Introducción al proceso de desarrollo de sistemas safety critical

Bilbao, 2010-09-21

Índice

- Introducción
- Escenarios
- Proceso
- Experiencias
- Conclusiones

Introducción

- Servicios de ingeniería de sistemas
  - C. Tecnológica
  - Diseño, desarrollo y verificación
  - Gestión de fabricación
  - Soporte y mantenimiento
- Sectores
  - Automatización industrial
  - Ferrocarril
  - Electromedicina

Escenarios

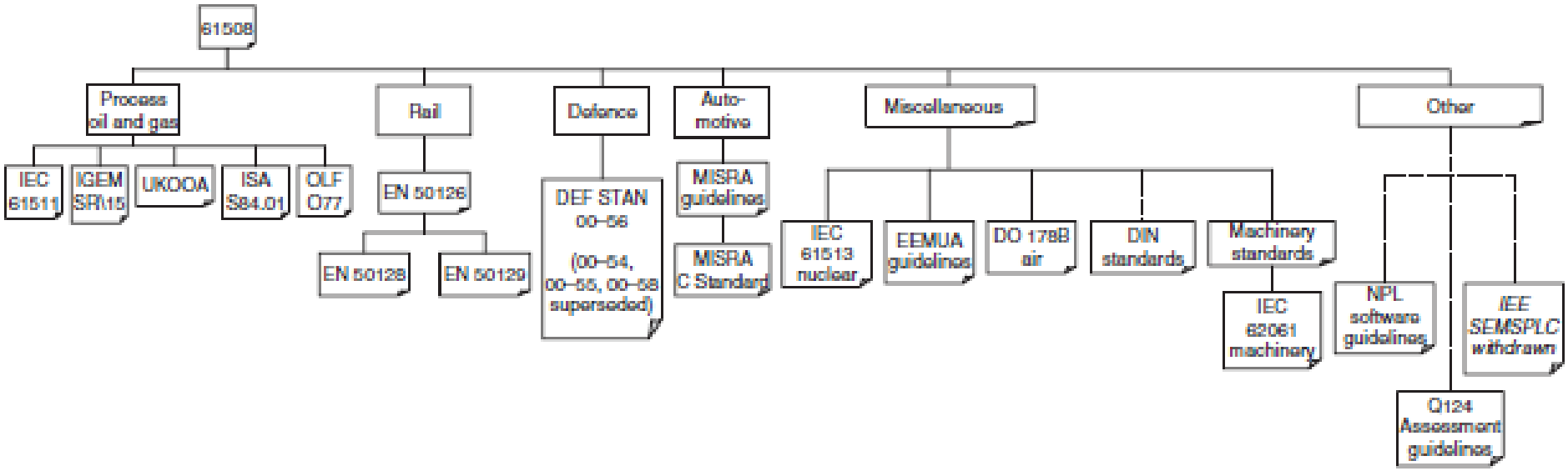
¿Hemos hecho todo lo humana y técnicamente posible para reducir al máximo la probabilidad de que nuestro sistema tenga un fallo de consecuencias peligrosas?

Escenarios

- Definir, diseñar, desarrollar, verificar y validar
- Instalar, operar, mantener y retirar

- Referencia o patrón
- Sistema de medición

Escenarios


61508
Process oil and gas
Rail
Defence
Auto-motive
Miscellaneous
Other
IEC 61511
IGEM SR\15
UKOOA
ISA S84.01
OLF 077
EN 50126
EN 50128
EN 50129
DEF STAN 00-56
(00-54, 00-55, 00-58 superseded)
MISRA guidelines
MISRA C Standard
IEC 61513 nuclear
EEMUA guidelines
DO 178B air
DIN standards
Machinery standards
IEC 62061 machinery
NPL software guidelines
IEE SEMSPLC withdrawn
Q124 Assessment guidelines

Proceso - Ingeniería de sistemas

- A systems engineering process is a process for applying *systems engineering* techniques to the development of all kinds of systems. Systems engineering processes are related to the stages in a *system life cycle*.
- Systems engineering is an *interdisciplinary* field of engineering that focuses on how **complex** engineering projects should be designed and managed

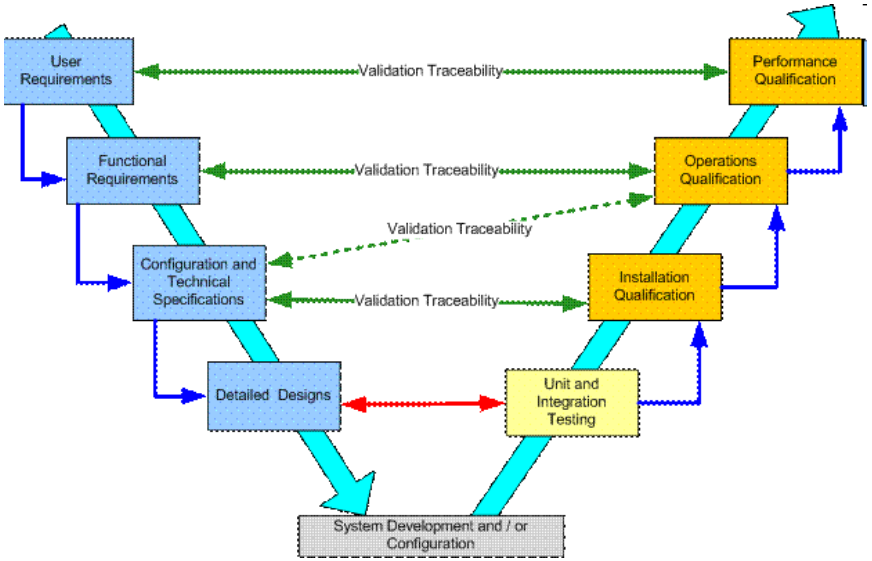
Proceso de ing. de sistemas - Disciplinas

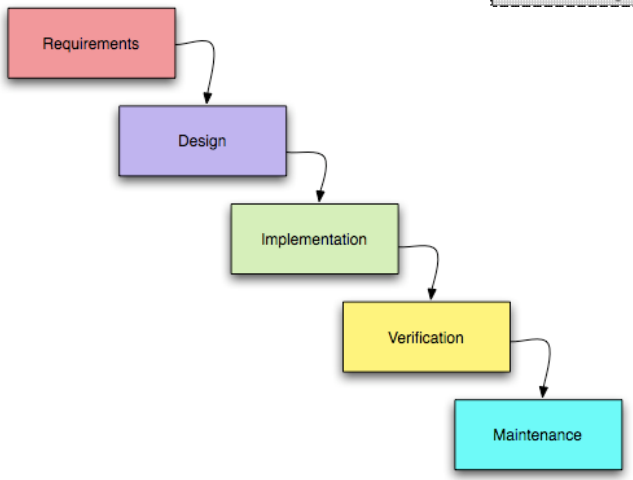
- Técnicas
  - Ingeniería de control
  - Ingeniería mecatrónica
  - Ingeniería industrial
- Relacionadas con las personas
  - Organización
  - Gestión de proyectos

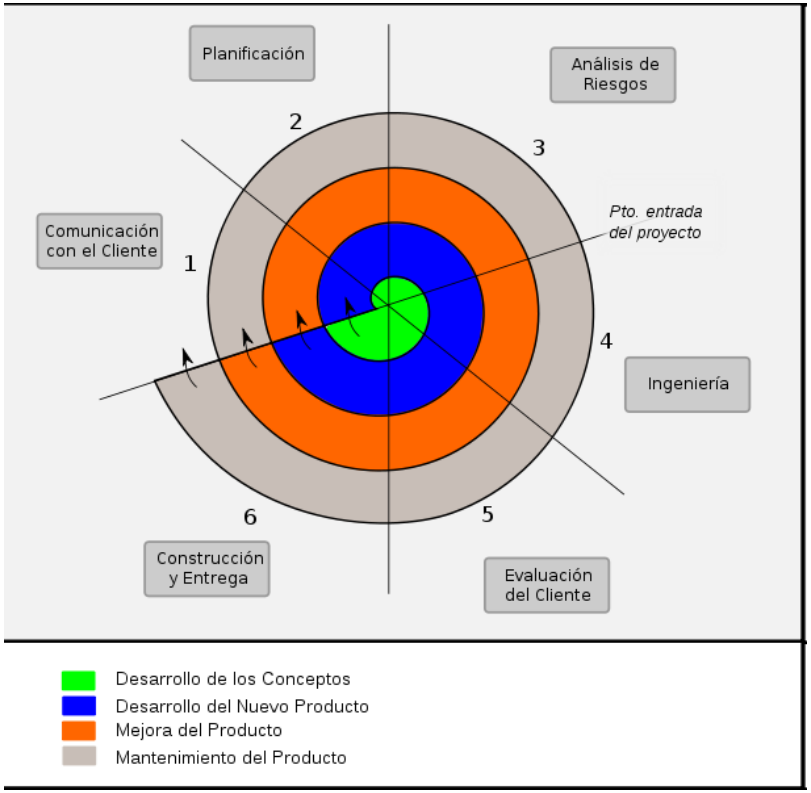
Proceso – Ciclo de vida del desarrollo

- Diferentes modelos: V, cascada, incremental, espiral…
- Diferentes situaciones regulatorias
  - Fijos
  - Sugeridos
  - Libres
- Integración de las actividades relacionadas con la seguridad en el ciclo de vida

Proceso – Ciclo de vida del desarrollo







Proceso – Inicio

- Requisitos y análisis
- Identificación de las funciones de seguridad o riesgos a mitigar
  - ¿Qué niveles debemos cumplir?
- Concepto de seguridad
  - ¿Cómo diseñamos nuestro sistema para alcanzar los requisitos de seguridad exigidos?

Proceso – Objetivos

- Maximizar la simplicidad
  - Facilitar el diseño y su verificación
  - Facilitar la comunicación
  - Facilitar el mantenimiento
- (De)Mostrar la trazabilidad
  - Desde el requisito hasta la validación, pasando por el código y el esquemático

Experiencias - Consideraciones

- Diferentes sectores y normativas
- A tener en cuenta
  - Duración y coste del proyecto
  - Compromiso de la empresa
    - En diferentes niveles y etapas
  - Objetivos a medio-largo plazo
    - ¿Completar el catálogo?
  - Importancia y prioridad del producto

Experiencias - Necesidades

- Formación
  - Proceso, herramientas y normativas
- *Safety (or RM) drives the project*
  - Es complicado *añadir* la seguridad a posteriori
- Equipo sólido y comprometido
  - Departamento de Calidad
  - ¿Responsable de seguridad?
- Colaboración con los NB

Experiencias – Realidades (Obstáculos)

- Multitarea y día a día
- Proyectos largos y costosos
  - Desarrollo y pruebas
  - Gestión del cambio
  - Certificación
- Complejidad inherente y artificial
  - Normativas e interpretación
  - Herramientas y proceso
  - Técnicas

Experiencias – Realidades (Obstáculos)

- Evolución de las normativas
  - Nuevas versiones
  - Indefiniciones
- Sistemas que combinan seguridad con otras funcionalidades
  - Separación en caso de fallo
  - Demostración
- Confundir seguridad con más documentación

Experiencias – Herramientas útiles

- Las que facilitan y gestionan la comunicación y la información
- Modelado del proceso y de los desarrollos
  - Diagramas estáticos (bloques) y dinámicos (Secuencia)
- Análisis de riesgos (tb para el proceso)
  - FMEA, Fault Trees, …
- Checklists
  - Revisiones de diseño, documentación

Conclusiones

- Sistemas complejos, desarrollos largos
- ¿Cómo podemos maximizar la reutilización de …
  - … los resultados técnicos?
  - … los procesos desarrollados?
  - … las lecciones aprendidas?
- ¿Cómo se pueden acelerar desarrollos posteriores?

Contacto

ULMA Embedded Solutions, S. Coop.

Garagaltza Auzoa, 51

20560 Oñati (Gipuzkoa)

Spain

Tel +34 943 25 03 00 / Fax +34 943 78 09 17

www.ulmaembedded.com

info@ulmaembedded.com