SIEMENS

Seguridad funcional para Automatización de Procesos

SIMATIC SIS

- Introducción
- Conceptos Básicos
- Análisis de Riesgos
- Historia
- Aplicaciones
- Certificaciones

SIEMENS

Introducción

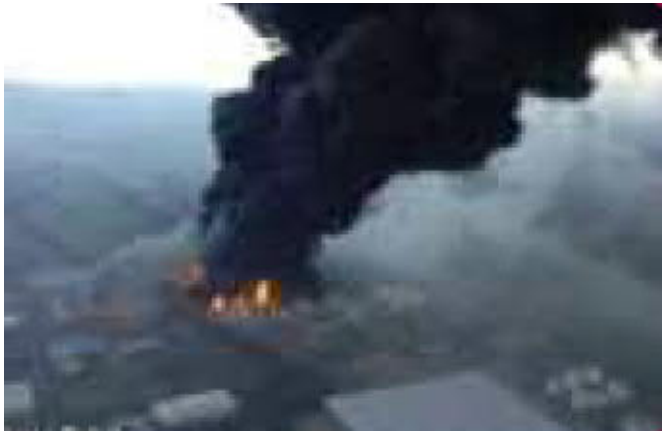
Seguridad funcional para Procesos industriales

Accidentes Industriales Desastrosos

Plataforma BP. Golfo de México 2010

11 personas fallecieron

Derrame de 4,9 millones de barriles de petróleo.



Refinería BP (USA, 2005)

15 personas fallecieron, 200 heridos.

Los accidentes industriales raramente suceden por una sola causa. Lo normal es que sean consecuencia de una combinación de eventos poco comunes que se piensa son independientes y que no deberían suceder al mismo tiempo.

Desafíos en Seguridad Funcional de Procesos

La seguridad funcional reduce el riego de accidentes relacionados con el proceso y asegura a:

Gente

Procesos

Ambiente

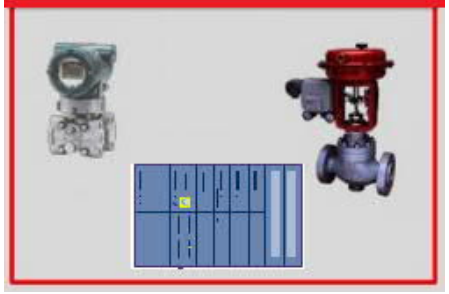
SIEMENS

Conceptos Básicos

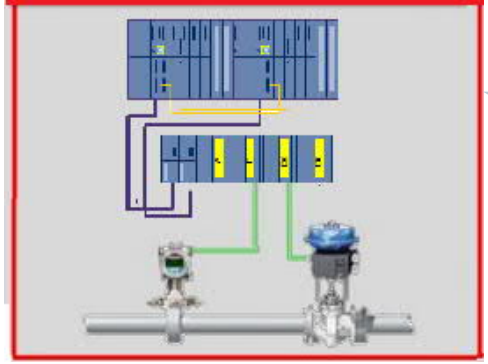
Seguridad funcional para Procesos industriales

Estandard de sistemas Instrumentados de seguridad para Sector de procesos

Fabricantes y Proveedores de Equipos IEC 61508



Diseñadores, integradores y Usuarios de sistemas Instrumentados de Seguridad IEC 61511



ANSI/ISA 84.00.01

SIEMENS

Peligro ("Hazard"): Es una fuente potencial de daño a las personas, ambiente o propiedad.

Riesgo: Es una combinación de la probabilidad de ocurrencia de un daño o de su severidad.

Riesgo = Probabilidad * Severidad

El riesgo se puede disminuir ya sea minimizando la probabilidad de ocurrencia del evento que genera el daño (prevención), minimizando la severidad del mismo (mitigación), o disminuyendo ambas. !!!! Recuerde el riesgo cero no existe!!!;

SIMATIC SIS
Definiciones Básicas

Riesgo Aceptable: El cual es aceptado si se le compara con el riego que se experimenta día a día.

Riesgo Tolerable: considerado que se han tomado todas las medidas necesarias para reducirlo a un valor por debajo del cual seria económicamente no viable.

Riesgo Inadmisible: El cual no se puede justificar bajo ninguna circunstancia

Que es seguridad?
De acuerdo a la norma IEC-61508, seguridad se define como :
"Libre de Riesgo Inadmisible"

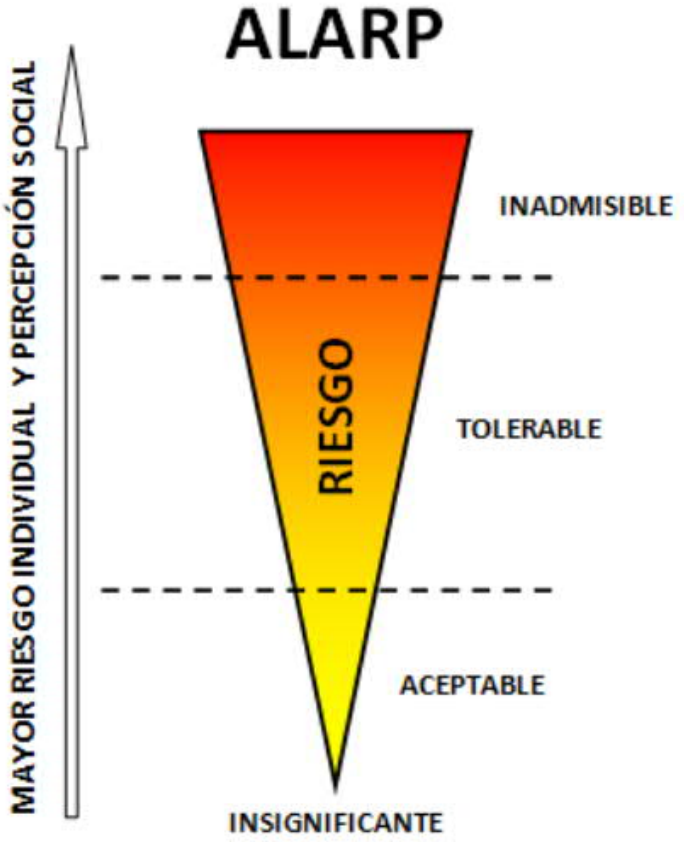
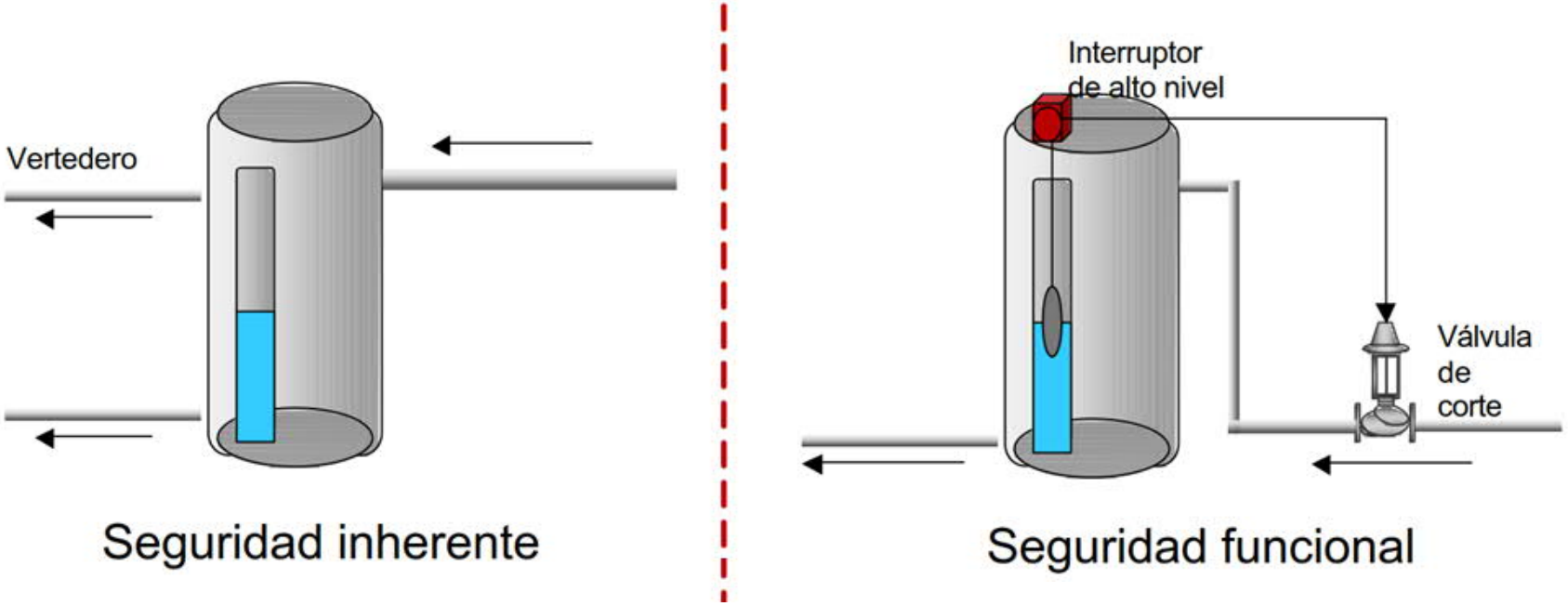


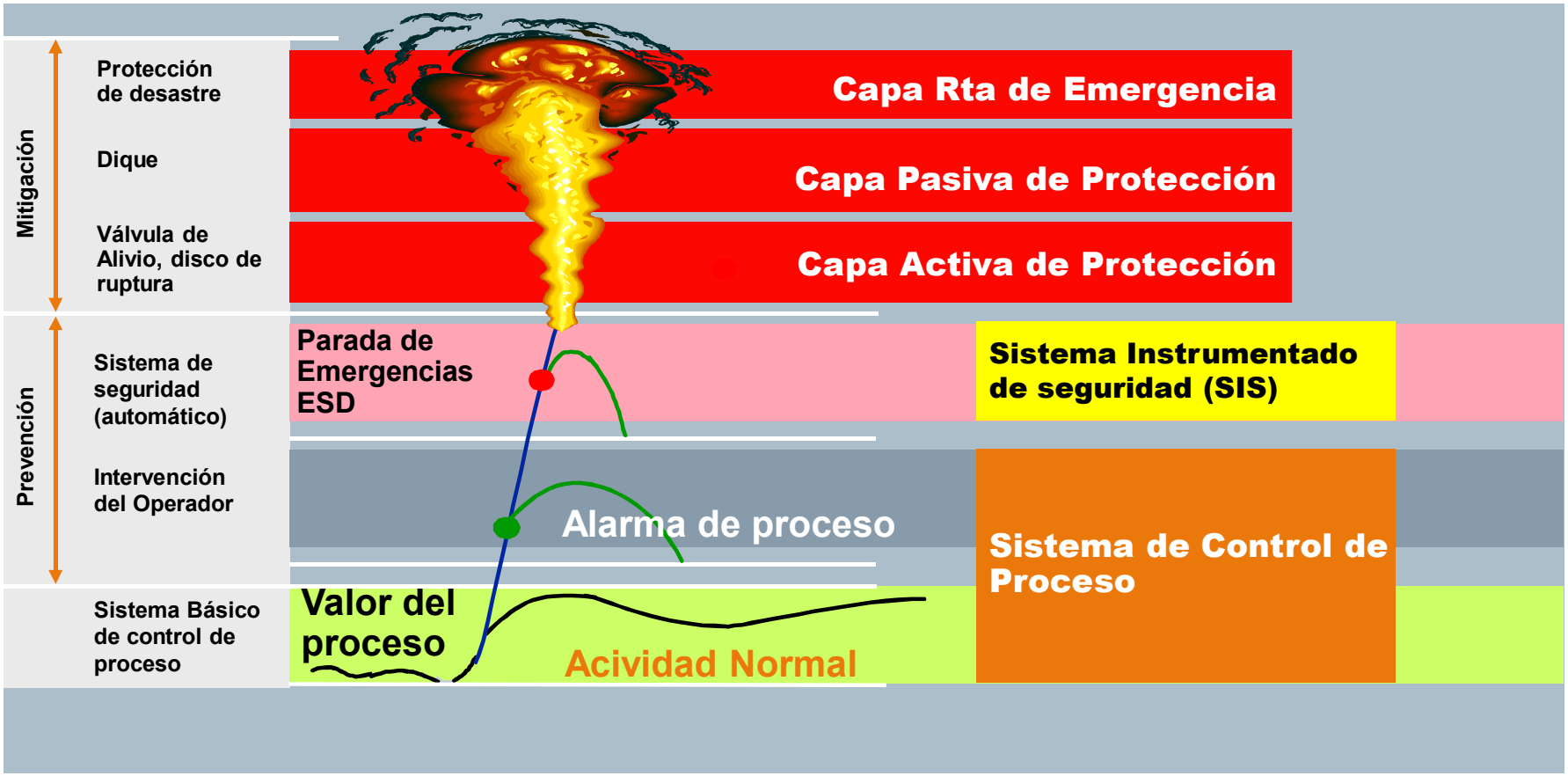
Figura1 . ALARP "***A**s **L**ow **A**s **R**easonably **P**racticable*", Fuente: WIkipedia

Seguridad Funcional

Es aquella parte de la seguridad en general, que depende del correcto funcionamiento de equipos eléctricos o electrónicos , de tecnologías o de instalaciones de reducción de riesgo externas. En general la seguridad funcional puede ser interpretada, como la adición de algún elemento externo al proceso o equipo bajo control que no sea parte inherente del propio proceso

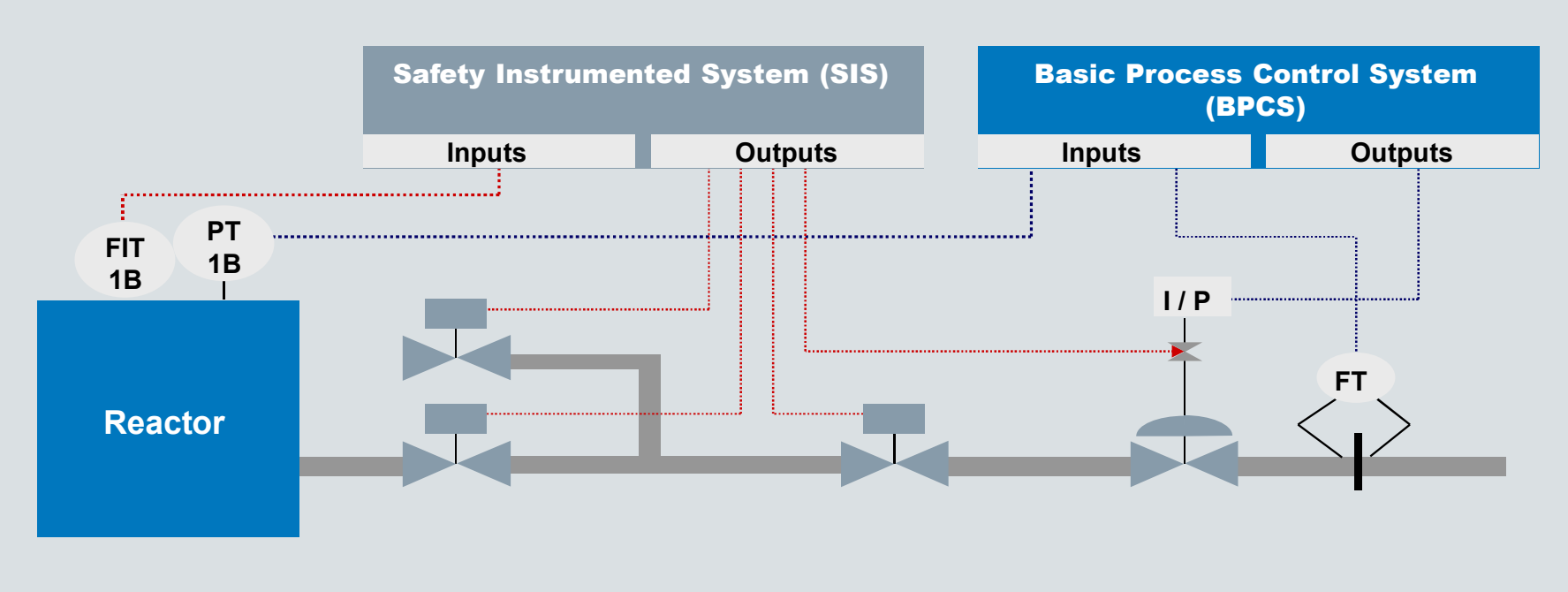


Seguridad en Procesos



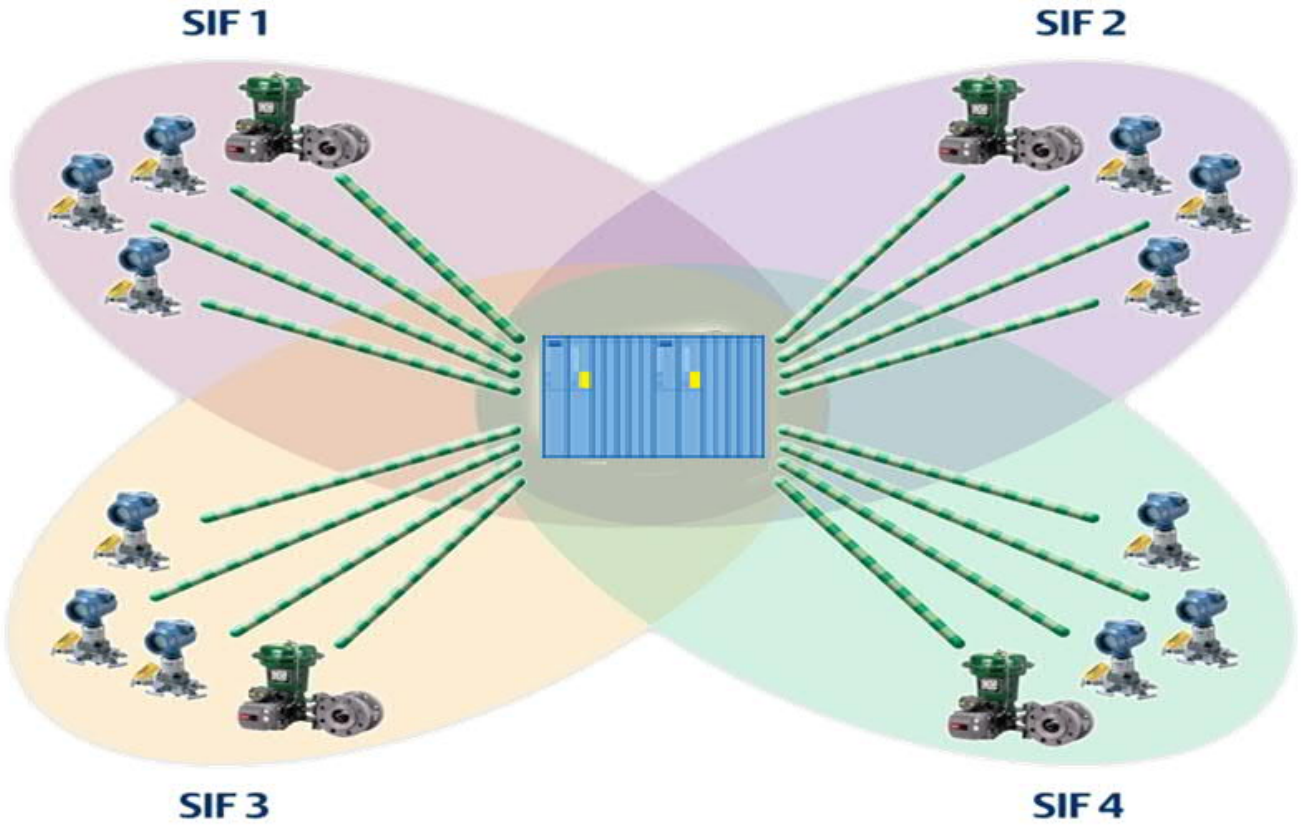
Sistema Instrumentado de Seguridad _ Safety Instrumented System (SIS)

Sistema Instrumentado de seguridad es una combinación de sensores, módulos lógicos y actuadores que detectan condiciones de funcionamiento anormales y devuelve la planta AUTOMÁTICAMENTE a un estado seguro nuevamente.



Hay separación (Independencia) del SBCP

Sistema Instrumentado de Seguridad _Safety Instrumented System (SIS)

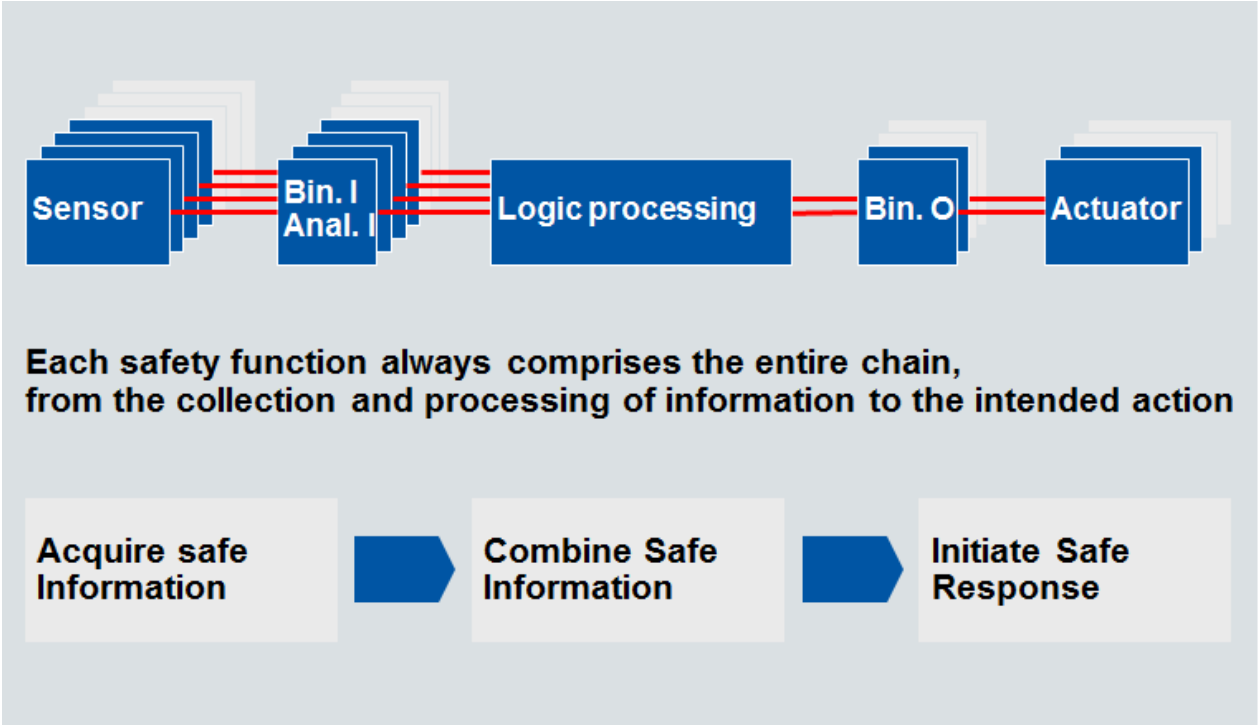


Un SIS comprende normalmente más de un SIF

Funcion Instrumentada de Seguridad
IEC 61508/11

SIEMENS

Considerando la función Instrumentada de seguridad completa de los lasos según a IEC 61508:

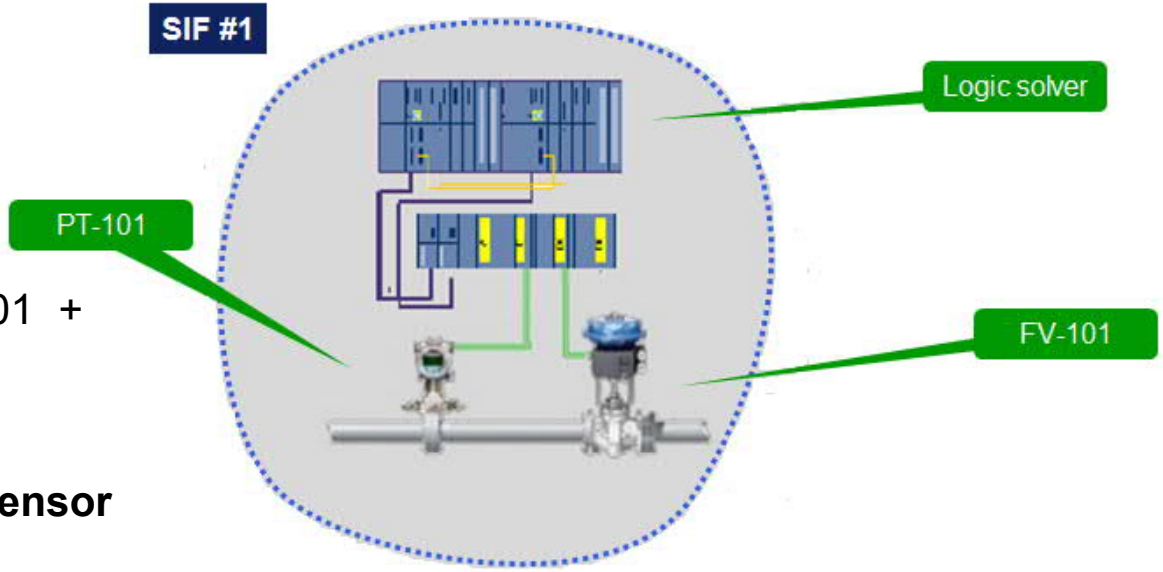


Es durmiente

Rendimiento de una Función Instrumentada de Seguridad IEC 61508/11

SIEMENS

El Rendimiento de una SIF depende de sus componentes:



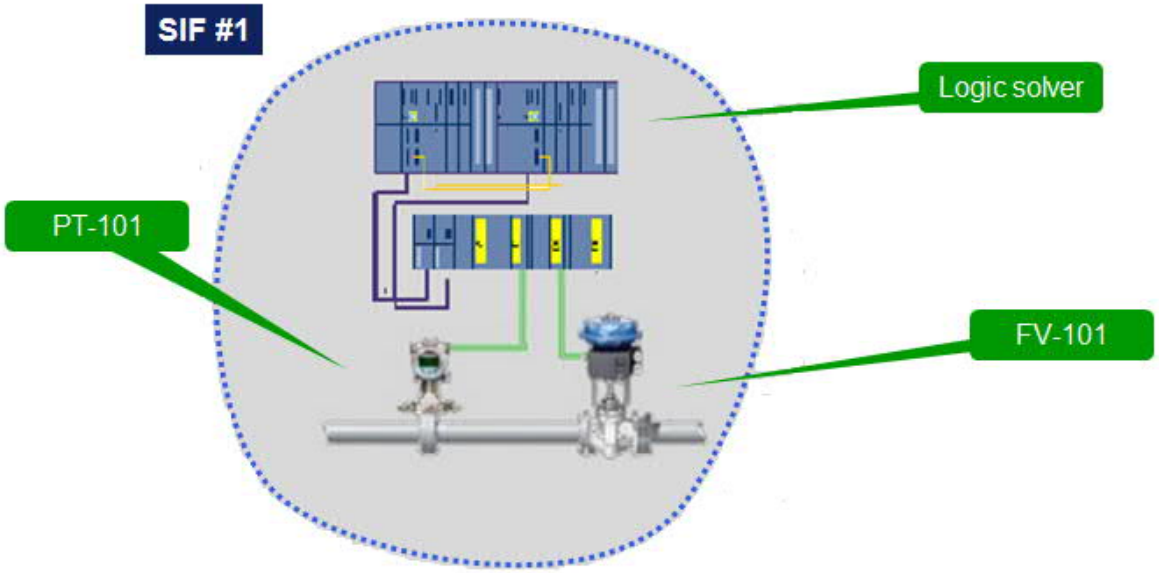
El Rendimiento de la SIF = Rendimiento PT-101 + Rendimiento de logic solver + Rendimiento FV-101

En otras palabras, esta SIF fallara si: Falla el sensor o Falla el logic solver o falla la válvula

Una cadena es tan fuerte como su eslabón mas débil

Nivel de integridad: Safety Integrity Level SIL

El rendimiento de cada elemento SIF, es medido de acuerdo a su capacidad de reducir el riego en "Ordenes de magnitud", o sea por su integridad funcional:



Safety Integrity Level (SIL)

SIL 1 → Reducirá el riesgo entre 1 y 2 órdenes de magnitud → al menos 10 veces

SIL 2 → Reducirá el riesgo entre 2 y 3 órdenes de magnitud → al menos 100 veces

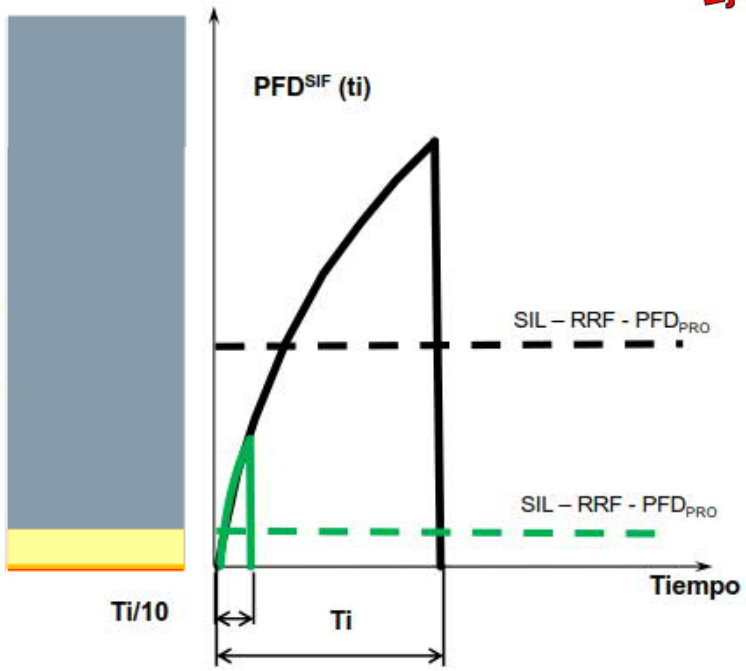
SIL 3 → Reducirá el riesgo entre 3 y 4 órdenes de magnitud → al menos 1.000 veces

SIL 4 → Reducirá el riesgo entre 4 y 5 órdenes de magnitud → al menos 10.000 veces

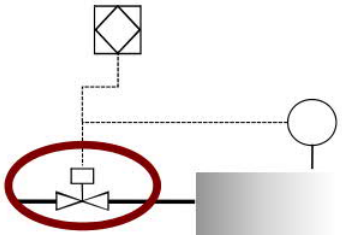
Safety Integrity Level SIL

SIL ("Safety Integrity Level"): Es un valor discreto (de 4 posibles de acuerdo a la IEC-61508 y 3 de acuerdo a la ANSI/ISA S84.01) que indica el grado de disminución de riesgo que está en capacidad de brindar las funciones de seguridad asignadas a un Sistema Instrumentado de Seguridad (SIS). El SIL está relacionado con la Probabilidad de Falla bajo demanda del sistema:

IEC61508 "Modo Demanda"	
PFDpro: 0.1 – 0.01	SIL 1
PFDpro: 0.01 – 0.001	SIL 2
PFDpro: 0.001 – 0.0001	SIL 3
PFDpro: 0.0001 – 0.00001	SIL 4



Ejemplo: Válvula



PDF: Probabilidad de fallar la función para la que se ha diseñado bajo demanda.

Factor de Reducción del Riesgo: Inverso de PFD

1/.0001 = 10,000

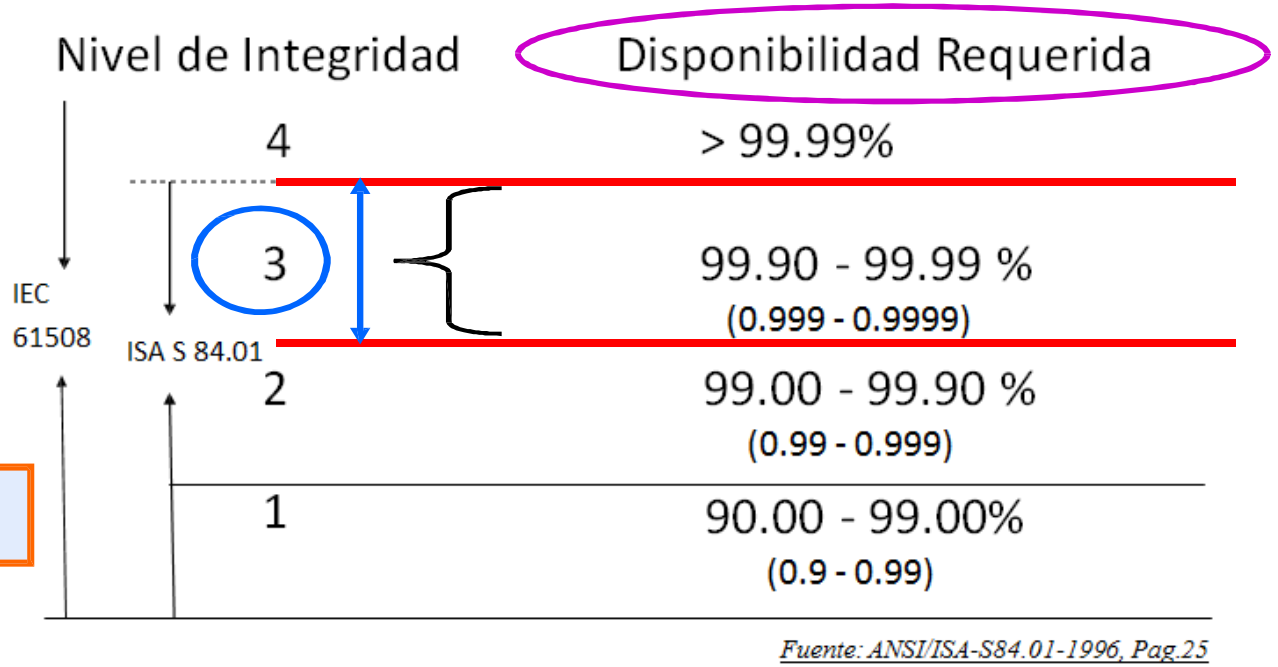
Más sobre el SIL (“Safety Integrity Level”):

SIEMENS

- Es una propiedad de la función de seguridad completa.
- Cada valor corresponde a un rango seleccionado de probabilidad de fallas de la función de seguridad.
- Es una medida cualitativa de la seguridad.
- Es una unidad métrica cuantitativa de la confiabilidad.
- No hay regulaciones que asignen un valor SIL a un proceso particular. No es una medida del riesgo.
- La asignación de SIL es una decisión que debe tomar la empresa.
- Cuanto más alto el nivel SIL, más estrictos son los requerimientos técnicos y administrativos

Safety Integrity Level SIL vs Disponibilidad

Disponibilidad: Probabilidad de estar saludable y poder hacer su tarea



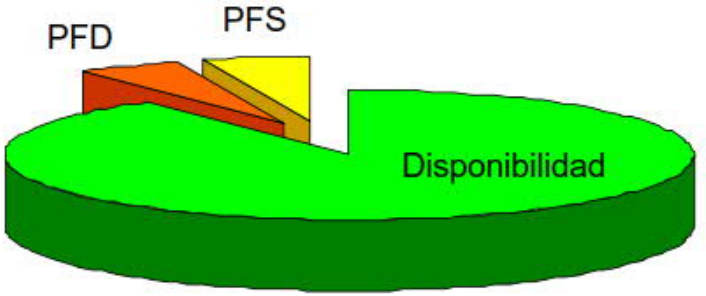
Fuente: ANSI/ISA-S84.01-1996, Pag.25

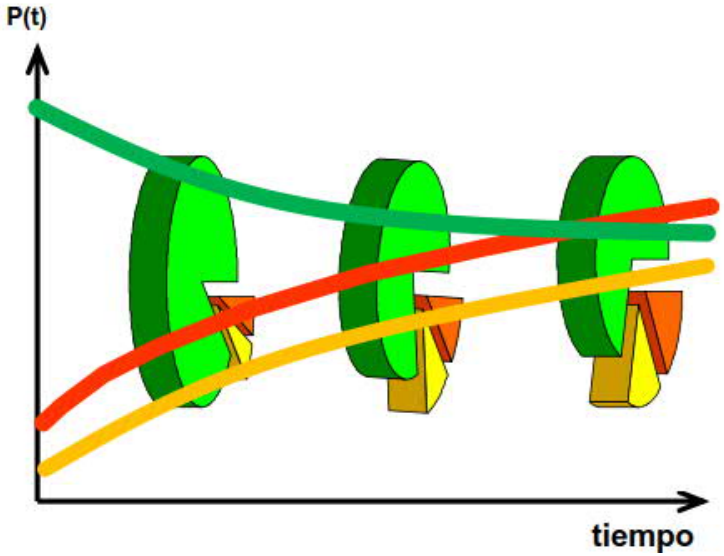
Disponibilidad = 1-PFD
1 - 0.0001 = 0.9999 = 99.99%

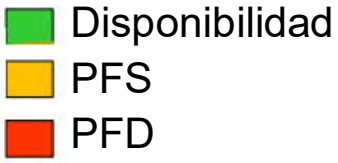
Modos de Falla de los equipos que hacen parte de una SIF

Tipo de falla

- Falla segura (λ_S) : Dispara en falso el sistema
- Falla peligrosa o en demanda (λ_D) : Hace que el sistema no actue







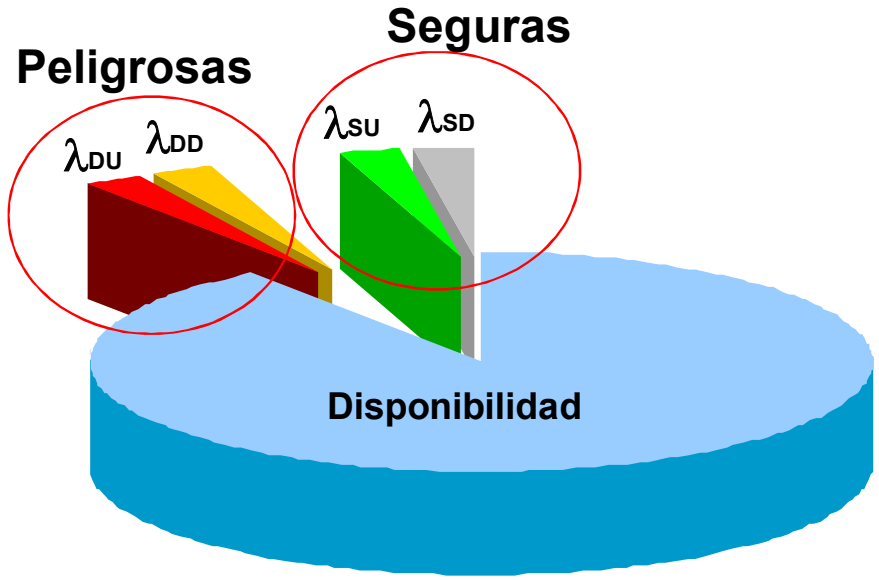
SIEMENS

Tasas de Fallo

- λ_S **(Tasa de todas las fallas "seguras")**
  - λ_{SD} (tasa de todas las fallas "seguras detectadas")
  - λ_{SU} (tasa de todas las fallas "seguras no detectadas")
- λ_D **(Tasa de todas las fallas "peligrosas")**
  - λ_{DD} (tasa de todas las fallas "peligrosas detectadas")
  - λ_{DU} (tasa de todas las fallas "peligrosas no detectadas")

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU}}$$

SFF = Safe Failure Fraction



SFF = Safe Failure Fraction

una medida de la probabilidad de obtener una falla peligrosa que no es detectada por autodiagnóstico automático

Arquitectura y fiabilidad de Hardware
Parámetros de arquitectura: Hardware tolerante a fallas (HFT)

SIEMENS

Hardware tolerante a fallas:

La cantidad de fallas que se pueden tolerar mientras se mantiene la función de seguridad

En este contexto:

Hardware tolerante a fallas N=N + 1 Una falla de Hardware puede resultar en perdida de la función de seguridad relevante

Architecture	Hardware Fault Tolerance
1oo1	0
1oo1D	0
1oo2	1
2oo2	0
2oo3	1
2oo2D	0
1oo2D	1
1oo3	2

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

NOTE A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function

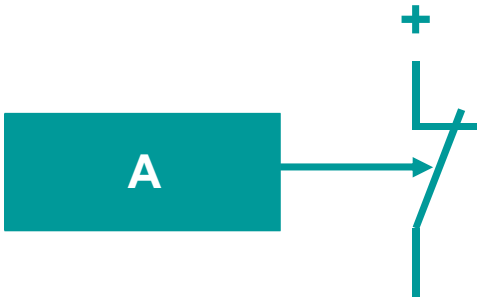
SIEMENS

Sistema de 1 canal (Single Channel):

Esta arquitectura consta de un solo canal, lo que significa que una sola falla peligrosa es suficiente para que la función instrumentada de seguridad sea ineficaz.

Fallo seguro: El contacto del relé se abre e interrumpe el suministro de energía

Falla Peligrosa: e.g. contactos soldados, interrupción del suministro de energía imposible



HFT = 0

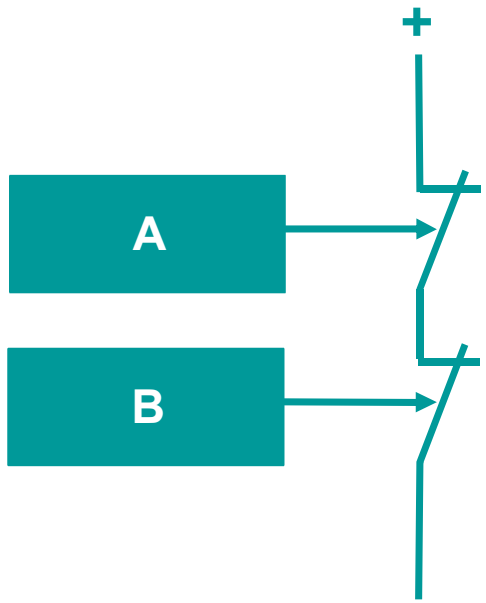
here: “safe” means de-energized

SIEMENS

2-channel (Dual Channel) System:

Salidas cableadas en **serie**.

1oo2:
El sistema necesita solo un canal para realizar la función instrumentada de seguridad.
→ Mayor disponibilidad de seguridad.



HFT = 1

here: “safe” means de-energized

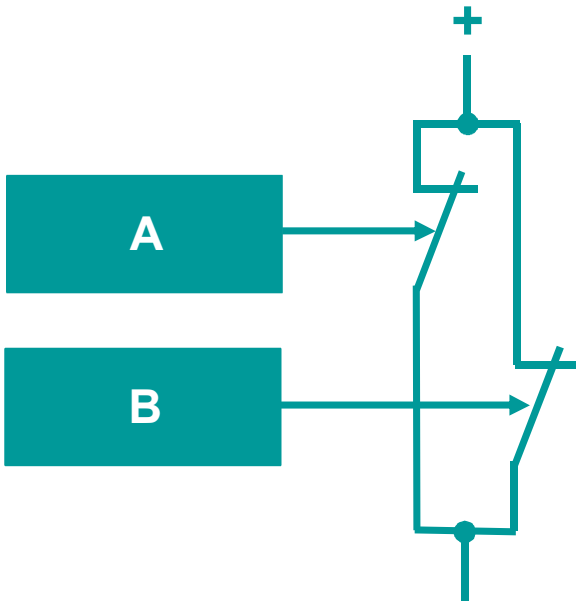
SIEMENS

2-channel (Dual Channel) System:

Salidas Cableadas en **paralelo**.

2 out of 2 (2oo2):
Ambos canales deben estar activados para realizar la función instrumentada de seguridad, es decir, si un canal falla, la función instrumentada de seguridad no puede realizarse.

→ mayor disponibilidad operativa
→ menor disponibilidad de seguridad



HFT = 0

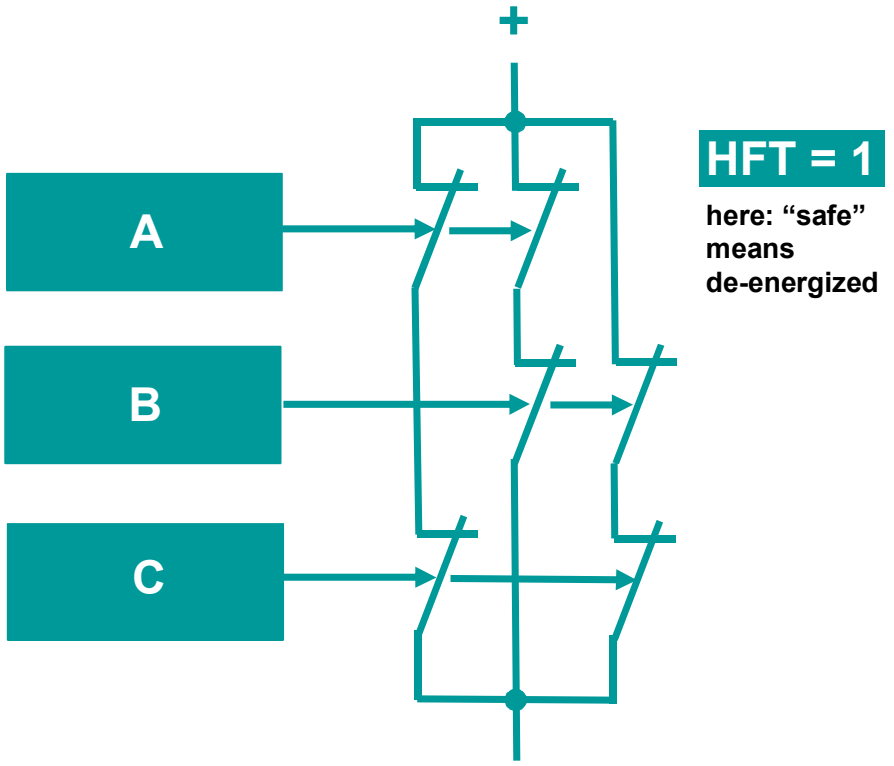
here: “safe” means de-energized

SIEMENS

3-channel (Triplicated) System (TMR):

Se necesitan al menos 2 canales en funcionamiento para realizar la función instrumentada de seguridad
→ mayor disponibilidad operacional

Si un canal falla, la función instrumentada de seguridad todavía se puede realizar
→ mayor disponibilidad de seguridad



SIEMENS

IEC 61508

HFT = 0
SFF > 99%

SIMATIC S7-400F = SIL 3, arquitectura 1oo1.

SIMATIC S7-400FH = SIL 3 2oo2 para el controlador! No votacion 2oo2, es HOT STAND BY 2oo2

Table 3 – Maximum allowable safety integrity level for a safety function carried out by a type B safety-related element or subsystem

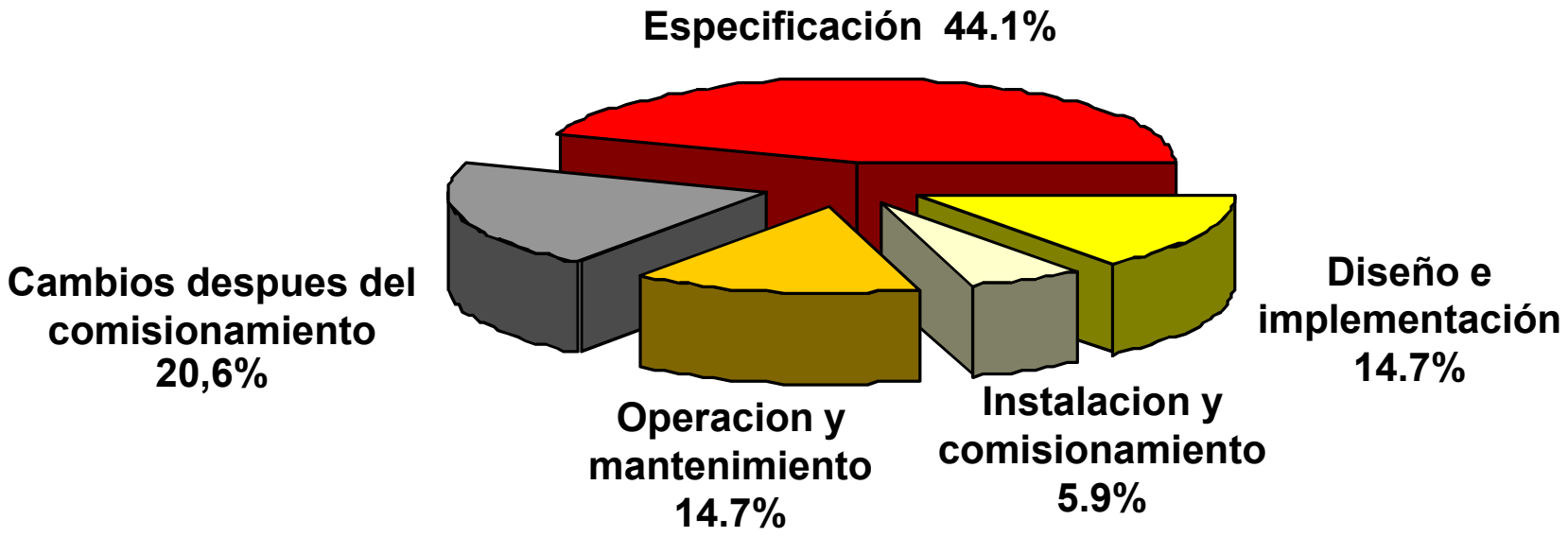
Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
<60 %	Not Allowed	SIL 1	SIL 2
60 % – <90 %	SIL 1	SIL 2	SIL 3
90 % – <99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

SIEMENS

Análisis de Riesgos

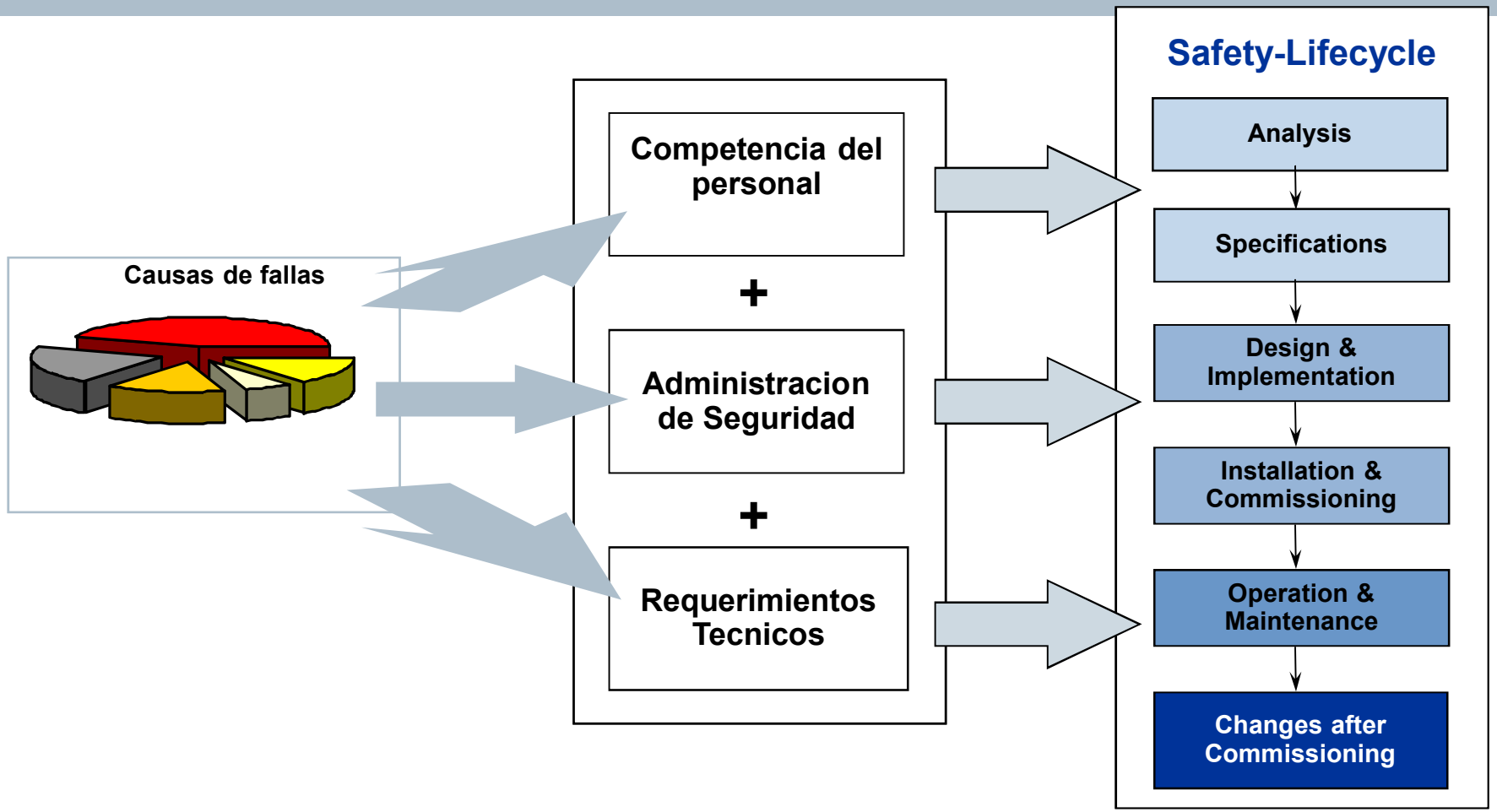
Seguridad funcional para Procesos industriales

Analisis de fallas de los sistemas de automatización

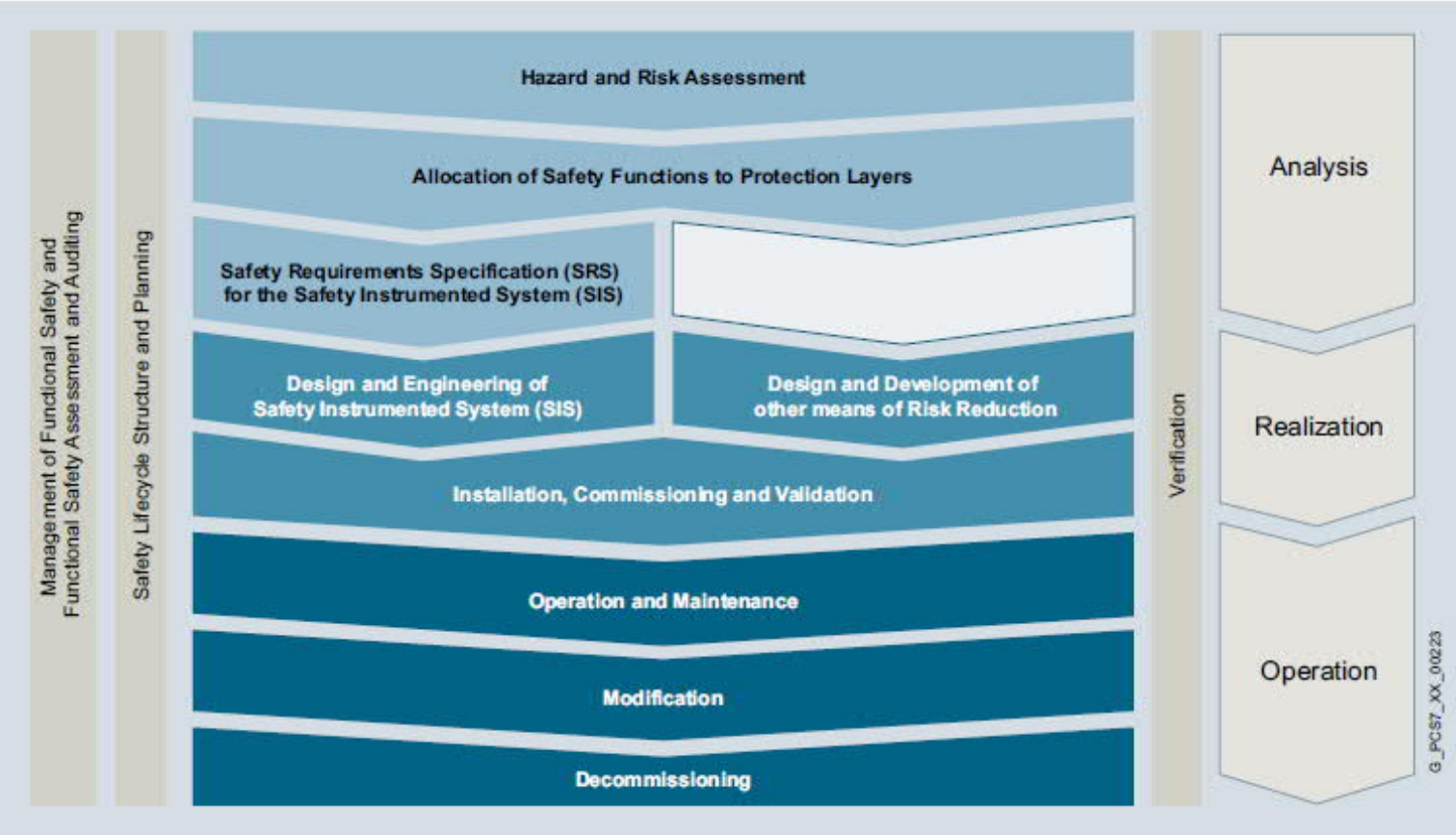


Note : Based on 34 investigated incidents in the UK
Health and Safety Executive (GB): Out of Control. Why control systems go wrong and how to prevent failure. HSE Books

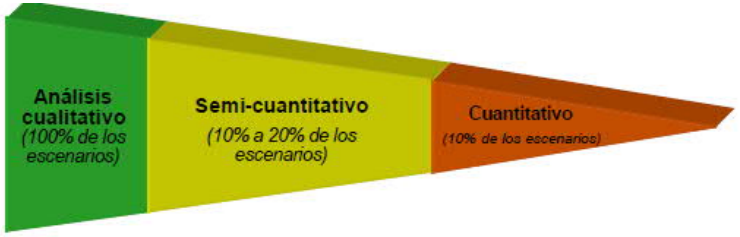
Análisis de fallas



The IEC 61511(ISA S84) Safety Lifecycle



The IEC 61511(ISA S84) Safety Lifecycle



Técnica	HAZOP, Matriz de riesgo	FMEA cuantificado, gráfico de riesgo	LOPA	Árbol de eventos	Árbol de fallas, de eventos, modelos de Markov
Aplicaciones simples	Bueno	Bueno	Bueno	Excesivo	Excesivo
Aplicaciones complejas	Pobre	Pobre	Justo	Justo	Bueno

Process Hazards Analysis

Estudio de Analisis de Riesgo

Obliga a las plantas a garantizar la seguridad de sus operaciones.

1.- HAZOP (HAZard and Operability study).- El mas utilizado, identifica Consecuencias no deseadas y da recomendaciones para mejorar el proceso (Diseño, Procedimientos, etc.)

2.- What if?.- Posibles consecuencias ante un incidente. Ejem. ¿Qué sucedería si la tubería se obstruye?

3.- Checklist Study.- Método directo, rápido y barato.

4.- FMEA (Failure Mode Effects and Diagnostics Analysis).- Detectar las fallas en el equipo de proceso y de control y analizar las consecuencias.

LOPA

Lopa

Initiating event	PL #1	PL #2	PL #3	PL #4	Consequence
Stirrer drive failed	Batch in Operation	Operator Intervention	Pressure high safety shutdown	Pressure relief value	Tolerable risk
			X		Explosion
		0.1			
	0.5				
0.5/yr					
					No consequence

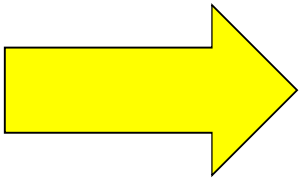
Tolerable risk according to IEC 61511-3 Table C2
PL = Protection Layer

Required PFD ≤ Tolerable risk / Probability of the Event
Example: PFD ≤ $1x10^{-5}$ /(0.5 x 0.5 x 0.1 x 0.07), PFD ≤ 0.006 --> SIL 2

Safety Requirement Specification (SRS)

Safety Requirement Specification

Requirements for the safety function	Requirements for the safety integrity



Todos los requerimientos necesarios para el diseño de funciones instrumentadas de seguridad deben ser especificados

Especificación de Requerimientos de Seguridad ó SRS (SRS)

SIEMENS

Clausula 10 de la IEC61511-1

No de SIF

No de diagrama

Descripción del peligro

Propósito del SIF

Descripción de la acción

Funcionamiento

Función Instrumentada de Seguridad

CESS DESIGN PROCEDURE NO. PD-

F DESCRIPTIONS

Client: ABC Company

Project Title: Area 1 SIS

Emerson Project Number: 1234567

Revision Date: 3/9/2006

SIF No.	P&ID No.	Hazard Description	SIF Purpose	Action Description	Function
SIF # 1	100	Overflow of Process Tank containing flammable materials resulting in ignition of flammable vapors and flash fire, leading to fatality due to exposure to fire.	Prevent overflow of Process Tank, 101.	On high level, close all inlet valves from feed sources greater than 10% of Process Tank volume. (For SIL verification calculations, only one valve is open at a time, even	1oo1 voting by high level switch. 5 sec delay. First out stays on graphic. Single block valve on each inlet gives 1oo1 voting on final elements.
SIF # 2	100	Runaway reaction in Process Tank during charging leads to catastrophic failure of vessel or blowout at pressure that is abnormally high; ignition of flammable vapors results	Prevent charging Chemical B to Process Tank, 101, when contents are too hot.	On high temperature, activate alarm to prompt operator response.	1oo1 voting by temperature sensor. 5 sec delay. First out stays on graphic. Alarm indication to operator to take action.
SIF # 3	100	Runaway reaction in East Tank or West Tank during processing leads to catastrophic failure of vessel or blowout at pressure that is abnormally high; ignition of	Prevent charging Chemical B with heat of reaction greater than Chemical A to Process Tank, 101, sourced from Chemical B weigh tanks, during processing to avoid	Immediately following the completion of Stage 2, close feed valves from any Chemical B with heat of reaction greater than Chemical A.	Active upon completion of Stage 2; inactive after completion of Stage 6. SIS indicates phase and recipe. No delay. First out stays on graphic. Single block valve on each inlet line