Disponibilidad del Proceso y de la Seguridad por medio de la Gestión de la Seguridad Funcional y la Confiabilidad

Gestión SIS - "El equilibrio entre la seguridad y la productividad"

Lic. Ricardo A. Vittoni - **RISKNOWLOGY**

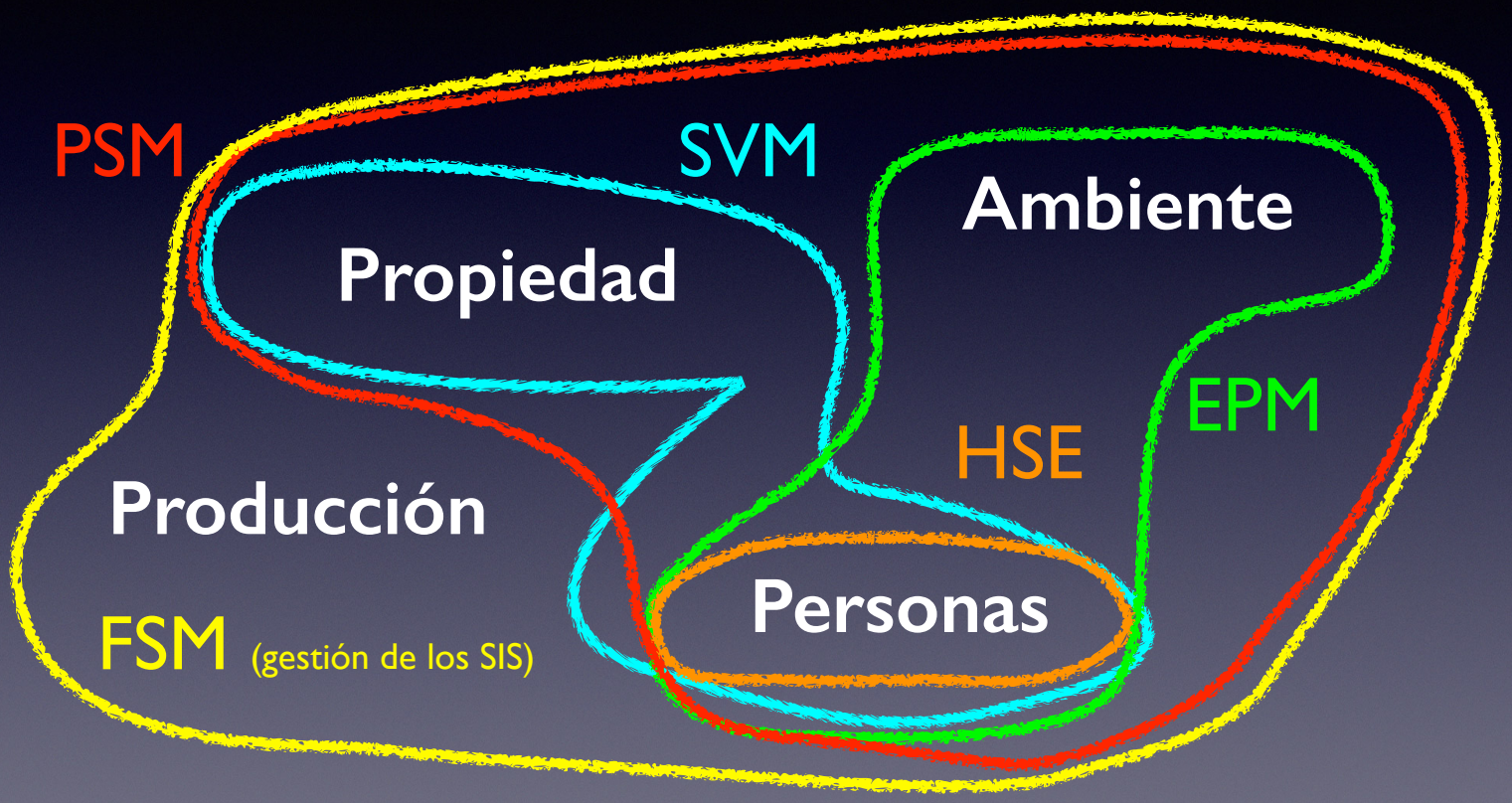
Objetivo

El objetivo de esta presentación es darles una **visión clara** acerca de cómo la apropiada **gestión** de la **seguridad funcional** y de la **confiabilidad** de los **sistemas instrumentados** de **seguridad (SIS)** influencia y ayuda a la **disponibilidad** del **proceso** y de la **seguridad**

¿Qué es Seguridad?

Es un **estado** en el que se está **libre de riesgos inaceptables** para las **personas**, tales como daños a la salud o muerte, ya sea en forma **directa** o **indirecta** como **resultado** de daños a los **activos** o al **ambiente**

¿Cómo se gestiona la Seguridad?



Gestión de los SIS

"El equilibrio entre la seguridad y la productividad"

Pero... ¿qué rol cumple el SIS?

Mitigación

Sistema de respuesta a emergencias

Emergency response layer

Diques y contenciones

Passive protection layer

Válvulas de alivio, discos de ruptura, **Sistemas F&G (SIS)**

Active protection layer

Prevención

ESD SIS (Sistema Instrumentado de Seguridad)

High High Trip
Isolated protection layer
Low Low Trip

Alarmas e intervención del operador

High Alarm
Process control layer
Low Alarm

Sistema de control del Proceso (BPCS o DCS)

High Level
Process control layer
Low Level

Diseño de la Planta y del Proceso

Inherent safe plant design

Nosotros instalamos

SIS

para

proteger

Personas

Ambiente

Propiedad

Pero **NO** instalamos

SIS para que causen **innecesarias**

Paradas de Planta

¿Verdad…?

Queremos

entonces

que el SIS

pero SIN

nos proteja

perder

Producción

Diseño

Mantenimiento

Hardware

Operación

Software

Pruebas

Competencia

Reparación

Instalación

Comisionado

Disponibilidad

Proceso

Seguridad

Análisis de Peligros y Riesgos

Proveedores

Gestión de la Seguridad Funcional

Planificación

Permiso para Operar

Documentación

Compras

Confiabilidad

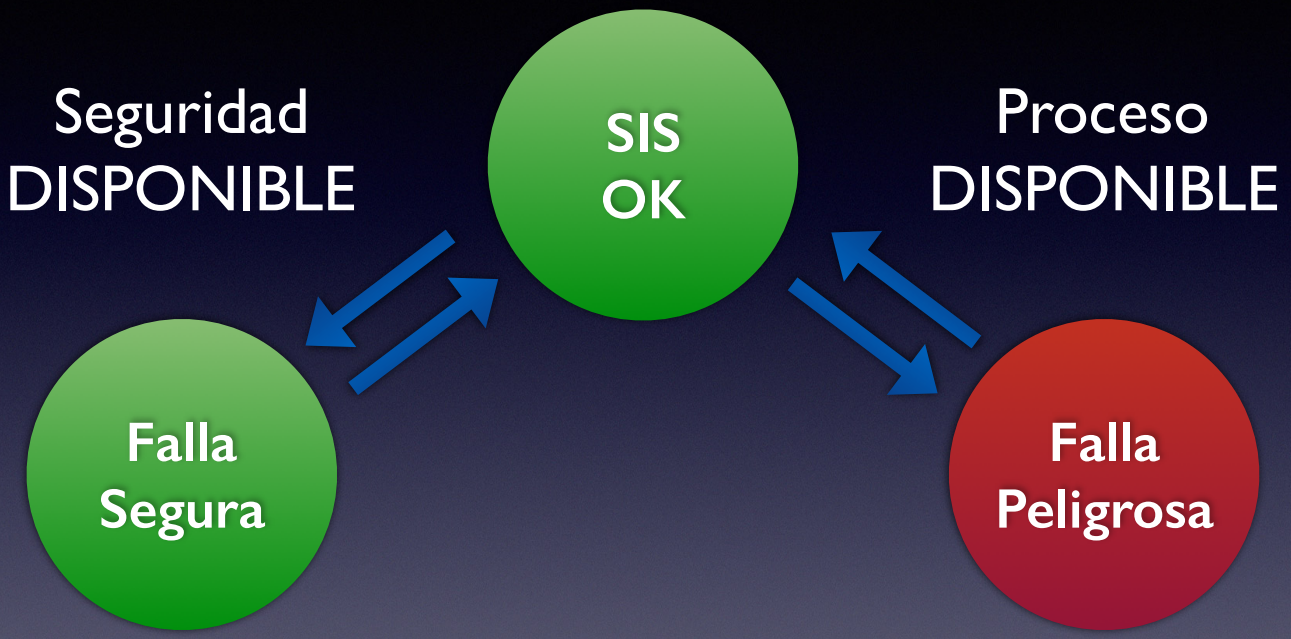
Disponibilidad del Proceso

$\neq$

Disponibilidad de la Seguridad

Pero ambas dependen de las fallas del SIS

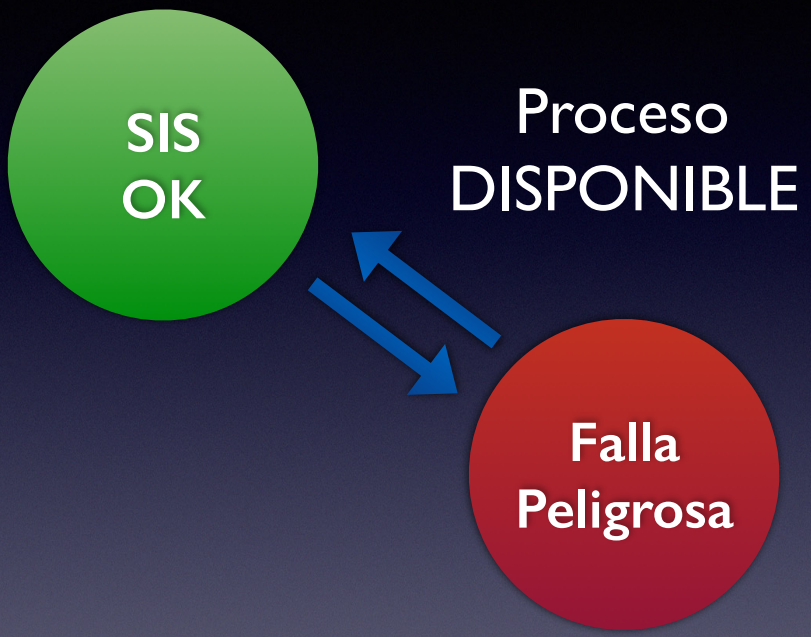
Proceso y Seguridad DISPONIBLES



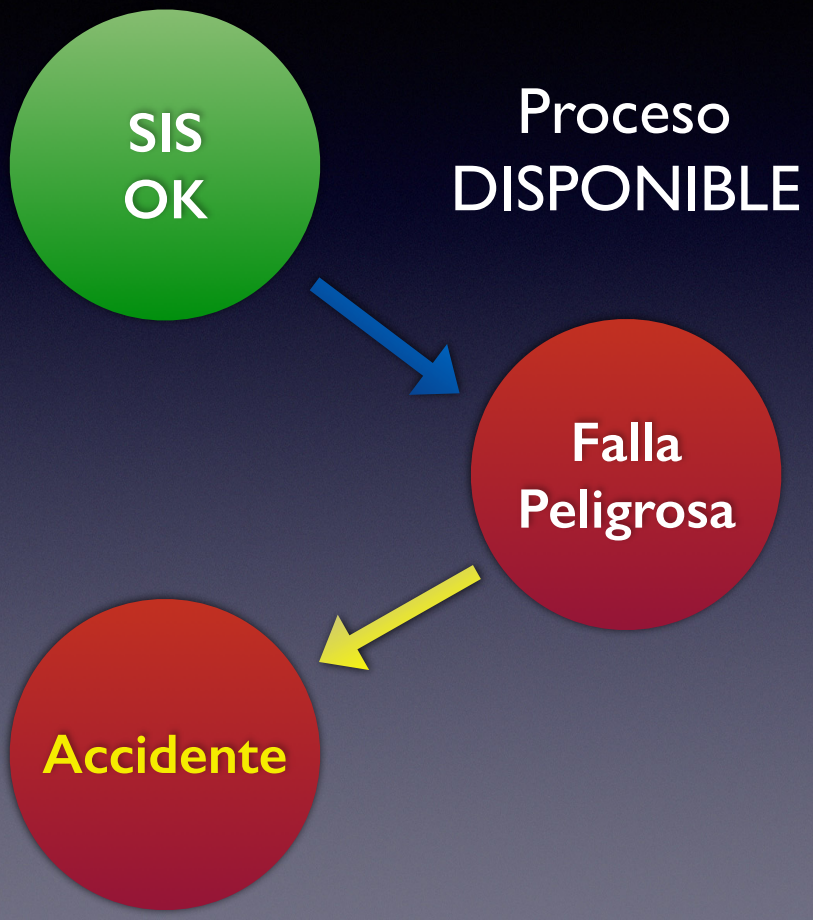
Proceso y Seguridad DISPONIBLES

Seguridad DISPONIBLE

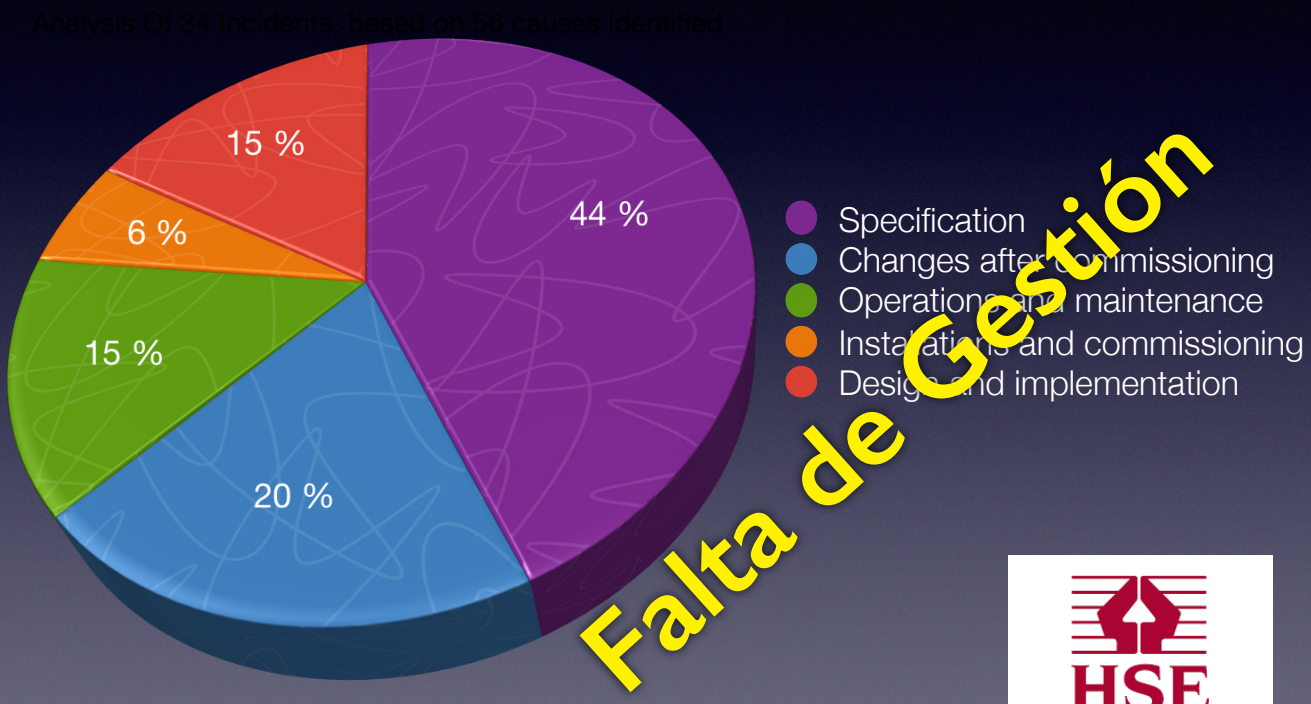
Proceso y Seguridad DISPONIBLES



Proceso y Seguridad DISPONIBLES



¿Por qué hay accidentes?



Falta de Gestión

Out of control: Why control systems go wrong and how to prevent failure?
(2nd edition, source: © Health & Safety Executive HSE – UK)

HSE
Health & Safety Executive

¿Por qué hay accidentes?

- 20% por fallas de inspección
- 12% por operación fuera del margen de diseño
- 9% por fallas en permisos de trabajo
- 7% por fallas en la capacitación y el entrenamiento
- 15% se producen durante el arranque y la parada
- En resumen, por...

Falta de Gestión

Fuente: Aseguradora Liberty, 2009

Veamos un ejemplo...

Falta de
Análisis de Riesgo

Falta de análisis
de Confiabilidad

¿Por qué ocurrió este accidente?

Falta de Gestión de la Seguridad Funcional

Breve cuestionario...

- Seguramente estas señales son muy conocidas por nosotros
  - ¿Pero realmente entendemos para qué están...?

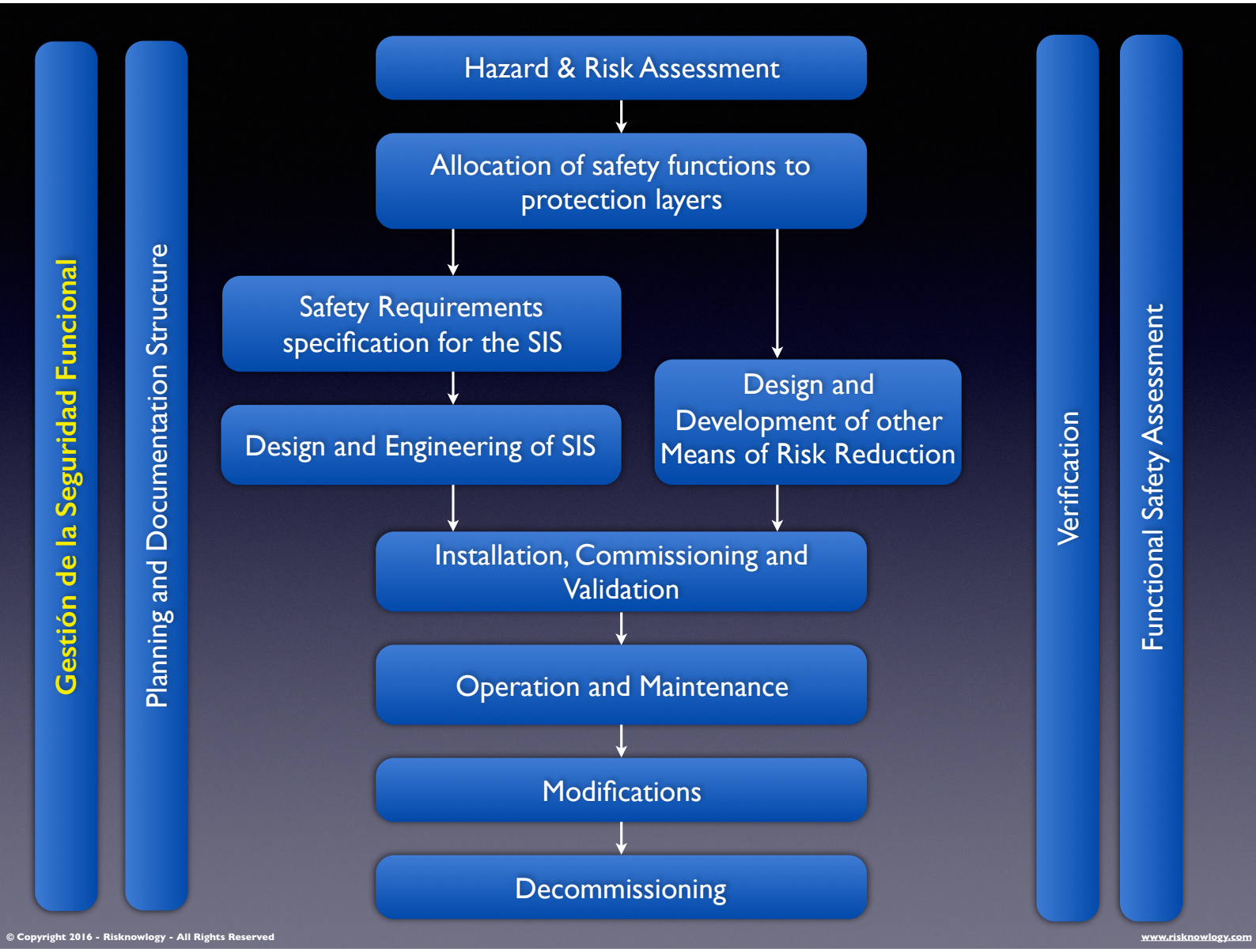
¿Qué es lo que está mal?

Gestión de la Seguridad Funcional

Es implementada por

>75%	de los fabricantes de PLCs de seguridad
30-40%	de los fabricantes de instrumentos
10-15%	de los fabricantes de válvulas
<5%	de los fabricantes de equipos accesorios
<5%	de los integradores de sistemas
0 %	de las empresas de ingeniería
<5%	de los usuarios

Source: Risknowlogy 2010



¿Cumple usted con la Norma?

Gobiernos, compañías de seguro, todos empiezan a hacer esta pregunta...

¿Está usted realizando la Gestión de la Seguridad Funcional?

¿Su trabajo es verificado? ¿Validado? ¿Auditado?

¿Están sus proveedores entregando productos y servicios de seguridad, de acuerdo con los requirimientos de IEC 61508/61511?

¿Cómo sabe si ellos lo están haciendo?

Toda respuesta del tipo "no estoy seguro", "parcialmente", "algunas veces", o simplemente "no" llevará en cualquier momento a la **indisponibilidad** de la **seguridad** y del **proceso**

¡El no cumplimiento cuesta!

¡El no cumplimiento cuesta!

Tolouse, Francia, setiembre 2001, **31 muertos**

Argelia, África, enero 2004, **27 muertos**

Texas, USA, marzo 2005, **15 muertos**

Golfo de México, abril 2010, **17 muertos**

Venezuela, agosto 2012, **39 muertos**

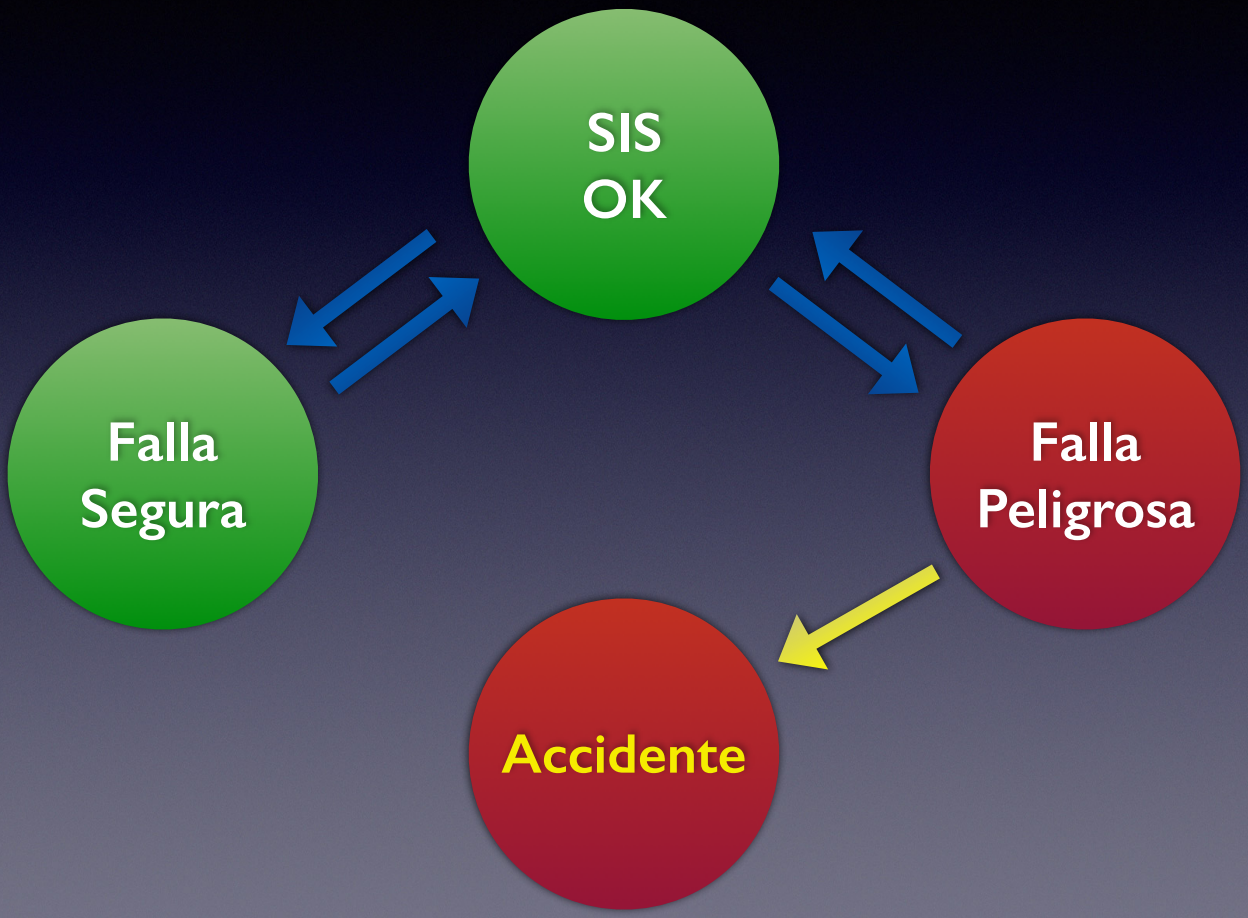
México, setiembre 2012, **26 muertos**

¡El no cumplimiento cuesta!

- Por otro lado, económicamente hablando, los daños a la producción son, muchas veces, mayores que los daños a la propiedad:
  - Pérdida media por evento, en refinerías, USD 120 Millones

Fuente: Aseguradora Liberty, 2009

Igualmente las fallas siempre están…



Pero podemos predecir el comportamiento de un SIS

¡La función de seguridad no trabaja!

Probabilidad de falla en demanda - PFD

Nivel de Integridad de la Seguridad - SIL

Parámetros de Diseño

¡La función de seguridad se ejecuta por sí sola!

Probabilidad de falla segura - PFS

Nivel de Disparo Espurio® - STL

Parámetros de Diseño

Nivel de Integridad de la Seguridad

SIL	PFDavg Low demand	PFH High demand, continuous demand
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

Nivel de Disparo Espurio®

STL	PFSavg Low demand	PFSh High demand, continuous demand
X	$\geq 10^{-(X+1)}$ to $< 10^{-X}$	$\geq 10^{-(X+5)}$ to $< 10^{-(X+4)}$
...	...	...
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

SIL versus STL

	SIL	STL
Conseuencias	Personas, Ambiente, Activos	Pérdida Producción, Paradas
Medida para	Disponibilidad de Seguridad	Disponibilidad del Proceso
Niveles	1 a 4	1 a… ilimitado
Alto nivel significa	Mayor protección	Mayor productividad
¿Basado en riesgo?	Sí	Sí
¿Quién lo especifica?	Usuario	Usuario

Debemos entonces evitar y controlar fallas

Cuanto menos fallas

Más confiabilidad

Para protegernos y para producir

Gestión de la Confiabilidad

Nos ayuda a...

Predecir la conducta de una falla

Monitorear nuestras predicciones

Tomar decisiones sobre la base de esas predicciones

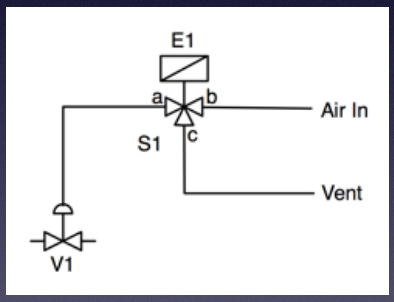
Decisiones Informadas de Confiabilidad

¿Qué significa?

Significa que tomamos conocimiento acerca de la información de confiabilidad del equipamiento, y la usamos para tomar decisiones según diferentes soluciones de diseño.

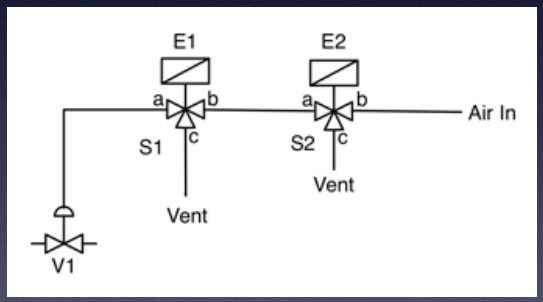
Ejemplo…

¿De qué forma conectaremos las válvulas solenoide: en 1oo1, en 1oo2 o en 2oo2?



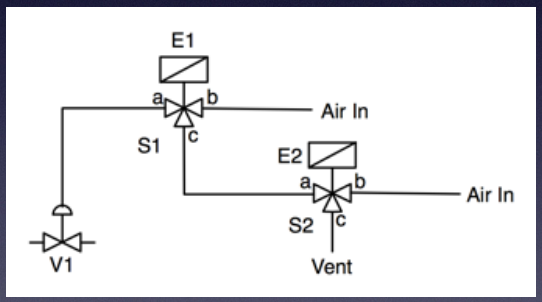
Disponibilidad del Proceso: ⬇

Disponibilidad de la Seguridad: ⬇



Disponibilidad del Proceso: ⬇

Disponibilidad de la Seguridad: ⬆



Disponibilidad del Proceso: ⬆

Disponibilidad de la Seguridad: ⬇

Decisiones Informadas...

Plant information		
Plant operational time	6	Years
Proof test every	6	Years
Proof test coverage	99 %	
Expect a demand every	14	Years
Expected demands	0,4285714	Per plant operational time
Equipment under investigation		
Type	Solenoid	
CAPEX	€5.000,00	Per equipment
OPEX	€200,00	Per equipment per year

Cost safety function not operating on demand (dangerous failure)		
Plant replacement cost	€5.000.000,00	
Loss of production	14	Days
Loss of production	€200.000,00	Per day
Loss of production	€2.800.000,00	Due to safety function not operating on demand
Cost safety function operating without a demand – Trip (safe failure)		
Equipment replacement cost	€500.000,00	
Loss of production (trip)	14	Days
Loss of production (trip)	€200.000,00	Per day
Loss of production (trip)	€2.800.000,00	Per spurious trip

Decisiones Informadas...

OPTION			COST			Probability	Prob. Scenario	Architecture probability
Architecture	Scenario	Equipment	CAPEX	OPEX	Losses	Scenario	Cost	Weighted cost
1oo1	Tripped	1	€5.000,00	€1.200,00	€3.300.000,00	0,000016405	€54,24	€9.257,67
	PFD	1	€5.000,00	€1.200,00	€7.800.000,00	0,000899445	€3.009,11	
	Available	1	€5.000,00	€1.200,00	€0,00	0,99908415	€6.194,32	
1oo2	Tripped	2	€10.000,00	€2.400,00	€3.300.000,00	0,000033627	€111,39	€12.664,47
	PFD	2	€10.000,00	€2.400,00	€7.800.000,00	0,000046017	€154,07	
	Available	2	€10.000,00	€2.400,00	€0,00	0,999920355	€12.399,01	
2oo2	Tripped	2	€10.000,00	€2.400,00	€3.300.000,00	0,000001095	€3,63	€18.513,30
	PFD	2	€10.000,00	€2.400,00	€7.800.000,00	0,001831566	€6.132,40	
	Available	2	€10.000,00	€2.400,00	€0,00	0,998167339	€12.377,28	

En resumen…

Trabajamos con procesos que requieren **capas de protección**

Un SIS el la última frontera, por lo cual **debe funcionar** muy bien

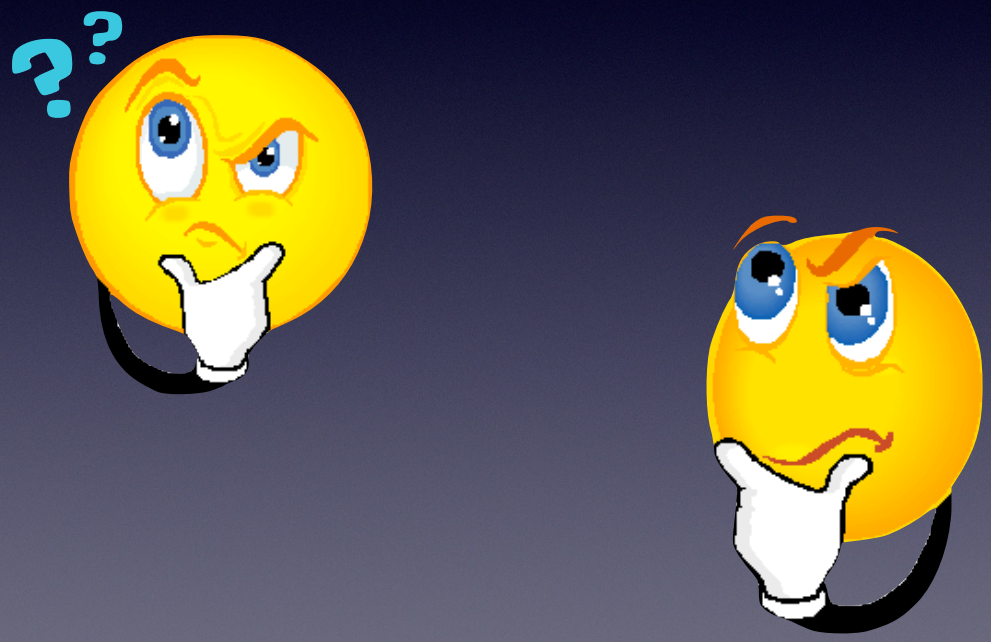
Necesitamos **gestión de la Seguridad Funcional**

Necesitamos **gestión de la Confiabilidad**

Necesitamos tomar **decisiones informadas**

para **proteger** a las personas, al ambiente, a la empresa y a la producción

¿Preguntas?



¡Gracias por su atención!

risknowlogy.com

rar@risknowlogy.com