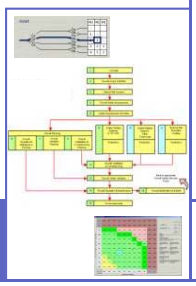
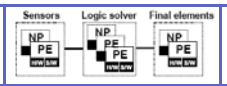
# Seguridad Funcional
# Conceptos Básicos

Guillermo Leanza
guillermo.leanza@gmail.com

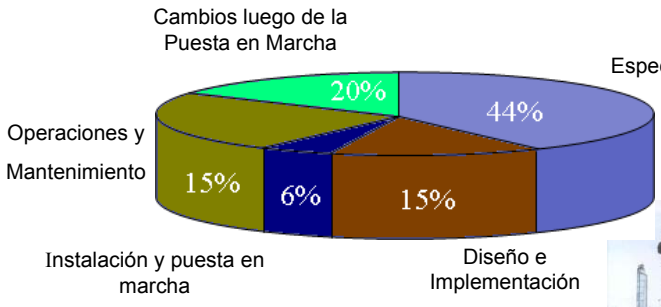


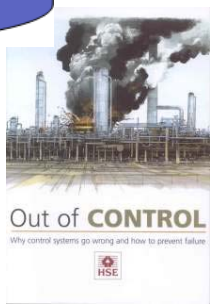



## Agenda

- Seguridad Funcional
- Conceptos
- Normas de referencia IEC61508
- Costo de la Seguridad Vs.
  - No seguridad
- Gestión de la Seguridad Funcional
- Proceso de certificación

## Causas de los accidentes




Luego del desastre de Piper Alpha en el Mar del Norte se encargó un estudio.

El reporte de este estudio, conocido como "Out of Control", es un compilado de 34 incidentes que involucran sistemas de control, hecho por el UK HSE.

## Riesgo

- Concepto intuitivo de riesgo

| Causa | Muertes por año |
|---|---|
| Fumar 10 cigarrillos por día | 1 en 200 ($500 \times 10^{-5}$) |
| Causas naturales a los 40 años | 1 en 700 ($140 \times 10^{-5}$) |
| Accidentes en viaje | 1 en 10000 ($10 \times 10^{-5}$) |
| Accidentes en el hogar | 1 en 10000 ($10 \times 10^{-5}$) |
| Accidentes en el trabajo | 1 en 50000 ($2 \times 10^{-5}$) |

- Nivel de exposición a las causas
  - A veces puede evitarse, a veces no
- Severidad de las consecuencias
  - Vida, salud, producción, activos, medio ambiente, imagen

## Peligros y Riesgo en la industria

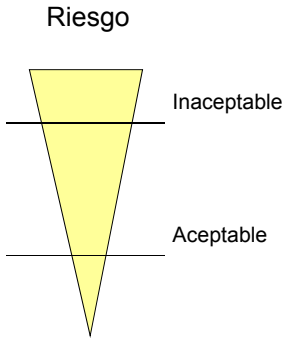
- Peligros (fuentes potenciales de daño)
  - Materiales: combustibles, tóxicos, radioactividad...
  - Condiciones: presión, temperatura...
- Consecuencias
  - Mensurables ($/evento, muertes/evento)
  - Clasificables (insignificantes, menores, serias, catastróficas)
- Definición RIESGO
  - R = F * C
    - Frecuencia de ocurrencia
    - Gravedad de las consecuencias

## Accidente

- Secuencia de eventos que provoca un daño
  - Peligro
    - Materiales + Condiciones (Procesos)
  - Evento iniciador
    - Falla tecnológica
    - Factor humano
    - Suceso externo
  - Eventos intermedios
    - Factores de propagación
    - Fallas de contención
  - Resultado
    - Fenómeno + Consecuencias

## Riesgo Tolerable

- Riesgo Inaceptable
  - Debe ser reducido a cualquier costo
  - Factores políticos, sociales, etc.
- Riesgo Aceptable
  - No requiere reducción
  - Decisión corporativa
- Riesgo Tolerable
  - Concepto “ALARP” As Low as Reasonably Practicable
  - Reducir mientras el costo no exceda el beneficio



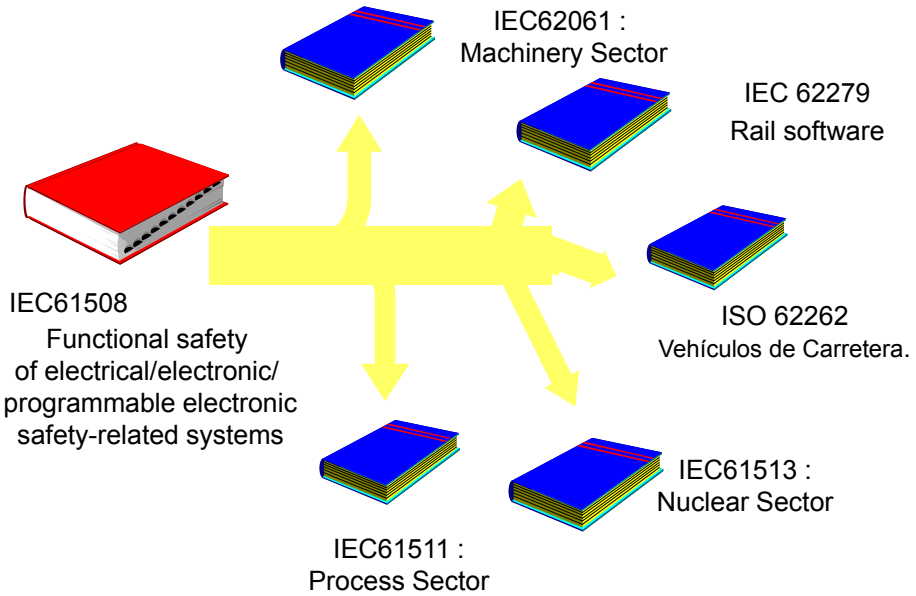

## Definiciones

- **Qué es Safety?**
  - Libre de *Riesgo Inaceptable* IEC 61508 -4 3.1.8
- **Qué es Functional Safety**
  - Un sistema es funcionalmente seguro si un mal funcionamiento no derivará en:
  - Lesiones o muertes humanas
  - Daño al medio ambiente
  - Pérdida de equipamiento o producción
- **Qué es un Sistema Iinstrumentado de Seguridad**
  - Una combinación de sensores, resolvedor lógico, y actuadores para llevar a cabo un Función de Seguridad

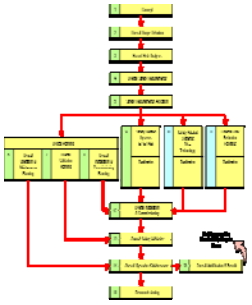
## El factor humano

- Se estima que entre el 80 y el 90% de los accidentes tienen origen humano
  - Acción incorrecta, inacción, mala especificación, mala implementación, mal mantenimiento, falta de entrenamiento...
- Problema cultural
  - “Aquí no puede pasar”
  - “Siempre funcionó así”
- Instalar “cultura de la seguridad”
  - Responsabilidad individual y colectiva
  - Sistema de Gestión de Seguridad
  - Responsabilidad corporativa


## Estándares genérios y de aplicación por sectores



## IEC 61508 - Responsables de las fases



**Pre Diseño**

**(Fases 1 to 5)**

***Usuario Final u operador***

**Diseño e Instalación (Fases 6 to 13)**

***Ingeniería / Proveedor Sistemas***

**OPERACION**

**(Fases 14 to 16)**

***Usuario Final u operador***

## Cumplimiento IEC 61508

***Los elementos de conformidad son necesarios en cada fase del Ciclo de Vida***

***La conformidad contempla productos y compañías aprobadas***

***Ítems de cumplimiento***

- Gestión de Seguridad Funcional
- \+ Requisitos Técnicos
- \+ Competencia de las personas
- \+ Evaluación de la Seguridad Funcional

***Ciclo de Vida de la Saguridad***

- Especificación
- Diseño
- Instalación y PEM
- Operación & Mantenimiento
- Cambios

PEM: Puesta en Marcha → Comisionamiento

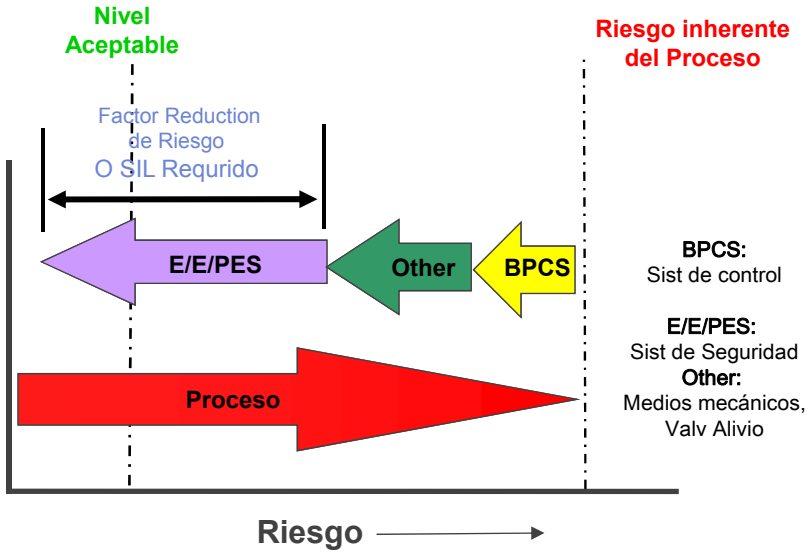
## Nivel de integridad de la seguridad (SIL)

**Según IEC 61508**
**Safety Integrity Level (SIL)**
Nivel discreto (uno de cuatro posibles) para especificar los requerimientos de integridad de las funciones de seguridad (SIF) que se realizarán mediante los sistemas relacionados con la seguridad (SIS), donde el nivel 4 tiene el más alto nivel de integridad de la seguridad, y el nivel 1 tiene el más bajo

Es una medición del desempeño general de un sistema de seguridad expresado en términos de “Probabilidad de falla sobre demanda” y (PFD= 1-Availability)

| SIL | PFD | Safety Availability | Risk Reduction |
|---|---|---|---|
| 4 | 0.0001 – 0.00001 | 0.99990 – 0.99999 | 10000 – 100000 |
| 3 | 0.001 – 0.0001 | 0.99900 – 0.99990 | 1000 – 10000 |
| 2 | 0.01 – 0.001 | 0.99000 – 0.99900 | 100 – 1000 |
| 1 | 0.1 – 0.01 | 0.90000 – 0.99000 | 10 – 100 |

## Reducción de Riesgo



## Puntos calves de IEC 61508

- Safety Management System
  - Ciclo de Vida
  - Planificación
  - Evaluación de cumplimento
  - Cadena de suministros
- Requerimientos Técnicos
  - Elección de tecnologías
  - Evaluación de riesgo
  - Especificaciones y Nivel SIL
- Capacidades
  - Roles & responsabilidades
  - Entrenamiento capacidades

## Concepto de ciclo de vida

- Un ciclo de vida nos ayuda de forma sistemática a
  - Afrontar actividades
  - Afrontar responsabilidades
  - Identificar capacidades requeridas por fase
  - Identificar necesidad de documentos
  - Trabajar en administración de la seguridad, actividades de verificación y validación
- Diferentes ciclos de vida pueden definirse por
  - Usuarios finales, integradores, desarrolladores, hardware, software...

## Gestión de la seguridad

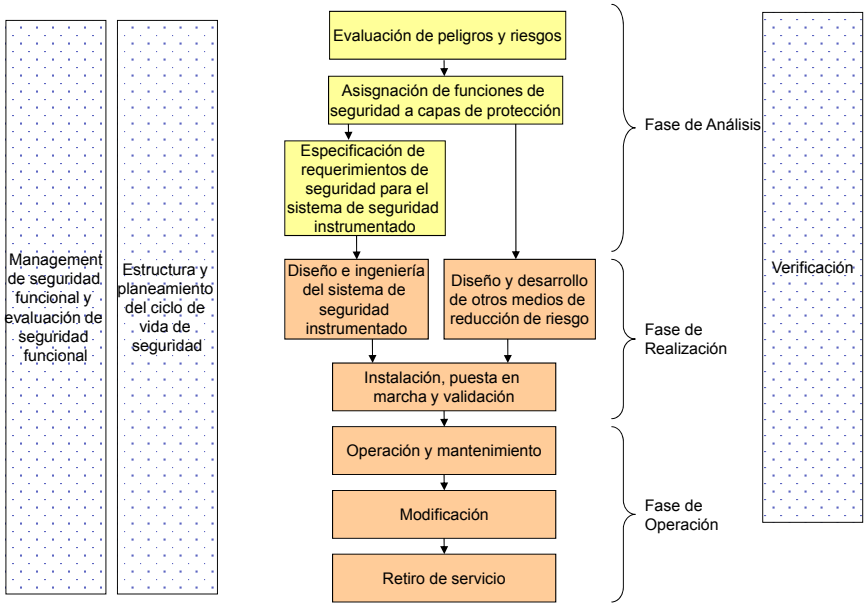
- Por que administramos la seguridad?
  - La seguridad debe ser el único beneficio en un proyecto
  - La seguridad no debe ocurrir por suerte
  - La seguridad debe estar documentada y ser repetible
- Objetivos
  - Definir todas las actividades técnicas y de administración durante el ciclo de vida del sistema de seguridad
  - Establecer responsabilidades o actividades para:
    - Personas
    - Departamentos
    - Organizaciones

## Especificación de Requerimientos de Seguridad (SRS)

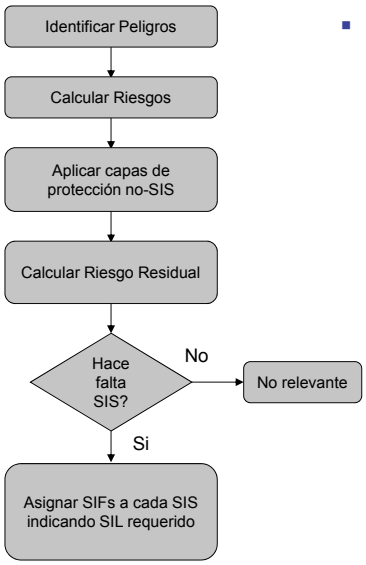
- Documento que especifica los...
  - Requerimientos funcionales
  - Requerimientos de integridad
  - Requerimientos de performance[1]
- Incluye requerimientos de hardware y software
- Base del diseño
  - La mayor fuente de errores
  - Los errores se propagan sin ser detectados (sistemáticos)
  - El sistema se valida contra la SRS

*[1]La norma habla de performance generalmente referida a la integridad (SIL) excepto en algunos puntos donde engloba capacidad, tiempo de respuesta, confiabilidad, disponibilidad, integridad, objetivos de seguridad y limitaciones. Aquí lo usamos en ese sentido, agregando también facilidad de uso y mantenimiento, soporte del proveedor, etcétera.*

## Concepto de ciclo de vida 61511




## Evaluación de Riesgo




- **Métodos de Análisis**
  - **Cualitativos**
    - Qué pasa si...
    - Listas de verificación
    - Matriz de Riesgo
    - Grafo de Riesgo
      - HAZOP
  - **Cuantitativos**
    - LOPA
    - FTA
    - ETA
    - Modelos de Markov
  - **Mixtos**
    - FMEA
    - Grafo de Riesgo Calibrado

## Costos: Ej Horno, Baja Presión de gas

Tomamos un horno de proceso

Falla por baja presión de gas en quemadores

- Producción diaria USD 300K
- Costo Reparación USD 2.000K
- Tiempo Inactivo 20 Días

Probabilidad de ocurrencia 1 vez cada 10 años

**Costo no mitigado (Anual) = (2.000K +20d * 300K)* 0,1= 800K**

**Costo no mitigado con una función de seguridad:**

SIL 1 800K* 0,1(RRF) = 80K

SIL 2 800K* 0,01(RRF) = 8K

SIL 3 800K* 0,001(RRF) = 0,8K

## Ej Horno: Baja Presión de gas (Cont.)

- Riesgo aceptado por la empresa USD 15K
- Nivel SIL requerido: SIL2
- Riesgo No mitigado SIL2 USD 8K

Costo del proyecto Aprox USD 100K *

Sensor, Lógica, actuador, ingeniería, montaje, etc

* (Se considera solo esta Función de Seguridad)

Costo Anual de mantenimiento USD 3 K

Prueba Sensor 0,5K, Prueba actuador 2K, Lógica 0,5K

- Costo SIS en 10 años USD 130K
- Costo mitigado 10 años Con SIS USD 80K
- **Costo No Mitigado en 10 años** **USD 8000K !!!!!**

## Propósito de un SIS

- **Protección de vidas Humanas**
- **Medio Ambiente**
- **Protección de equipamiento**
- **Valores e inversiones**
- **Imagen corporativa**


## Modos de Falla

- Un sistema de seguridad debe ser medido por su características de falla
- Un sistema de seguridad tiene dos tipos de falla:

**Fallas de iniciación**

- Falla segura
- Ostensible (overt)
- Espúrea
- Significa costo de producción

**Fallas de inhibición**

- Falla Peligrosa
- Encubierta (covert)
- Potencialmente peligrosa
- Se deben descubrir por pruebas

## Requerimientos de un SIS

- **Funcionalidad**: que haga lo que tiene que hacer (confiabilidad)
- **Integridad**: que esté disponible para hacerlo (disponibilidad)
  - Que actúe cuando tiene que actuar
    - Requerimiento de seguridad – Concepto de ”falla riesgosa”
  - Que no actúe cuando no tiene que actuar
    - Requerimiento de producción – Concepto de ”falla segura”
- **Performance**: que lo haga en tiempo y forma
- Otros requerimientos: costo, flexibilidad, apertura, etc.

## Fallas en el Sistema de Seguridad

- Las fallas del sistema de seguridad pueden ser:
  - Aleatorias
  - Causa Común
  - Sistemáticas
- Cada una de estas fallas pone al sistema de seguridad en un estado específico.

## Fallas Aleatorias

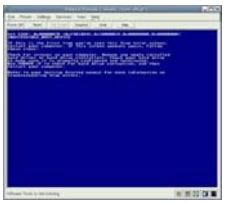
- Definición:
  - Falla espontánea de un componente de hardware
    - Permanentes – existen hasta ser reparadas
    - Dinámicas – sólo en ciertas circunstancias
- IEC 61508
  - Medidas para control de fallas (tablas)
  - Estudios cualitativos y cuantitativos de confiabilidad del hardware (probabilidad de falla en demanda PFD)

## Fallas de Causa Común

- Definición:
  - Son aquellas fallas simultaneas o coincidentes de dos o mas canales en un sistema de múltiples canales que causan que causan una falla en el sistema de seguridad
  - Normalmente relacionadas con eventos ambientales (inundaciones, tormentas, etc.)
- IEC 61508
  - Diversidad
  - Consideradas en el calculo de PFD

## Fallas Sistemáticas

- Definición:
  - Falla oculta en el diseño o la implementación
    - Software o Hardware
    - Especificaciones de diseño
    - Manuales de usuario, etc.
    - Errores de diseño

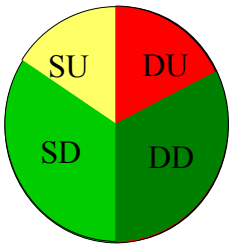


- IEC 61508
  - Medidas para evitar fallas (tablas)
  - NO incluidas en cálculo de PFD

## Seguridad del Sistema Versus Proceso

| Seguridad del sistema | Proceso o equipo bajo control |
|---|---|
| Estado Normal | Disponible<br>No hay fallas internas |
| Estado seguro | Disparado, no disponible (Tripped)<br>El sistema falla en una forma que la función de seguridad es actuada sin que haya demanda |
| Estado peligroso | Disponible pero no protegido<br>El sistema falla en una forma que la función de seguridad no puede ser realizada ante una demanda |
| Estado intermedio | Disponible pero se necesita reparar el sistema de seguridad.<br>La función de seguridad puede ser realizada no obstante haya fallas de uno o más componentes. ( hay un tiempo para normalizarlo) |

## Modos de falla y Tasa de fallas




- Tasa de Falla Total
  - Falla Segura
  - Segura Detectada
  - Segura No Detectada
  - Fallas Peligrosas
  - Peligrosa Detectada
  - Peligrosa NO detectada

## Detección de fallas

- Pueden detectarse de 3 maneras
  - Operación normal
  - Pruebas periódicas
  - Diagnósticos internos

## Detección por operación normal

- La operación del proceso revela las fallas del equipo
- Parada de una parte del proceso debido al sistema de seguridad

- * Esta detección no es útil cuando se pretende mantener un proceso de producción estable

## Detección por Pruebas periódicas

- Que es una prueba periódica?
- Es una prueba que se realiza cada cierto tiempo pero no en forma automática
  - Iniciadas por una acción humana
  - Probar que cierre de una válvula
  - Probar que mide correctamente un transmisor

## Detección por diagnósticos

- Es una diagnóstico frecuente y automático que se lleva a cabo sin la intervención de ninguna acción humana
- Normalmente son “built-in”
- Pueden ser de hardware o software

## Fracción de Falla Segura (SFF)

- Por que la necesitamos?
- Los requerimientos de PFD solos no son suficientes para declarar que un sistema es seguro
- Es una medición de la efectividad de los diagnósticos internos

**SFF** =(**λ** sd + **λ** su + ʌ dd ) / (**λ** sd + **λ** su + **λ**dd + **λ** du)

**λ** = Tasa de falla

sd = segura detectada su = segura NO detectada

dd = peligrosa detectada du = peligrosa NO detectada

## Diseño de Hardware

- Determinado por
  - Probabilidad de falla en demanda (PFD) → SIL
  - Baja /Alta demanda del proceso
  - Tipo A o B de componentes
  - Tolerancia a falla de Hardware
  - Fracción de falla segura
  - Restricciones en la arquitectura

## Safety Integrity Level

- Tres propiedades SIL importantes
  - Aplica a la función de seguridad completa
  - SIL más alto significa requerimientos más estrictos
  - Requerimientos técnicos y no técnicos

| SIL | PFD* | Disponibilidad de Seguridad | Reducción de riesgo |
|---|---|---|---|
| 4 | 0,0001-0,00001 | 0,9999-0,99999 | 10.000-100.000 |
| 3 | 0,001-0,0001 | 0,999-0,9999 | 1.000-10.000 |
| 2 | 0,01-0,001 | 0,99-0,999 | 100-1.000 |
| 1 | 0,1-0,01 | 0,9-0,99 | 10-100 |

* Probabilidad de falla “on demand”

## Proof Test (Ensayo periódico)

- **Proof Test**
- **Ensayo periódico:** Ensayo realizado para revelar defectos no detectados de un sistema instrumentado deseguridad de manera que, si fuera necesario, se pueda restaurar el sistema en su funcionalidad de diseño.

## Tolerancia a fallas de hardware (HFT)

- Tolerancia a fallas de hardware
  - De N significa que N+1 faltas podrían causar pérdida de la función de seguridad
  - Es una medida de redundancia
  - Debe ser determinada por subsistema
    - Sensor
    - Lógica
    - Actuación

## Ejemplos de HFT

| Ejemplo | Redundancia | HFT |
|---|---|---|
| 1oo1 | 0 | 0 |
| 2oo2 | 2 | 0 |
| 1oo2 | 2 | 1 |
| 2oo3 | 3 | 1 |
| 1oo3 | 3 | 2 |
| 2oo4 | 4 | 2 |

## Subsistemas tipo A

- Un subsistema es tipo A si

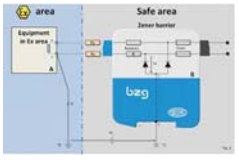
  - Los modos de falla están bien definidos

**Y**

  - El comportamiento de la falla puede determinarse completamente

**Y**

  - Hay suficiente información sobre la falla



## Subsistemas tipo B

■ Un subsistema es tipo B si

- Uno o mas modos de falla no están perfectamente definidos

**O**

- El comportamiento de la falla no puede determinarse completamente

**O**

- No hay suficiente información sobre la falla

## Restricciones de arquitectura en 61508 Sist Tipo A

| Safe Failure Fraction | Hardware Fault Tolerance | | |
|---|---|---|---|
| | 0 | 1 | 2 |
| < 60% | SIL 1 | SIL 2 | SIL 3 |
| 60% - 90% | SIL 2 | SIL 3 | SIL 4 |
| 90 - < 99% | SIL 3 | SIL 4 | SIL 4 |
| ≥ 99% | SIL 3 | SIL 4 | SIL 4 |

## Restricciones de arquitectura en 61508 Sist Tipo B

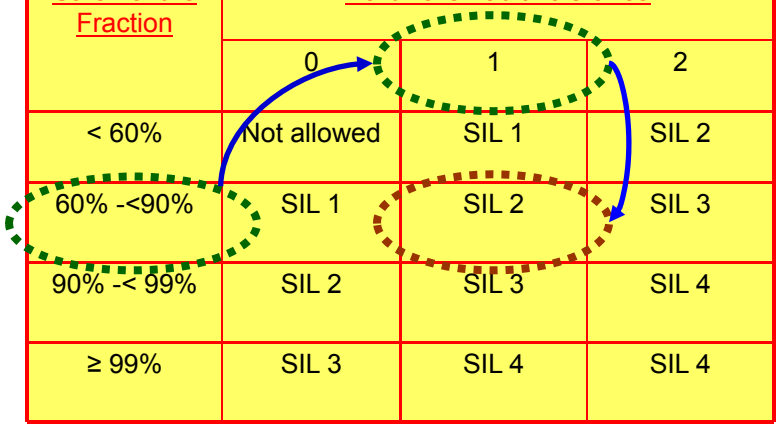
| Safe Failure Fraction | Hardware Fault Tolerance | | |
|---|---|---|---|
| | 0 | 1 | 2 |
| < 60% | Not allowed | SIL 1 | SIL 2 |
| 60% -90% | SIL 1 | SIL 2 | SIL 3 |
| 90 -< 99% | SIL 2 | SIL 3 | SIL 4 |
| ≥ 99% | SIL 3 | SIL 4 | SIL 4 |

## Ej. Restricciones de arquitectura en 61508 Sist Tipo A

| Safe Failure Fraction | Hardware Fault Tolerance | | |
|---|---|---|---|
| | 0 | 1 | 2 |
| < 60% | SIL 1 | SIL 2 | SIL 3 |
| 60% - 90% | SIL 2 | SIL 3 | SIL 4 |
| 90 - < 99% | SIL 3 | SIL 4 | SIL 4 |
| ≥ 99% | SIL 3 | SIL 4 | SIL 4 |

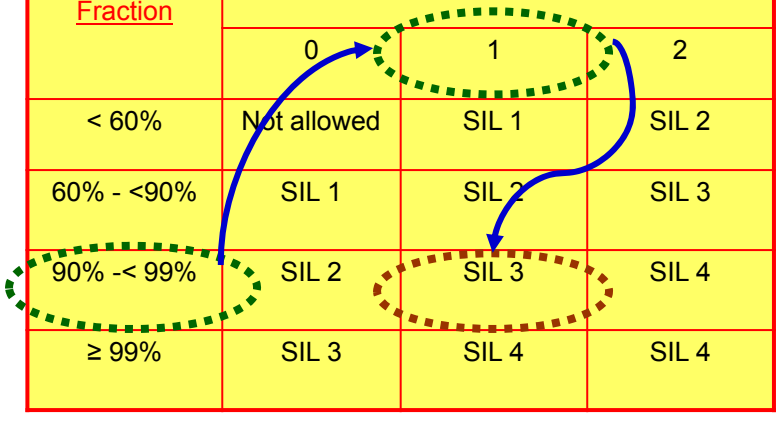
## Ej. Restricciones de arquitectura en 61508 Sist Tipo B

| Safe Failure Fraction | Hardware Fault Tolerance | | |
|---|---|---|---|
| | 0 | 1 | 2 |
| < 60% | Not allowed | SIL 1 | SIL 2 |
| 60% -<90% | SIL 1 | SIL 2 | SIL 3 |
| 90% -< 99% | SIL 2 | SIL 3 | SIL 4 |
| ≥ 99% | SIL 3 | SIL 4 | SIL 4 |



## Ej. Restricciones de arquitectura en 61508 Sist Tipo B

| Safe Failure Fraction | Hardware Fault Tolerance | | |
|---|---|---|---|
| | 0 | 1 | 2 |
| < 60% | Not allowed | SIL 1 | SIL 2 |
| 60% - <90% | SIL 1 | SIL 2 | SIL 3 |
| 90% -< 99% | SIL 2 | SIL 3 | SIL 4 |
| ≥ 99% | SIL 3 | SIL 4 | SIL 4 |



## Certificación:

- Un ente acreditado (Ej. TUV) certifica el cumplimiento de la norma
- Ej. Certificación de una organización
- (Functional Safety Management)
- Similar a ISO9001


TÜV NORD

Certificate

Honeywell Process Solutions
1250W Sam Houston Pkwy S
Houston, TX 77042
USA
has introduced a

-Functional Safety Management-

in accordance with

IEC 61511 and IEC 61508

for the execution of project engineering of microprocessor based safety systems based on the Honeywell Global Project Engineering Process. The Functional Safety Management Process includes design, development and maintenance of hardware, configuration and application software

IEC 61511:2004
Safety Instrumented Systems for the Process Industry Sector
IEC 61508:2000
Functional safety of electrical/electronic programmable safety related systems

This voluntary certificate is issued with respect to audit report SLA-0204/2006-01AR and does not replace any specific certification required for safety related E/E/PES or µC

## Certificación

- Ej. Certificación de un producto
- Para ser usado en Seguridad funcional hasta SIL3


TÜV Rheinland Group

TÜV Industrie Service GmbH
Automation, Software und Informationstechnologie

ZERTIFIKAT
CERTIFICATE

Nr./No. 968/EZ 195.00/05

## Certificación de una Válvula Solenoide

CERTIFICATE

**No.: 968/EZ 345.01/13**

| | | | |
|---|---|---|---|
| **Product tested** | Safety Solenoid Valve with integrated Safety Controller, Neles ValvGuard | **Certificate holder** | Metso Automation Inc.<br>Vanha Porvoontie 229<br>01380 Vantaa<br>Finland |
| **Type designation** | VG9000F | **Manufacturer** | see certificate holder |
| **Codes and standards forming the basis of testing** | IEC 61508 Parts 1-7:2010<br>IEC 61511-1:2003 + Corr. 1:2004 | | |
| **Intended application** | Safety-related Emergency Shut-down.<br><br>The product is of type A and has a Safety Capability of SC 3 acc. to IEC 61508. Accordingly it can be used in applications up to SIL 3 acc. to IEC 61508 and IEC 61511. The requested HFT depends on the requirements of the application. | | |
| **Specific requirements** | The instructions of the associated Installation, Operating and Safety Manual shall be considered. | | |

Preguntas?