplo Sistema Control Higrometría : SCR
Atributo	• Omisión de Atributo • Realización Incorrecta de un Atributo • Introducción Atributo no especificado	• Para el cálculo del Requisito RF28 se necesita además valores de al menos un 80% de las sondas de área • Algoritmos no idóneos de determinación de áreas higrométricas. Si el número de sensores es bajo, ver RF28, el algoritmo genera resultados poco fiables
Interacción entre funciones	• Omisión alguna función interacción • Función interacción incorrecta • Función de interacción no necesaria	• Actuador recibe señales dispares (Sensor(i)=alto/alto y Sensor(j)=bajo/bajo) por Sensores diferentes simultáneamente y no sabe qué hacer.

Aplicación Sistema Control Higrometría (III)

Uso de los Modos de Fallo.

Identificación Defectos y Fallos

Tipología Fallo	Característica	Modo Posibles Fallo	Ejemplo Sistema Control Higrometría : SCR
Input/Output (Hardware, Errores Humanos y Software)	• Datos (Cantidad, Valor, Tipo y Rango) • Timing (Tiempos, Duración, Frecuencia y Carga)	Pocos / demasiados datos Valor incorrecto Fuera de rango Tipo incorrecto Demasiado temprano / tarde No hay input/output en el intervalo de tiempo definido Frecuencia demasiado rápida / lenta Duración demasiado corta / larga Sobrecarga	El Operador necesita datos de Área. Si no recibe datos de todos y cada una de las sondas no puede decidir Una pérdida de corriente de un Sensor y la posterior conexión puede generar datos corruptos fuera del rango definido para el Tipo (Integer 0 .. Integer'last) Cuando se detecta señal Baja/Media, se espera recibir / confirmar datos de área y del Operador durante tiempo espera de 24 h. en verano y 100 h. en invierno. Si en este intervalo de tiempo no hay confirmación de ambos el actuador se quedaría en standby permantente Operador recibe señales dispares (Sensor(i)=alto/alto y Sensor(j)=bajo/bajo) por Sensores diferentes simultáneamente y no sabe qué hacer. Necesita más información Error protocolo Operador. Operador activa Actuadores en contra de más del 90% de datos de las Sondas.

Aplicación Sistema Control Higrometría (IV)

Uso de los Modos de Fallo.

Identificación Defectos y Fallos

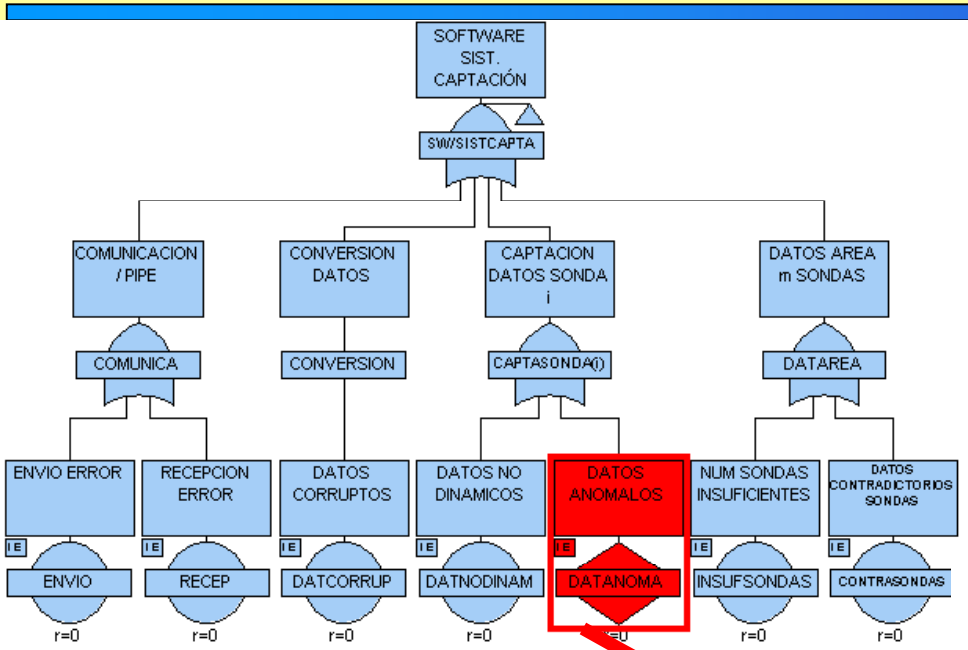
Tipología Fallo	Característica	Modo Posibles Fallo	Ejemplo Sistema Control Higrometría : SCR
Interacción múltiple	Comunicación	Desincronización	La acción de Baja/Baja ocurre cuando las *n* sondas de n de área (100%) señalan en la misma dirección y en un intervalo de tiempo dado (confirmación por todas en menos de 1h.). El Proceso P_1 necesita confirmación en este plazo de tiempo de los procesos P_2 a P_n
Soporte / Recursos	Procesos : Propiedad y Liberación de Recursos, Tiempos.	Deadlock Lockout	Crítico para Sistemas tiempo real. No aplica a nuestro Sistema
Soporte / Plataformas Físicas	Soporte físico	CPU / degradación función	Pérdida de CPU si no soporta ambientes humedad 100% y temperatura 60ºC. Requisito RE4.
		Memoria / degradación prestaciones	Datos de memoria corruptos cuando algún sensor ha perdido corriente eléctrica (CPU del Sistema central no), y se restablece energía del sensor
		Periféricos / Mal funcionamiento	Datos de memoria corruptos cuando secuencia de arranque del Sistema no sigue Procedimiento
		Otros soportes	

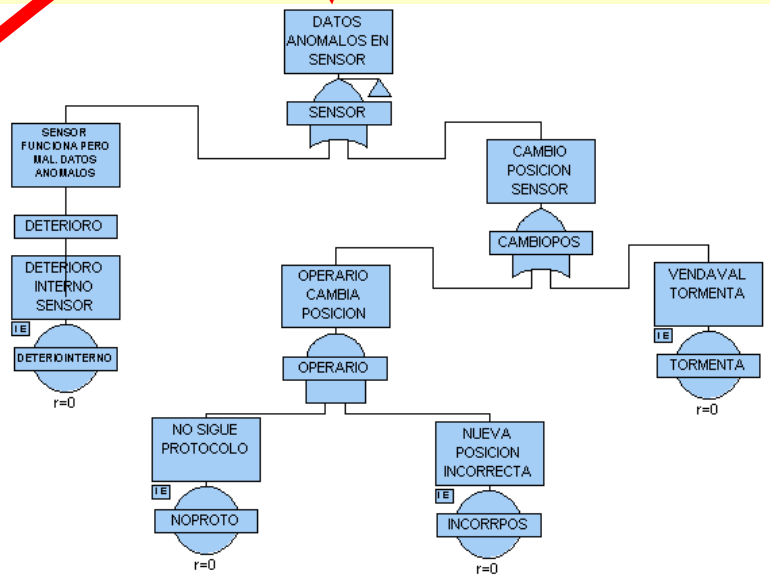
Aplicación Sistema Control Higrometría (V)

Uso de los Modos de Fallo.
Identificación Defectos y Fallos

Tipología Fallo		Característica	Modo Posibles Fallo	Ejemplo Sistema Control Higrometría : SCR
Entorno ambientales	/	Destrucción inmediata Degradación progresiva	Interferencia electrónica Interferencia otras señales Presión barométrica, ingravidez, fuegos, temperaturas, atmósfera salina, humedad, desastre natural	Pines de conexiones de sensores pueden romperse por enganches, tirones de maquinaria pesada o vendaval. Rotura cables en campo sistemas Control / Sensor (tractores, excavadoras) Posibles interferencias Corriente eléctrica / señales a tarjeta de CPU central Sondas y sensores se mueven y cambian su posición ante fuertes tormentas o errores de Operarios. Los datos de las medidas tomadas por las sondas fuera de lugar no tienen validez. Posibilidad corrupción Base Datos (véase Figura 4 aplicación FTA/SFTA)

SFTA ejemplo del SCR





Integración de FTA/SFTA del Subsistema Software CCR –Captación, Conversión y Registro- datos de Sensores en Campo del Sistema SCR