

Técnicas cuantitativas de fiabilidad aplicables en las áreas de proceso de gestión de riesgos (RSKM), verificación (VER) y validación (VAL) de CMMi[®]

Luis Redondo
Métodos y Tecnología

Objetivo de la ponencia

- Mostrar algunas técnicas de fiabilidad que ayudan a realizar con éxito las áreas de proceso de CMMi[®]:
 - Verificación (VER)
 - Validación (VAL)
 - Gestión de Riesgos (RSKM)

Verificación - VER

- *The purpose of Verification (VER) is to ensure that selected work products meet their specified requirements.*
- Las actividades de verificación tienen que asegurar que se está construyendo **correctamente el sistema.**

Verificación - VER

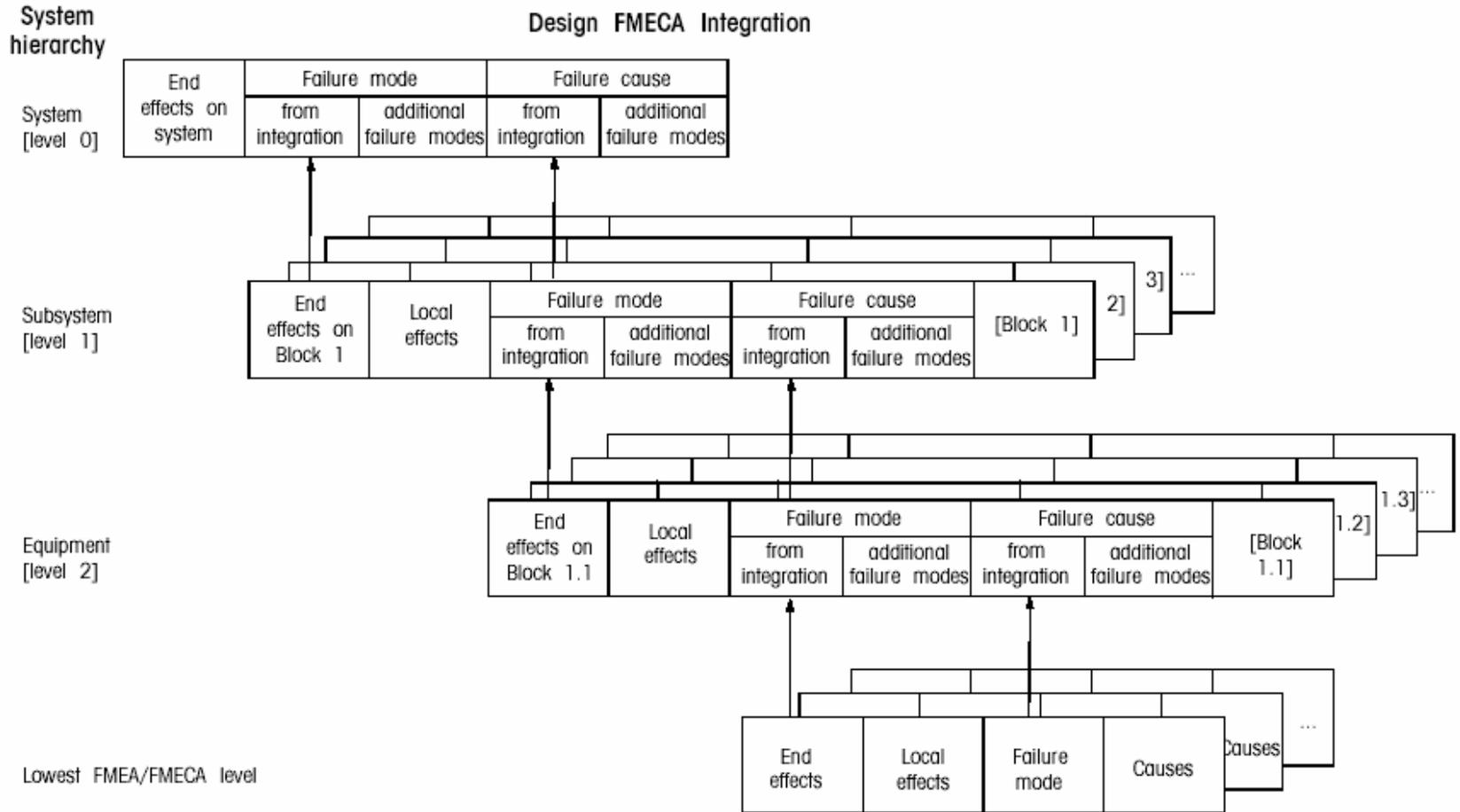
- **SP 1.1-1 Select Work Products for Verification:** *Select the work products to be verified and the verification methods that will be used for each.*
- Algunos métodos de verificación: *inspections, peer reviews, audits, walkthroughs, analyses, simulations, testing, and demonstrations.*
- Proponemos:
 - **FMECA de producto (del diseño).**
 - **RBDs y PMTC.**

FMECA – Failure Modes, Effects and Critical Analysis

- **Técnica inductiva** (*bottom-up*, de particular a general) con el objeto de descubrir problemas que puedan provocar situaciones críticas.
- **Búsqueda sistemática** de Modos de Fallo, Causas y Efectos.

| Componente | Modo de Fallo | Efecto(-s) | S | Causa(-s) | O | Control(-es) detección y recuperación | D | Acción recomendada | Responsable y fecha terminación acción |
|------------|---------------|------------|---|-----------|---|---------------------------------------|---|--------------------|--|
| | | | | | | | | | |

Proceso FMECA



Fuente: European Cooperation for Space Standardization (ECSS)

Beneficios al aplicar FMECA en el diseño HW/SW

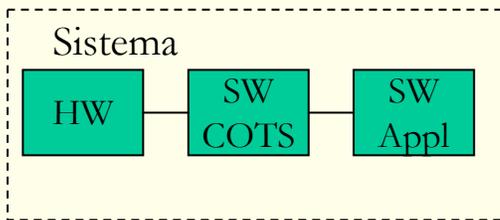
- **Identificar y documentar** fallos, sus causas, efectos y mecanismos de recuperación.
- **Asegurar** que se cumplen las guías de tolerancia a fallos.
- **Verificar** la corrección de las acciones de recuperación.
- **Recomendaciones de diseño:**
 - **Mejorar** el cubrimiento de la tolerancia a fallos.
- **Recomendaciones para pruebas:**
 - **Facilitar** el diseño de casos de prueba de escenarios negativos.

Modelos de disponibilidad

- **Cada componente** contribuye a la disponibilidad final:
 - **Hardware:** Máquinas, discos, ...
 - **Redes de comunicación:** Routers, switches, cables...
 - **SO y COTS:** Unix, BBDD, middleware, ...
 - **SW de Aplicación.**
- Debemos identificar las **configuraciones:** single, single con recuperación, redundancias cluster (A/A), redundancias spare (A/P), ...
- Técnicas que se pueden emplear:
 - **Reliability Block Diagrams (RBDs).**
 - **Procesos Markov en Tiempo Continuo (PMTTC).**

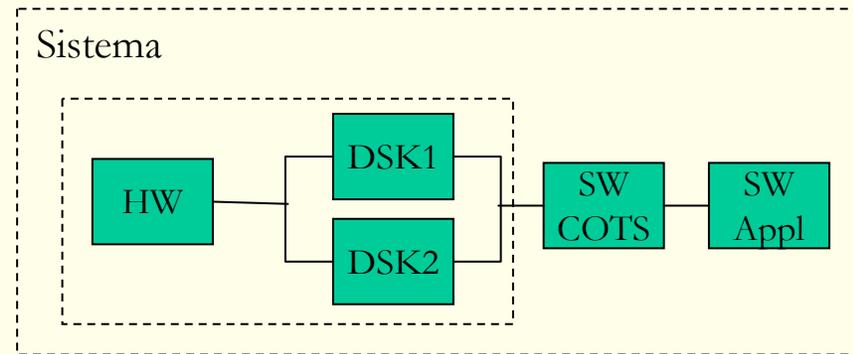
RBDs – Reliability Block Diagrams

- Muy fáciles de usar.
- Insuficiente para representar configuraciones complejas porque sólo podemos representar 2 estados por componente.
- No obstante, es una técnica muy aplicable en Sistemas Intensivos en Software cuando se emplea junto con Markov.



$$R_s = R_{HW} * R_{SW-COTS} * R_{SW-APP}$$

RDB Sistema sin redundancias



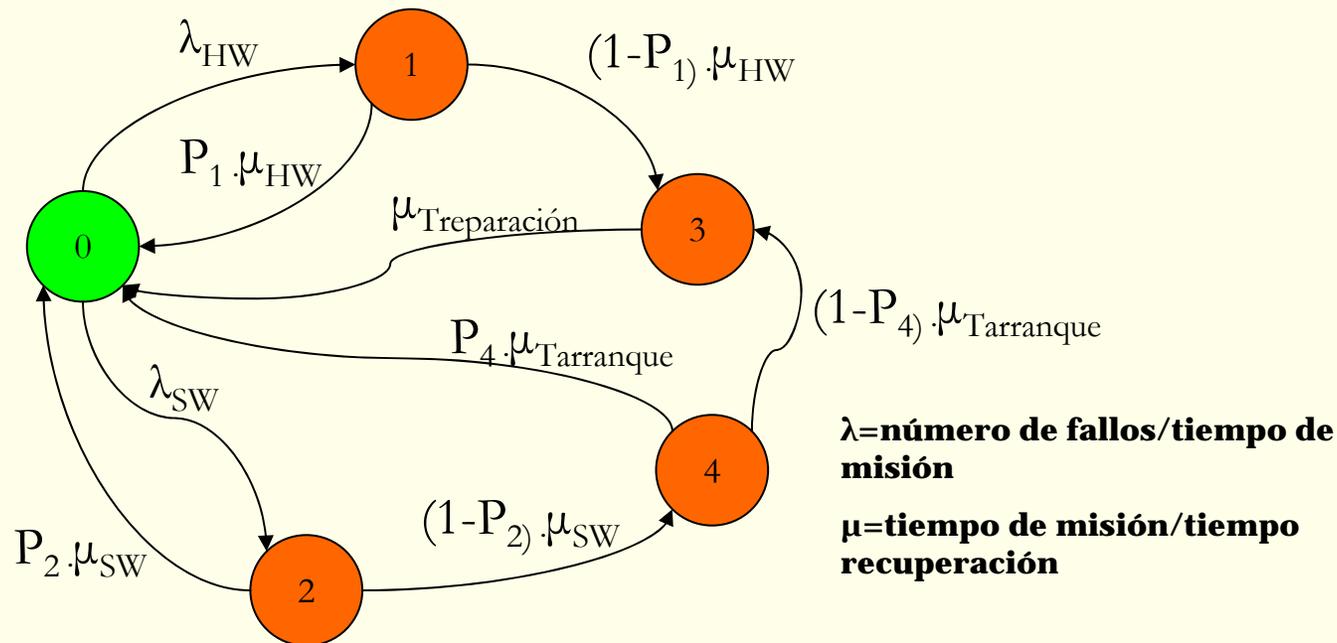
$$R_s = R_{HW} * [1 - \prod (1 - R_{DSK_i})] * R_{SW-COTS} * R_{SW-APP}$$

RDB Sistema con una redundancia HW

PMTC - Procesos de Markov en Tiempo Continuo

- Un Proceso de Markov consiste en un conjunto de Estados y de posibles Transiciones entre ellos, sin memoria.
- El sistema permanece en un estado por un tiempo definido y pasa a otro estado de acuerdo con una tasa de transición -transition rate.

PMTC - Procesos de Markov en Tiempo Continuo



Modelo de Markov con mecanismos de recuperación ante fallos HW y SW

Validación - VAL

- *The **purpose of Validation (VAL)** is to demonstrate that a product or product component fulfills its intended use when placed in its intended environment.*
- Las actividades de validación tienen que asegurar que se está construyendo el **sistema correcto.**

Validación - VAL

- **SP 1.1-1 Select Products for Validation:**
Select products and product components to be validated and the validation methods that will be used for each.
- Proponemos:
 - **Perfiles operacionales.**
 - **Modelos de Crecimiento de Fiabilidad SW (SGRM).**

Perfil operacional (I)

¿Qué es?

- Un perfil operacional es un conjunto completo de operaciones con sus probabilidades de ocurrencia.
 - Una **operación** es una tarea lógica a nivel de sistema (funcional e independiente del HW/SW) que la inicia un usuario, otro sistema o el propio sistema. Además cuando termina, vuelve el control al iniciador.
 - Una operación puede ser **uno o más casos de uso**.
 - **Probabilidad de ocurrencia** es la probabilidad de invocar la operación sobre el conjunto total de operaciones.

Perfil operacional (II)

¿Para qué sirve?

- Para ser **más eficaces** en el desarrollo y en las pruebas, esto es, comenzar por lo que más se va a emplear. Seamos prácticos.

¿Cómo se aplica?

1. Identificar todos los iniciadores de las operaciones.
2. Crear y revisar la lista de operaciones.
3. Determinar tasas de ocurrencia
 - › Número de veces de ejecución por unidad de tiempo.
4. Calcular las probabilidades de ocurrencia de cada operación:
 - › Tasa de ocurrencia de operación dividida entre la tasa total.

SRGM - Modelos de Crecimiento de Fiabilidad Software (I)

¿Qué son?

- Son gráficas que reflejan el **patrón de defectos** de un Aplicativo SW basándose en datos obtenidos durante las fases formales de pruebas.
- En Software, λ **varia** continuamente porque a medida que vamos arreglando fallos, se pueden introducir nuevos defectos.

¿Para qué se emplean? Para predecir:

- El número de fallos residuales.
- Cuando deberíamos parar de hacer pruebas.

SRGM - Modelos de Crecimiento de Fiabilidad Software (II)

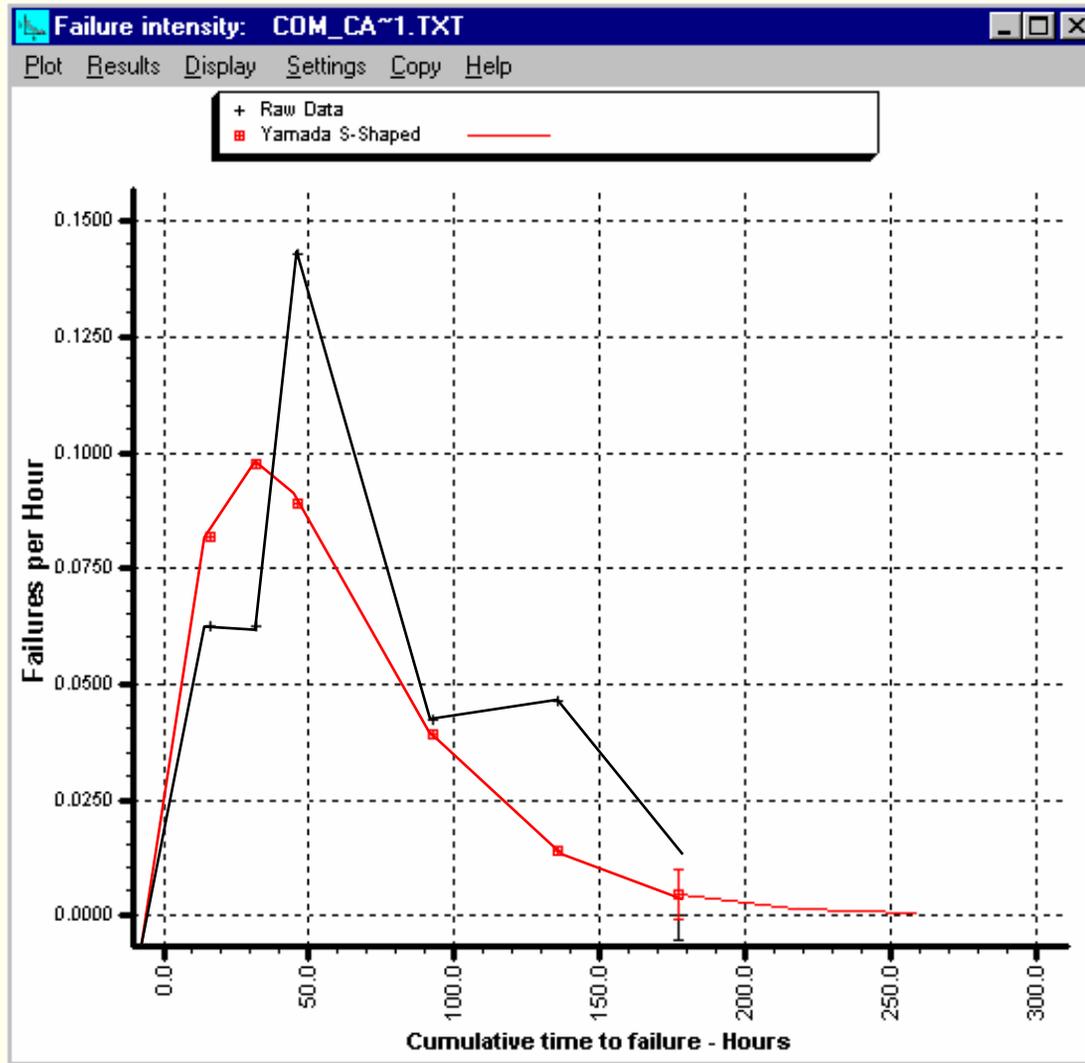
¿En qué se basa - *Rationale*?

La ocurrencia de fallos durante las pruebas formales puede ser un buen indicador de la fiabilidad del producto en explotación.

¿Cómo se trabaja básicamente con los Modelos de Crecimiento de Fiabilidad?

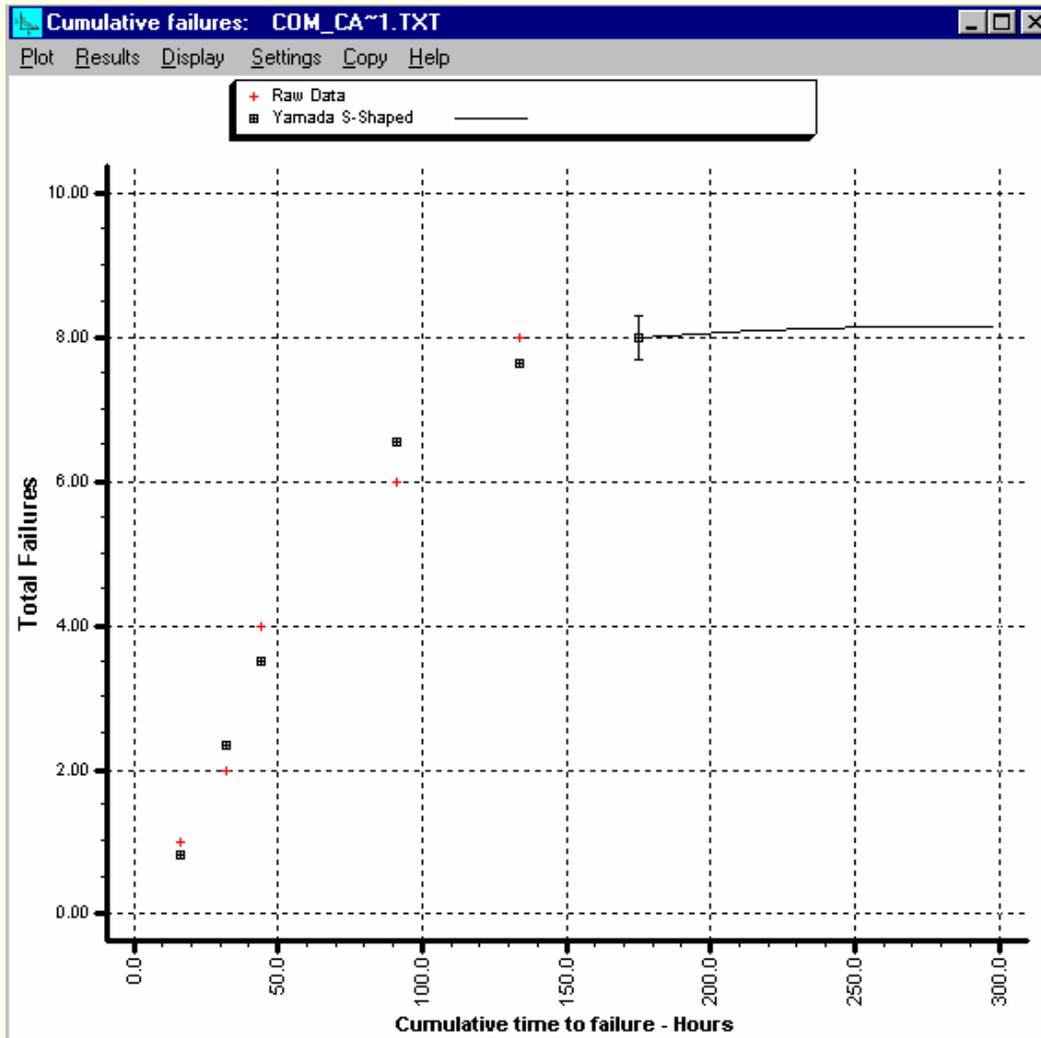
1. Recoger datos “fiabiles” de incidencias y esfuerzos.
2. Aplicar catálogo de modelos: Goel-Okumoto NHPP, Yamada S-Shaped, ...
3. Seleccionar modelo que mejor se ajusta.
4. Obtener los fallos residuales y tasa de fallos.

Modelos Crecimiento Fiabilidad SW (III)



En este caso concreto, el modelo Yamada S-Shaped considera el tiempo de aprendizaje.

Modelos Crecimiento Fiabilidad SW (III)



- **Nº total de fallos estimados en el proyecto: 8.17731**
- **Porcentaje estimado de fallos encontrados durante las pruebas: 97.83%**
- **Nº total de fallos latentes estimados: 0.17731**
- **Porcentaje de fallos estimados por aparecer: 2.17%**

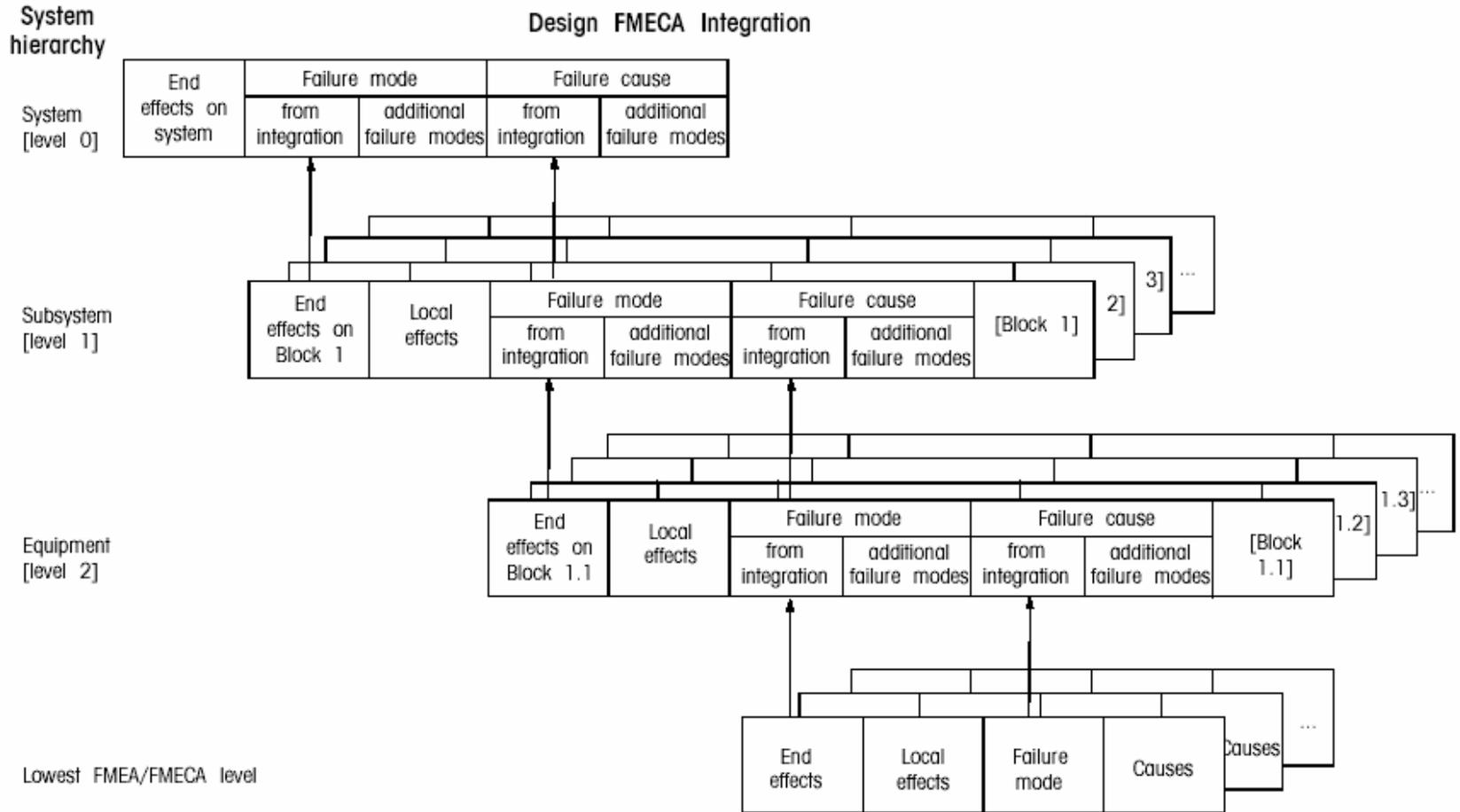
Proceso de Gestión de Riesgos-RSKM

- *The purpose of Risk Management (RSKM) is to identify potential problems before they occur so that risk-handling activities can be planned and invoked as needed across the life of the product or project to mitigate adverse impacts on achieving objectives.*
- *Risk management must consider both internal and external sources for cost, schedule, and technical risk*

Proceso de Gestión de Riesgos-RSKM

- SP 2.1-1 *Identify Risks*. “Performance risks” puede incluir riesgos relativos a:
 - Análisis y diseño
 - Fabricación
- Proponemos:
 - **FMECA de producto y de proceso** (SAE J-1739)

Proceso FMECA



Fuente: European Cooperation for Space Standardization (ECSS)

Resumiendo

- FMECA de producto, RBDs y PMTC en la verificación de requisitos RAMS.
- Perfiles operacionales y SRGM en la validación de sistemas: GO-NOGO del sistema a explotación.
- FMECA de producto y de procesos en la gestión de riesgos.



Gracias por la atención prestada

lredondo@mtp.es