ALTER TECHNOLOGY TÜV NORD:

SEGURIDAD FUNCIONAL EN 61508

INDUSTRIA ESPAÑOLA

XV CONGRESO CONFIABILIDAD 2013

World´s leader in engineering, testing and procurement of high reliability electronic with more than 26 years of experience

Supporting Aeronautic industry in all segments

INDEX

INDEX

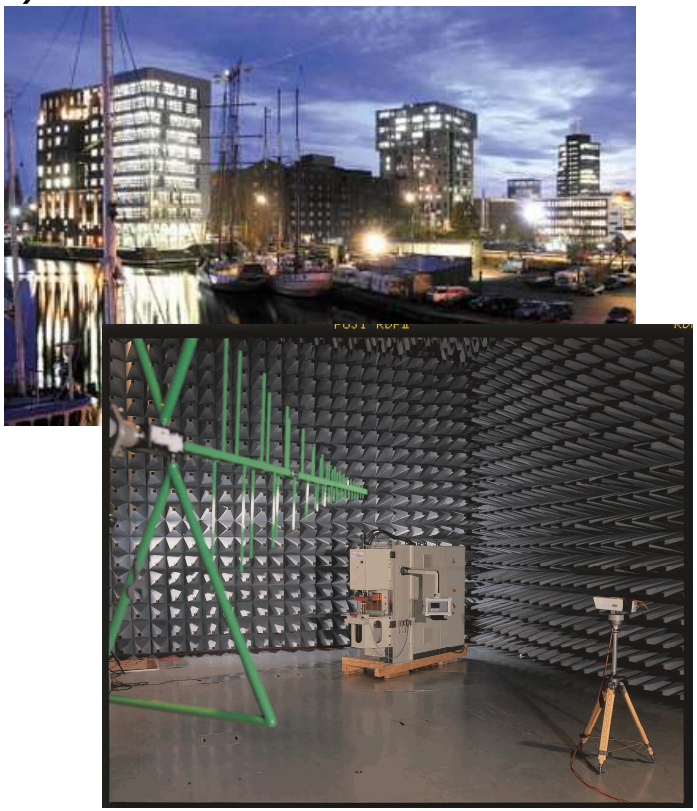
TÜV NORD - Overview
SEGURIDAD FUNCIONAL

- TÜV NORD key locations Germany:

  - HQ in Hannover (+ Lab activities)
  - Hamburg (+ Lab activities, i.e. EMC chambers)
  - Essen (+ Lab activities)
  - Bremen (service Office)

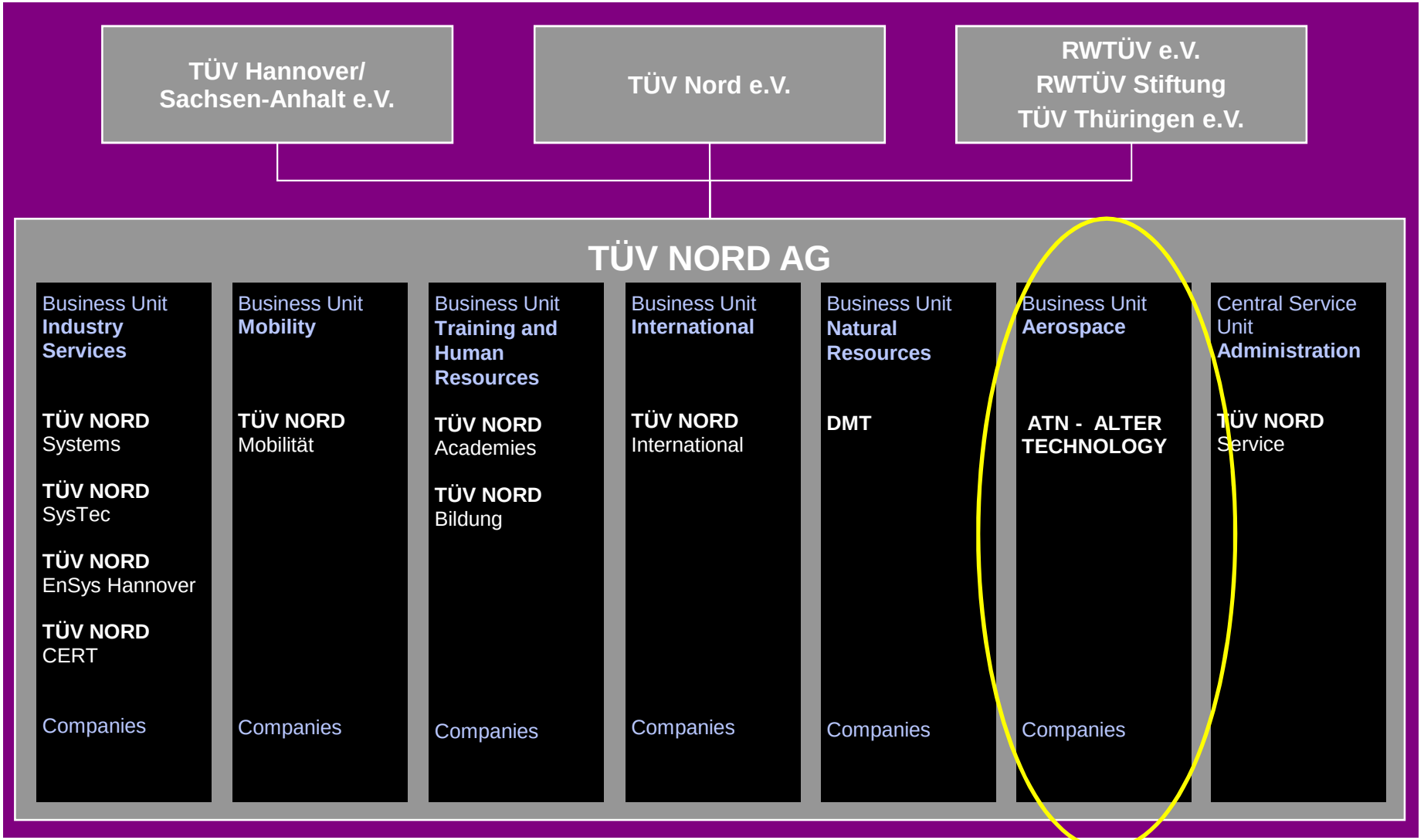
- ALTER TECHNOLOGY key locations

  - Madrid, Spain
  - Seville, Spain
  - Toulouse, France
  - Rome, Italy
  - Portsmouth, UK
  - service offices worldwide



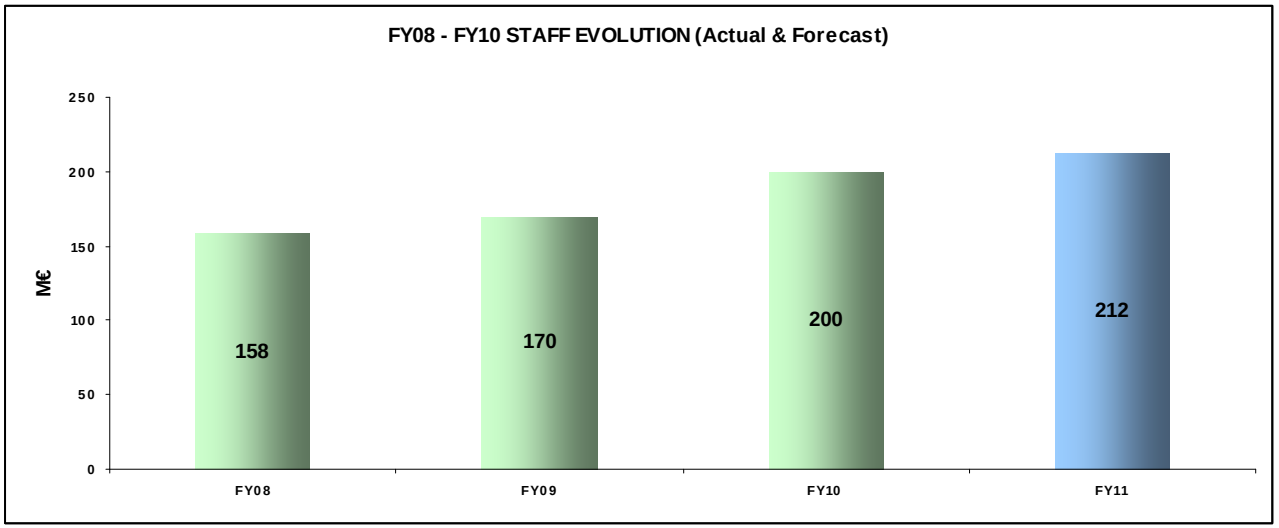
TÜV NORD - Overview
SEGURIDAD FUNCIONAL

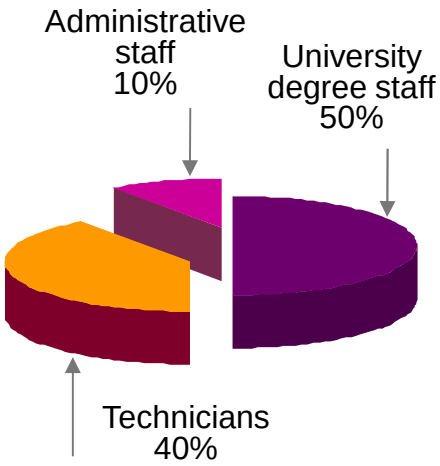
TÜV NORD - Overview
SEGURIDAD FUNCIONAL



About ALTER TECHNOLOGY TÜV NORD

Staff






Seville


Madrid


Toulouse

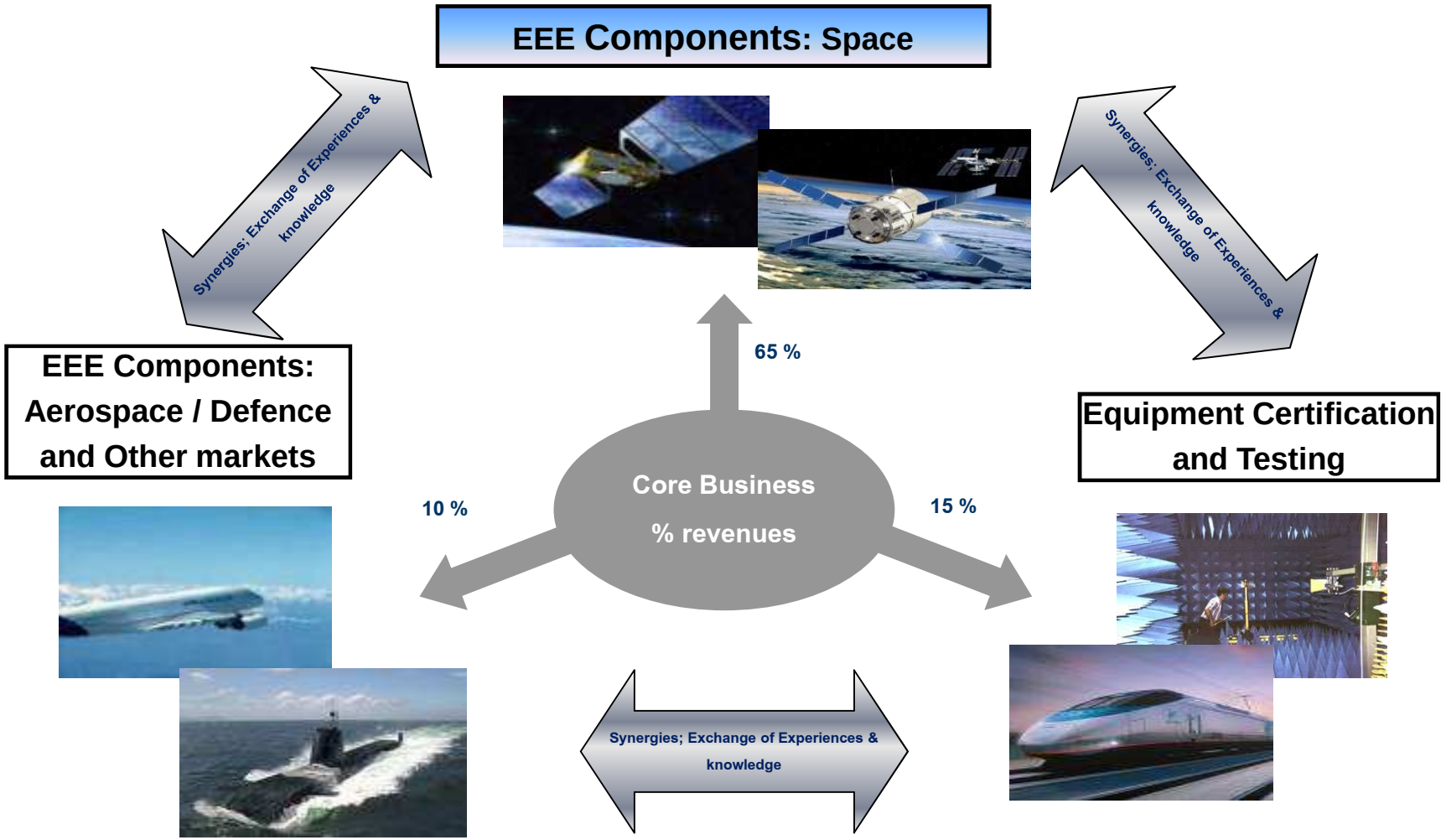

Rome


Portsmouth


Shanghai

About ALTER TECHNOLOGY TÜV NORD

Business Structure



Space sector - High Reliability EEE Components

Space sector : a zero failure culture

Space is a hostile environment for satellites

<u>Environmental extremes:</u>

- Temperature: Temperature extremes from -185 ◦C to +300 ◦C can be experienced by components open to the space environment.
- Radiation: Ionizing and non ionizing effects.
- Mechanical Stresses: Vibration, acceleration, thermal shock. During launch and normal working life
- Vacuum

Space sector - High Reliability EEE Components

Space Sector : **Projets**

AEOLUS AMAZONIA ARTEMIS ATV BEPI-COLOMBO CBERS COLUMBUS

COMS CURIOSITY ENVISAT GALILEO GLOBALSTAR GLONASS GOCE

GONETS GOSAT HELIOS1 & 2 H-IIA HERMES HERSCHEL-PLANCK





HISPASAT HTV HUYGENS-CASSINI INSAT INTEGRAL ISO JEM

KOMPSAT LEOSTAR LISA-PATHFINDER MARS EXPRESS METEOSAT

METOP MSG PLANET C PLSV PROTEUS RADARSAT ROSETTA SAC-D

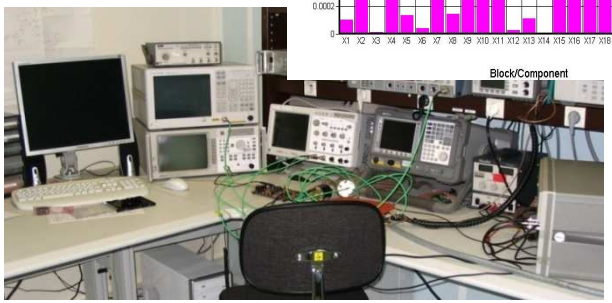
SAOCOM SILEX SMART-1 SMOS SOLAR-ORBITER SPACEBUS

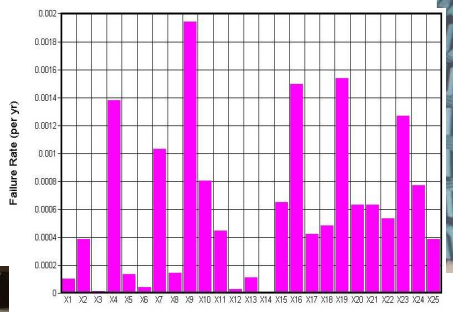
SPOT 4, 5 STAR-TRACKER SWARM TACIS VEGA VENUS-EXPRESS

Certification & Testing

Engineering & Testing: Electrical & Electronic Equipment & System

Electromagnetic compatibility (EMC) & safety	Environmental testing	Optoelectronics and radiofrequency	Reliability engineering & failure analysis RAMS	Telecom CPE - Operators -	Electronic security systems





Engineering & Testing: **Markets**

- Aerospace & Defence

- Security & Fire

Electromagnetic compatibility

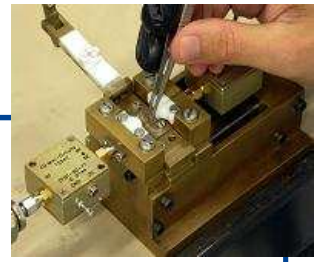
Environmental

Electronic Equipment

Electrical Safety

Functional

- Railway & Traffic



- Energy
- Telecom
- Medical

Certification of complex systems: some examples

Simulator INDRA EC175 (Eurocopter)

Primary surveillance radar INDRA ASR12+

SENER heliostat

Reliability – RAMS (Reliability, Availability, Maintainability and Safety)

Engineering

From Feasibility and Design phases to Manufacturing
RAMS Programs (tasks to meet the RAMS objectives of the product)

System Reliability

Reliability goal/requirement development and analysis. Breakdown to subsystems

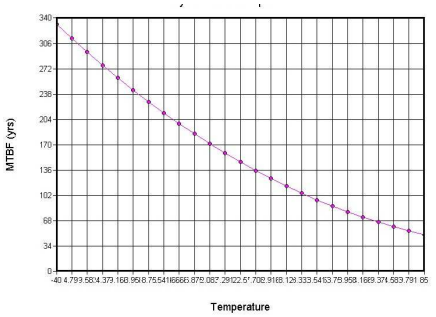
Reliability prediction

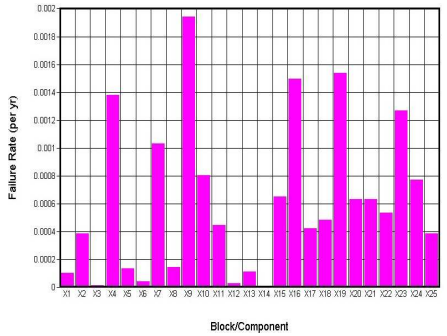
Failure Rate, MTBF, MTTR y MTTF
FTA (Fault Tree Analysis)

Failure modes, effects and critically analysis (FMEA)

Analysis of potential failure modes for determination of the effect of failures on the system.

Safety Analysis → Functional Safety





INDEX

SEGURIDAD FUNCIONAL

"La prevención de accidentes no debe considerarse una imposición legal, sino un deber humano y un imperativo económico". Werner von Siemens, 1880

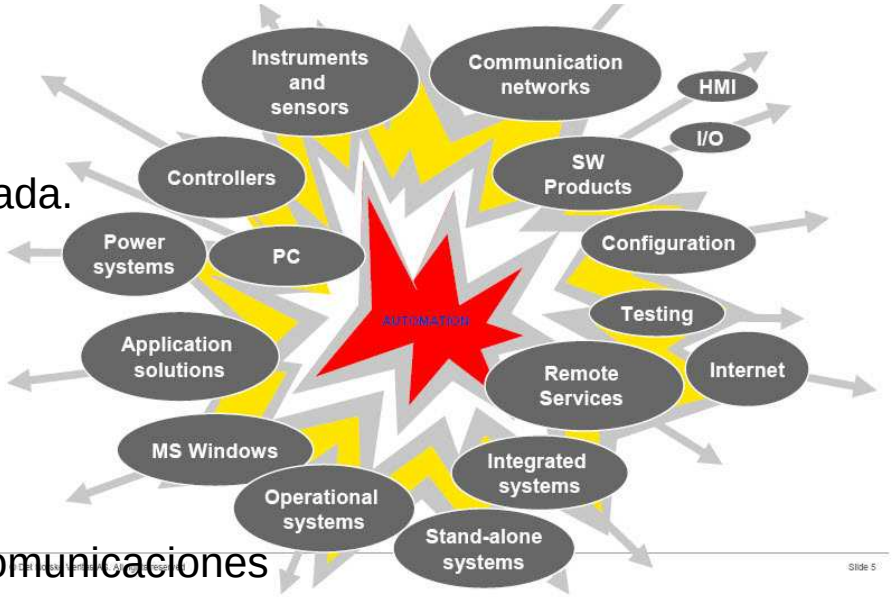
- Principales accidentes industriales

Accidente	Suceso	Consecuencias
Seveso (Italia), 1976	Reacción química fuera de control que provoca el venteo de un reactor, con liberación a la atmósfera de dioxina	•Sin muertes •Evacuación de más de 1.000 personas •Abortos espontáneos y contaminación del suelo •Autoridades ilocalizables (fin de semana) •Las primeras medidas se tomaron a los cuatro días
Camping Los Alfaques, Tarragona(España), 1978	Explosión de un camión sobrecargado de propileno al chocar contra un camping	•260 muertos •Destrucción completa del camping
Bhopal (India), 1984	**Escape de isocianato de metilo en una planta de fabricación de insecticidas**	***20.500 muertes directas y el mismo número de personas en condiciones críticas .** **•Unas 150.000 personas requirieron tratamiento médico** **•Efectos a largo plazo: cegueras, trastornos mentales, lesiones hepáticas y renales** **•La nube tóxica atravesó una de las vías de evacuación**

SEGURIDAD FUNCIONAL

- Evolución de la seguridad:
  - Evolución de las tecnologías.
  - Enlace entre la fiabilidad y la seguridad asociada.
  - Modelo tradicional

    Cajas negras no manipulables



  - Nuevo modelo:
  - Complejidad de los sistemas electrónicos y comunicaciones
  - Sistemas de control programables -> Fácilmente manipulables
  - Mayor exigencia en rentabilidad/producción
  - Aumento de las fuentes de error, peligros y riesgos asociados.
  - La complejidad de los sistemas electrónicos programables se hace complicado determinar el comportamiento de éstos frente a posibles fallos.
- El objetivo último es minimizar el riesgo de lesiones, pero también la perdida de materiales, energía, disponibilidad de máquinas, de procesos, cuidado del medioambiente, etc…

SEGURIDAD FUNCIONAL

Definición de seguridad funcional:

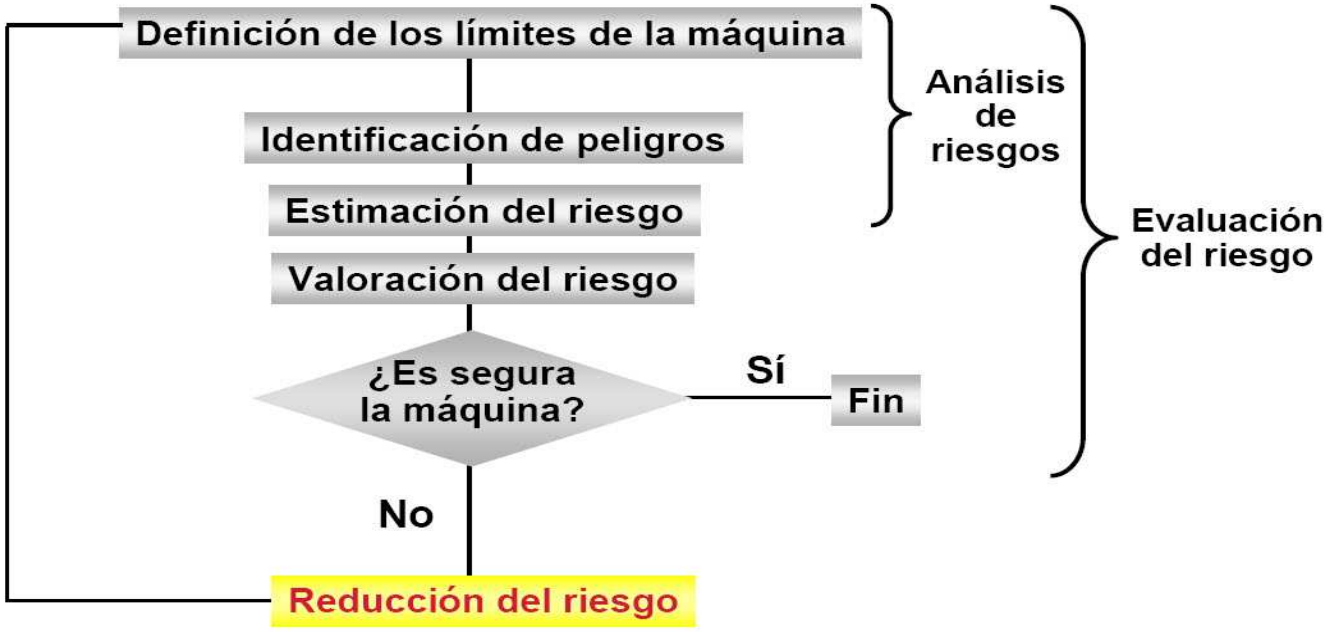
- La seguridad funcional es la parte de la seguridad global que depende del funcionamiento correcto del proceso o equipo en respuesta a sus entradas, cuando la seguridad depende del funcionamiento correcto de un sistema eléctrico (E), electrónico (E) y electrónico programable (PE) (abreviado: E/E/PE).

- Por tanto, el término **seguridad funcional** (Functional Safety) se refiere a la parte de la seguridad global de un sistema consistente en que sus componentes o subsistemas eléctricos, electrónicos, programables y sistemas de control/mando con implicaciones en materia de seguridad respondan de forma adecuada ante cualquier estímulo de fallo externo (peligros): errores humanos, HW/SW o cambios en su entorno de funcionamiento.

- Seguridad Funcional no es: Security, Seguridad eléctrica, Incendios o Radiológica, etc…

METODOLOGIA COMÚN ANÁLISIS SEGURIDAD

- Al igual que en resto de normativas/metodologías sobre seguridad, la evaluación de riesgos (evaluación del riesgo estadístico) desempeña el papel clave en el desarrollo de los requisitos de la seguridad funcional.
- Peligro vs. Riesgo: El peligro está siempre presente mientras que el riesgo es la posibilidad de que el peligro ocurra, y su evaluación implica identificar la severidad de su aparición en el sistema.
- La estimación del riesgo es un proceso iterativo. Esto significa que puede ser necesario ejecutar el proceso más de una vez. La estimación del riesgo y la especificación del SIL se realiza básicamente para cualquier peligro cuyo riesgo deba reducirse mediante dispositivos técnicos de control.

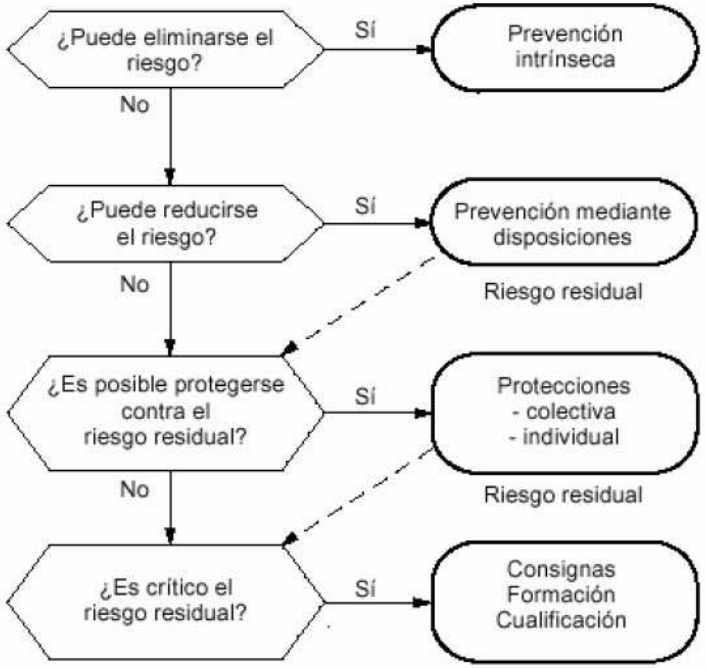


METODOLOGIA COMÚN ANÁLISIS SEGURIDAD

La estimación del riesgo se realiza teniendo presente,

- la gravedad de las lesiones (S),
- la frecuencia y la duración de la exposición al peligro (F),
- la probabilidad de que se produzca un suceso peligroso (W) y
- la posibilidad de evitar o de limitar el daño (P).

El riesgo se puede reducir por cambios de diseño, incorporar sistemas complementarios control / redundancias, protecciones o mediante cualificación y formación adecuada al personal.



ENFOQUE SEGURIDAD FUNCIONAL EN 61508
SIS y CAPAS DE PROTECCION

- En el caso de instalaciones, se suele utilizar el término de Capas de protección. Los riesgos potenciales exigen que se adopten criterios estrictos tanto en el diseño como en las adopciones de medidas de seguridad. Cada capa esta compuesta de equipos y/o procedimientos de control que actúan conjuntamente con las otras capas de protección para controlar y/o mitigar los riesgos de los procesos.
- Las capas de prevención son las que tienen como propósito detectar y evitar el suceso, deben actuar antes de la perdida de materia, energía o lesiones. Estas capas reducen el riesgo reduciendo la frecuencia del suceso: Sistema básico de control, alarmas críticas e intervención humana, los SIS, y dispositivos físicos como válvulas de seguridad, discos de ruptura o válvulas rompedoras de vacio.
- Las capas de mitigación: Son las que minimizan las consecuencias del suceso: fire&gas, emergency shut down, válvulas de aislamiento, aislamiento de deflagraciones, etc…
- Por último encontramos las capas de respuesta de la instalación ante emergencias y repuesta de la comunidad ante la emergencia.

LEGISLACION Y NORMATIVAS SEGURIDAD FUNCIONAL

CAOS EN PATRONES DE SEGURIDAD FUNCIONAL:

Problema histórico de la industria al tener cumplir con infinidad de normas de seguridad, muchas solapadas, y filosofías de diseño y arquitecturas diferentes, ejemplos son:

- **Practicas o especificaciones de la empresa**
- **Códigos de práctica locales :**

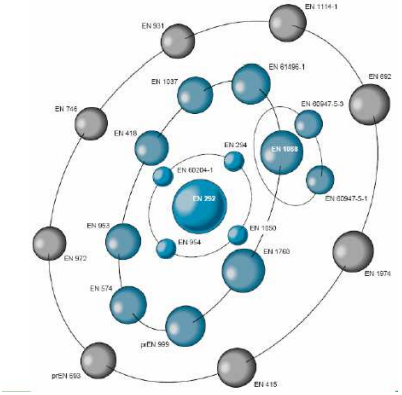
–AICHE: “Guías de Automatización Segura en Procesos Químicos”

–NFPA: estándares que aplican a calderas, hornos y sistemas de control de quemadores

–API RP 14C (USA 1974) “Sistemas de Parada en Plataformas Petrolíferas”

–DIN VDE 19250 / 19251 (Alemania 1989), DIN VDE 0801 (Alemania 1991)

–ISA SP84 (USA 1995) o ANSI/ISA 84.01 (USA 1996).



- **Legislación o Recomendaciones por Autoridades reguladoras**

-HSE PES (Reino Unido 1987)

–OSHA 29CFR 1910 (USA 1999) “Gestión de la Seguridad en el Proceso de Plantas Químicas altamente peligrosas”

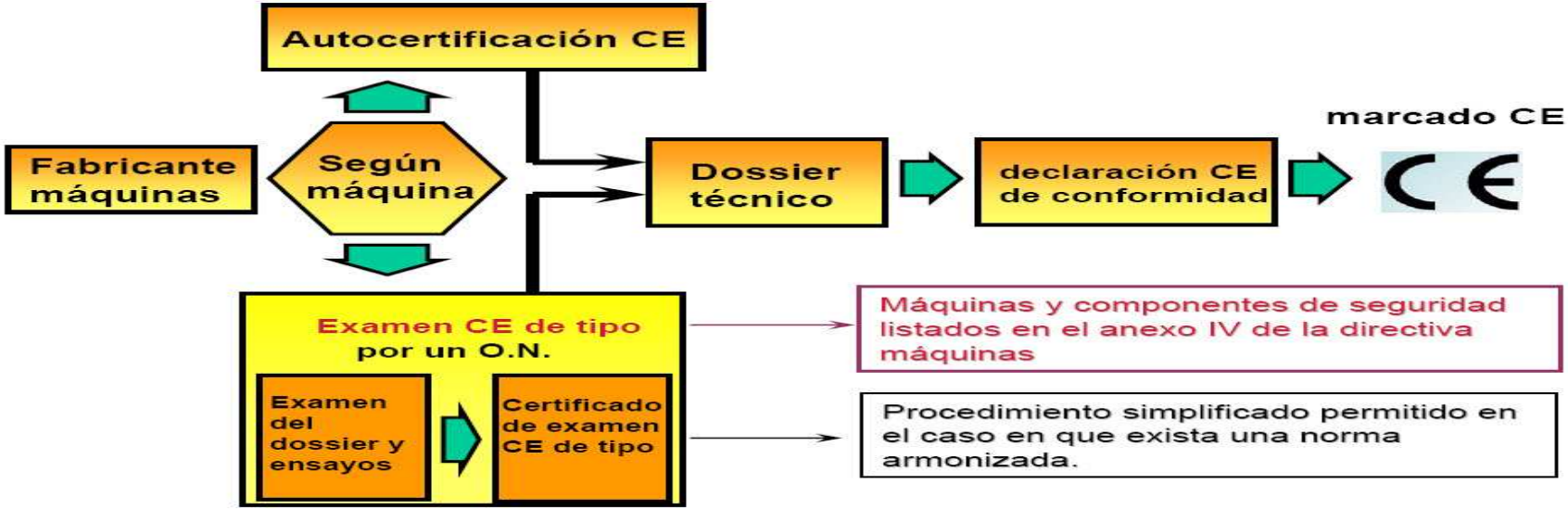
–Directiva Seveso II 96/82 (CEE 1996) y su traslado al RD 1254/1999 (16 Julio 99) de “Prevención de accidentes graves en los que intervienen sustancias peligrosas

NUEVOS MARCOS GLOBALES REGULADORES (ie: MARCADO CE):

*Directivas

*Normas

LEGISLACION Y NORMATIVAS SEGURIDAD FUNCIONAL



- **Directiva Máquinas:2006/42/CE**
- **Directiva Sistemas Ferroviarios 2008/57/EC**
- **Directiva Vehículos a Motor 2007/46/EC**
- **Directiva Vehículos Agricultura 2003/37/EC**
- **Directiva Pesticidas 2009/128/EC**
- **Directiva Equipos de presión 97/23/EC**

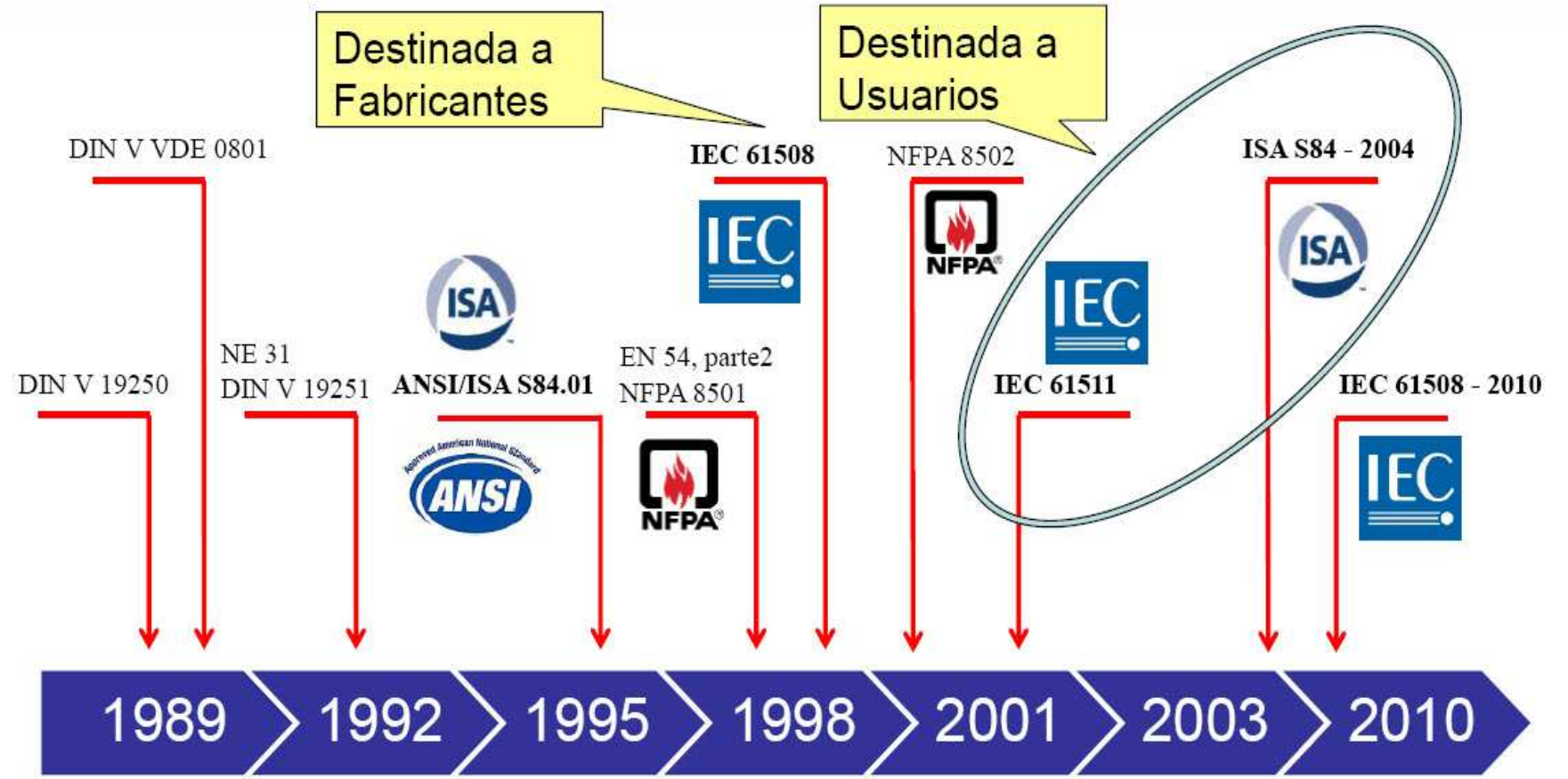
- Trabajo de análisis para asignar directiva de aplicación y normativas cuyo uso cumple con los requisitos de la directiva - > Normas armonizadas.

LEGISLACION Y NORMATIVAS SEGURIDAD FUNCIONAL

- Norma Armonizada: Documento o especificación técnica relacionado con una Directiva, adoptada por un Organismo Oficial de Normalización. Mantiene su carácter de voluntariedad, aunque el cumplimiento de la misma proporciona la presunción de conformidad respecto a los requisitos esenciales de la directiva aplicable relacionada. Por tanto, constituyen el mejor medio de prueba del cumplimiento de estos requisitos.

LEGISLACION Y NORMATIVAS SEGURIDAD FUNCIONAL

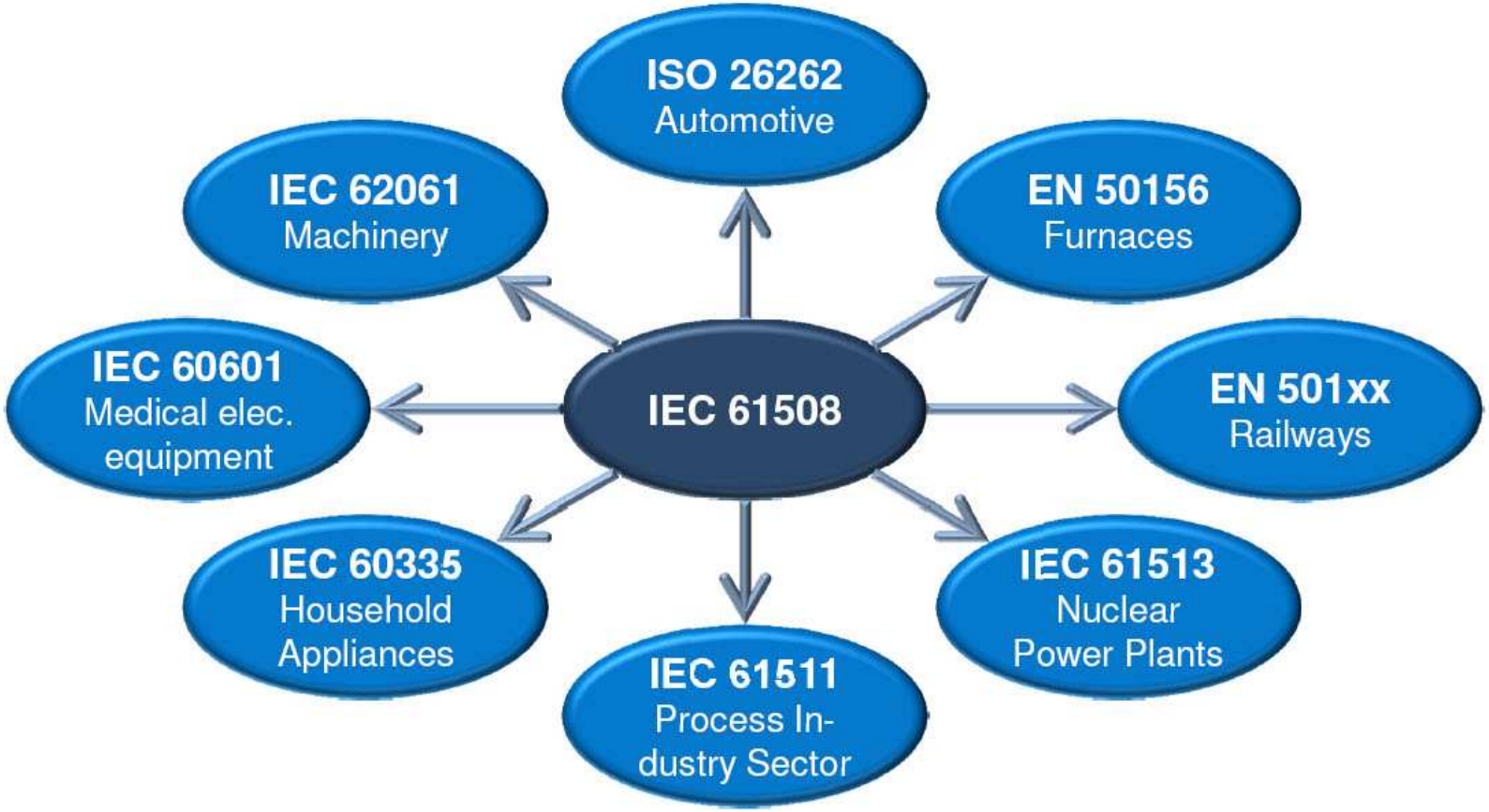
Convergencia de la seguridad funcional: EN 61508



LISTADO DE NORMAS SEGURIDAD

Norma	Descripcion
EN 13849-1	Seguridad de la maquinaria; partes de los sistemas de control relacionadas con la seguridad Esta norma tiene el propósito de proporcionar una ruta de transición directa de las categorías de las normas previas EN 954-1. Es Norma Armonizada ISO 12100: Nueva, sustituyendo a 14121, 12100-1 y 12100-2
EN 62061	Seguridad de la maquinaria; seguridad funcional de sistemas de control eléctricos, electrónicos y programables relacionados con la seguridad Esta norma es la implementación específica para maquinarias de IEC/EN 61508. Proporciona requisitos aplicables al diseño de nivel del sistema de todos los tipos de sistemas de control eléctricos relacionados con la seguridad de la maquinaria y también para el diseño de subsistemas o dispositivos no complejos. Requiere que los subsistemas programables o complejos cumplan con la norma IEC/EN 61508 Es Norma Armonizada
EN 61800-5-2	Adjustable speed electrical power drive systems - Part 5-2: Safety requirements – Functional. Es una norma armonizada en la directiva de maquinas 2006/42/EC
EN 61511	Seguridad funcional - Sistemas instrumentados de seguridad (SIS) para el sector de las industrias de procesos Esta norma es la implementación específica de la norma IEC/EN 61508 del sector de procesos.
EN 61513	Nuclear Power Plants: Provides requirements and recommendations for the instrumentation and control for systems important to safety of nuclear power plants
EN 50128	Rail : EN 501xx provides a specific interpretation for railway applications
EN 17894	For programmable electronic systems in Marine applications (derived from 61508). A new standard for the Maritime Industry
EN 26262	A diferencia de la norma IEC 61508, este estándar fue elaborado en cooperación con la industria del automóvil y teniendo en consideración sus necesidades específicas. La electrónica de los vehículos necesita ser certificada según el estándar ISO 26262,

LISTADO DE NORMAS SEGURIDAD



INDEX

EN 61508:2011
ESTRUCTURA

- **EN/IEC 61508: Seguridad funcional de los sistemas eléctricos /electrónicos /electrónicos programables relacionados con la seguridad**

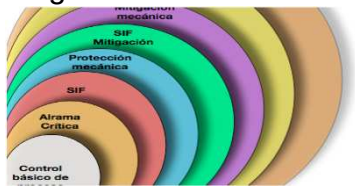
- Parte 1: Introduce el concepto de seguridad funcional y proporciona una vista general de las normas de la serie IEC 61508.
- Parte 2: Requisitos para los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad
- Parte 3: Requisitos de software
- Parte 4: Conceptos y abreviaturas
- Parte 5: Ejemplos para determinar el nivel de integridad de seguridad (1)
- Parte 6: Directrices para la aplicación de las partes 2 y 3
- Parte 7: Instrucciones de aplicación para procedimientos y medidas

EN 61508:2011
AMBITO Y CLAVES

First edition: 1998
Second and latest edition: 2011

- El estándar mundial se encuentra en el IEC 61508, en el que se define el tipo de evaluación del riesgo así como las normas y procedimientos para diseñar sensores, actuadores y sistemas de control y procesamiento lógico. El objetivo es evitar y controlar errores en cada componente de un **Sistema Instrumentado de Seguridad (SIS).**
- No es norma armonizada en ninguna directiva, pero es la base de Best Practices y se pueden justificar requisitos de directivas en función de ella.
- La norma IEC 61508 ofrece la ventaja de un procedimiento uniforme y *harmonizado* descrito y definido a nivel internacional, que contribuye de esta forma a una seguridad legal.

- La calificación de un componente conforme a IEC 61508 y/o IEC 61511 queda registrada con una declaración de conformidad (DoC).
- Pero el enfoque de EN61508, y derivadas, viene marcado por tres conceptos para lograr la seguridad funcional:
  - **Función instrumentada de seguridad (SIF)**
  - **El nivel de integridad de la seguridad (SIL)**
  - **Gestión del Ciclo de vida (Auditoría externa)**

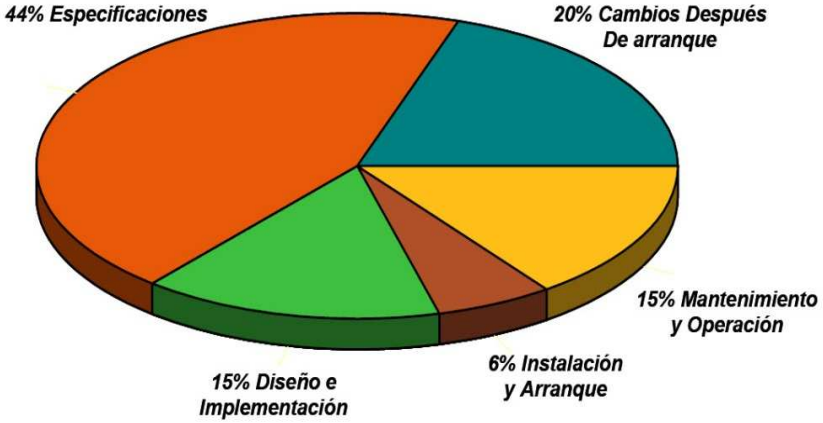


- Además, se realiza un "manual de seguridad" que resume todas las características e información de seguridad que los usuarios y planificadores necesitan para desarrollar y manejar un sistema instrumentado de seguridad. Los manuales de seguridad forman parte de la documentación de cada equipo calificado como SIL.
- La tarea de identificar y análizar los riesgos indican los requisitos de las SIF. La cuantificación de riesgos proporciona los requisitos de integridad de la seguridad (SIL). El nivel de "seguridad funcional" de un sistema instrumentado de seguridad se divide en etapas desde SIL1 a SIL4 (SIL = Safety Integrity Level). La mayoría de aplicaciones con requisitos relacionados con la seguridad tienen una clasificación SIL 1 y SIL 2, y SIL 3 en algunos casos.

EN 61508:2011
AMBITO Y CLAVES

El estándar IEC 61508 es una normativa “paraguas” , basa su estrategia en el seguimiento del ciclo de vida de la seguridad y proporciona:

- Las bases para el uso de dispositivos eléctricos / electrónicos / electrónicos programables en aplicaciones de seguridad.
- Las consideraciones que deberán tener en cuenta todos los implicados en la aplicación desde el concepto hasta la especificación, el diseño, la instalación, la operación, el mantenimiento y la desinstalación final.
- Nunca se puede alcanzar el 0 en riesgos.
- La seguridad funcional debe ser introducida desde el comienzo del diseño.
- Los riesgos no tolerables deben ser reducidos (técnica de ALARP)



Aplica a todos los sistemas E/E/EP relacionados con la seguridad, independientemente del tipo de industria, destacando:

- Industria de procesos,
- Industria manufaturación,
- Medicina: radiología, etc.
- Transporte: Señalización ferroviaria, sistemas de frenado, elevadores, etc.

EN 61508:2011
SIS – SIF – SIL

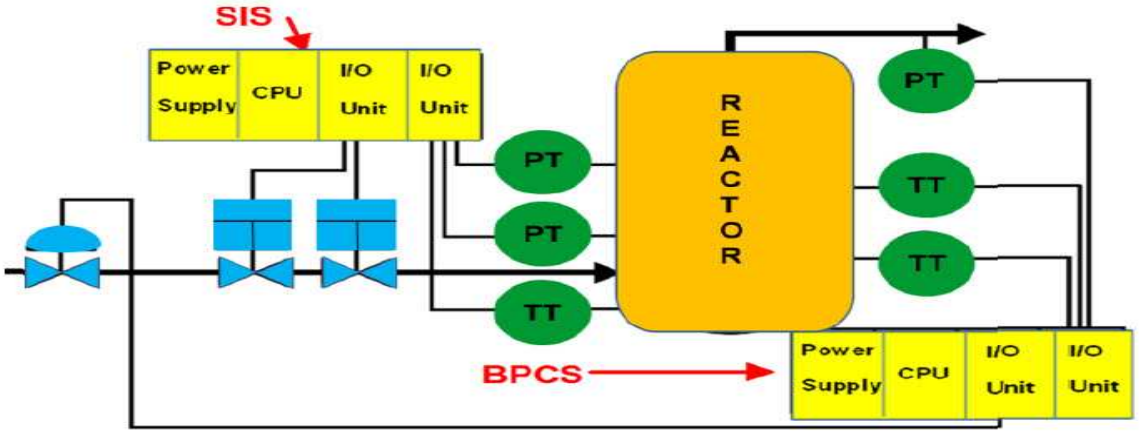
Sistema Instrumentado de Seguridad (SIS): Un Sistema compuesto por sensores, lógica y elementos finales de control o actuación (SIF), con el propósito de llevar el proceso a un estado seguro cuando determinadas condiciones preestablecidas son violadas. El SIS debe disponer de unas condiciones de seguridad y fiabilidad que garanticen su correcto funcionamiento cuando se les demanda. El SIL global del SIS determina cual es el nivel de seguridad del SIS.

Un SIS tiene el objetivo de:

1. Llevar de forma automática un proceso industrial a un estado seguro (cuando se alcanza la seguridad=riesgo tolerable) cuando se incumplen condiciones previamente establecidas.

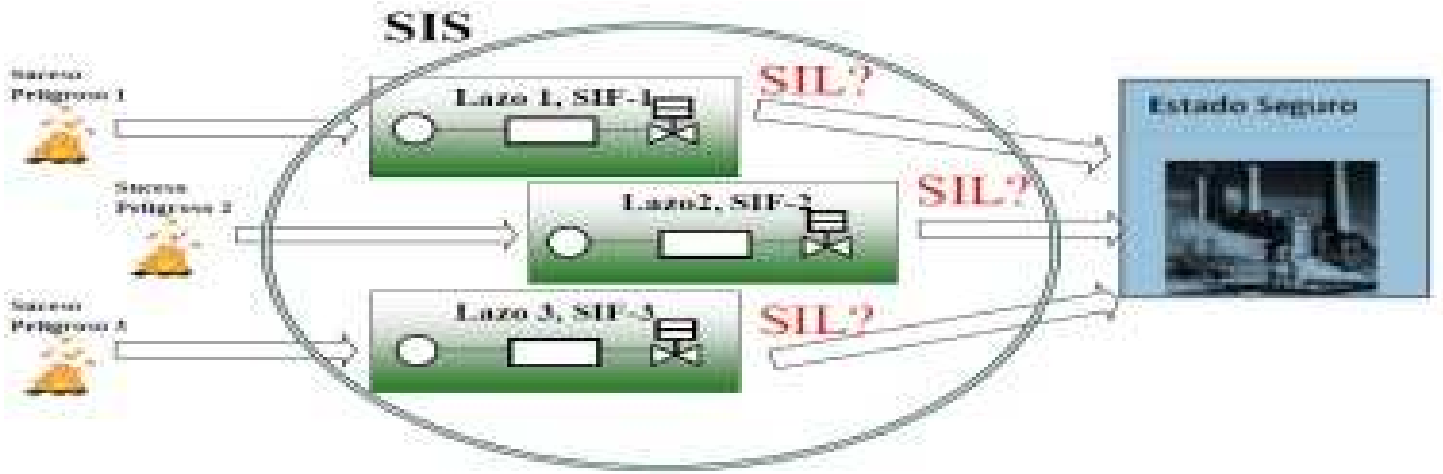
2. Permitir que un proceso siga adelante de forma segura cuando se cumplen los requisitos especificados (Funciones permisivas)

3.Actuar mitigando las consecuencias de un peligro industrial.



EN 61508:2011
SIS – SIF – SIL

- **SIF**: Es la Función de seguridad instrumentada, a ser implementada por el SIS, con un nivel de integridad de la seguridad especificado que es necesaria para alcanzar una condición de seguridad funcional y que puede ser una función instrumentada de protección de seguridad o una función instrumentada de control de seguridad". Es la encargada de describir cómo un determinado lazo, compuesto de sensores, logic solver y elementos finales, ejecutará la acción para llevar al sistema a su posición de seguridad.



- Integridad de la Seguridad - **SIL:** Indica la disponibilidad de un Sistema de Seguridad, es decir "La probabilidad de que un sistema relacionado con la seguridad ejecute de forma satisfactoria las funciones de seguridad requeridas en todas las condiciones especificadas en un periodo de tiempo especificado". Especificar la Integridad de la Seguridad no consiste en definir solo que es lo que debe hacer el sistema de seguridad, sino también en especificar la bondad con la cual dicho sistema debe llevar acabo su función. Existen 4 Niveles de Seguridad (SIL-Safety Integrity Level) y para calcularlos numéricamente se asocia un parámetro: la PFDavg, que indica la probabilidad media de fallo al ejecutar, bajo demanda, la función para la cual ha sido diseñado

EN 61508:2011
SIS – SIF – SIL

- Un SIS Puede abarcar múltiples funciones de seguridad(SIF) cada una de ellas con un SIL diferente, y actuar de múltiples formas para prevenir múltiples resultados peligrosos.

Relación de índices SIL con probabilidad de fallo en demanda			
SIL	Consecuencias	Disponibilidad requerida (%)	PFD media[2]
4'	Daños catastróficos en el exterior	> 99,99	10^{-5} -10^{-4}
3	Daños humanos en el interior y daños materiales en el exterior	99,90-99,99	10^{-4}-10^{-3}
2	Daños materiales y posibles daños humanos en el interior	99,00-99,90	10^{-3}-10^{-2}
1	Pequeños daños materiales en el interior	90,00 - 99,00	10^{-2} -10^{-1}

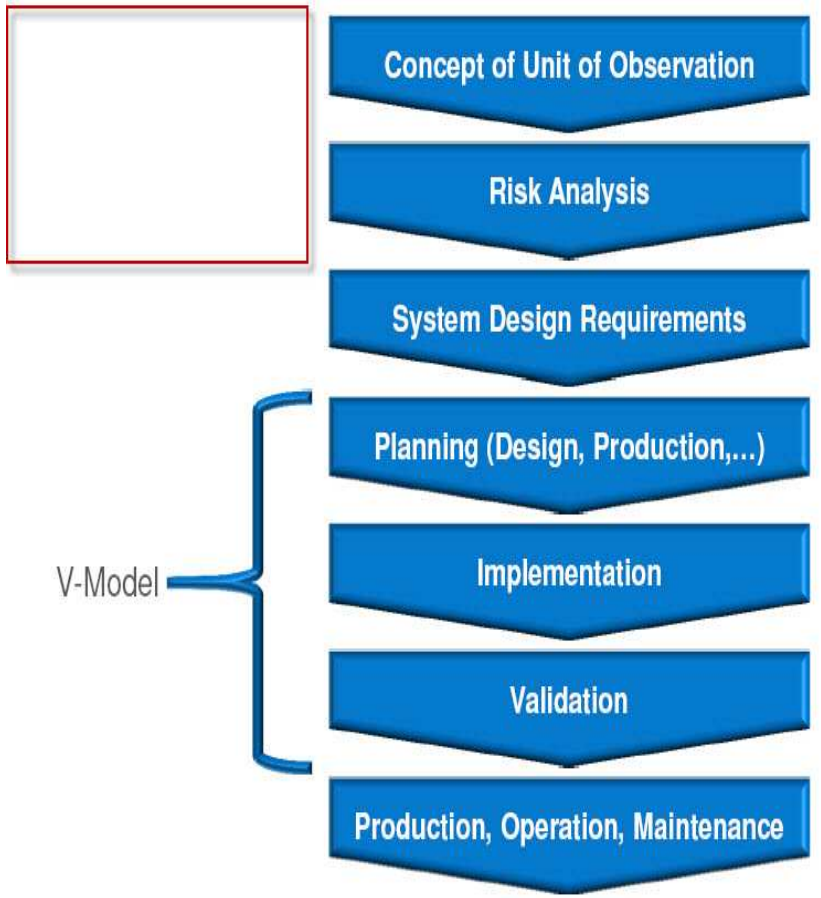
SIL	PFD	Fallo máximo aceptado del SIS
SIL 4	>=10^{-5} to <10^{-4}	Un fallo peligroso en 10000 años
SIL 3	>=10^{-4} to <10^{-3}	Un fallo peligroso en 1000 años
SIL 2	>=10^{-3} to <10^{-2}	Un fallo peligroso en 100 años
SIL 1	>=10^{-2} to <10^{-1}	Un fallo peligroso en 10 años

- Modos de operación:
- Modo en demanda (baja demanda) , basado en PFD Avg
- Modo en continuo (alta demanda), basado en PFH (clásico tasa de fallos)

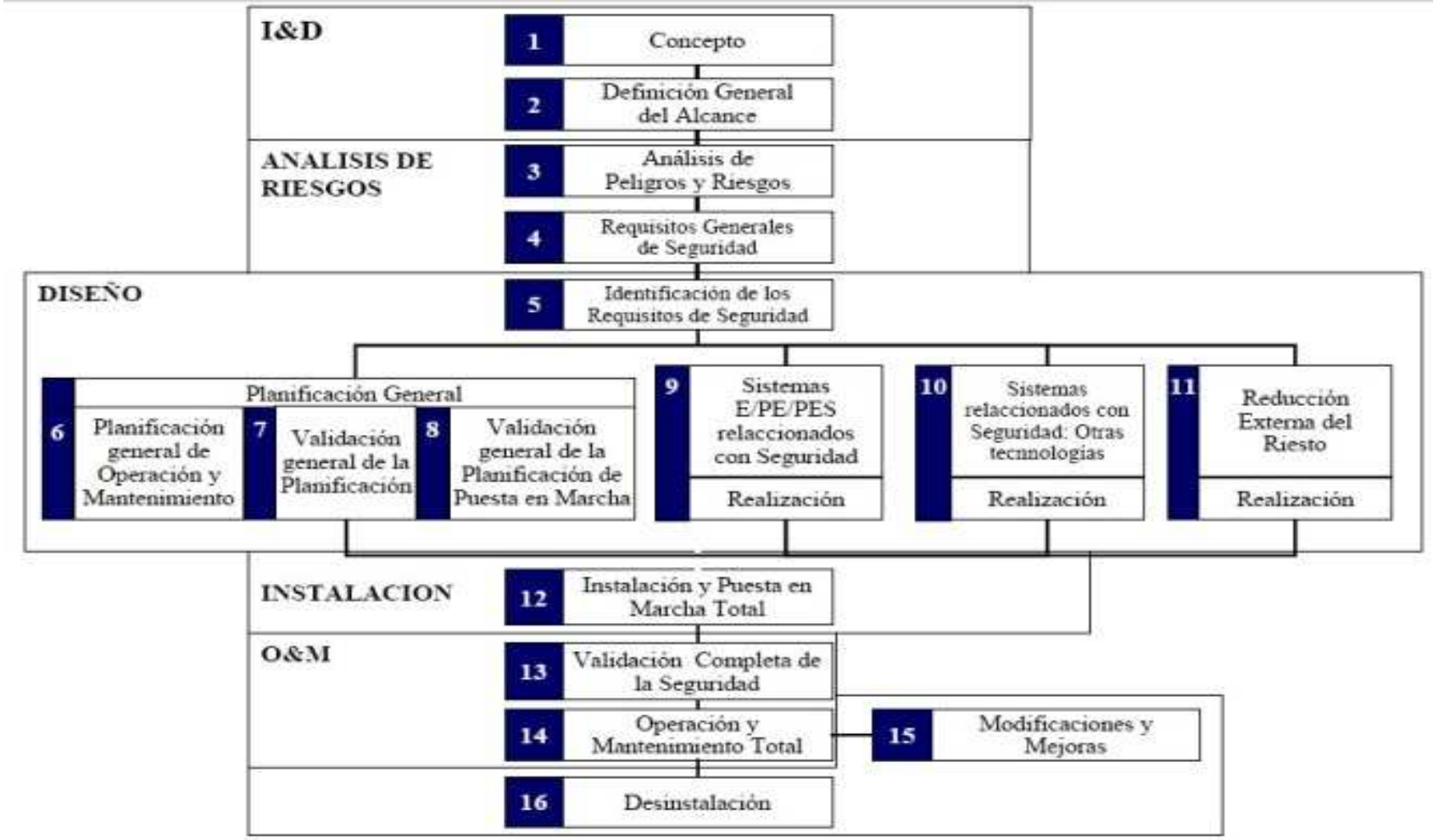
Clasifica las arquitecturas según sistemas MooN, Tolerancia de fallo de HW (HFT=N-M) 2oo4, 1oo1

EN 61508:2011
CICLO DE VIDA

1. -Diseño conceptual I&D del proceso, desarrollo de ingeniería básica y detalle
2. -Análisis de riesgos (ie: HAZOP)
3. -Cálculo del índice SIL
4. -Desarrollo de las especificaciones de los requisitos de seguridad (SRS)
5. -Diseño conceptual del SIS y verificación del diseño
6. -Diseño detallado del SIS
7. -Instalación y comisionado
8. -Operación y mantenimiento
9. -Desmantelamiento y retirada del servicio.



EN 61508:2011
METODOLOGIA DE ANÁLISIS



EN 61508:2011
METODOLOGIA DE ANÁLISIS

- En el diseño conceptual I&D se detalla el nivel de independencia y el grado de formación del equipo de asesores que dictamine y evalúe el Nivel de Seguridad, indicando para cada SIL la recomendación de trabajar con personas, equipos y organizaciones independientes.

En esta fase hay que identificar peligros/riesgos , definir SIF y asignar niveles de SIL para cada SIF.

Hay varias técnicas para el análisis SIL:

1. Cualitativas: Grafico de riesgos
2. Semicualitativas: Grafico de riesgo equilibrado, matrices de riesgo
3. Semicuantitativas: Análisis LOPA o de las capas de protección
4. Cuantitativas: Análisis de Markov, análisis cuantitativo de riesgos (ACR)

- En la siguiente fase ,el análisis de riegos se puede hacer mediante una o varias técnicas:

1. bases de datos de incidentes,
2. análisis de peligros y operatividad (HAZOP)- La más recomendada es la HAZOP, más rigurosa y estructurada e identifica riesgos en las primeras etapas del diseño.
3. análisis what if?,
4. listas de chequeo,
5. análisis de modos de fallo, efectos y consecuencias FMECAS,
6. arboles de fallo, etc…

La técnica elegida dependerá de los propósitos objetivos, y de los datos y recursos disponibles.

EN 61508:2011
METODOLOGIA DE ANÁLISIS

- En la fase de SRS: Debe incluir los SIL para cada SIF, requisitos de fiabilidad para disparos en falso, se deben incluir todos los modos de operación y todas sus condiciones de operación, incluido el arranque y paro y el mantenimiento. Los SRS deben ser expresados y estructurados para que sean claros, específicos, sostenibles, factibles, comprendidos y aplicados

- A continuación de realiza el diseño conceptual del SIS, en base a los SIF/SIL identificados previamente. En la norma se asigna una relación para cada SIF de su SIL, PFD y RRF.

El calculo de cada PFD de cada elemento del SIS hay varias técnicas para calcularlo (FTA, Markov, RBD) dependiendo de parámetros como :

- Tasa de fallos (Lambda): Números de fallo por unidad de tiempo
- Tasa de autodiagnóstico (C) : el porcentaje de fallos detectados en pruebas de autodiagnóstico
- Frecuencia del intervalo de pruebas (T), es el intervalo de tiempo en el que se comprueba el equipo funciona correctamente.
- MTTR, el tiempo medio necesario para reparar e sistema una vez que ha fallado.

Es muy importante para la 61508 que el SIS no debe verse aceptado por otras capas de protección, debe ser independiente, ie: del sistema de control del sistema.

Otra novedad de la 61508 es que refleja unos requisitos mínimos de tolerancia a los defectos de HW (f(SIL) y f(SFF-Tasa fallo seguro)). El SSF (o STR) es la proporción de fallos aleatorios de FW de un componente que da lugar a fallo seguro, falla al detectar un peligro.

EN 61508:2011
METODOLOGIA DE ANÁLISIS

- En el diseño e instalación del SIS hay que verificar que los elementos reales instalados cumplen con la especificación de SIL diseñada.

Las pruebas (FAT / SAT) pueden realizarse online o offline, en función del proceso y sus características (posibilidad de parar, by pass?, coste de parada, …). Deben realizarse chequeos independientes para cada SIF.

- Operación y Mantenimiento, en el que se detallan los pasos a seguir ante un fallo de operación o durante las actividades rutinarias de mantenimiento incluyendo aquellos pasos relativos a la gestión. Es un paso fundamental en la 61508, hay que asegurar que el SIF mantiene su SIL.

  Los SIS compuestos por varios SIF no son sistemas en demanda continua, por tanto es imprescindible hacer un seguimiento de los componentes de cada SIF.

EN 61508:2011
GESTION DEL CICLO DE VIDA

Puesta en marcha de un sistema de gestión de la seguridad funcional y su ciclo de vida, en línea con ISO9001, ayuda:

1. Desarrollar un sistema de gestión de la seguridad funcional
2. Integrar este sistema de gestión en el general de calidad del sistema/instalación.

- Especificar actividades gerenciales y técnicas durante el Ciclo de Vida de Seguridad, para alcanzar y mantener la Seguridad Funcional.
- Especificar las responsabilidades de las personas y organizaciones en las distintas actividades.
- Definir la formación necesaria de las personas y organizaciones para la implementación de las distintas etapas del Ciclo de Vida.
- Proporcionar una metodología común a nivel corporativo para la gestión, durante todo su Ciclo de Vida, de los Sistemas Instrumentados de Seguridad.
- Eliminar incertidumbres sobre la integridad del sistema de seguridad, eficiencia en los costes y disponibilidad de las funciones de seguridad en las instalaciones.
- Proporcionar trazabilidad y posibilidad de auditar todo el sistema de seguridad. … etc…

INDEX

CONCLUSIONES

- En 2014 se publicará IEC 61508 : 2014
- USA está muy extendido y la equivalente ISA-S84.01 es de obligado cumplimiento.
- En Europa (España) es voluntaria, depende de seguros, requisitos del cliente final, etc..
  - CAF, Dimetronics (Siemens), INDRA Sistemas, SIEMSA, etc…
- Esquema básico aplicable a Ciberseguridad (EN 27000), nuevas oportunidades de negocio y necesidades.
- Requisito incluido en los catálogos de la mayoría fabricantes electrónica de control.
- INCREMENTO DE LA PRESENCIA DE TERCERA EMPRESAS DE FORMACIÓN Y CERTIFICACIÓN ESPAÑA EN61508:

  - ALTER TECHNOLOGY TUV NORD
  - VEGA
  - TUV SUD
  - SGS
  - TUV RHEINLAND
  - VDE
  - EXIDA (CFSE, y CFSP niveles de Exida)
  - ISF Consulting
  - BUREAU VERITAS

http://www.isa-spain.org
http://www.iec.ch/functionalsafety
http://www.tuv-nord.com/es

CONCLUSIONES

Evaluación

				
Sistema de gestión de motores SIMOCODE pro 3UF7 con módulos de ampliación de seguridad DM-F	ASIsafe 1) Módulos de entrada seguros 2) Monitor de seguridad (ASIsafe Solution local) 3) Salidas AS-I seguras	Sistema de seguridad modular SIRIUS 3RK3	Controladores SIMATIC	Periferia SIMATIC
Hasta SIL 3	Hasta SIL 3	Hasta SIL 3	Hasta SIL 3	Hasta SIL 3
Hasta PL e	Hasta PL e	Hasta PL e	Hasta PL e	Hasta PL e
Hasta cat. 4	Hasta cat. 4	Hasta cat. 4	Hasta cat. 4	Hasta cat. 4
NFPA 79, listado en NRTL	NFPA 79, listado en NRTL	NFPA 79, listado en NRTL	NFPA 79, NFPA 85, listado en NRTL, IEC 61511	NFPA 79, NFPA 85, listado en NRTL, IEC 61511

CONCLUSIONES

Razones para el cumplimiento voluntario:

- Esquema básico para el cumplimiento de legislaciones globales de seguridad
- Aumentar su seguridad legal
- Incrementar la seguridad de las instalaciones mediante estas medidas preventi
- Optimizar sus procesos y garantizar una operación fluida y segura
- Obtener una opinión neutral, externa y experta (terceros certificando)
- Adecuarse a los seguros y requisitos impuestos, disminución de las pólizas
- Adecuarse a los requisitos del licitatorio final
- Adaptarse a las buenas practicas descritas en la norma
- Control de seguridad de todo el ciclo de vida de la instalación / sistema.
- Incorporar seguridad a los planes de mantenimiento ordinarios del sistema.
- Diseño y compra de los elementos con niveles de SIL adecuados.
- Desarrollar SRS, requisitos de compra
- Disminución de perdidas financieras, por costes materiales propios, lucro cesante y responsabilidad civil derivados de accidentes graves en el sistema/instalaciones.
- Mayor rentabilidad en sistemas de producción, cliente final lo pedirá porque aumenta su rentabilidad producción:

GRACIAS POR SU ATENCION

ALTER TECHNOLOGY TÜV NORD
RAFAEL RODRIGUEZ
Integration Manager
Certification & Testing Division

C/ de la Majada 3
28760 Tres Cantos / Madrid
Tel. +34 918041893
Mobile +34 607 564741
Rafael.rodriguez@altertechnology.com