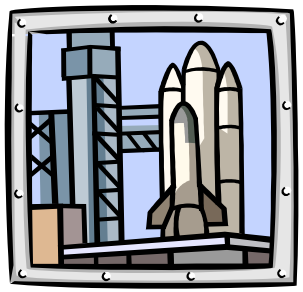
¿Cuál es la madurez que necesitarían los procesos para el desarrollo de sistemas de software crítico?

Patricia Rodríguez, Josefina Alonso, José Carlos Sánchez

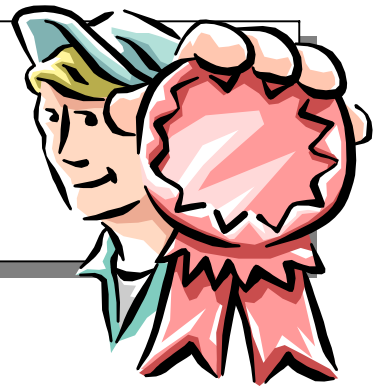
SoftWcare,S.L

Introducción

- Necesidad de certificar y homologar sistemas críticos (automóviles, aviones, aparatos médicos...) cuya criticidad reside en los productos software que contienen.



Problemática



- El objetivo de la certificación/homologación consiste en asegurar un mínimo riesgo de fallo del sistema o al menos un nivel de riesgo aceptable
- Esta certificación u homologación es complicada debido a la creciente incorporación de nuevas tecnologías (por ejemplo, software)

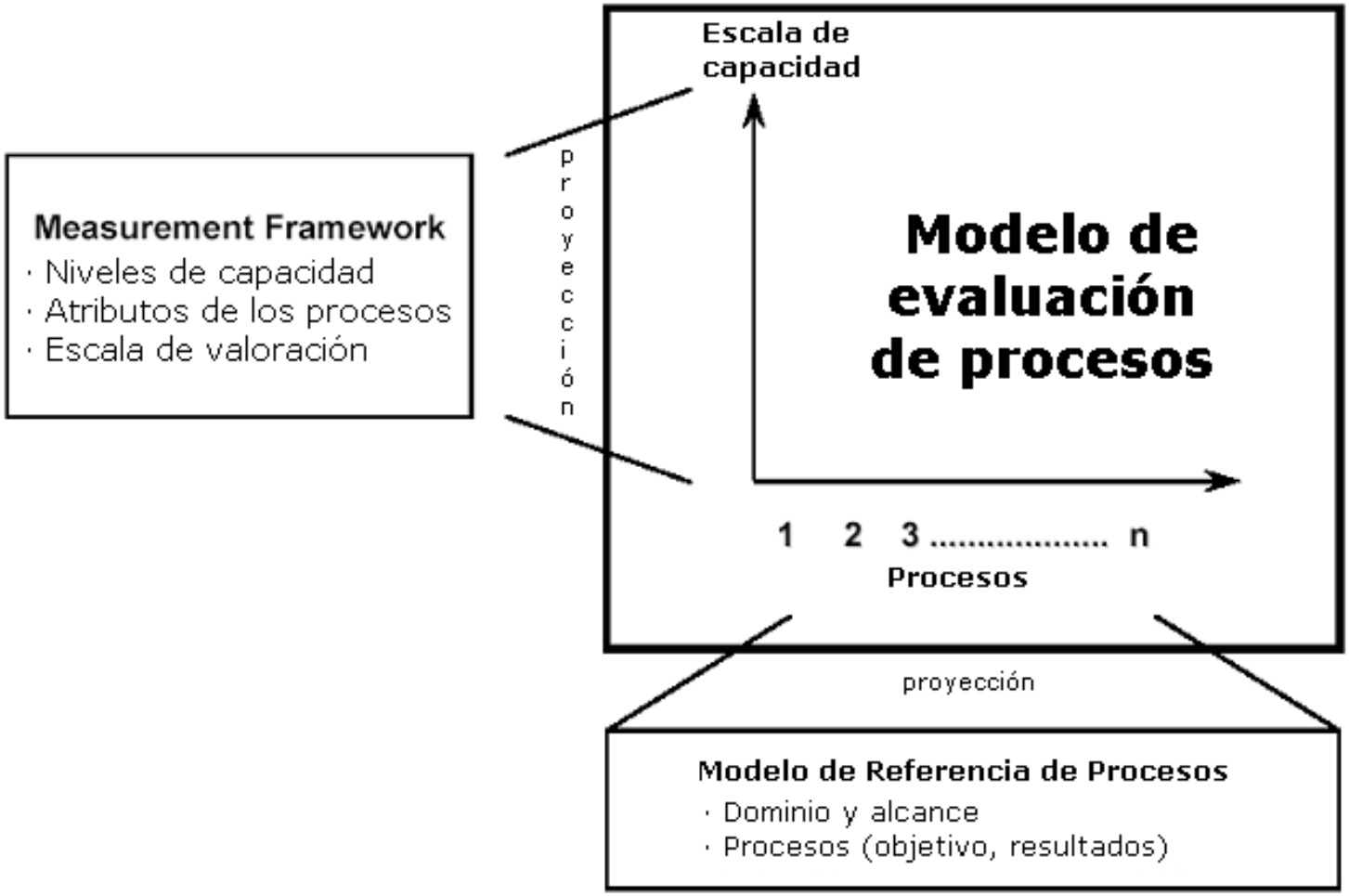
Argumento

- Plantear la certificación del proceso software en vez del producto SW.
  - Deben relacionarse los modelos de evaluación de procesos ya existentes (CMM, SPICE) con los requisitos de seguridad (“safety”) del sistema.
  - Definir los “perfiles de madurez” para cada nivel de criticidad (SILs)

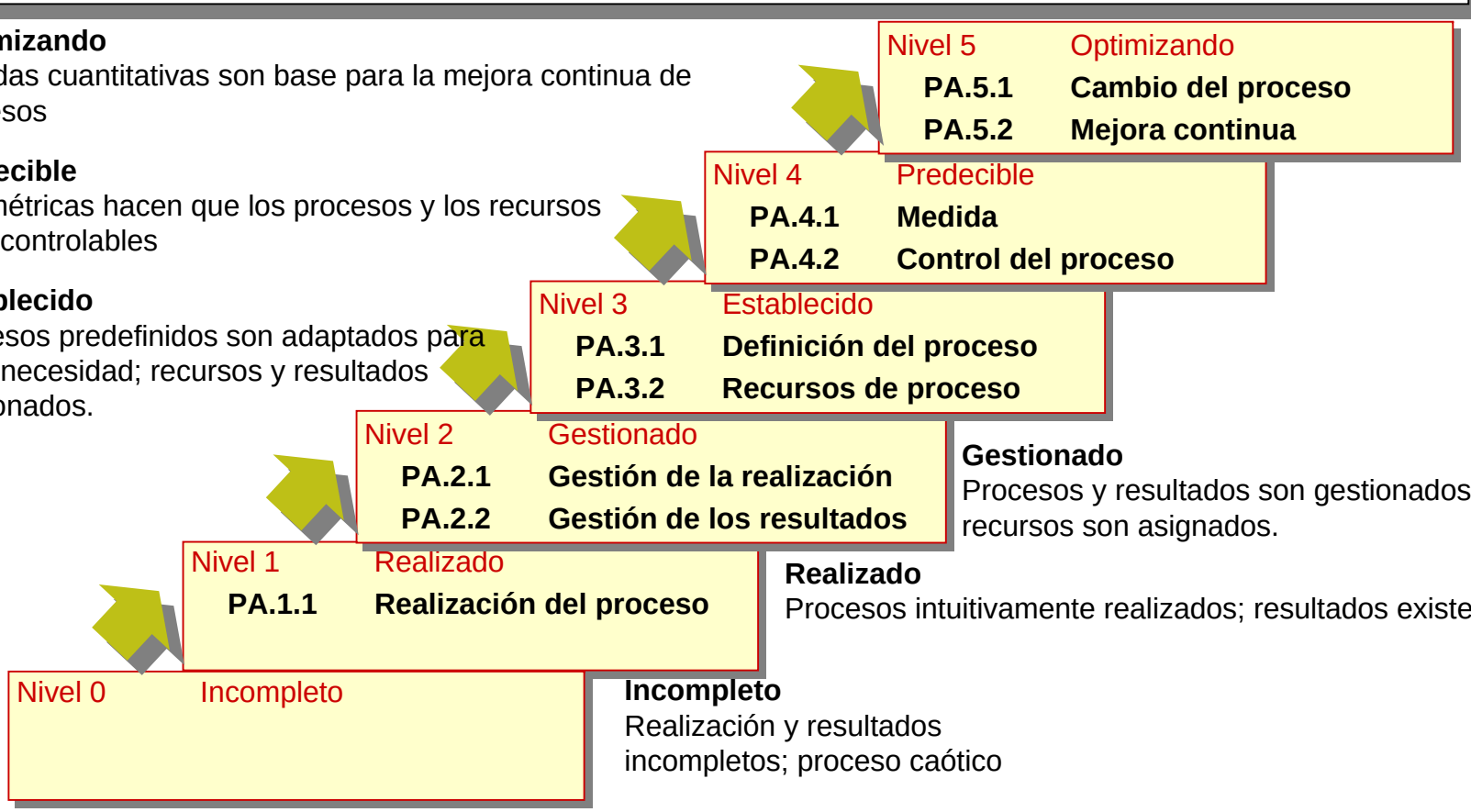
ISO/IEC 15504

- ISO/IEC 15504 o SPICE (Software Process Improvement and Capability dEtermination): Consenso internacional sobre la necesidad y los requisitos para un modelo y método de referencia de evaluación de procesos

Arquitectura SPICE



Arquitectura SPICE



Optimizando
Medidas cuantitativas son base para la mejora continua de procesos

Predecible
Las métricas hacen que los procesos y los recursos sean controlables

Establecido
Procesos predefinidos son adaptados para cada necesidad; recursos y resultados gestionados.

Gestionado
Procesos y resultados son gestionados y los recursos son asignados.

Realizado
Procesos intuitivamente realizados; resultados existentes

Incompleto
Realización y resultados incompletos; proceso caótico

Objetivos de las evaluaciones de procesos

- Determinación de la capacidad
- Mejora de procesos
- **Evaluar cumplimiento de determinados requisitos del ciclo de vida de desarrollo de software**

Niveles de criticidad

- Niveles de criticidad asignados según severidad y frecuencia de fallos de software (f_{SW}=100%)
- Cuanto más severos y frecuentes sean los fallos más alto es el riesgo y más alto el nivel de criticidad => más exigencias.
- Diferencias en la definición de los SILs para los dominios

Niveles de Criticidad y el estándar IEC61508

Método o técnica	Categoría	SIL 1	SIL 2	SIL 3	SIL 4
Uso de estándares de código	Estándares de código	HR	HR	HR	HR
Clases de equivalencia y pruebas de partición	Pruebas de caja negra	R	HR	HR	HR
Pruebas de estrés	Pruebas de funcionamiento	R	R	HR	HR
Análisis de flujo de control	Inspecciones	---	R	R	HR
Leyenda: 'HR' – altamente recomendado; 'R' – recomendado; '---' no es necesario					

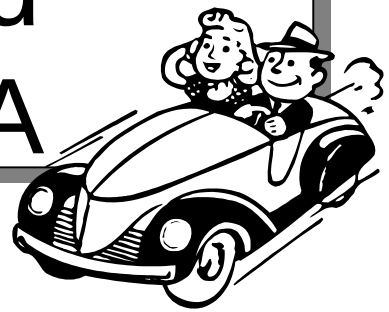
- Además de actividades:
  - Métodos, medidas y personal especializados, organización indep.

Niveles de Criticidad y el estándar DO178B

Actividad	Clases de software			
	A	B	C	D
El código fuente cumple los requisitos de bajo nivel.	●	●	○	
El código fuente implementa la arquitectura del software.	●	○	○	
El código fuente es verificable.	○	○		
El código fuente es acorde a los estándares.	○	○	○	
La cobertura de las pruebas de todas las estructuras internas del software es completa	●	●		

LEYENDA	
	● → La actividad debería realizarse por personas u organizaciones independientes. ○ → La actividad debería satisfacerse. (en blanco) → El cumplimiento de la actividad queda a elección del usuario.

Niveles de Criticidad y el estándar MISRA



Actividad	Clases de software			
	1	2	3	4
Lenguajes de codificación y compiladores	Utilización de un lenguaje estructurado	Utilización de un subconjunto restringido de lenguaje estructurado. Utilización de compiladores validados	Como para el nivel 2	Uso de compiladores certificados independientemente con reglas formales de sintaxis y semántica
Pruebas	Mostrar que se cumplen los requisitos. Plan de pruebas repetible.	Pruebas de caja negra	Pruebas de caja blanca a todos los módulos de código – midiendo la cobertura. Pruebas de estrés Análisis estático de sintaxis	100% pruebas de caja blanca a los módulos 100% pruebas de los requisitos 100 pruebas de integración

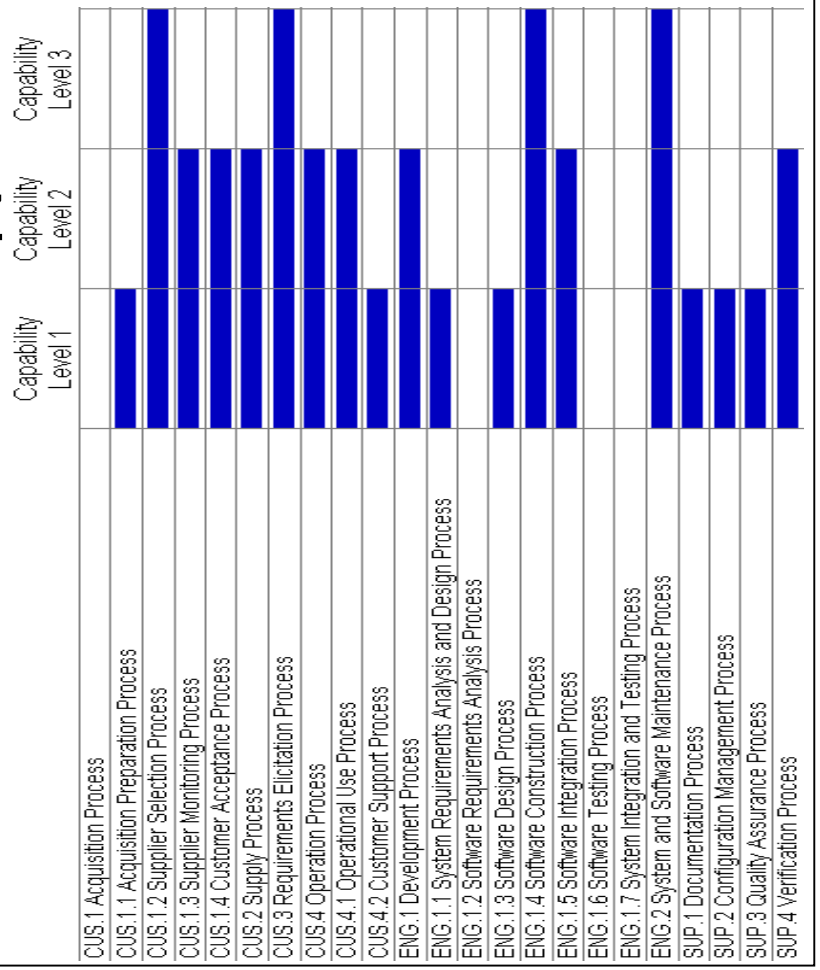
ISO9001 y los sistemas críticos

- ISO9001 no garantiza más allá del nivel más bajo de criticidad (SIL1)
- ISO 9001 se correspondería con el nivel 3 de madurez de procesos
- ISO 9001 no es específica para software e ISO90003 no es específica para software crítico

Perfiles de Madurez y Criticidad de Producto Software

- Para cada nivel,

un perfil de madurez



Cambios a los modelos de evaluación de procesos

- Actividades, documentación y salidas adicionales a los Procesos
- Más exigencias para el Personal
- Independencia de la organización
- Exigencias específicas respecto a los métodos, y herramientas y medidas específicas (ej cobertura).

Método general para definir perfiles de madurez

- Vincular los procesos con los niveles de criticidad mediante un análisis de la relación existente entre el riesgo de los procesos y el éxito de los proyectos [S4S]: método sin validar

Proceso		Criticidad			
		A	B	C	D
CUS.2.2	Entrega	4	3	3	1
CUS.3	Análisis de Requisitos	4	3	3	1
CUS.4	Operación	4	4	3	2
CUS.4.1	Uso operacional	4	4	3	2
CUS.4.2	Suporte al cliente	4	4	3	2

Perfiles de Madurez y Criticidad de Producto Software

- Para algunos (departamento de defensa de EE.UU.) el alcanzar un determinado nivel de madurez de proceso no garantiza un nivel adecuado de calidad en el desarrollo de sistemas críticos.
- Pero para otros es la única salida para agilizar la certificación

Conclusiones

- Estado actual:
  - ISO 9001 y modelos de evaluación de procesos, insuficientes
  - Necesidad de armonización y añadidos en diferentes dominios
- Solución
  - Un determinado nivel de madurez por nivel de criticidad

Conclusiones

- Problemas:
  - Resultarán exigencias de un nivel de madurez elevado, inasumible
  - Buen proceso no garantiza buen producto => Riesgo inevitable en no asegurar la calidad de cada producto