Navantia

XII Congreso de Confiabilidad

Cádiz, 24 a 26 de Noviembre de 2010

Fiabilidad y Mantenibilidad en el Diseño de Sistemas de Mando y Control de Buques Militares

Antonio J. Vázquez Gutiérrez

SISTEMAS FABA

Antonio José Vázquez Gutiérrez

Navantia – Sistemas FABA

Departamento de Ciclo de Vida

Sección de Sistemas de Combate y Comunicaciones

Responsable Técnico de Actividades de Ingeniería Logística

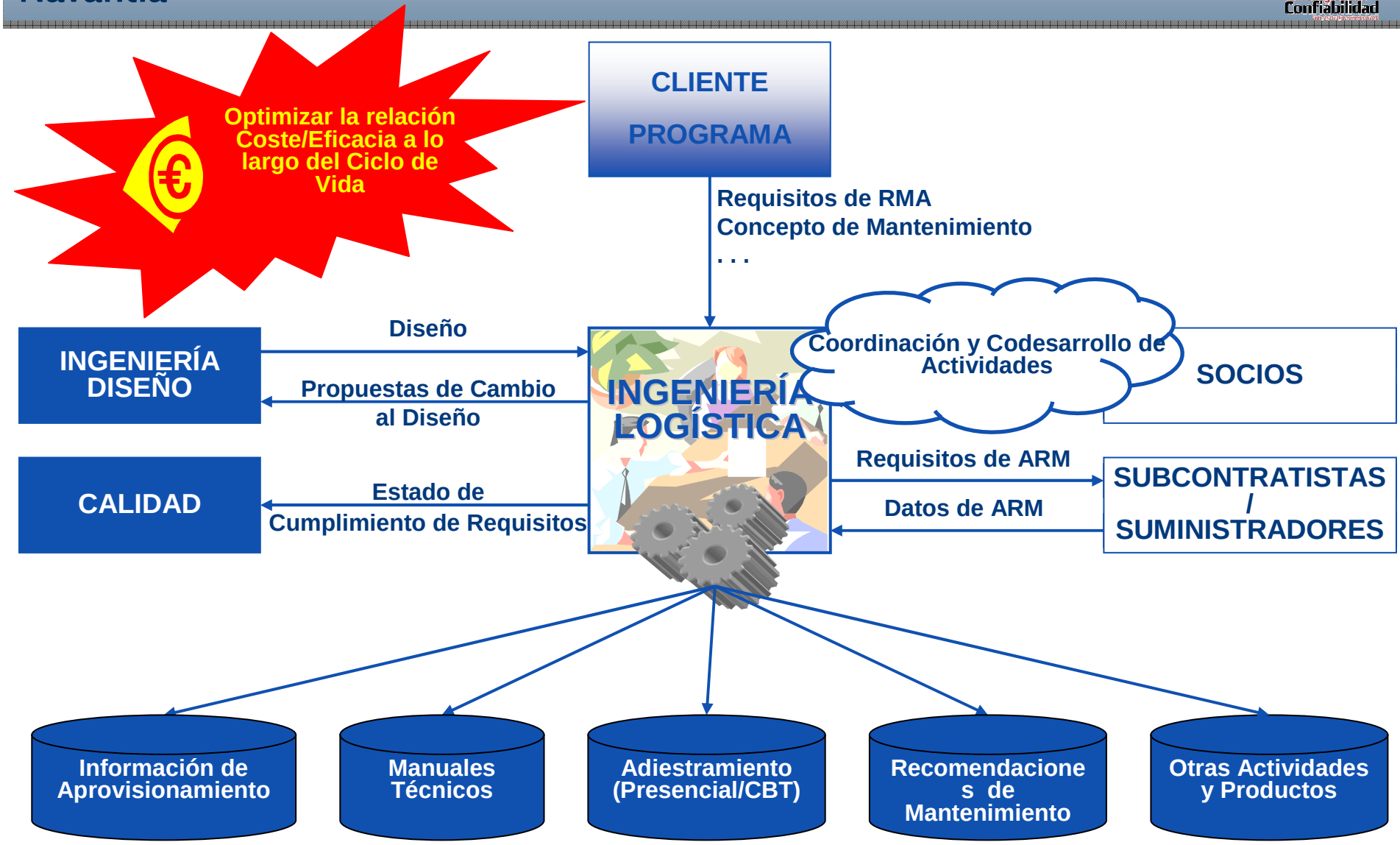
Actividades de Apoyo al Ciclo de Vida

- Análisis Logísticos
  - Análisis de Fiabilidad
  - Análisis de Mantenibilidad
  - Análisis de Modos de Fallo, Efecto y Criticidad (FMECA)
  - LSA (Logistic Support Analysis)
  - LORA (Level Of Repair Analysis)
  - Etc.
- Elaboración de Documentación de Apoyo
  - Manuales Técnicos (Operación y Mantenimiento)
  - Planes de Mantenimiento
  - Recomendación de Repuestos, Herramientas especiales, Equipos de prueba, etc.
  - Catalogación OTAN
- Adiestramiento (Presencial/CBT)
  - Gestión de Cursos
  - Impartición de Cursos
  - Desarrollo de Sistemas de Adiestramiento por Ordenador (CBT)
- Sostenimiento de Sistemas:
  - Gestión de la Configuración
  - Gestión de Obsolescencia y Refrescos tecnológico
  - Gestión de Programas de Sostenimiento
  - Gestión de la Cadena de Suministro (Repuestos, reparaciones, reciclaje)
  - Asistencia Técnica Remota/Helpdesk
  - Análisis de Costes de Ciclo de Vida

Ingeniería Logística

Op. de Sostenimiento

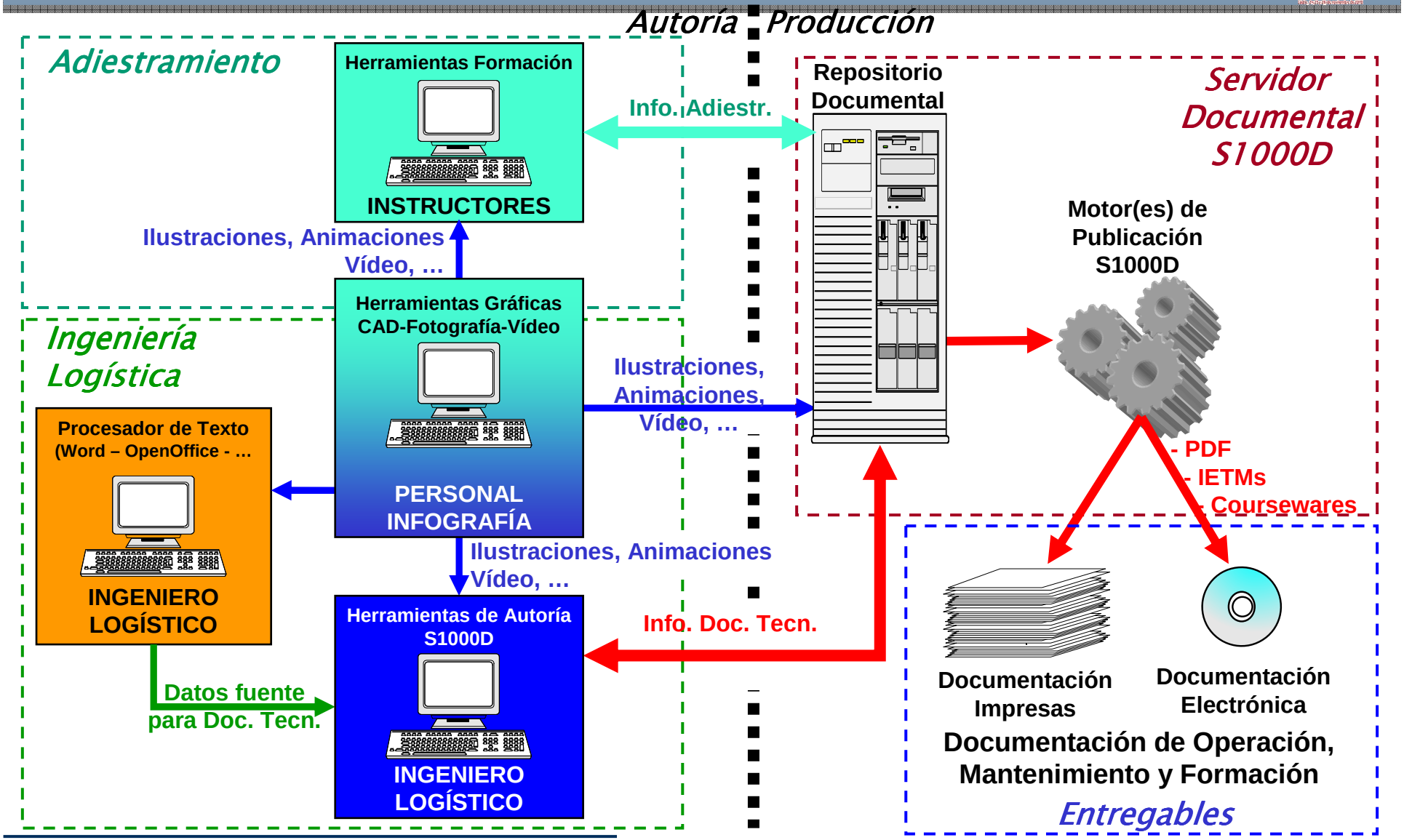
El Entorno de Ingeniería Logística



Actividades de Ingeniería Logística en Fase de Diseño

- Análisis Logísticos:
  - Demostrar que el sistema cumple los requisitos especificados → Recomendar cambios cuando no se alcanzan los objetivos.
  - Son la base para planificar todas las actividades de Ciclo de Vida (planes de mantenimiento, repuestos, etc.).
  - Los principales son:
    - Análisis de Modos de Fallo, Efectos y Criticidad (FMECA)
    - Análisis de Fiabilidad:
      - Reducir de fallos en el largo plazo.
      - La fiabilidad es dependiente de la Robustez del diseño y de calidad y fiabilidad de los componentes.
    - Análisis de Mantenibilidad:
      - Minimizar el Tiempo Inoperativo «downtime» -> Reducir los tiempos de reparación.
      - Reducir los Costes por Mantenimiento.
    - Análisis de Seguridad y Riesgos:
      - Identificar y eliminar o reducir los riesgos relacionado con la seguridad en el ciclo de vida.
- Documentación de Apoyo:
  - Recomendaciones de Apoyo (Repuestos, Herramientas Especiales, Equipos de prueba, etc.)
  - Documentación de Mantenimiento
  - Planes de Mantenimiento
  - Manuales Técnicos y Adiestramiento
    - Ayudan a reducir la no fiabilidad relacionada con los Factores Humanos

Sistema Documental y de Adiestramiento



Contenido

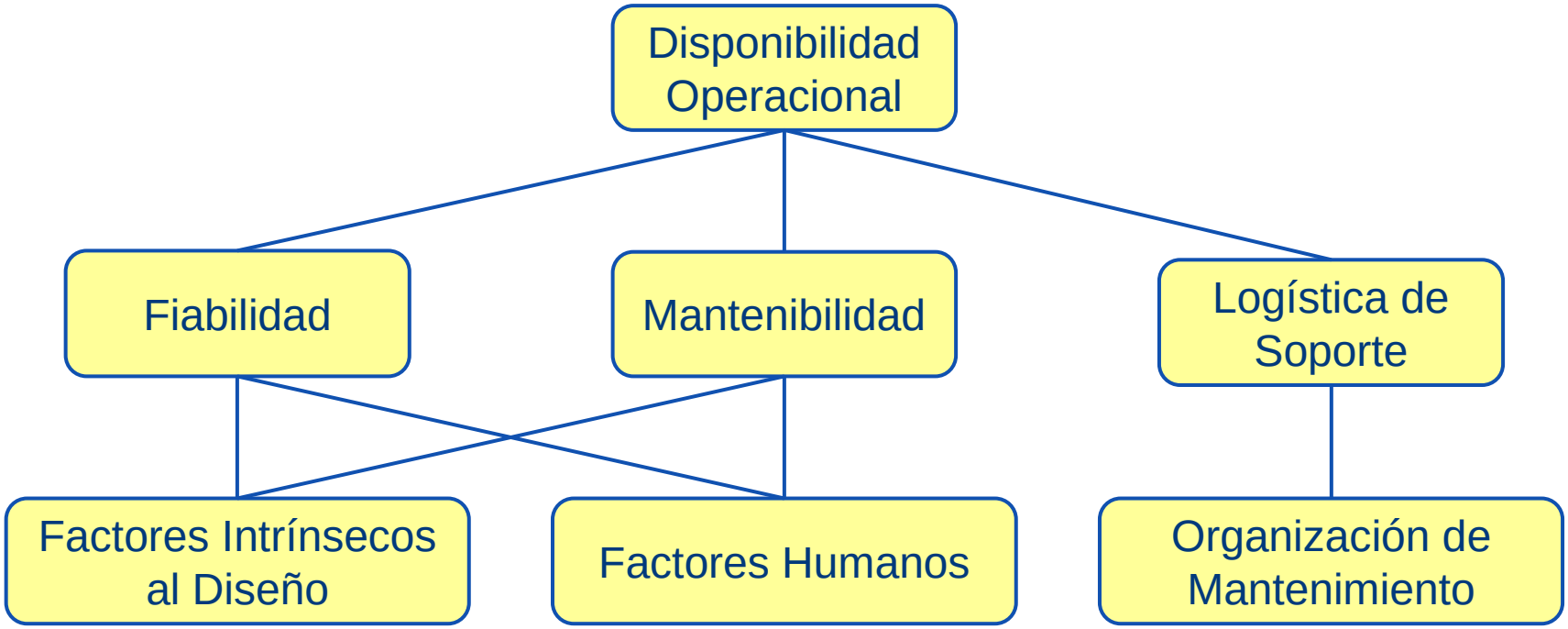
- Introducción
- Disponibilidad y Factores que la condicionan.
- El Diseño Centrado en Fiabilidad
- Diagrama de Flujo de Alto Nivel del Proceso
- Modelo de fiabilidad y los elementos a considerar
- Mantenibilidad de Sistemas
- Conclusiones

Introducción

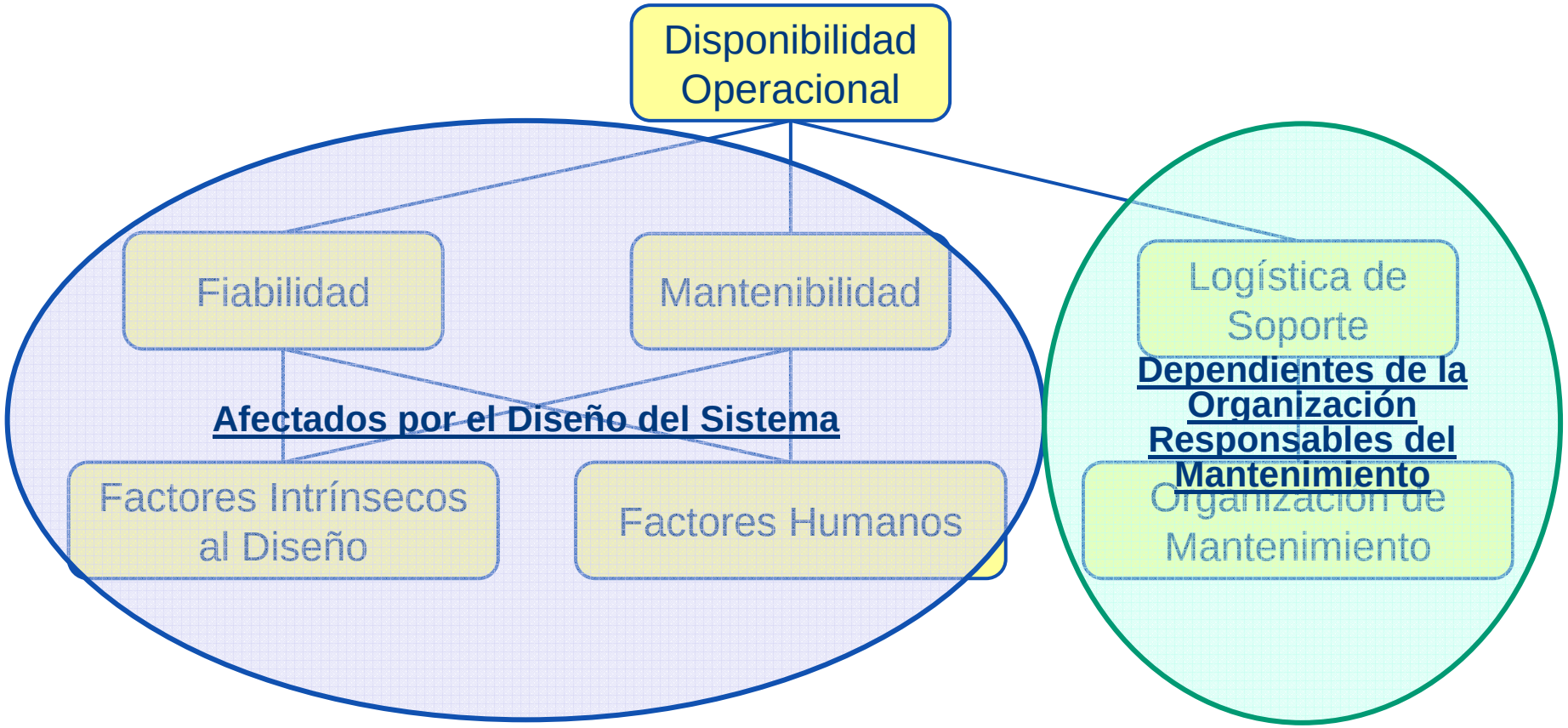
- El Sistema de Mando y Control es el elemento integrador del Sistema de Combate → Es fundamental asegurar una alta disponibilidad.
  - Depende en gran medida de la fiabilidad y mantenibilidad del sistema
  - Es clave considerar estos aspectos desde la fase de diseño
- En el Ciclo de Vida de los Sistemas, el periodo de diseño representa un pequeño porcentaje.

- Las decisiones de Diseño condicionan toda la vida operativa de los sistemas.
  - Según estadísticas, hasta el 60% de los temas relacionados con los fallos y la seguridad pueden evitarse realizando rediseño.
- Una vida operativa de los sistemas del orden de 30 años o más obliga a tener en cuenta que:
  - Un esfuerzo de mejora en fase de diseño puede reducir el Coste de Ciclo de Vida de un sistema
  - La tecnología evoluciona muy rápidamente.
  - Las necesidades operacionales para los que se diseñan los sistemas cambian.
- Una consecuencia de los análisis de RCM (“Reliability Centered Maintenance” – Mantenimiento Centrado en la Fiabilidad) es la necesidad, en ocasiones, de rediseñar como resultado de no considerar, en tiempo de diseño, la Mantenibilidad de los sistemas (fallos ocultos y/o catastróficos).

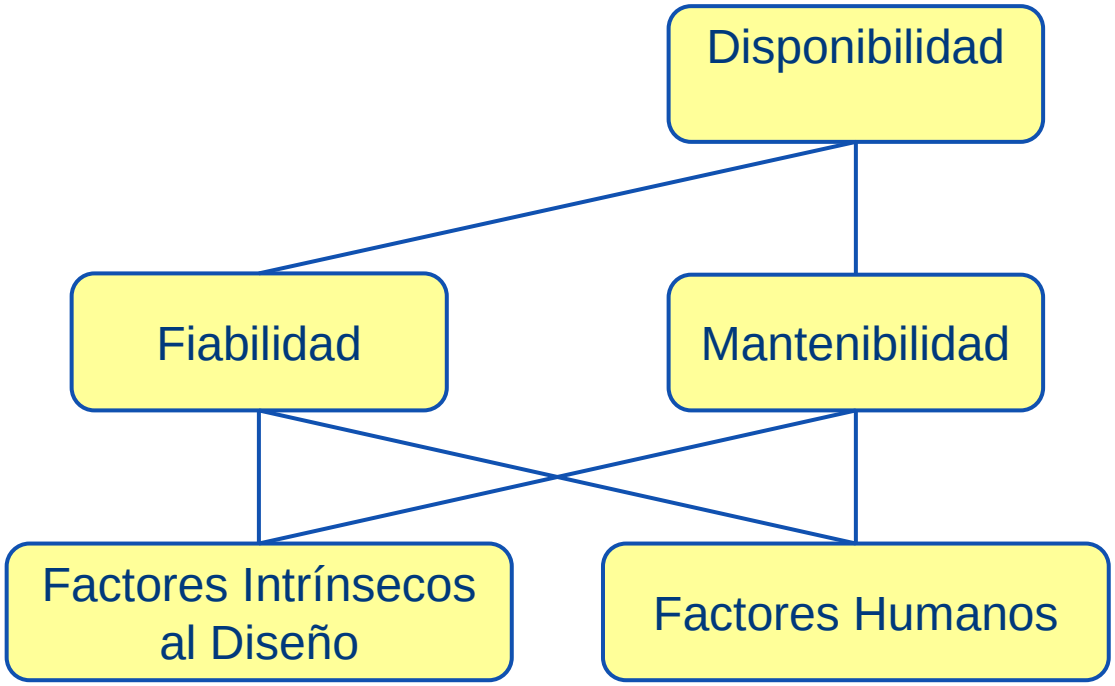
Disponibilidad Operacional



Disponibilidad Operacional



Disponibilidad Inherente



- Análisis de Fiabilidad y Mantenibilidad
- FMECA → RCD
- Recomendaciones de Rediseño
- …

- LORA
- Documentación de Operación y Mantenimiento
- Adiestramiento
- …

Factores Humanos

- El 80% de los fallos de un sistema se deben a factores humanos:
  - Mala Operación de los Sistemas → Resultados no esperados, Incremento de averías.
  - Mala ejecución de los Mantenimientos → Reducción del tiempo entre fallos.

- Existen diversas técnicas para mejorar la fiabilidad humana en fase de diseño (HAZOP «Hazard and Operability Analysis», HEART «Human Error Assessment and Reduction Technique», FTA «Fault Tree Analysis», etc.)

- Los **Manuales** de Operación y Mantenimiento y el **Adiestramiento** son **Piezas Claves** en la mejora de la Fiabilidad Humana y **deben mantenerse** durante el todo el ciclo de vida de un Sistema

Diseño Centrado en Fiabilidad (I)

- El 80% de los costes del Ciclo de Vida de un Sistema corresponden a la fase de explotación del mismo (Operación y Mantenimiento)

- IDEAL: Diseño libre de Fallos - ¿Viable económica o técnicamente?
  - Definir un Mantenimiento Coste/Eficaz
    - Priorizar Mantenimiento PROACTIVO
- OBJETIVO: **Maximizar la DISPONIBILIDAD**

- La Fiabilidad afecta a:
  - Disponibilidad
  - Seguridad y Medio Ambiente
  - Calidad y Prestigio
  - Coste/Rendimiento

Diseño Centrado en Fiabilidad (II)

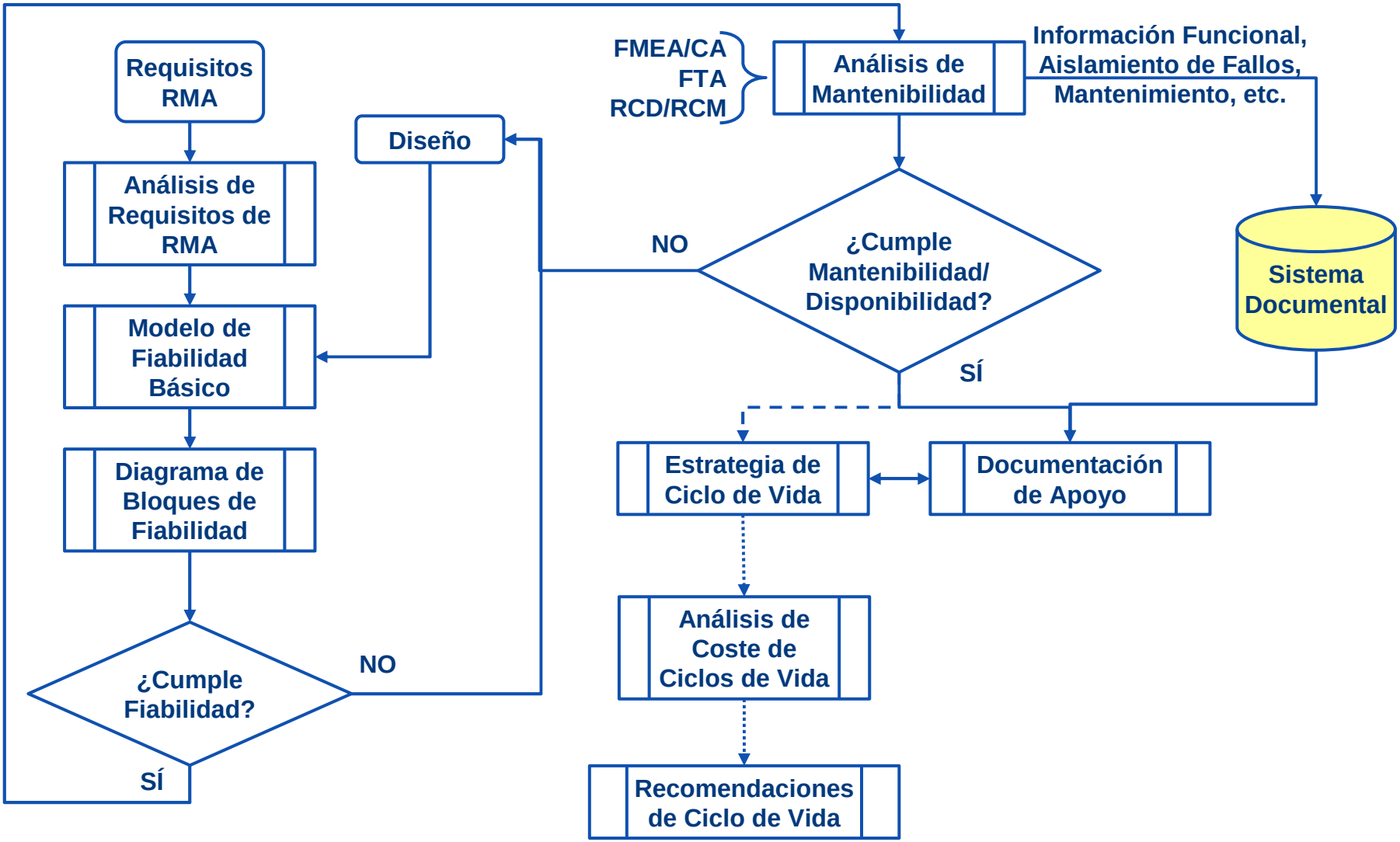
- Una consecuencia de la aplicación de las técnicas de RCM *("Reliability Centered Maintenance"*) es, en ocasiones, el REDISEÑO -> El diseño original no consideró la Mantenibilidad => Importancia del RCD (*"Reliability Centered Design"*).

- Diseño = Funcionalidad + Fiabilidad + Mantenibilidad => Garantizar el Coste/Eficacia a lo largo del Ciclo de Vida.

- Un buen diseño debe considerar:
  - La necesidad de proporcionar una buena relación Coste/Eficacia:
    - Orientado a maximizar la fiabilidad del sistema
    - Simplificar/facilitar las tareas de mantenimiento
  - La definición de Repuestos
  - Los Ciclos de Refresco Tecnológicos

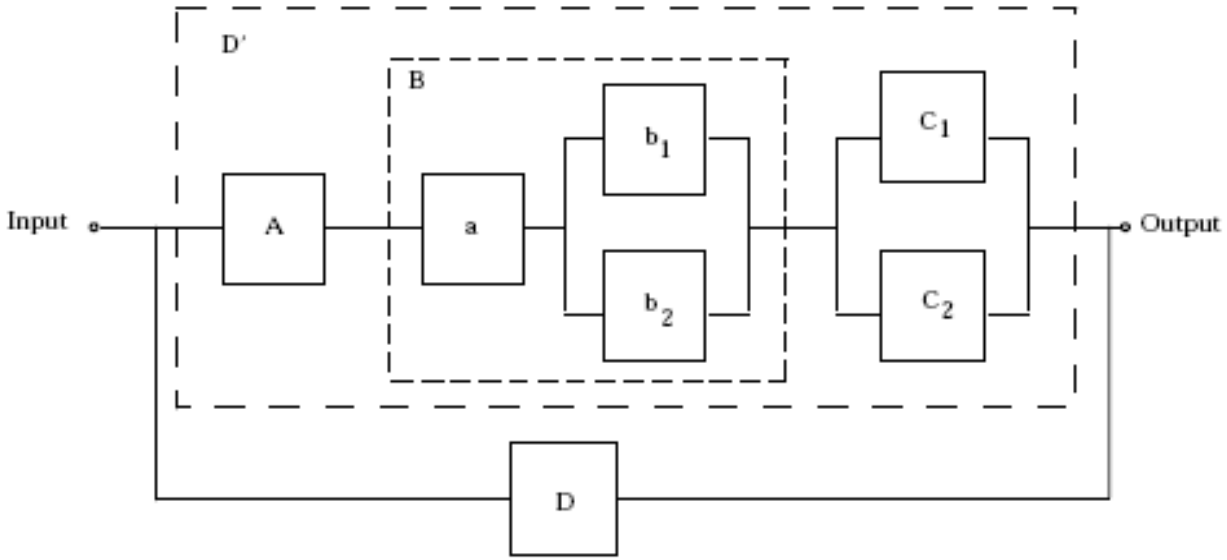
¡ ¡ ¡ Debemos garantizar lo que un sistema HACE, no lo que ES ! ! !

Diagrama de Flujo de Alto Nivel del Proceso de Análisis de Fiabilidad y Mantenibilidad



Modelo de Fiabilidad

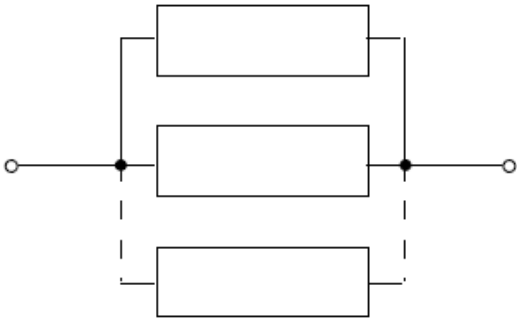
- Para poder para predecir la Fiabilidad y Disponibilidad de un Sistema primero necesitamos modelarlo.
- El Modelo debe tener en cuenta la **Redundancia Física y Funcional** existente en el Diseño.



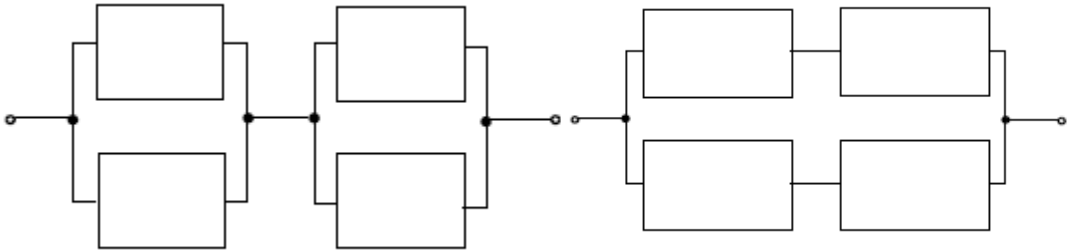
- La fiabilidad de los elementos redundados no es independiente para cada uno. Por ejemplo, la fiabilidad de dos elementos redundantes es una función del tiempo definida como:

$$R(t) = P_a(t) + P_b(t) - P_a(t) \cdot P_b(t)$$

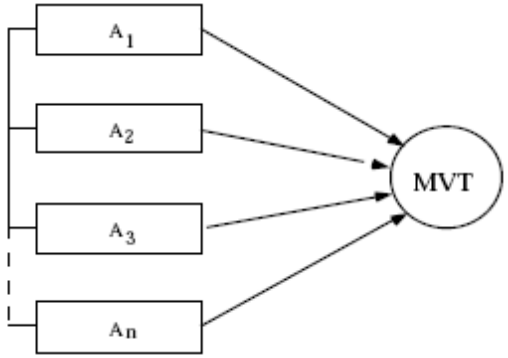
Técnicas de Redundancia



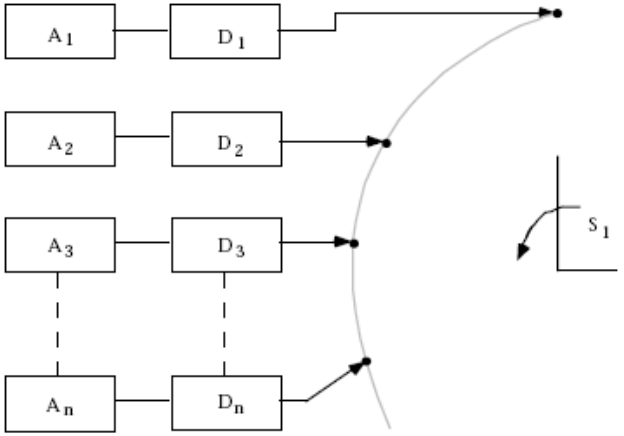
Redundancia Simple Paralelo



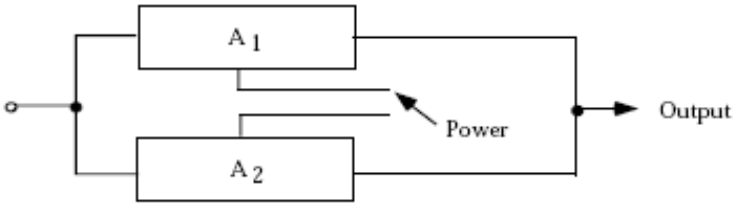
Redundancia Bimodal Paralelo/Serie y Serie/Paralelo

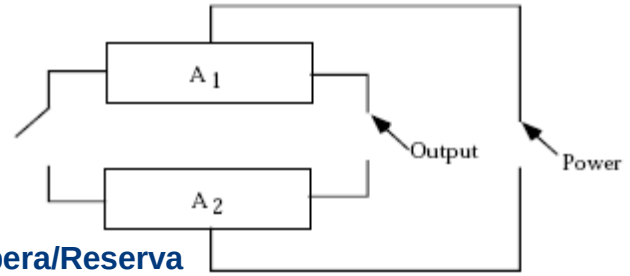


Redundancia con Lógica de Control Adaptativo



Redundancia con Operación en Espera/Reserva

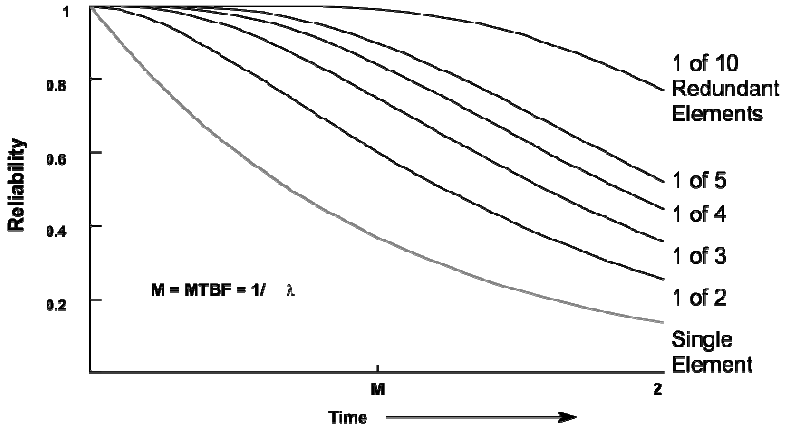




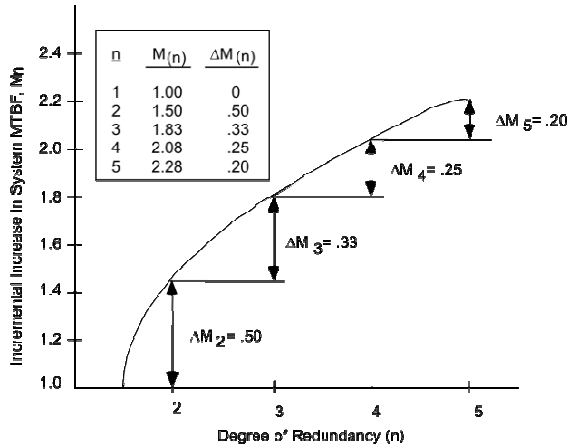
Redundancia en Espera/Reserva

Consideraciones a la Redundancia

- La ganancia adicional de fiabilidad para los elementos redundantes disminuye rápidamente conforme añadimos más elementos redundantes.
- Añadir más elementos redundantes conlleva un incremento del coste de adquisición y de mantenimiento.
- La efectividad de estas técnicas de redundancia no está sólo en la disminución real de la tasa de fallos del sistema, sino en la posibilidad de realizar reparaciones mientras el sistema sigue funcionando, lo cual conlleva un alto incremento la disponibilidad.
- Al añadir elementos redundantes hay que tener en cuenta la **necesidad de métodos de chequeo** de los componentes del sistema. Al tener elementos redundantes, puede ocurrir que no fuésemos conscientes de la pérdida de la función de redundancia. -> ***¡¡¡Riesgo de añadir Fallos Ocultos!!!***
- Un fallo en un elemento redundado puede tener efecto en su redundante.



(a) Simple Active Redundancy for One of n Element Required



(b) Incremental Increase in System MTBF for n Active Elements

Factores que Caracterizan la Fiabilidad

- Los datos de fiabilidad (MTBF o tasas de fallo) proporcionados por los fabricantes, ya sean teóricos o prácticos, están referidos a unas condiciones de trabajo determinadas.
- No es posible usar el dato suministrado de modo directo en nuestro modelo, ya que sus condiciones de cálculo pueden diferir de las de uso de nuestro sistema.
- Tendremos que adaptar el dato en función del Entorno, de la Calidad de los componentes y de la Temperatura de operación.
  - *En general, el MTBF es suministrado como un dato más de catálogo del componente, por lo que los fabricantes suelen incluir sólo el mejor dato para ellos, que debe ser considerado como el peor caso para nosotros. Si no hay información del entorno de cálculo, una buena hipótesis es suponer que se ha calculado para un entorno "Ground Benign", una calidad de fabricación Comercial y una temperatura especificada entre 20 y 30ºC.*

Factores que Caracterizan la Fiabilidad
Entorno – Calidad – Temperatura

Al entorno

Desde el entorno	G_B	G_F	G_M	N_S	N_U	A_{IC}	A_{IF}	A_{UC}	A_{UF}	A_{RW}	S_F
G_B	X	0.5	0.2	0.3	0.1	0.3	0.2	0.1	0.1	0.1	1.2
G_F	1.9	X	0.4	0.6	0.3	0.6	0.4	0.2	0.1	0.2	2.2
G_M	4.6	2.5	X	1.4	0.7	1.4	0.9	0.6	0.3	0.5	5.4
N_S	3.3	1.8	0.7	X	0.5	1.0	0.7	0.4	0.2	0.3	3.4
N_U	7.2	3.9	1.6	2.2	X	2.2	1.4	0.9	0.5	0.7	8.3
A_{IC}	3.3	1.8	0.7	1.0	0.5	X	0.7	0.4	0.2	0.3	3.9
A_{IF}	5.0	2.7	1.1	1.5	0.7	1.5	X	0.6	0.4	0.5	5.8
A_{UC}	8.2	4.4	1.8	2.5	1.2	2.5	1.6	X	0.6	0.8	9.5
A_{UF}	14.1	7.6	3.1	4.4	2.0	4.2	2.8	1.7	X	1.4	16.4
A_{RW}	10.2	5.5	2.2	3.2	1.4	3.1	2.1	1.3	0.7	X	11.9
S_F	0.9	0.5	0.2	0.3	0.1	0.3	0.2	0.1	0.1	0.1	X

Environmental Factors as Defined in MIL-HDBK-217

G_B- Ground Benign; G_F Ground Fixed; G_M- Ground Mobile; N_S- Naval Sheltered; N_U- Naval Unsheltered; A_{IC}- Airborne Inhabited Cargo; A_{IF}- Airborne Inhabited Fighter; A_{UC}-Airborne Uninhabited Cargo; A_{UF} -Airborne Uninhabited Fighter; A_{RW} - Airborne Rotary Winged; S_F- Space Flight

A la temperatura

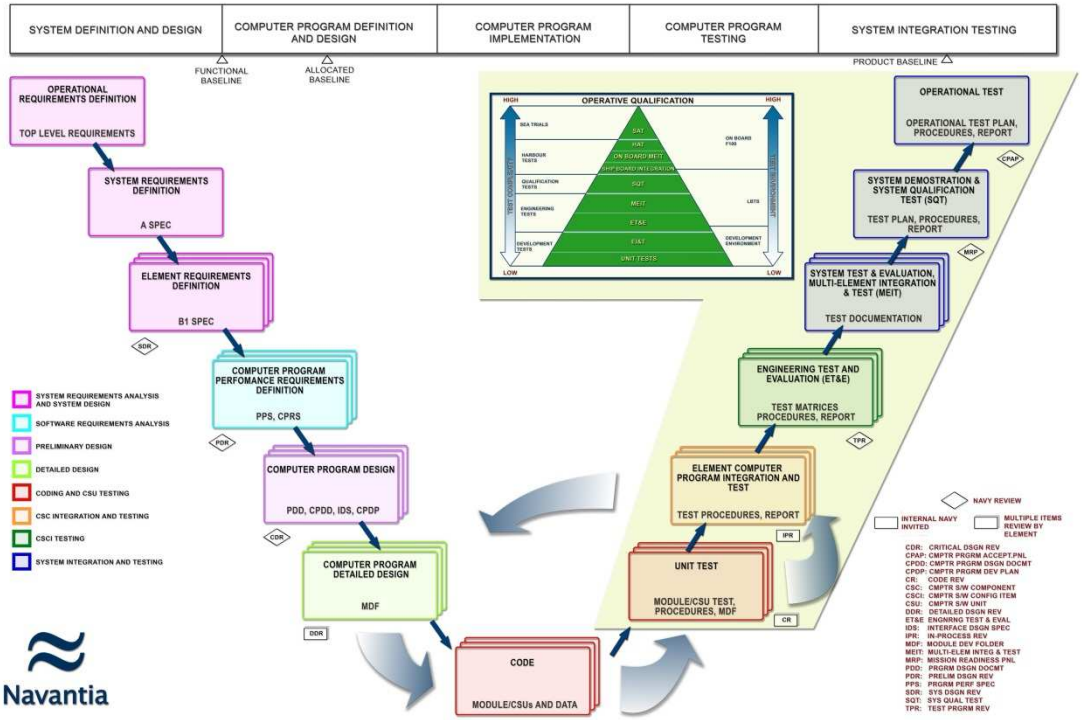
Desde la temperatura	10	20	30	40	50	60	70
10	X	0.9	0.8	0.8	0.7	0.5	0.4
20	1.1	X	0.9	0.8	0.7	0.6	0.5
30	1.2	1.1	X	0.9	0.8	0.6	0.5
40	1.3	1.2	1.1	X	0.9	0.7	0.6
50	1.5	1.4	1.2	1.1	X	0.8	0.7
60	1.9	1.7	1.6	1.5	1.2	X	0.8
70	2.4	2.2	1.9	1.8	1.5	1.2	X

A la calidad

Desde la calidad	Espacial	Militar	Rugerizado	Comercial
Espacial	X	0.8	0.5	0.2
Militar	1.3	X	0.6	0.3
Rugerizado	2.0	1.7	X	0.4
Comercial	5.0	3.3	2.5	X

Fiabilidad del Software (I)

- El software es parte fundamental de un Sistema, ya que controla o desempeña la mayor parte de la funcionalidad del mismo. Por ello ha de ser diseñado y desarrollado en paralelo con el hardware para dotar de la funcionalidad al mismo.
- Es muy importante el proceso de desarrollo del mismo, para garantizar que el no presenta fallos durante las fases de explotación de los sistemas.



Fiabilidad del Software (y II)

- Existen diferencias entre la fiabilidad del Hardware y del Software, las más importantes serían que ni las horas de funcionamiento ni la frecuencia de uso influyen en la tasa de fallos del Software.
- Hay diferentes modelos de predicción de fiabilidad del software, entre los que destacan el *"Musa's Execution Time Model"*, el *"Putnam's Model"*, y dos modelos desarrollados por el Rome Laboratory, el *"TR-92-52"* y el *"TR-92-15"*.
- Cuando hablamos de fallos en el software debemos distinguir tres tipos de fallo:
  - Requisitos ambiguo, no se han especificado correctamente los objetivos y funciones a desarrollar por el Software
  - Fallo en el Diseño del Software o en la documentación que describe correctamente el diseño -> Diseño poco apropiado para facilitar su mantenimiento
  - Código Erróneo, fallo en el código para cumplir con el diseño software.
- Otro aspecto fundamental cuando analizamos fallos en el software es el usuario y la interfaz hombre máquina.

Se garantiza una fiabilidad elevada en el software sometiéndolo a un proceso de pruebas adecuado.

Asociado al proceso de pruebas es básico un estricto Control del Configuración que permita tener una trazabilidad de los requisitos probados y de los cambios introducidos en el sistema

Cálculo de Mantenibilidad de Sistemas

- La Mantenibilidad de un sistema hay que definirla en función de los modos de fallo.
- Ejemplo:

Modo de Fallo A	Modo de Fallo B
MTBF = 1.000 horas TR = 0,1 horas	MTBF = 20.000 horas TR = 19 horas

  - Ciclo de Trabajo = 5.000horas/año
  - Vida del Sistema = 8 años sin Refrescos Tecnológicos ≡ 40.000 horas
  - Fallos Asociados al Modo A = 40
  - Fallos Asociados al Modo B = 2

$$MTTR = \frac{0.1h * 40\,fallos + 19h * 2\,fallo}{42\,fallos} = 1h$$

- Según se puede ver en el ejemplo, el tiempo medio de reparación es el tiempo promedio de los períodos de tiempo usados para cada una de las reparaciones realizadas en un tiempo determinado de un sistema (tiempo de evaluación).

$$MTTR = \frac{\sum_{T} TTR}{CR}$$

Donde:

MTTT: "Mean Time To Repair" (Tiempo Medio de Reparación)
T: Tiempo de Evaluación
TTR: "Time To Repair" (Tiempo de Reparación)
CR: Cantidad de Reparaciones en el tiempo T

Aspectos Claves para Mejorar la Mantenibilidad

- Accesibilidad y Modularidad.
- Capacidad de Restauración del Sistema.
- Aislamiento de Fallos.
- Proceso de Reemplazo.
- Disponibilidad de Repuestos, Herramientas y Equipos de Pruebas.
- Disponibilidad de Personal con el suficiente Nivel de Cualificación (Adiestramiento).
- Calidad de la Documentación de Apoyo.
- Gestión de la Configuración.
- Definir el Plan de Ciclo de Vida en fase de Diseño → Condiciona todas las decisiones relacionadas con los puntos anteriores.

Conclusiones

- Las decisiones tomadas en fase de diseño, que representa aproximadamente el 20% de coste de ciclo de vida de un sistema, condicionan la fase operativa que representa un 80%.
- El objetivo de las técnicas de análisis de Fiabilidad y Mantenibilidad es aumentar la disponibilidad desde el punto de vista **funcional** del Sistema.
- Aunque el objetivo ideal de las técnicas de estudios de fiabilidad es ir hacia un diseño libre de fallos, esto, en la mayoría de los casos no es coste/eficaz, por lo que es necesario incluir el concepto mantenibilidad desde las fases tempranas del diseño.
- Es muy importante prestar atención a los elementos catastróficos desde las fases tempranas del diseño, ya que su detección durante las fases operativas de un sistema conlleva un rediseño del mismo.
- El factor humano es clave en fiabilidad de un Sistema → Una buena Documentación y Formación reduce su impacto
- Es necesario introducir el concepto de Ciclo de Vida en la fase de diseño

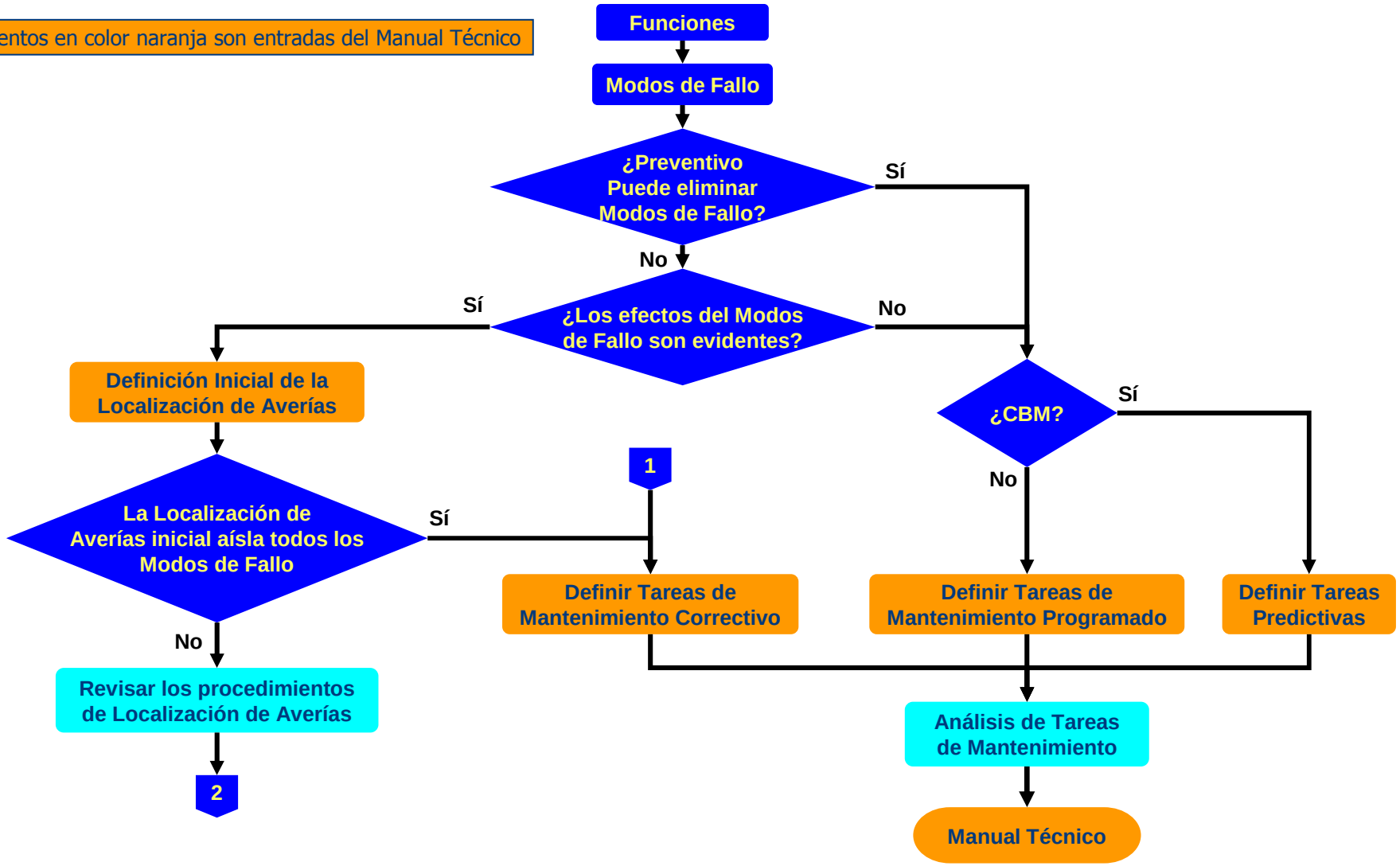
Los estudios de Disponibilidad en Fase de Diseño son ESTRATÉGICOS de cara a tener el Ciclo de Vida más eficiente.

DIAPOSITIVAS DE BACKUP

¡¡¡Un modo de fallo que afecte a la seguridad o al medioambiente y que NO disponga de alguna tarea de mantenimiento proactivo que lo evite/detecte hace necesario el rediseño de un sistema!!!

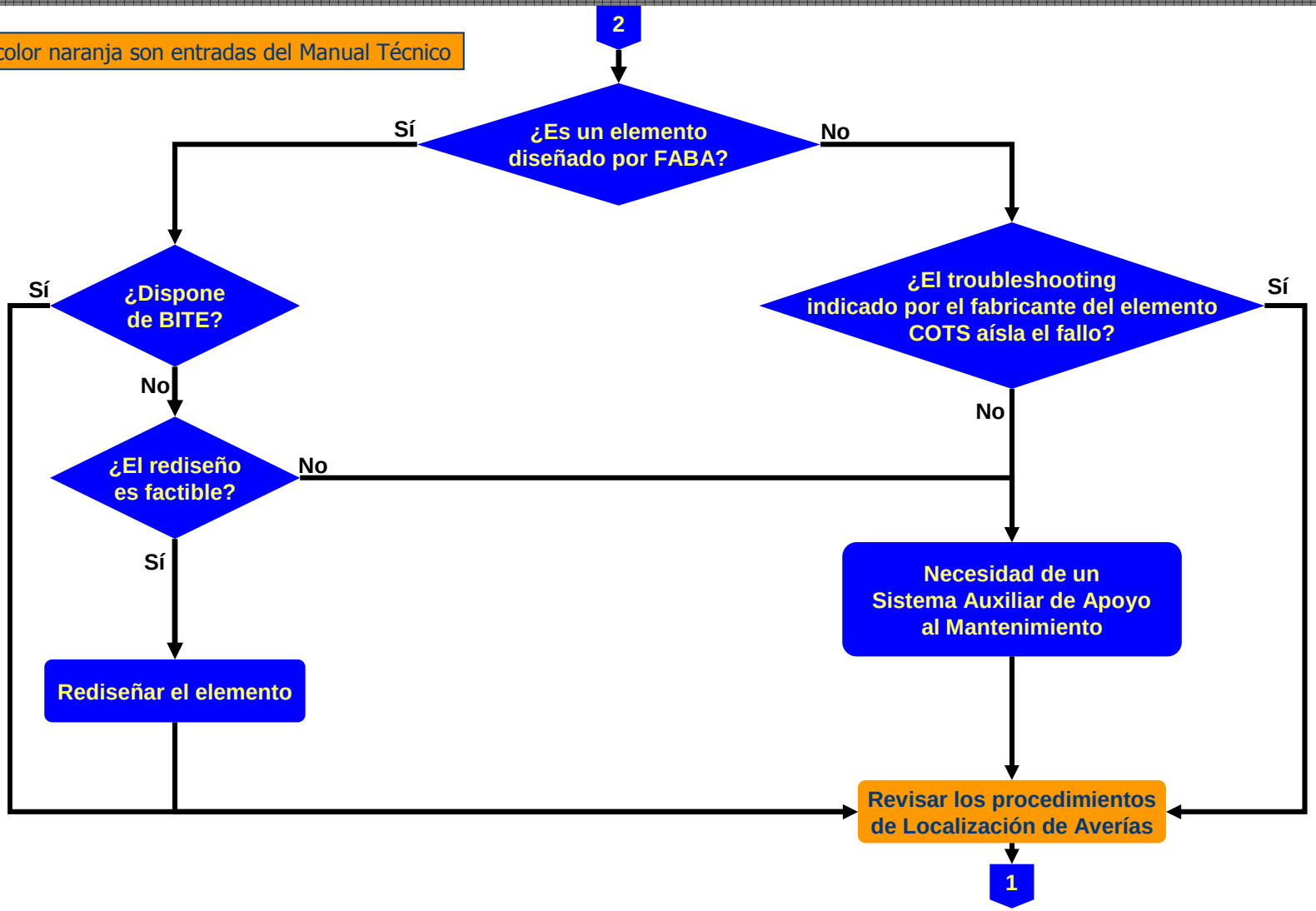
Definición del Mantenimiento Proceso (I)

Elementos en color naranja son entradas del Manual Técnico

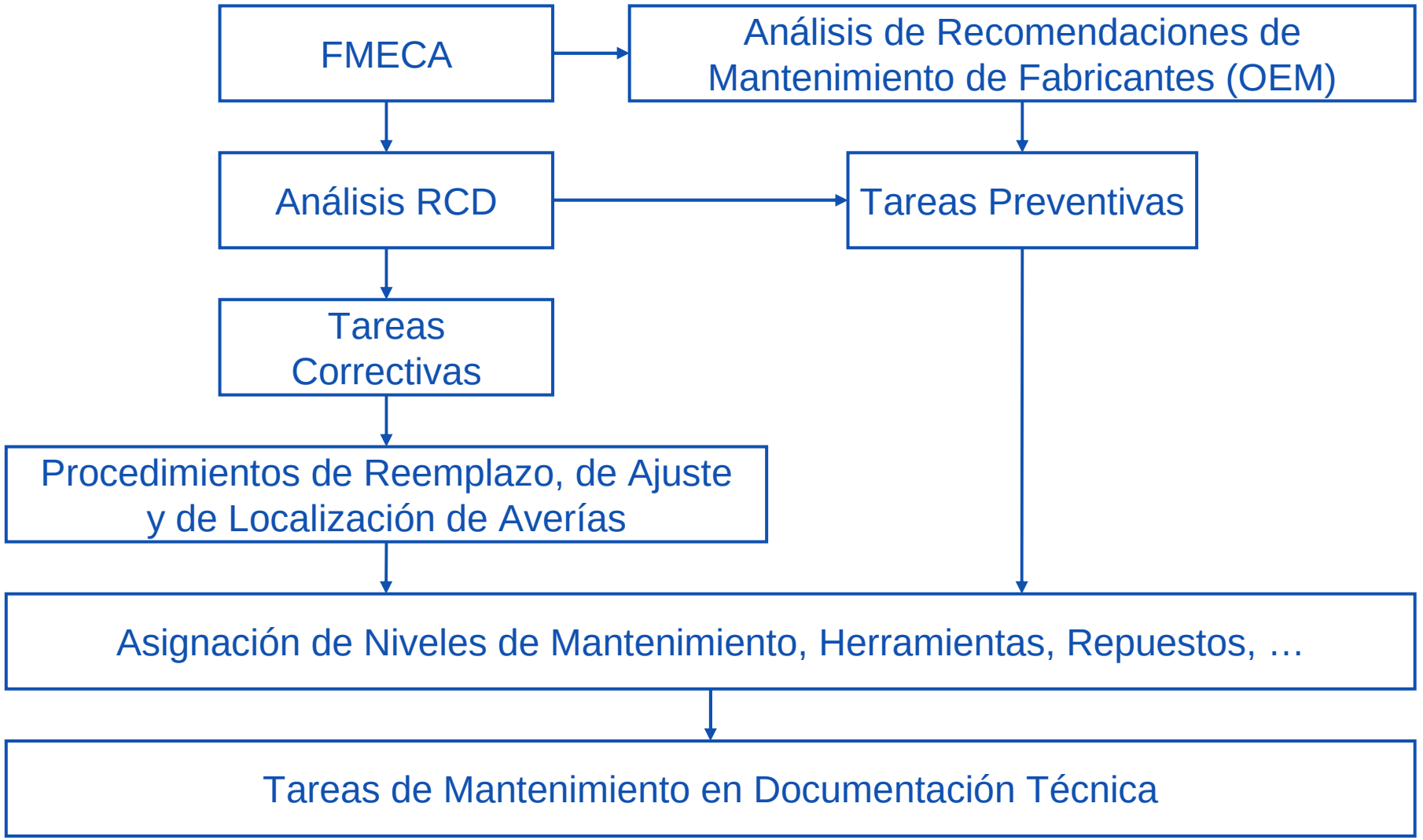


Definición del Mantenimiento Proceso (y II)

Elementos en color naranja son entradas del Manual Técnico



Documentación del Mantenimiento



Cálculo de Mantenibilidad de Sistemas (y II)

- Según se ha podido ver en el ejemplo anterior, el MTTR se define como el tiempo promedio de los períodos de tiempo usados para cada una de las reparaciones realizadas en un tiempo determinado de un sistema (tiempo de evaluación). Entonces, el MTTR es:

$$MTTR = \frac{\sum_{T} TTR}{CR}$$

Donde:

MTTT: "Mean Time To Repair" (Tiempo Medio de Reparación)
TTR: "Time To Repair" (Tiempo de Reparación)
T: Tiempo de Evaluación
CR: Cantidad de Reparaciones en el tiempo T

Fiabilidad de Elementos Redundantes

La fiabilidad de dos elementos redundantes es una función del tiempo definida como:

$$R(t) = P_a(t) + P_b(t) - P_a(t) \cdot P_b(t)$$

Por lo tanto, para una distribución exponencial:

$$R(t) = e^{-\lambda_a t} + e^{-\lambda_b t} - e^{-(\lambda_a t + \lambda_b t)}$$

Con lo que:

$$MTBF = \int_0^\infty R(t)dt = \int_0^\infty (e^{-\lambda_a t} + e^{-\lambda_b t} - e^{-(\lambda_a t + \lambda_b t)})dt \Rightarrow MTBF = \frac{1}{\lambda_a} + \frac{1}{\lambda_b} - \frac{1}{\lambda_a + \lambda_b}$$

En el caso de tres elementos redundantes:

$$MTBF = \frac{1}{\lambda_a} + \frac{1}{\lambda_b} + \frac{1}{\lambda_c} - \frac{1}{\lambda_a + \lambda_b} - \frac{1}{\lambda_a + \lambda_c} - \frac{1}{\lambda_b + \lambda_c} + \frac{1}{\lambda_a + \lambda_b + \lambda_c}$$

Actividades de Apoyo al Ciclo de Vida

- Análisis Logísticos
  - Análisis de Fiabilidad
  - Análisis de Mantenibilidad
  - LSA (Logistic Support Analysis)
  - LORA (Level Of Repair Analysis)
  - Etc.
- Elaboración de Documentación de Apoyo
  - Manuales Técnicos (Operación y Mantenimiento)
  - Planes de Mantenimiento
  - Recomendación de Repuestos, Herramientas especiales, Equipos de prueba, etc.
  - Catalogación OTAN
- Adiestramiento (Presencial/CBT)
  - Gestión de Cursos
  - Impartición de Cursos
  - Desarrollo de Sistemas de Adiestramiento por Ordenador (CBT)
- Sostenimiento de Sistemas:
  - Gestión de la Configuración
  - Gestión de Obsolescencia y Refrescos tecnológico
  - Gestión de Programas de Sostenimiento
  - Gestión de la Cadena de Suministro (Repuestos, reparaciones, reciclaje)
  - Asistencia Técnica Remota/Helpdesk
  - Análisis de Costes de Ciclo de Vida

Ingeniería Logística

Op. de Sostenimiento

Los análisis de Fiabilidad y Mantenibilidad en fase de Diseño son los Cimientos de un Ciclo de Vida eficiente

Clases de Mantenimiento

- Mantenimiento Predictivo (Mantenimiento Basado en la Condición).
- Mantenimiento Preventivo
- Mantenimiento Correctivo
- Mantenimiento Detectivo