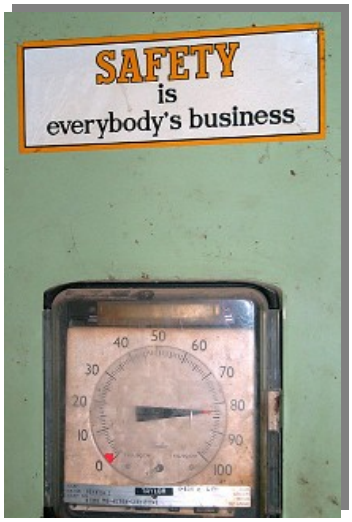
Welcome to PHOENIX CONTACT

Basics of Functional Safety in Process Industry

A practical approach to
IEC 61511 / EN61511 (SIL)



And safety is a life time commitment !!

2 | Basics of Functional Safety in Process Industry | W. Grote

AGENDA

1. **Introduction**
2. **Why do we care for Functional Safety?**
   - Examples of historical accidents in process industry
   - Short overview of standards and regulations
3. **Identification and Quantification of Risks**
   - What is a risk?
   - Risk identification (HAZOP)
   - Risk Analysis
   - How to quantify the risk?
4. **Parameter for SIL-Classification**
   - Types of failure
   - HFT, SFF, PFD, λ, MTBF
   - SIF / SIS
   - SFF Analysis / PFD

3 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

Just one week news from the paper (1)

07.10 Canada 050710-04 Sarnia, Ontario. Suncor Energy Products Inc. A fire broke out but was contained to a process heater in the refinery's naphtha pre-treating unit. ...

07.10 Japan 050710-05 Ehime Prefecture, on the island of Shikoku. Shikoku Electric Power Co Inc. The Ikata Nuclear Power Plant experienced a vapour leak, but the leak was contained and there was no danger of radiation escaping. ..

07.12 USA 050712-06-A Naturita, CO. EnCana Oil & Gas. A natural gas well about 30km (20 miles) west of Naturita leaked, sending gas into the air over southern Colorado, prompting flight restrictions and forcing EnCana to evacuate some of its employees from the area. ...

07.12 USA 050712-09 Ponder, Denton County, TX. Lightning apparently struck a chemical tank at a gas well, starting a fire. ...

4 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

Just one week news from the paper (2)

07.12 USA 050712-13-A North Slope, AK. ConocoPhillips Alaska Inc. A leaky well casing reportedly caused a spill of about 4,000 litres (1,050 US gallons) of diesel fuel and an unknown amount of salty produced water at the Kuparuk oil field. ...

07.12 USA 050712-14 Fort Atkinson, WI. NASCO. According to the Fort Atkinson Fire Chief, petroleum-based products fuelled a fire that destroyed one of two main buildings at a plastics manufacturing plant. ...

07.13 USA 050713-05 Commerce City, CO. Suncor Energy USA. A gasoline leak in an underground pipeline forced the evacuation of a refinery and a wastewater treatment plant. ...

07.13 Mexico 050713-12 Gulf coast port of Coatzacoalcos, in eastern Veracruz state. Pemex. Mexico's state-owned oil company, Pemex, said two researchers were killed in a pipeline explosion. ...

Just one week news from the paper (3)

07.14 China 050714-08 Taiyuan, Shanxi Province. Two people were killed in an oil tanker explosion in a suburban village. ...

07.14 Norway 050714-11 Oslo. Shell. The E18, the main highway leading to Oslo from the west, was closed to all traffic for nearly eight hours after an explosion at a Shell gas station. ...

07.14 Netherlands 050714-14 Rotterdam , Rotterdam. Royal Dutch/Shell. The 416,000 bpd Rotterdam refinery, the largest in Europe and one of the biggest in the world, shut down at 11.00 because of a power outage. ...

07.15 USA 050715-03 Pearland, Brazoria County, TX. A fuel tank caught fire and exploded, possibly after being struck by lightning. ...

07.15 USA 050715-08 Brownsville, TX. Texas Gas Co. A gas leak prompted street closures around the Port of Brownsville, but did not pose any health dangers. ...

67 incidents in 1 week ; this selection petroleum/gas/oil : 13 incidents

What we want to avoid!
Major Incidents

Flixborough, UK 1974

- Chemical plant explosion
- killed 28 people and seriously injured 36
- **Start to change the laws for chemical processes to increase the safety of the industry**

7 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

What we want to avoid!
Major Incidents

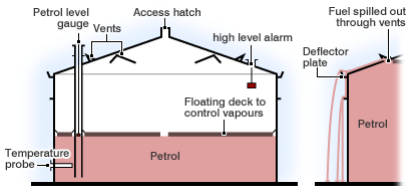
Piper Alpha, UK 1988

- Oil rig explosion and fire
- Killed 167 men. Total insured loss was about £1.7 billion (US$ 3.4 billion)
- Biggest offshore disaster in history
- **15 years after Flixborough, UK 1974!**

8 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

What we want to avoid!
Major Incidents



Buncefield UK, December 2005

- UK's biggest peacetime blaze
- Handled around 2.37 million metric tonnes of oil products a year
- Disaster struck early in the morning when unleaded motor fuel was pumped into storage tank
- **Safeguards on the tank failed** and none of the staff on duty realized its capacity had been reached

9 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

What we want to avoid!
Major Incidents

Texas City, Texas 2005

- Oil refinery explosion
- **The third largest refinery in the U.S.**
- Killed 15 people

10 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

What we want to avoid!

Major Incidents

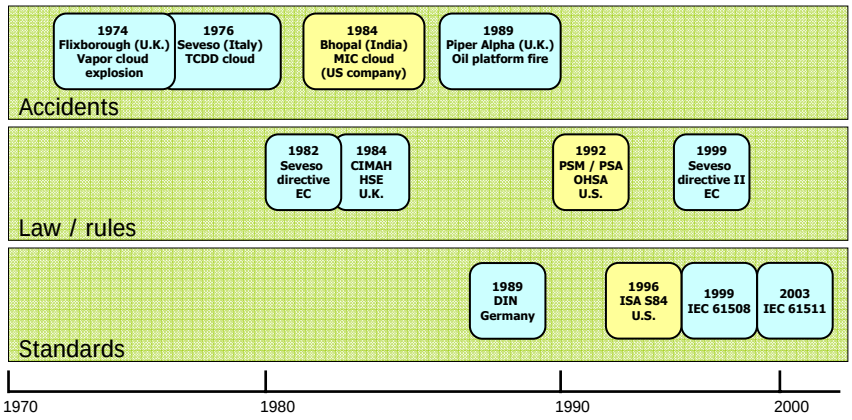
Deepwater Horizon,
Gulf of Mexico, April 2010

Extend of damage:

- HSE;
  - 11 Workers missing
- Economic damage:
  - Sept 2010: 11 Billion $
- Environmental damage:
  - mid June 2010 approximately 5 million barrels of oil spilled

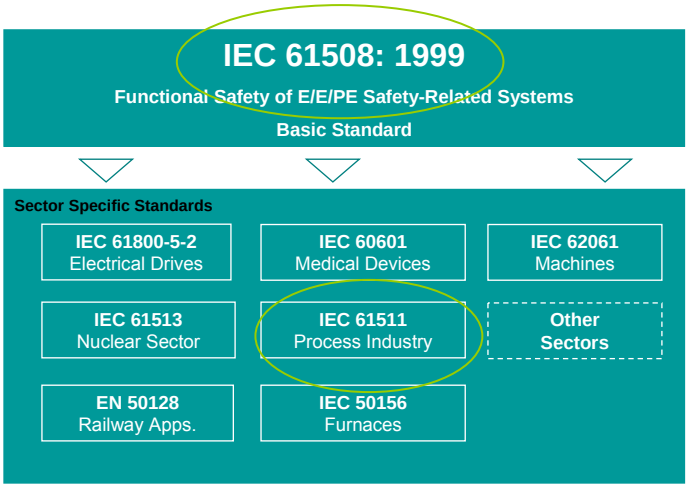
PHOENIX CONTACT INSPIRING INNOVATIONS

History of functional safety standards



PHOENIX CONTACT INSPIRING INNOVATIONS

IEC 61508
and Sector Specific Standards

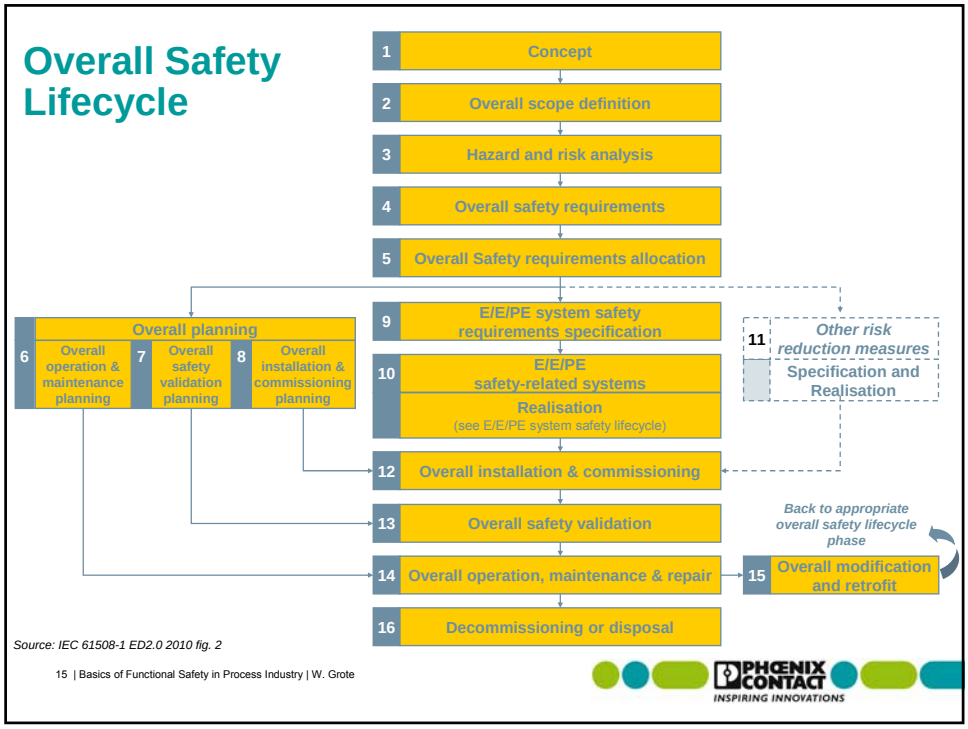


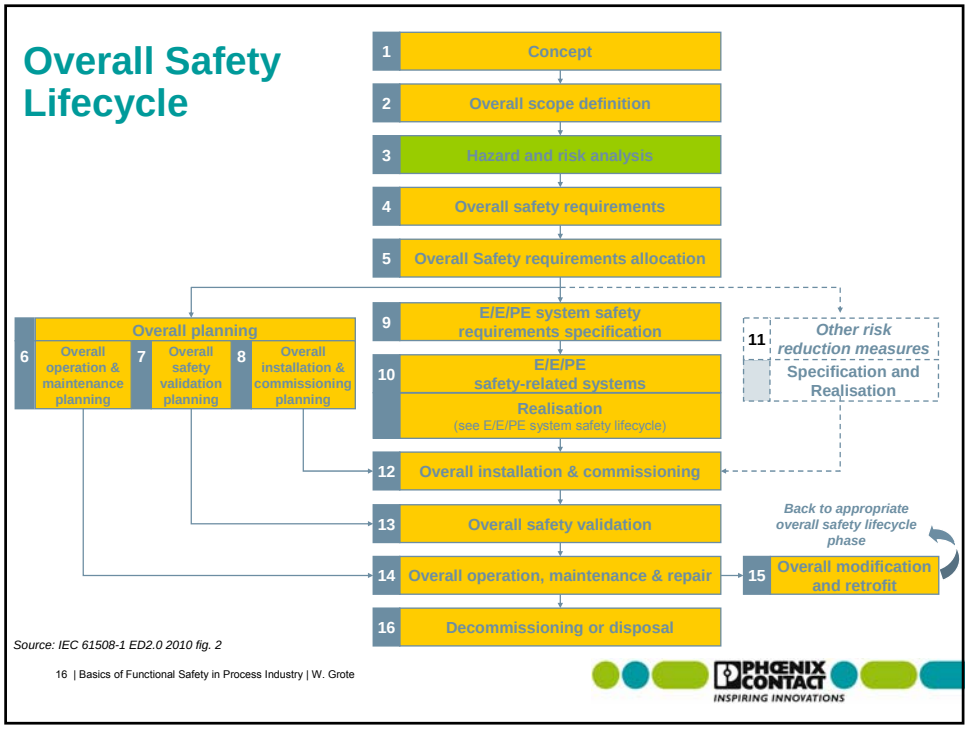
13 | Basics of Functional Safety in Process Industry | W. Grote

AGENDA

1. Introduction
2. Why do we care for Functional Safety?
   - Examples of historical accidents in process industry
   - Short overview of standards and regulations
3. Identification and Quantification of Risks
   - What is a risk?
   - Risk identification (HAZOP)
   - Risk Analysis
   - How to quantify the risk?
4. Parameter for SIL-Classification
   - Types of failure
   - HFT, SFF, PFD, λ, MTBF
   - SIF / SIS
   - SFF Analysis / PFD

14 | Basics of Functional Safety in Process Industry | W. Grote


Overall Safety Lifecycle
1 Concept
2 Overall scope definition
3 Hazard and risk analysis
4 Overall safety requirements
5 Overall Safety requirements allocation
6 Overall planning
Overall operation & maintenance planning
7 Overall safety validation planning
8 Overall installation & commissioning planning
9 E/E/PE system safety requirements specification
10 E/E/PE safety-related systems
Realisation
(see E/E/PE system safety lifecycle)
11 Other risk reduction measures
Specification and Realisation
12 Overall installation & commissioning
13 Overall safety validation
14 Overall operation, maintenance & repair
15 Overall modification and retrofit
Back to appropriate overall safety lifecycle phase
16 Decommissioning or disposal
Source: IEC 61508-1 ED2.0 2010 fig. 2
15 | Basics of Functional Safety in Process Industry | W. Grote
PHOENIX CONTACT
INSPIRING INNOVATIONS


Overall Safety Lifecycle
1 Concept
2 Overall scope definition
3 Hazard and risk analysis
4 Overall safety requirements
5 Overall Safety requirements allocation
6 Overall planning
Overall operation & maintenance planning
7 Overall safety validation planning
8 Overall installation & commissioning planning
9 E/E/PE system safety requirements specification
10 E/E/PE safety-related systems
Realisation
(see E/E/PE system safety lifecycle)
11 Other risk reduction measures
Specification and Realisation
12 Overall installation & commissioning
13 Overall safety validation
14 Overall operation, maintenance & repair
15 Overall modification and retrofit
Back to appropriate overall safety lifecycle phase
16 Decommissioning or disposal
Source: IEC 61508-1 ED2.0 2010 fig. 2
16 | Basics of Functional Safety in Process Industry | W. Grote
PHOENIX CONTACT
INSPIRING INNOVATIONS

What is a Hazardous Situation?

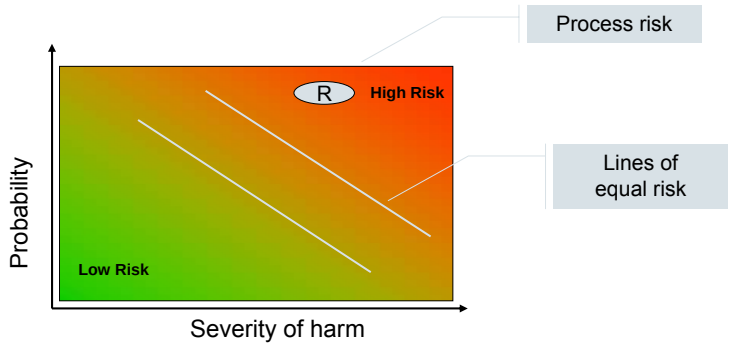
A hazardous situation can be caused by a potential source of danger.

17 | Basics of Functional Safety in Process Industry | W. Grote

What is a Risk?

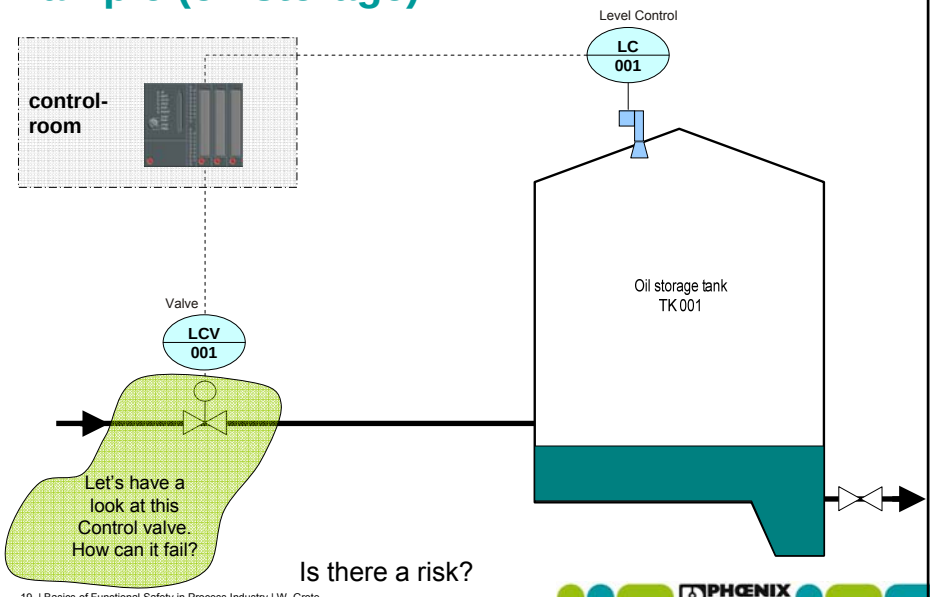
Combination of the probability of occurrence of harm and the severity of that harm.

(IEC 61508-4, 3.1.6)



18 | Basics of Functional Safety in Process Industry | W. Grote

Example (oil storage)



19 | Basics of Functional Safety in Process Industry | W. Grote

Failure modes of control valve

Failure	Consequence
Sticky	Loss of control
Cavitation	Damage
Passing	Integrity HSE
Leaking gland	Spill small HSE
Noise	Damage valve
Corrosion	Major leak
Closing	Spurious Trip (random error)
Not closing	Hazard (HSE)
…	…

20 | Basics of Functional Safety in Process Industry | W. Grote

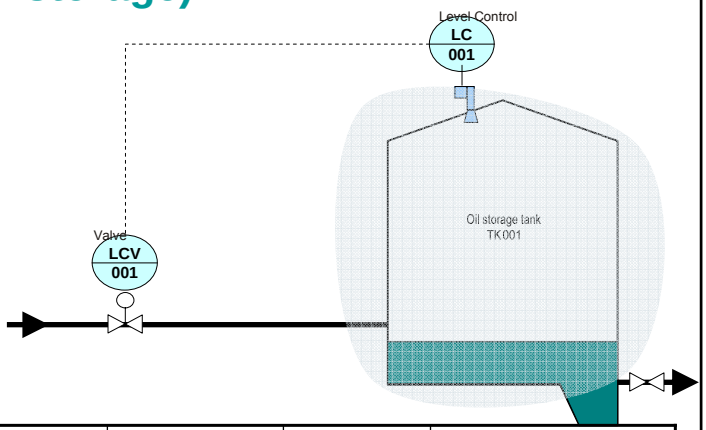
Examples for deviation

Guideword +	Parameter =	Deviation
No	amount / flow	No flow
High	pressure	High pressure
Low	level	Low level
High	temperature	High temperature
…	…	…

Guideword + Parameter = Deviation

21 | Basics of Functional Safety in Process Industry | W. Grote

Example (oil storage)

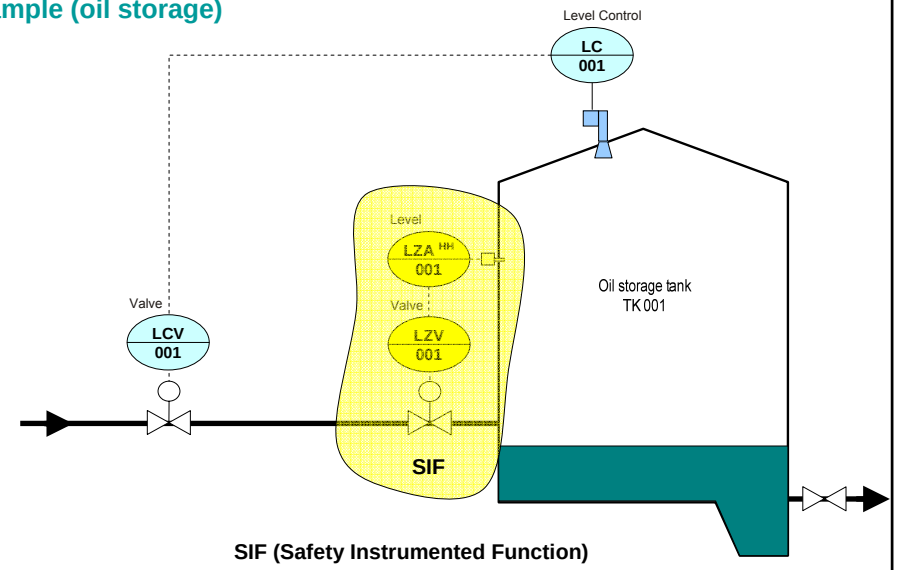


No	Guideword	Deviation	Reason	Effect/Impact	Take action
1.	High	High level	Stuck open	High Level	High level protection
2.	High	High level	Defective level control	High Level	High level protection

22 | Basics of Functional Safety in Process Industry | W. Grote

Result, HAZOP for High Level protection

Example (oil storage)



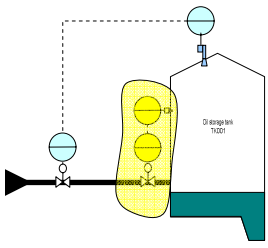
SIF (Safety Instrumented Function)

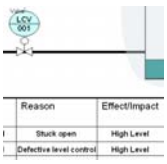
PHOENIX CONTACT INSPIRING INNOVATIONS

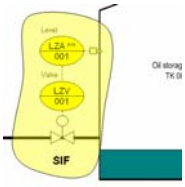
What is a HAZOP - Analysis?

- **HAZOP (Hazard and operability):**

- **Prognosis**
  - **Locating**
    - **Estimation**
      - **Counteractions**

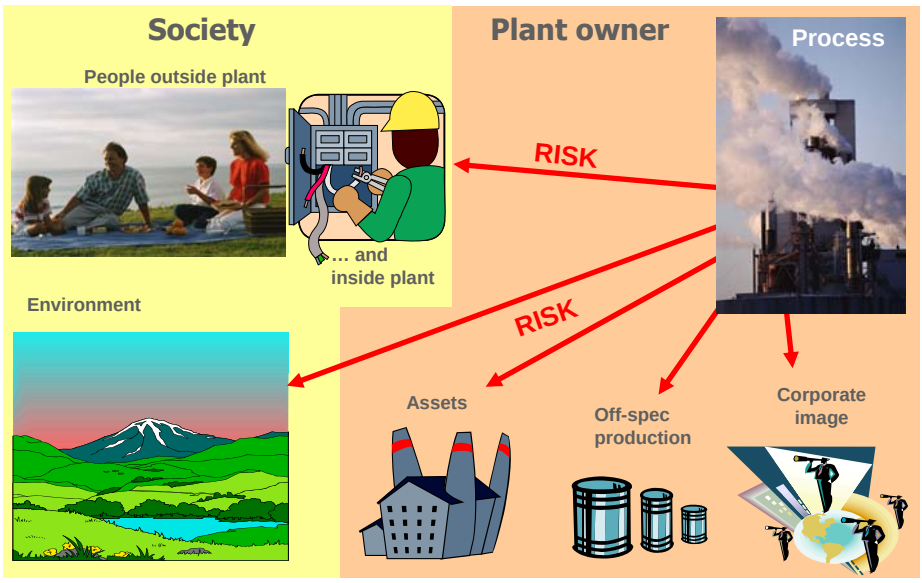






PHOENIX CONTACT INSPIRING INNOVATIONS

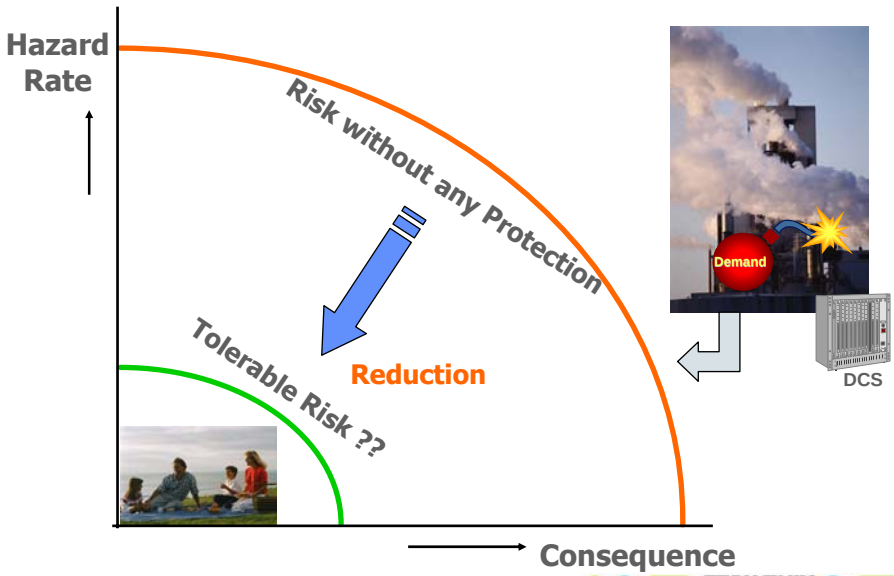
What has to be protected ?



25 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

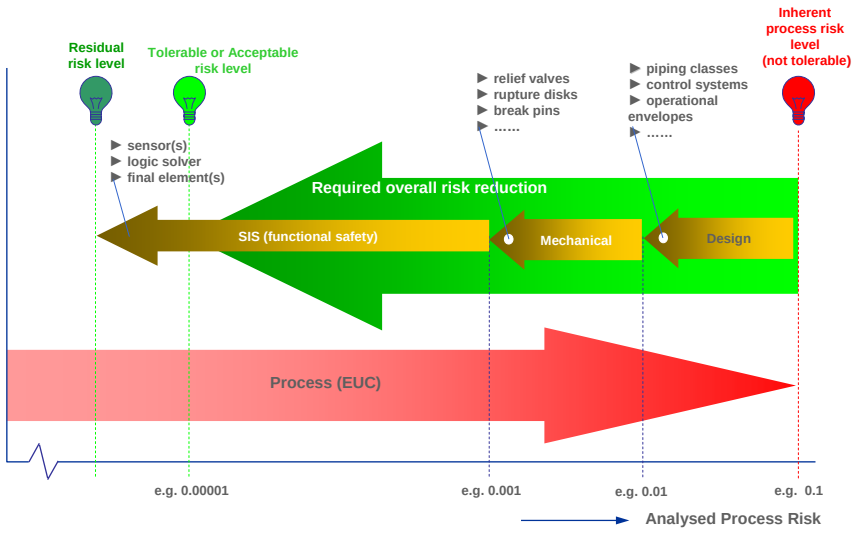
Risk Reduction



26 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

Process risk

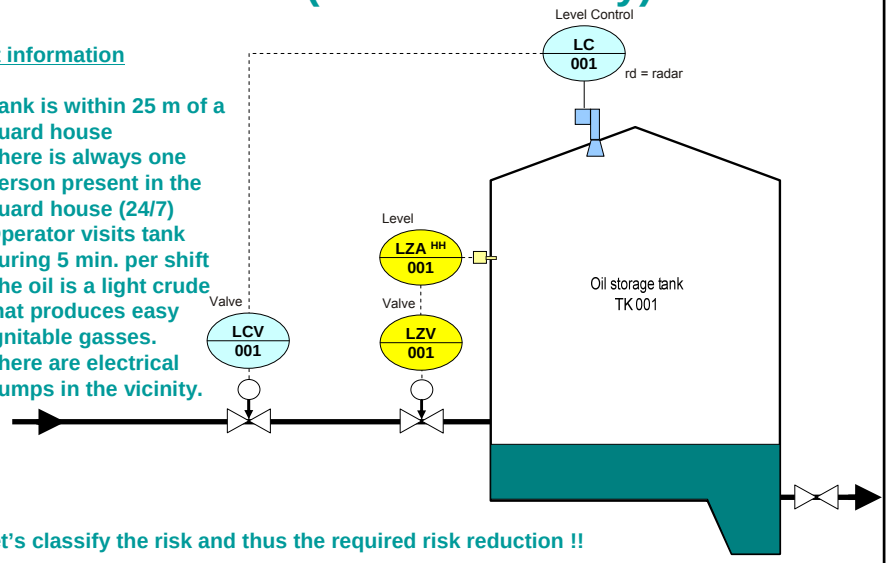


27 | Basics of Functional Safety in Process Industry | W. Grote

SIL classification (Personal Safety)

Plant information

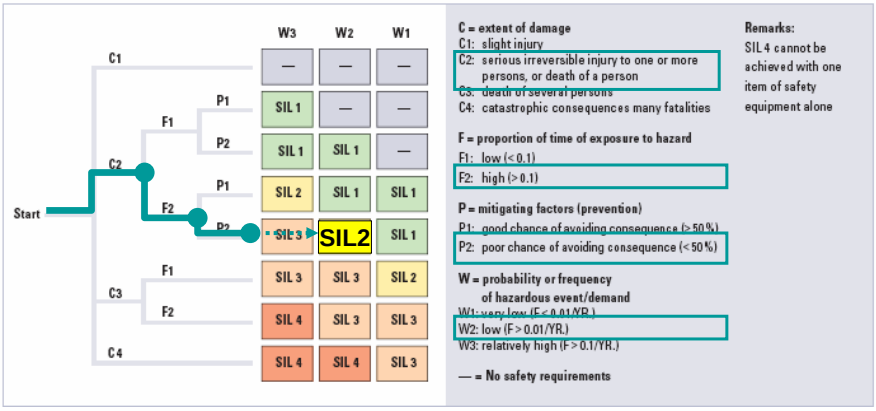
- Tank is within 25 m of a guard house
- There is always one person present in the guard house (24/7)
- Operator visits tank during 5 min. per shift
- The oil is a light crude that produces easy ignitable gasses.
- There are electrical pumps in the vicinity.



Let's classify the risk and thus the required risk reduction !!

28 | Basics of Functional Safety in Process Industry | W. Grote

Risk graph



Risk graph for injury to persons in accordance with IEC 61508 / IEC 61511

What is SIL?

IEC 61511/61508 describes four safety levels that describe the measures for handling risks from plants or plant components.

The Safety Integrity Level (SIL) is a relative measure of the probability that the safety system can correctly provide the required safety functions for a given period of time.

The higher the safety integrity level (SIL), the greater the reduction of the risk.

Safety Integrity Levels (SIL)

Demand mode	
SIL **Safety Integrity Levels**	**RRF** **Risk reduction factor**
SIL 1	**100 to 10**
SIL 2	**1000 to 100**
SIL 3	**10000 to 1000**
SIL 4	**100000 to 10000**

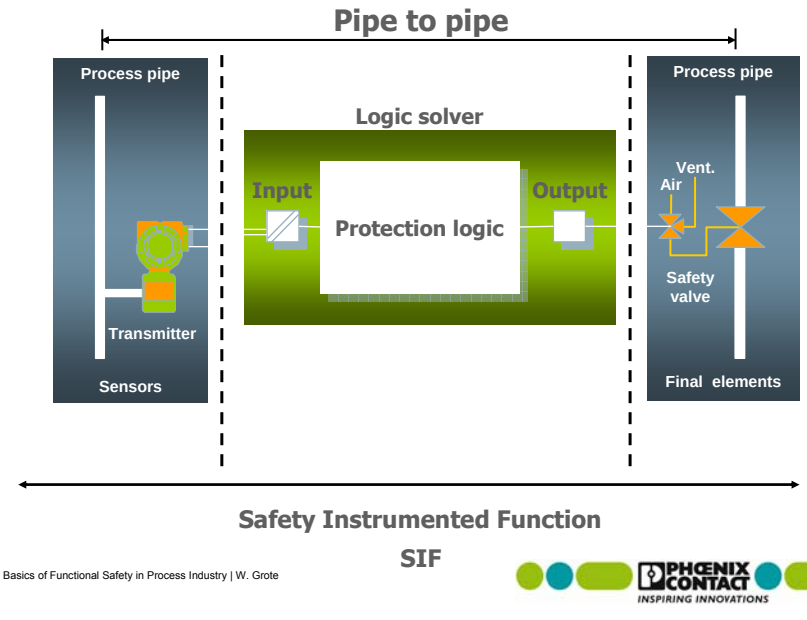
Through the SIL level we define how good the safety instrumented function (SIF) has to be !!

The SIL level is defined for the total set of components of the safety instrumented function (SIF).

31 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

Pipe to pipe



32 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

AGENDA

1. Introduction
2. Why do we care for Functional Safety?
   - Examples of historical accidents in process industry
   - Short overview of standards and regulations
3. Identification and Quantification of Risks
   - What is a risk?
   - Risk identification (HAZOP)
   - Risk Analysis
   - How to quantify the risk?
4. **Parameter for SIL-Classification**
   - Types of failure
   - HFT, SFF, PFD, λ, MTBF
   - SIF / SIS
   - SFF Analysis / PFD

33 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

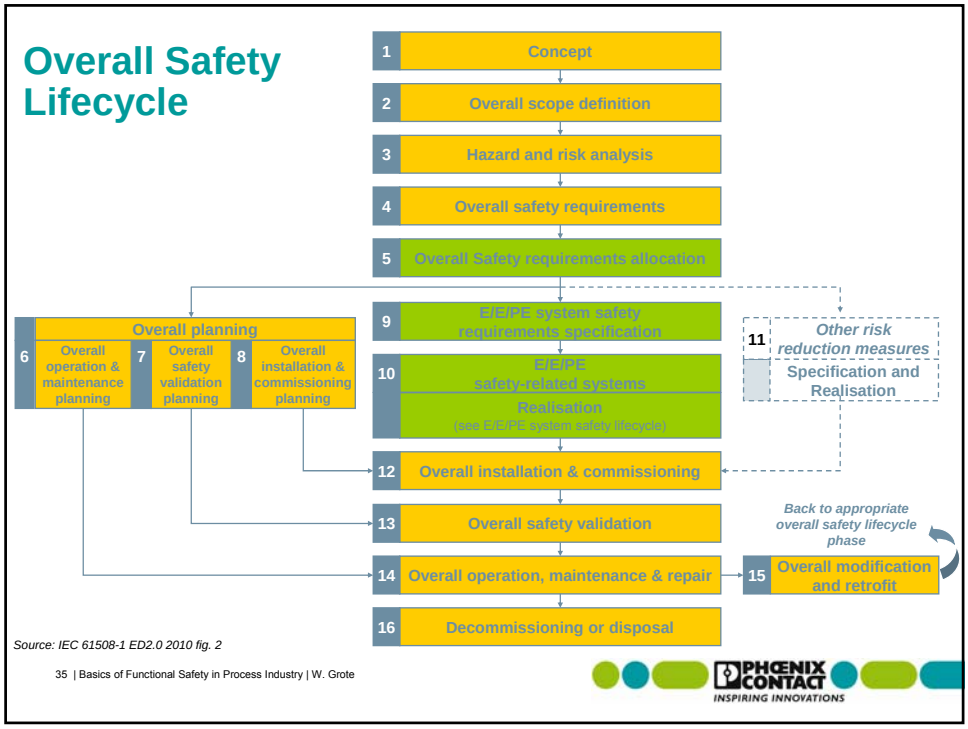
Types of Failure

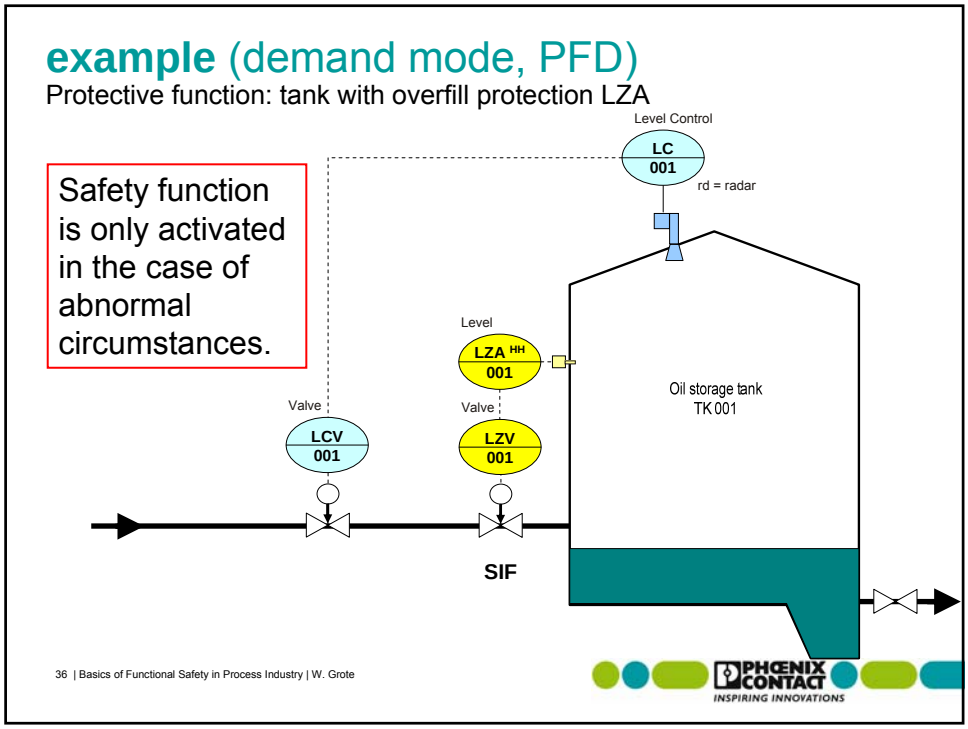
Two reasons for the loss of the safety function:

- **Systematic failure (controllable), for example:**
  - measurement range wrong
  - Sensor/ Actuator off permitted operating temperature
  - wrong Sensor for the medium
- **Random failure (uncontrollable), for example:**
  - Hardware failure
  - Failure of sensor

34 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS


Overall Safety Lifecycle
1 Concept
2 Overall scope definition
3 Hazard and risk analysis
4 Overall safety requirements
5 Overall Safety requirements allocation
6 Overall planning
Overall operation & maintenance planning
7 Overall safety validation planning
8 Overall installation & commissioning planning
9 E/E/PE system safety requirements specification
10 E/E/PE safety-related systems
Realisation
(see E/E/PE system safety lifecycle)
11 Other risk reduction measures
Specification and Realisation
12 Overall installation & commissioning
13 Overall safety validation
Back to appropriate overall safety lifecycle phase
14 Overall operation, maintenance & repair
15 Overall modification and retrofit
16 Decommissioning or disposal
Source: IEC 61508-1 ED2.0 2010 fig. 2
35 | Basics of Functional Safety in Process Industry | W. Grote
PHOENIX CONTACT
INSPIRING INNOVATIONS


example (demand mode, PFD)
Protective function: tank with overfill protection LZA
Safety function is only activated in the case of abnormal circumstances.
Level Control
LC 001
rd = radar
Level
LZA HH 001
Valve
LCV 001
Valve
LZV 001
Oil storage tank TK 001
SIF
36 | Basics of Functional Safety in Process Industry | W. Grote
PHOENIX CONTACT
INSPIRING INNOVATIONS

HFT (Hardware Fault Tolerance)

Dangerous fault tolerance level :

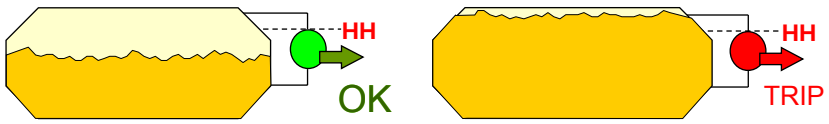
- **HFT = 0** 1 channel:
  one mistake means the loss of safety
- **HFT = 1** Redundant version:
  works in presence of 1 fault
- ...

37 | Basics of Functional Safety in Process Industry | W. Grote

Safety Instrumented Function

(Definition Dangerous Failure)

NO Fail



Dangerous Failure

38 | Basics of Functional Safety in Process Industry | W. Grote

Demands from IEC standards:

1. Hardware Fault Tolerance
2. Safe Failure Fraction

PHOENIX CONTACT INSPIRING INNOVATIONS

Demands on the system architecture

(acc. – IEC 61511)

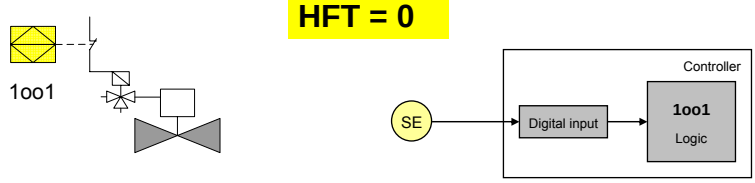
Requirement for the sensors, actuators, non-progr. Logic Systems (solvers)

SIL	minimum hardware fault tolerance
1	0
2	1
3	2
4	It sets out specific requirements. See IEC 61508

PHOENIX CONTACT INSPIRING INNOVATIONS

Fault Tolerance
Example Sensor 1oo1

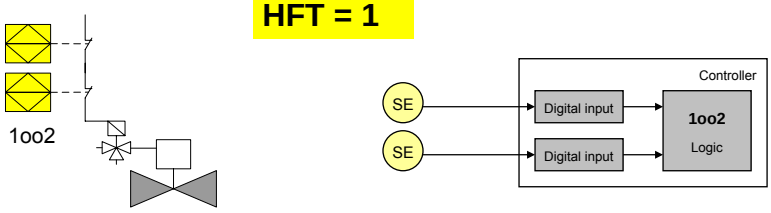
HFT = 0



- 1oo1 – The reaction is triggered and the sensor detects a dangerous state. (no Dangerous Fault Tolerance requirement)
- High probability of a dangerous failure

Fault Tolerance
Example Sensor 1oo2

HFT = 1

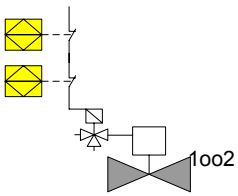


- 1oo2 – The reaction is triggered when one of the two sensors detects a dangerous state. (DFT – Dangerous Fault Tolerance)
- Significant reduction of the probability of a dangerous defect

Hardware Fault Tolerance (HFT)

Example:

In a system with a hardware fault tolerance of 1, where the failure of a component, given the proper function of security remain.



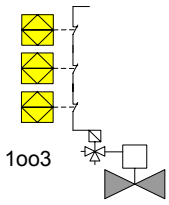
1oo2

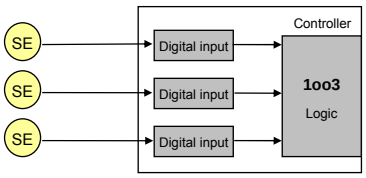
Definition: Voting
How many sensors or subsystems do I need to reach a safe condition?

Fault Tolerance

Example Sensor 1oo3

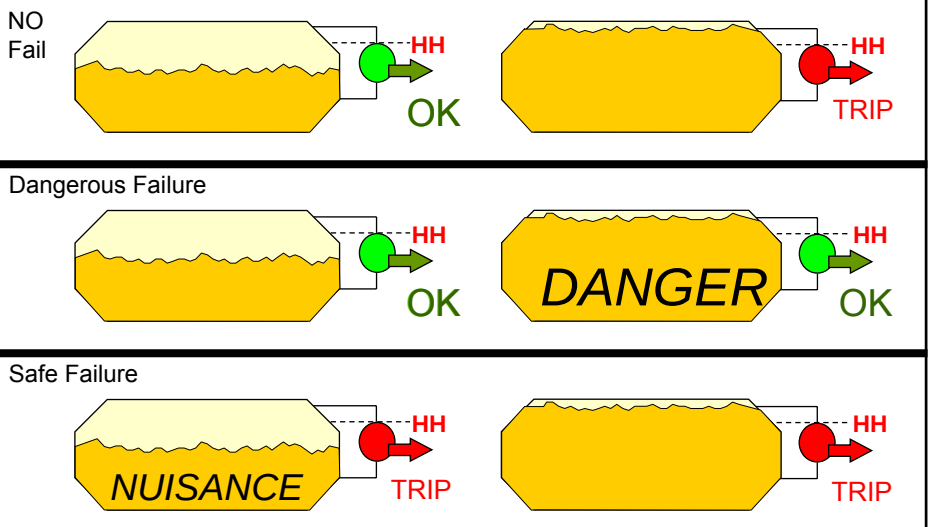
HFT = 2





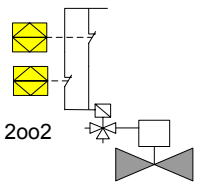
- 1oo3 – The reaction takes place when one of the three sensors detect a dangerous condition. (DFT – Dangerous Fault Tolerance)
- Very high reduction of the probability of a dangerous failure

Safety Instrumented Function
(Definition Dangerous & Safe Failure))

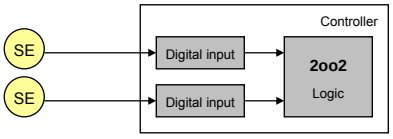


45 | Basics of Functional Safety in Process Industry | W. Grote

Fault Tolerance
Example Sensor 2oo2



HFT = 0

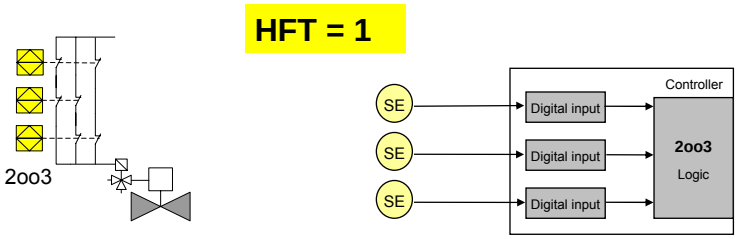


- 2oo2 - The reaction takes place when both sensors detect a dangerous condition. (SFT – Safe Fault Tolerance)
- Lower probability of a random error (spurious trip), which means we have a higher availability of the plant
- Higher probability of a dangerous failure

46 | Basics of Functional Safety in Process Industry | W. Grote

Fault Tolerance

Example Sensor 2oo3



- 2oo3 – The reaction takes place when two of the three sensors detect a dangerous condition. (DFT & SFT)
- Significant reduction of the probability of a dangerous defect (has an error tolerance of 1)
- Lower probability of a random error (spurious trip)

Summary “Architectural constraints”

Hardware Fault Tolerance (HFT)

- A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function.
- is a measure of redundancy
- is determined for each sub-system (each component)
- the weakest link of a subsystem determines the fault

The voting is defined as follows

- The number of paths (N), which is the sum of the redundant paths (M) are required to run the safety function.
- Frequently referred to as NooM or XooY
- Examples 1oo2, 2oo3, 2oo4, etc.

Examples fault tolerance requirements

Dangerous fault tolerance level:

HFT=0: 1oo1 (no DFT requirement), 2oo2, 3oo3, 4oo4, 5oo5

HFT=1: 1oo2, 2oo3, 3oo4, 4oo5 (works in presence of 1 fault)

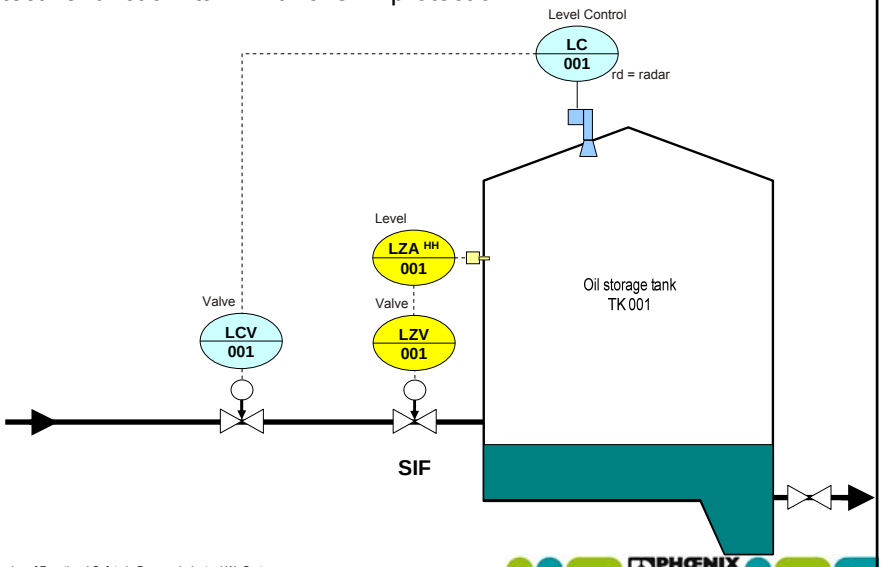
HFT=2: 1oo3, 2oo4, 3oo5, 4oo6 (works in presence of 2 faults)

The following systems are **Safe Fault Tolerant**:

2oo2, 2oo3, 3oo3, 2oo4, 3oo4, 4oo4, 2oo5, 3oo5, 4oo5, 5oo5, etc.

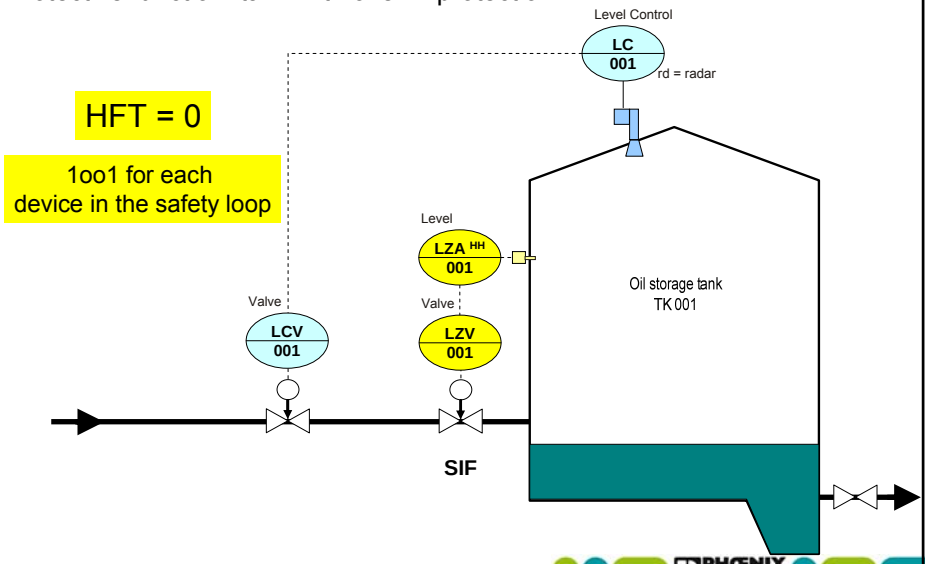
example (demand mode)

Protective function: tank with overfill protection LZA



example (demand mode)

Protective function: tank with overfill protection LZA



51 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

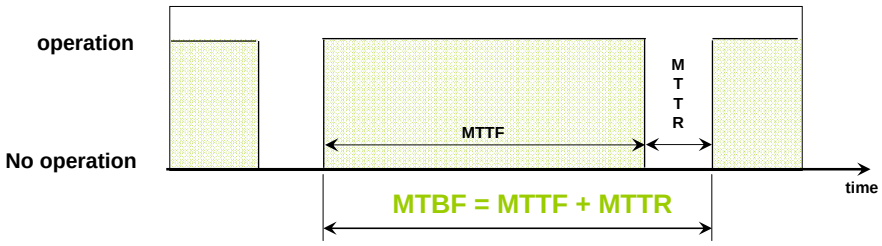
Demands from IEC standards:

1. Hardware Fault Tolerance
2. Safe Failure Fraction

52 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

Mean Time Between Failures (MTBF)



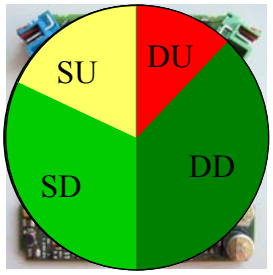
MTBF is the expectation of the operating time between failures

MTTF = Mean Time To Failure

MTTR = Mean Time To Restore (Detect + Repair)

Failure rate including diagnosis

How devices fail?



Total failure rate λ

- Safe failure
  - Safe detected (SD)
  - Safe undetected (SU)
- Dangerous failure
  - Dangerous detected (DD)
  - **Dangerous undetected (DU)**

Only for devices with constant failure rate

MTBF = 1 / λ

acc. IEC 61508 Teil 7 D.2.3.2

Safe Failure Fraction (SFF)

IEC 61508 / 61511

$$SFF = \frac{\lambda^{SD} + \lambda^{SU} + \lambda^{DD}}{\lambda^{SD} + \lambda^{SU} + \lambda^{DD} + \lambda^{DU}} = 1 - \frac{\lambda^{DU}}{\lambda^{Total}}$$

What is it?

- A measure of the effectiveness of the built-in diagnostic

55 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

Architectural constraints

Hardware safety integrity

Safe Failure Fraction (SFF)		Hardware Fault Tolerance (HFT)		
Typ A	Typ B	N = 0	N = 1	N = 2
---	0% …< 60%	---	SIL1	SIL2
0% …< 60%	60% …< 90%	SIL1	SIL2	SIL3
60% …< 90%	90% …< 99%	SIL2	SIL3	SIL4
≥ 90%	≥ 99%	SIL3	SIL4	SIL4

IEC 61508 Teil 2, Kap. 7.4.3.1.1 / Tab. 2&3

The behaviour of **“simple” (type A)** devices under fault conditions can be completely determined. The failure modes of all constituent components are well defined. Such components are metal film resistors, transistors, relays, etc.

The behaviour of **“complex” (type B) devices** under fault conditions cannot be completely determined. The failure mode of at least one component is not well defined. Such components are e. g. microprocessors.

56 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

Safety manual

Extract datasheet / safety manual

(MACX MCR-UI-UI-UP)

Type A-device (acc. EN 61508-2)
Architectural 1oo1
HFT = 0

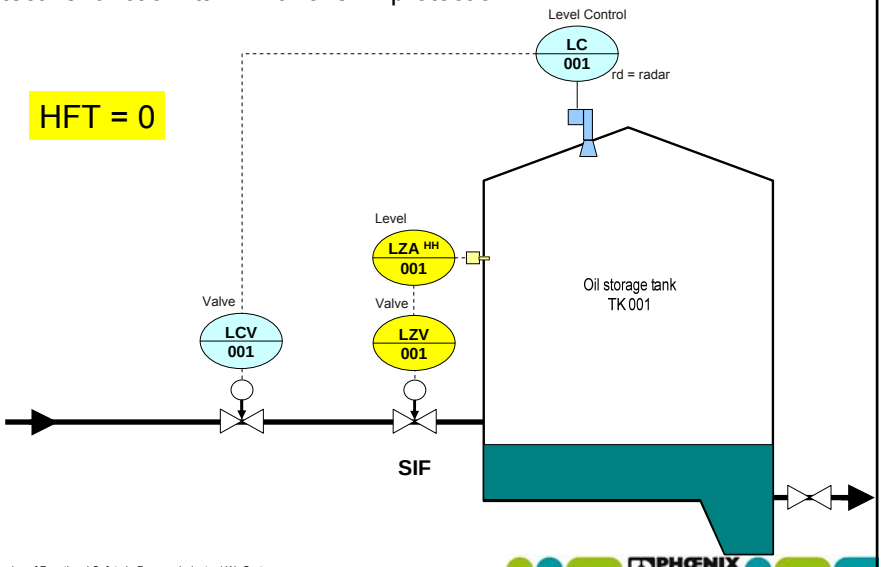
λsd	λsu	λdd	λdu	SFF
0	1,5 x 10^{-7}	0	5,89 x 10^{-8}	85,9 %

Question:
What is the highest SIL-ability?

PHOENIX CONTACT INSPIRING INNOVATIONS

SFF Consideration: (demand mode, PFD)

Protective function: tank with overfill protection LZA



PHOENIX CONTACT INSPIRING INNOVATIONS

Architectural constraints

Hardware safety integrity

Safe Failure Fraction (SFF)		Hardware Fault Tolerance (HFT)		
Typ A	**Typ B**	**N = 0**	**N = 1**	**N = 2**
---	0% …< 60%	---	SIL1	SIL2
0% …< 60%	60% …< 90%	SIL1	SIL2	SIL3
60% …< 90%	90% …< 99%	SIL2	SIL3	SIL4
≥ 90%	≥ 99%	SIL3	SIL4	SIL4

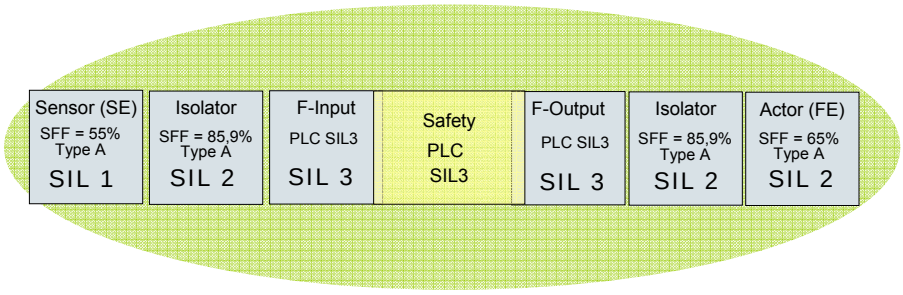
IEC 61508 Teil 2, Kap. 7.4.3.1.1 / Tab. 2&3

The behaviour of **“simple” (type A)** devices under fault conditions can be completely determined. The failure modes of all constituent components are well defined. Such components are metal film resistors, transistors, relays, etc.

The behaviour of **“complex” (type B) devices** under fault conditions cannot be completely determined. The failure mode of at least one component is not well defined. Such components are e. g. microprocessors.

SFF Consideration:

Qualification of the individual components:



SFF analysis of all components:

SFF component allows only SIL 1

But, we need SIL2, How to achieve?

Architectural constraints

Hardware safety integrity

Safe Failure Fraction (SFF)		Hardware Fault Tolerance (HFT)		
Typ A	**Typ B**	**N = 0**	**N = 1**	**N = 2**
---	0% …< 60%	---	SIL1	SIL2
0% …< 60%	60% …< 90%	SIL1	SIL2	SIL3
60% …< 90%	90% …< 99%	SIL2	SIL3	SIL4
≥ 90%	≥ 99%	SIL3	SIL4	SIL4

IEC 61508 Teil 2, Kap. 7.4.3.1.1 / Tab. 2&3

The behaviour of **"simple" (type A)** devices under fault conditions can be completely determined. The failure modes of all constituent components are well defined. Such components are metal film resistors, transistors, relays, etc.

The behaviour of **"complex" (type B) devices** under fault conditions cannot be completely determined. The failure mode of at least one component is not well defined. Such components are e. g. microprocessors, ASICs.

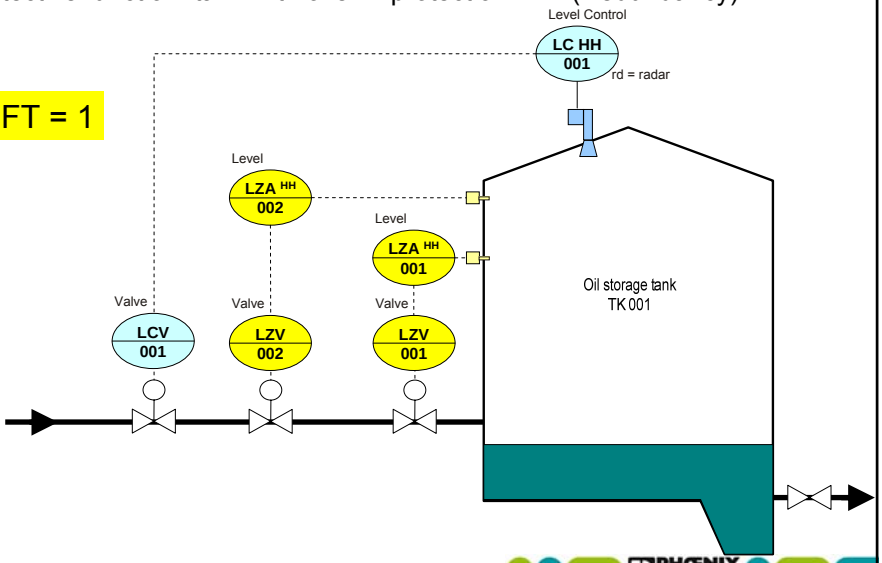
61 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

SFF Consideration: (demand mode, PFD)

Protective function: tank with overfill protection LZA (Redundancy)

HFT = 1

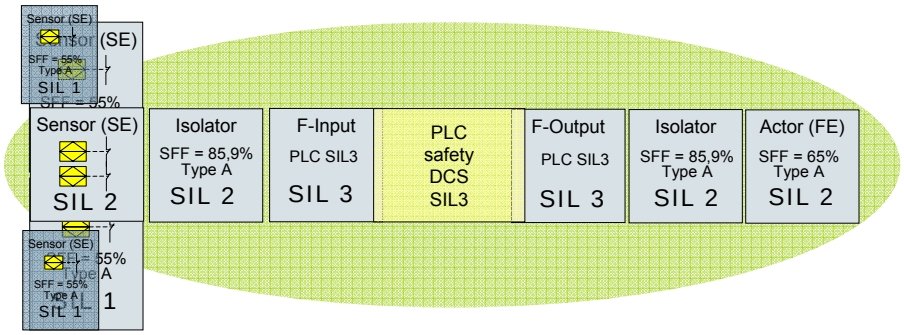


62 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

SFF Consideration:

Qualification of the individual components:



SFF analysis of all components:

SFF component now allows SIL 2

Conclusion:

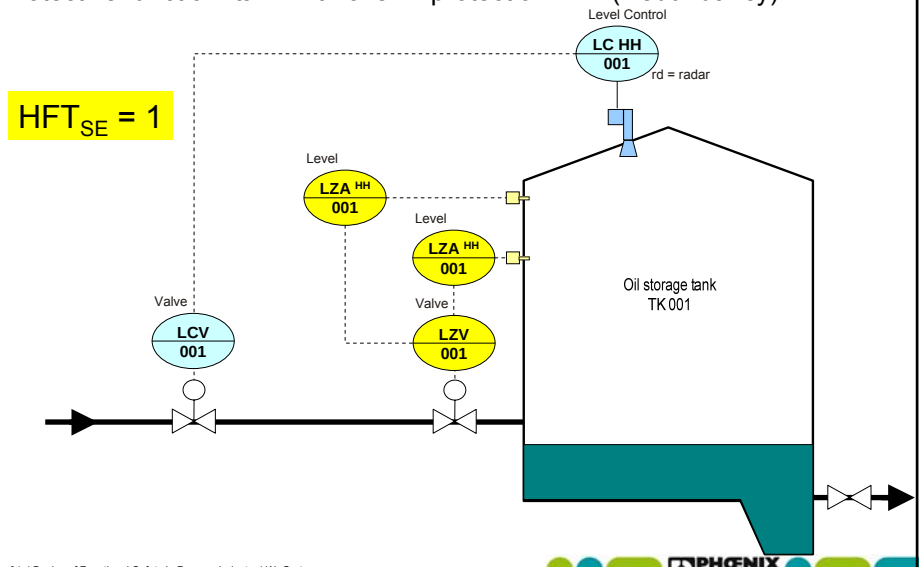
Redundancy requirements depend on the suitability of the individual components.

Question: Is this solution good enough?

PHOENIX CONTACT INSPIRING INNOVATIONS

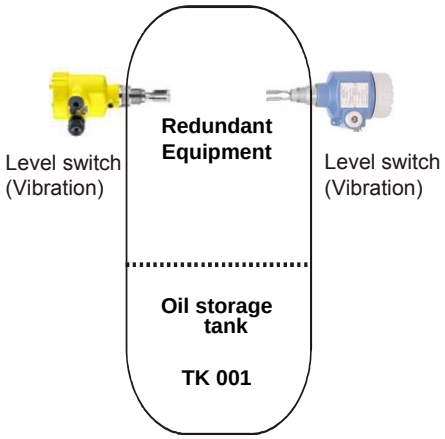
SFF Consideration: (demand mode, PFD)

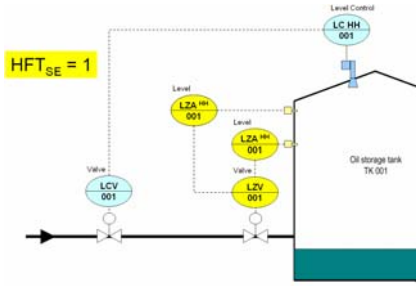
Protective function: tank with overfill protection LZA (Redundancy)



PHOENIX CONTACT INSPIRING INNOVATIONS

Solution of hardware fault tolerance





65 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT
INSPIRING INNOVATIONS

Redundancy

What is redundancy?

Definition:

- The use of multiple elements or subsystems to achieve the same (or parts of) safety function

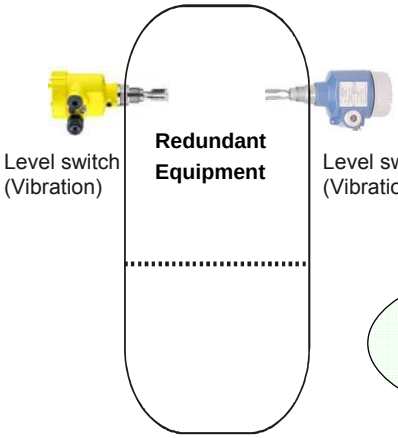
How redundancy can be achieved

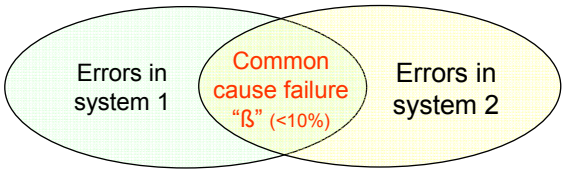
- By the same hardware and / or SW or through diversity
- Does not always help against common cause failure

66 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT
INSPIRING INNOVATIONS

Examples of redundancy

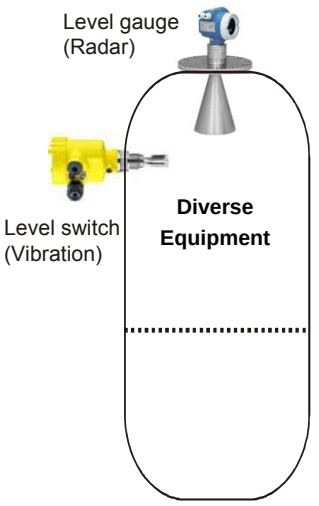


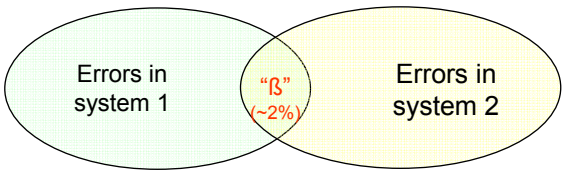


The beta factor is the failure rate for the simultaneous failure of two or more channels following an incident with a common cause.

67 | Basics of Functional Safety in Process Industry | W. Grote

Examples of diverse redundancy

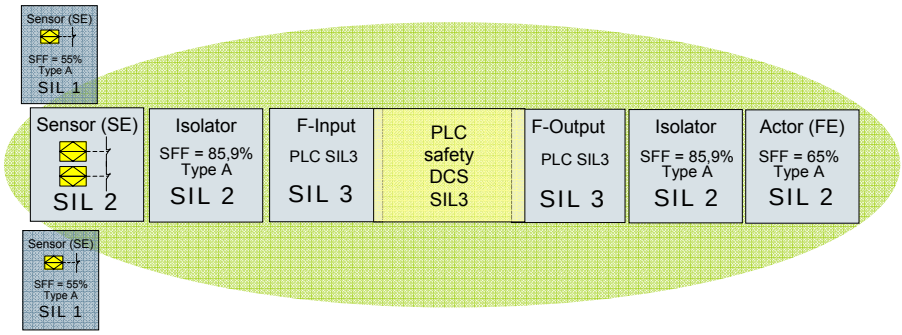




The beta factor is the failure rate for the simultaneous failure of two or more channels following an incident with a common cause.

68 | Basics of Functional Safety in Process Industry | W. Grote

SFF Consideration:



SFF analysis of all components:

SFF component now allows SIL 2

Conclusion:

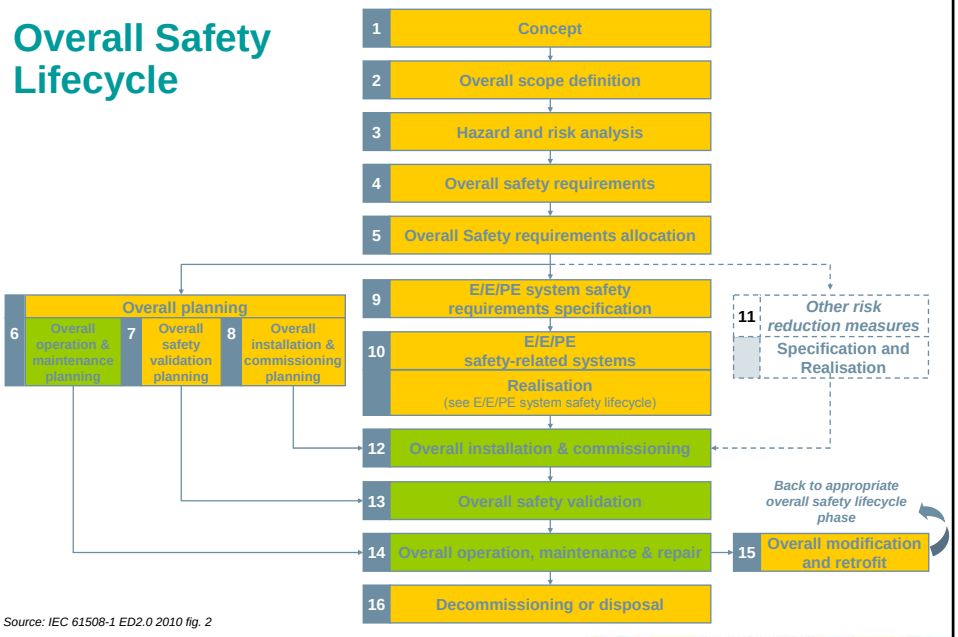
Redundancy requirements depend on the suitability of the individual components.

From an architectural view required SIL achieved, but ….

69 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

Overall Safety Lifecycle



Source: IEC 61508-1 ED2.0 2010 fig. 2

70 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

PFD_{avg} (Probability of Failure on Demand)

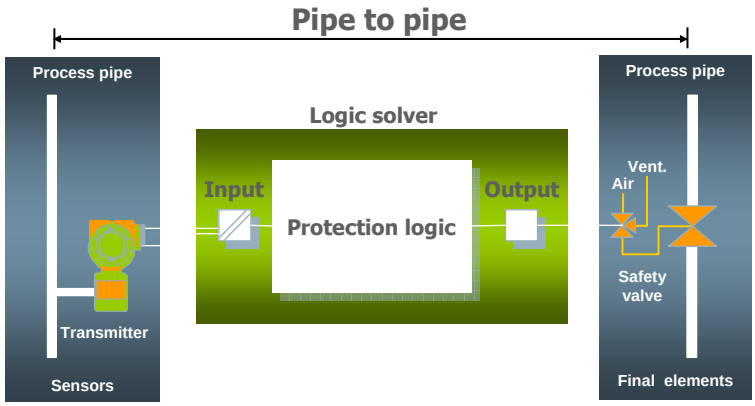
demand mode		
SIL Safety Integrity Level	**PFD** Probability of failure on demand	**RRF** Risk Reduction Factor
SIL 4	$>=10^{-5}$ to $<10^{-4}$	100000 to 10000
SIL 3	$>=10^{-4}$ to $<10^{-3}$	10000 to 1000
SIL 2	$>=10^{-3}$ to $<10^{-2}$	1000 to 100
SIL 1	$>=10^{-2}$ to $<10^{-1}$	100 to 10

PFD -> predominant in process industry!

71 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

SIL defines required loop PFD



SIL → PFD_{target} for the SIF

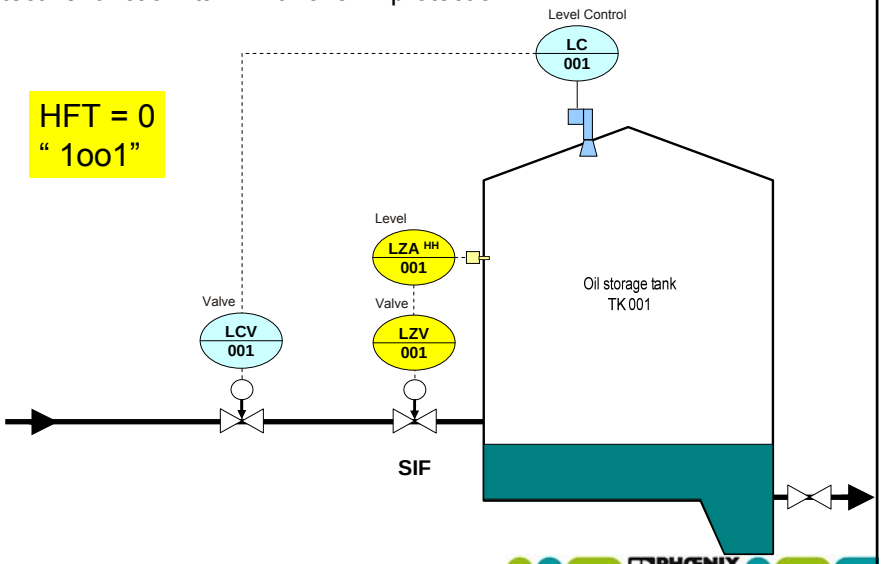
$PFD_{SIF} = PFD_{sensor(s)} + PFD_{logic\ solver} + PFD_{final\ element(s)}$

72 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

Simple example (demand mode)

Protective function: tank with overfill protection LZA



PHOENIX CONTACT INSPIRING INNOVATIONS

Formulas IEC 61508-6

Architecture	Mode: with low demand rate	Mode: High demand or continuous mode
1oo1	$PFD_G = (\lambda_{DU} + \lambda_{DD}) \bullet t_{CE}$ $t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$	$PFH_G = \lambda_{DU}$
1oo2	$PFD_G = 2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right)$ $t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$ $t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$	$PFH_G = 2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} + \beta_D \lambda_{DD} + \beta\lambda_{DU}$ $t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$
2oo3	$PFD_G = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right)$ $t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$ $t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$	$PFH_G = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} + \beta_D \lambda_{DD} + \beta\lambda_{DU}$ $t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$
1oo2D	$PFD_G = 2(1-\beta)\lambda_{DU}((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU} + \lambda_{SD})t_{CE}' t_{GE}' + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right)$ $t_{CE}' = \frac{\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) + (\lambda_{DD} + \lambda_{SD})MTTR}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}}$ $t_{GE}' = \frac{\lambda_{DU}\left(\frac{T_1}{3} + MTTR\right) + (\lambda_{DD} + \lambda_{SD})MTTR}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}}$	$PFH_G = 2(1-\beta)\lambda_{DU}((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU} + \lambda_{SD})t_{CE}' + \beta_D \lambda_{DD} + \beta\lambda_{DU}$ $t_{CE}' = \frac{\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) + (\lambda_{DD} + \lambda_{SD})MTTR}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}}$

PHOENIX CONTACT INSPIRING INNOVATIONS

PFD simplify acc. ANSI / ISA S-84.01

1oo1 $PFD_{avg} = \left[\lambda_{DU} \times \frac{TI}{2} \right]$

1oo2 $PFD_{avg} = \left[(\lambda_{DU})^2 \times \frac{TI^2}{3} \right] + \left[\beta \times \lambda_{DU} \times \frac{TI}{2} \right]$

1oo3 $PFD_{avg} = \left[(\lambda_{DU})^3 \times \frac{TI^3}{4} \right] + \left[\beta \times \lambda_{DU} \times \frac{TI}{2} \right]$

2oo3 $PFD_{avg} = \left[(\lambda_{DU})^2 \times TI^2 \right] + \left[\beta \times \lambda_{DU} \times \frac{TI}{2} \right]$

2oo4 $PFD_{avg} = \left[(\lambda_{DU})^3 \times TI^3 \right] + \left[\beta \times \lambda_{DU} \times \frac{TI}{2} \right]$

λ_{DU} = Proportion of dangerous undetected faults

β = Error that impacts on more than one channel of a redundant system (Common Cause)

TI = Interval between manual functional testing of component

75 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

Implementation PFD_{avg} ($T_{[PROOF]}$ = 1 Jahr)

SIF
Safety Instrumented Function

Sensor (SE)	Isolator	F-Input / Safety PLC / F-Output	Isolator	Actor (FE)
SFF = 83% Typ A	SFF = 85% Typ A	SFF = 99%	SFF = 83% Typ A	SFF = 65% Type A
HFT = 0	HFT = 0	HFT = 0	HFT = 0	HFT = 0
λ_{DU} = 43 FIT	λ_{DU} = 60 FIT	λ_{DU} = 3 FIT	λ_{DU} = 73 FIT	λ_{DU} = 124 FIT
PFDavg = 1,9E-4	**PFDavg = 2,7E-4**	**PFDavg = 1E-6**	**PFDavg = 3,2E-4**	**PFDavg = 1,1E-3**
SIL 2	**SIL 2**	**SIL 3**	**SIL 2**	**SIL 2**

$PFD_{SIF} = PFD_{Sensor} + PFD_{Isolator} + PFD_{PLC} + PFD_{Isolator} + PFD_{Actuator}$

$PFD_{SIF} = 1{,}9*10^{-4} + 2{,}7*10^{-4} + 1*10^{-6} + 3{,}2*10^{-4} + 1{,}1*10^{-3}$

$PFD_{SIF} = 0{,}001881 = \sim 1{,}9*10^{-3}$

SIL 2 requirement is achieved at $T_{[Proof]}$ = 1 Year → $PFD_{aim} \geq 10^{-3} \ldots < 10^{-2}$

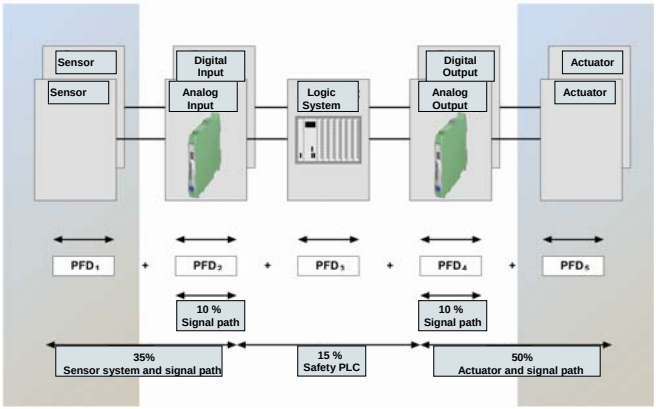
1 FIT = 1 mistakes/ 10^9 h

76 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

Verification of a SIS

SIS= Safety **I**nstrumented **S**ystem



A safety instrumented system for one or more safety instrumented functions.

A safety instrumented system includes sensor(s), Logic system (solver) and actuator(s).

Failure distribution in a safety instrumented control circuit

77 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

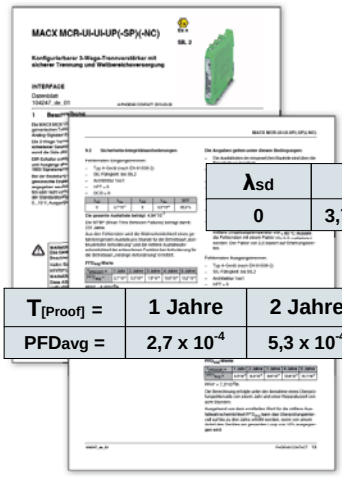
Summary

- We know the history of the standards
- We are able to identify the risks (HAZOP) and quantify (Risk graph).
- We know the important SIL parameter (HFT, SFF, PFD,...)
- We are able to do a SFF – Analysis and a simple PFD - calculation.

78 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

Safety Manual (Extract datasheet)



(MACX MCR-UI-UI-UP)
Type A-device (acc. EN 61508-2)
SIL-ability: bis SIL2
Architectural 1oo1
HFT = 0
DCD = 0

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0	$3{,}7 \times 10^{-7}$	0	$6{,}0 \times 10^{-8}$	85,9%

$T_{[Proof]}$ =	1 Jahre	2 Jahre	3 Jahre	4 Jahre	5 Jahre
PFDavg =	$2{,}7 \times 10^{-4}$	$5{,}3 \times 10^{-4}$	$7{,}9 \times 10^{-4}$	$10{,}6 \times 10^{-4}$	$13{,}2 \times 10^{-4}$

PHOENIX CONTACT INSPIRING INNOVATIONS

Definitions

Term	Description
CDF	**C**umulative **D**istribution **F**unction
Electrical/electronical/programmable electronical systems (E/E/PES)	A term used to embrace all possible electrical equipment that may be used to carry out a safety function. Thus simple electrical devices and programmable logic controllers (PLCs) of all forms are included.
Equipment under control (EUC)	Equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities.
ESD	**E**mergency **S**hut-**D**own
ETA	**E**vent **T**ree **A**nalysis
FME(C)A	**F**ailure **M**ode **E**ffect (and **C**riticality) **A**nalysis
FMEDA	**F**ailure **M**ode **E**ffect and **D**iagnostics **A**nalysis
FIT	**F**ailures in **T**ime
FTA	**F**ault **T**ree **A**nalysis
Hazardous event	hazardous situation which results in harm
HAZOP	**HAZ**ard and **OP**erability study
HFT	**H**ardware **F**ailure **T**olerance
IEC/EN 61508	Standard of functional safety of electrical/electronical/programmable electronical safety-related systems
IEC/EN 61511	Standard of functional safety: safety instrumented systems for the process industry sector
LDM	**L**ow **D**emand **M**ode – where the frequency of demands for operation made on a safety related system is no greater than one per year and no greater than twice the proof test frequency.

PHOENIX CONTACT INSPIRING INNOVATIONS

Definitions

MooN	**M** out of **N** channels
MTBF	**M**ean **T**ime between **F**ailures
MTTF	**M**ean **T**ime to **F**ailure
MTTR	**M**ean **T**ime to **R**epair
PDF	**P**robability **D**ensity **F**unction
PFD	**P**robability of **F**ailure on **D**emand – mean failure probability in the demand case – the probability that a safety system will not execute its function when it is required to do so.
PFD_{avg}	**A**verag**e** **P**robability of **F**ailure on **D**emand
PFH	**P**robability of dangerous **F**ailure per **H**our
Risk	Combination of the probability of occurrence of harm and the severity of that harm. Calculated as the product between incident frequency and incident severity
SFF	**S**afe **F**ailure **F**raction – proportion of non-dangerous failures – the ratio of the rate of safe faults plus the rate of diagnosed/recognized faults in relation to the total failure rate of the system.
SIF	**S**afety **I**nstrumented **F**unction

81 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

Definitions

SIS	**S**afety **I**nstrumented **S**ystem – A SIS (Safety system) comprises one or more safety functions; for each of these safety functions there is a SIL requirement.
SIL	**S**afety **I**ntegrity **L**evel – One of four discrete stages in specifying the requirements for the safety integrity of the safety functions, which are assigned to the E/E/PE safety-related system, in which the Safety Integrity Level 4 represents the highest stage and the Safety Integrity Level 1 represents the lowest stage of safety integrity.
SLC	**S**afety **L**ife **C**ycle – Covers all aspects of safety, including the initial conception, design, implementation, installation, commissioning, validation, maintenance and decommissioning of the risk-reducing measures.
Safety	The freedom from unacceptable risk of physical injury or of damage to the health of persons, either directly or indirectly, as a result of damage to property or the environment.
Safety function	Function to be implemented by an E/E/PE safety-related system, other technology safety-related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event.
Tolerable risk	Risk, which is accepted in a given context based upon the current values of society.

82 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS

Thank you for your attention.
Be safe!

Questions???

TÜVRheinland FSEngineer

83 | Basics of Functional Safety in Process Industry | W. Grote

PHOENIX CONTACT INSPIRING INNOVATIONS