Basics of Functional Safety in Process Industry

Wilfried Grote

And safety is a life time commitment !!

AGENDA

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

PHOENIX CONTACT INSPIRING INNOVATIONS

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

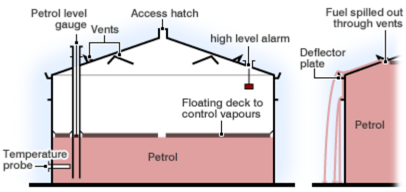
PHOENIX CONTACT INSPIRING INNOVATIONS

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
- **14 years after Flixborough, UK 1974!**

PHOENIX CONTACT INSPIRING INNOVATIONS

What we want to avoid!
Major Incidents

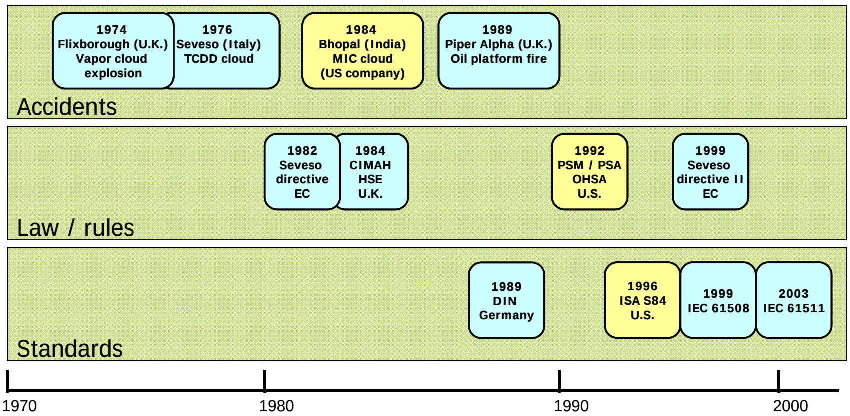


Buncefield UK, December 2005

- 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

PHOENIX CONTACT INSPIRING INNOVATIONS

History of functional safety standards



7 Basics of Functional Safety in Process Industry

Historical Background

- The Council Directive 96/82/EC (Comah) forms the legal basis regarding the control of plants with major accident hazards. Trigger was a chemical accident happened in the town of Seveso, Northern Italy, in July 1976.
- In Germany, the Act for the Protection Against Immissions (12. BImSchV) supplemented with an Incident Regulation has been adopted.
- The Incident Regulation referred to DIN19250 and DIN 19251 which define requirement classes AK 1-8. DIN 19250 and DIN 19251 expired on July 31, 2004.
- From the 1st of August 2004, IEC 61508 and IEC 61511 provide an adequate basis for risk assessment and certification of assessed systems to ensure compliance with the Incident Regulation for the future. The standards define four safety integrity levels: SIL1 to SIL4

8 Basics of Functional Safety in Process Industry

IEC 61508
and Sector Specific Standards

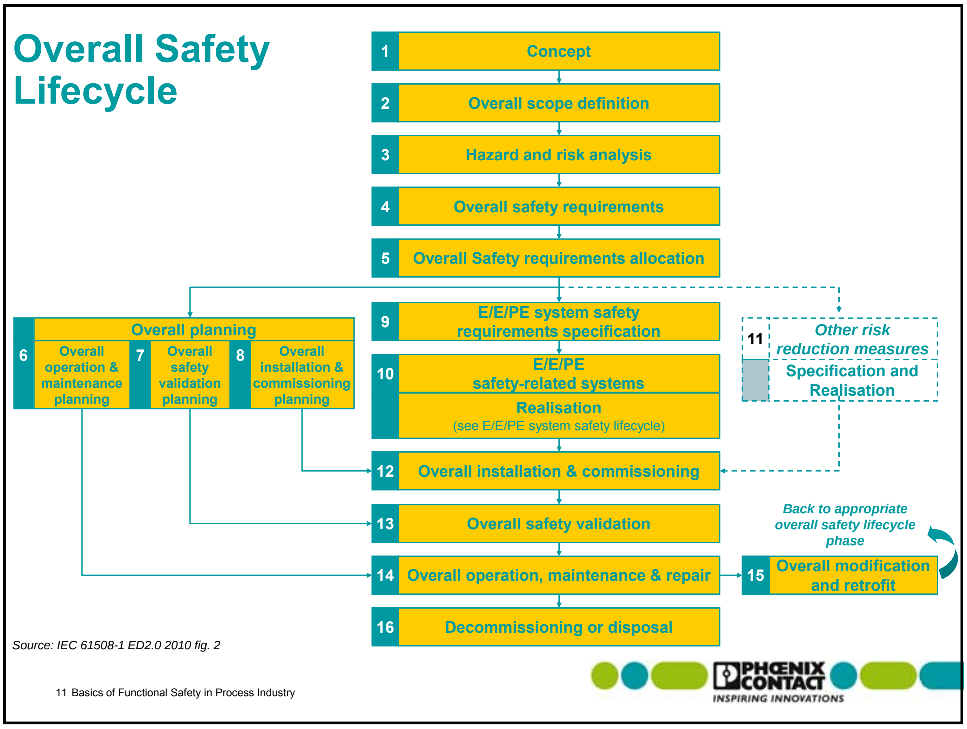
IEC 61508: 1999
Functional Safety of E/E/PE Safety-Related Systems
Basic Standard

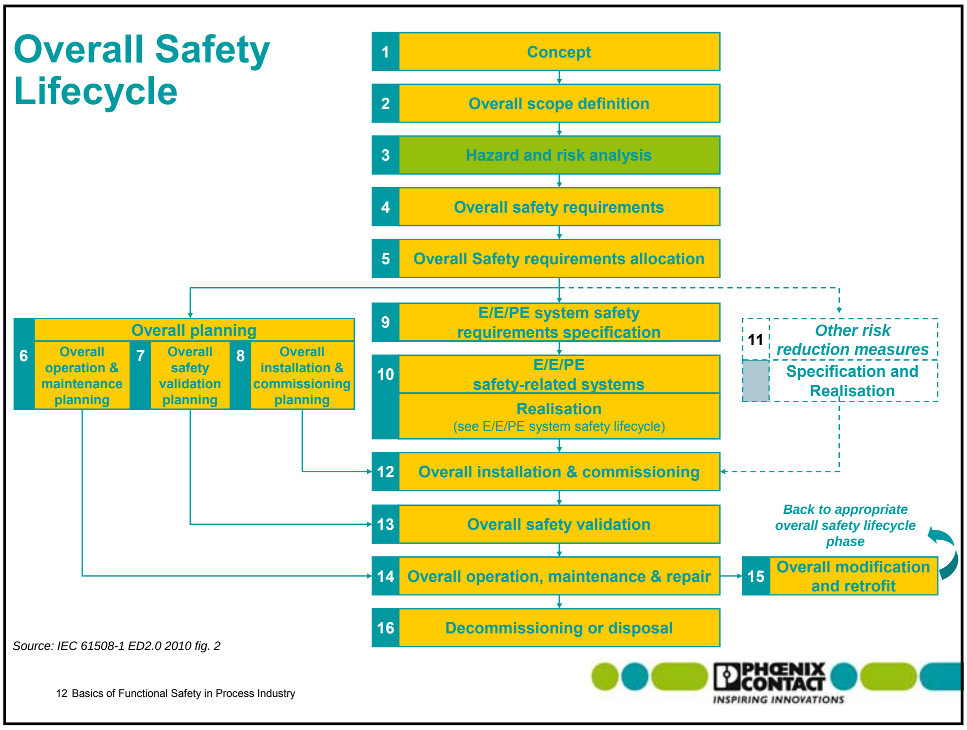
Sector Specific Standards

IEC 61800-5-2 Electrical Drives	**IEC 60601** Medical Devices	**IEC 62061** Machines
IEC 61513 Nuclear Sector	**IEC 61511** Process Industry	**Other Sectors**
EN 50128 Railway Apps.	**IEC 50156** Furnaces	

AGENDA

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


Overall Safety Lifecycle
1 Concept
2 Overall scope definition
3 Hazard and risk analysis
4 Overall safety requirements
5 Overall Safety requirements allocation
Overall planning
6 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
11 Basics of Functional Safety in Process Industry
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
Overall planning
6 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
12 Basics of Functional Safety in Process Industry
PHOENIX CONTACT
INSPIRING INNOVATIONS

What is a Hazardous Situation?

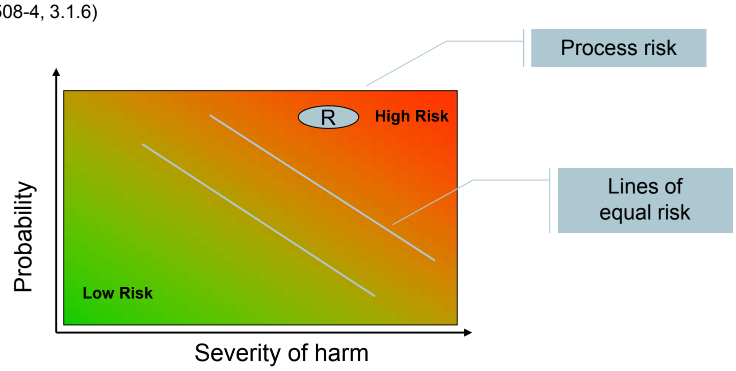
A hazardous situation can be caused by a potential source of danger.

PHOENIX CONTACT INSPIRING INNOVATIONS

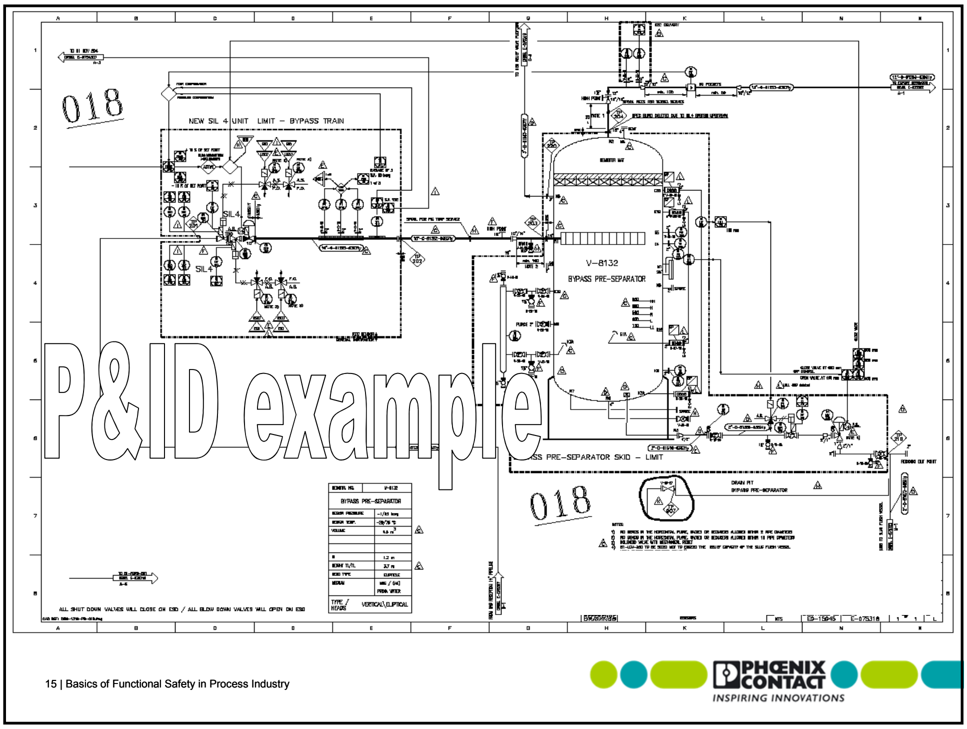
What is a Risk?

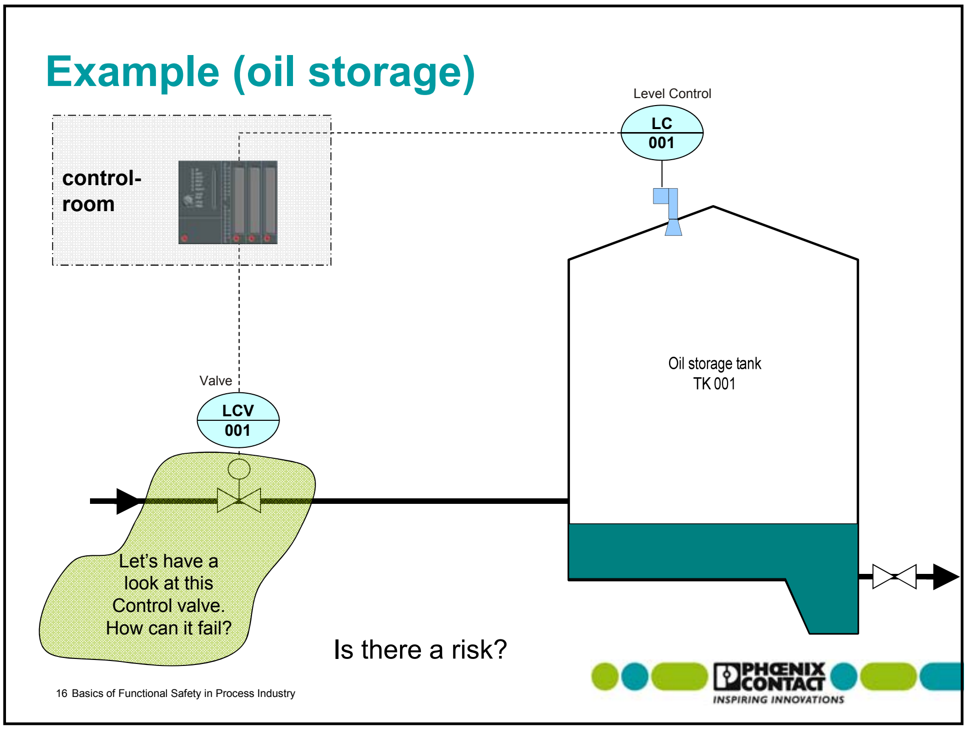
Combination of the probability of occurrence of harm and the severity of that harm.

(IEC 61508-4, 3.1.6)



PHOENIX CONTACT INSPIRING INNOVATIONS

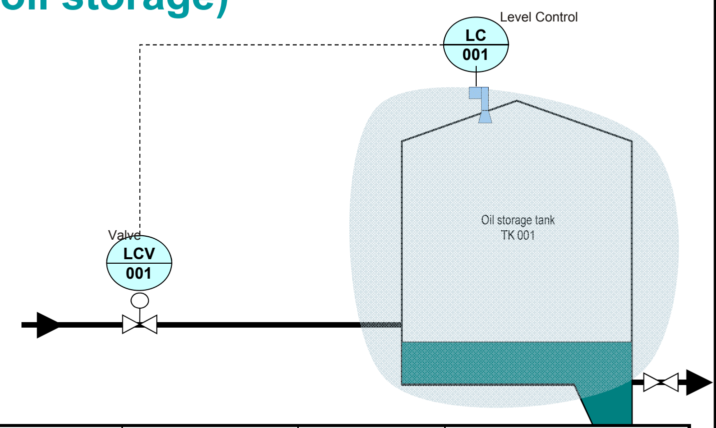

P&ID example
018
NEW SIL 4 UNIT LIMIT – BYPASS TRAIN
V–8132
BYPASS PRE-SEPARATOR
018
15 | Basics of Functional Safety in Process Industry
PHOENIX CONTACT
INSPIRING INNOVATIONS


Example (oil storage)
Level Control
LC
001
control-
room
Oil storage tank
TK 001
Valve
LCV
001
Let's have a look at this Control valve. How can it fail?
Is there a risk?
16 Basics of Functional Safety in Process Industry
PHOENIX CONTACT
INSPIRING INNOVATIONS

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)
…	…

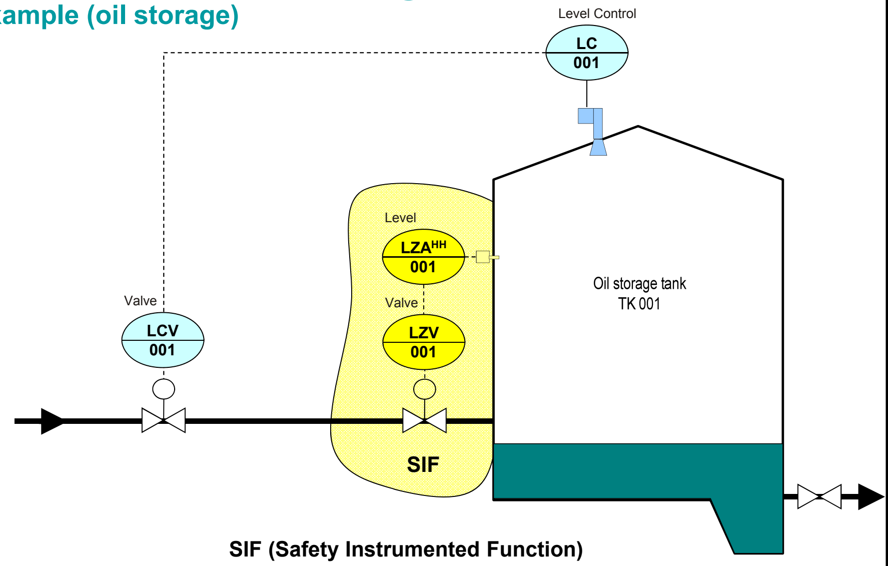
Example (oil storage)



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

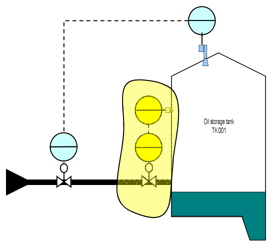
Result, HAZOP for High Level protection

Example (oil storage)



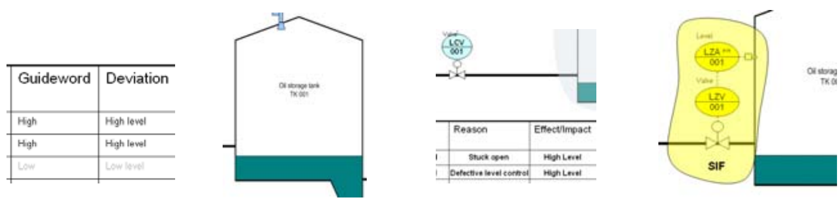
SIF (Safety Instrumented Function)

What is a HAZOP - Analysis?



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

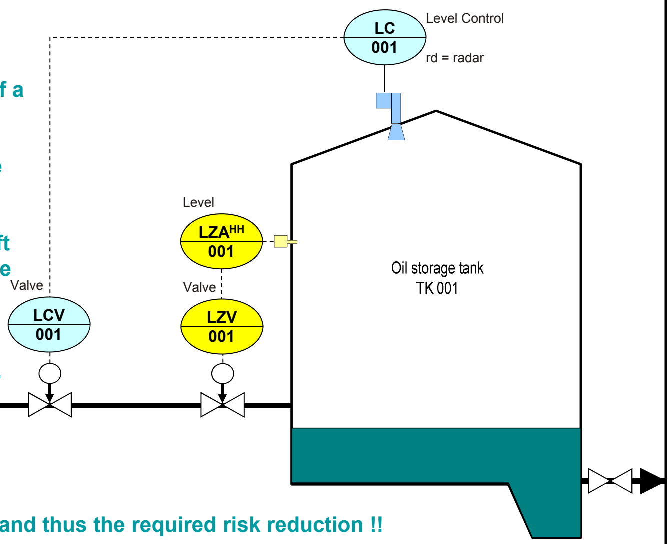
- **Prognosis**
  - **Locating**
    - **Estimation**
      - **Counteractions**



SIL classification (Personal Safety)

Plant information

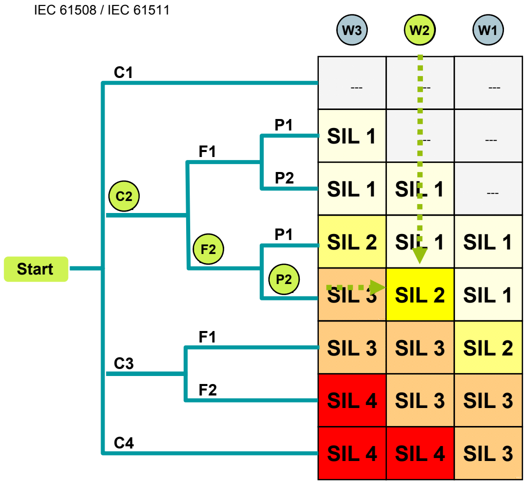
- Tank is within 25 m of a guard house
- There is always one person present in the guard house (24/7)
- Operator visits tank during 5 min. per shift
- The oil is a light crude that produces easy ignitable gasses.
- There are electrical pumps in the vicinity.



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

Risk graph Example (oil storage)

Quelle:
IEC 61508 / IEC 61511



Consequence C:
C1: Minor injury
C2: Serious permanent injury to one or more persons; death to one person
C3: Death to several people
C4: Very many people killed,

Frequency of, and exposure time in, the hazardous zone (F):
F1: Rare to more often exposure in the hazardous zone
F2: Frequent to permanent exposure in the hazardous zone

Possibility of avoiding the hazardous event (P):
P1: Possible under certain conditions
P2: Almost impossible

Probability of the unwanted occurrence (W):
W1: A very slight probability that the unwanted occurrences will come to pass and only a few unwanted occurrences are likely
W2: A slight probability that the unwanted occurrences will come to pass and few unwanted occurrences are likely
W3: A relatively high probability that the unwanted occurrences will come to pass and frequent unwanted occurrences are likely

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.

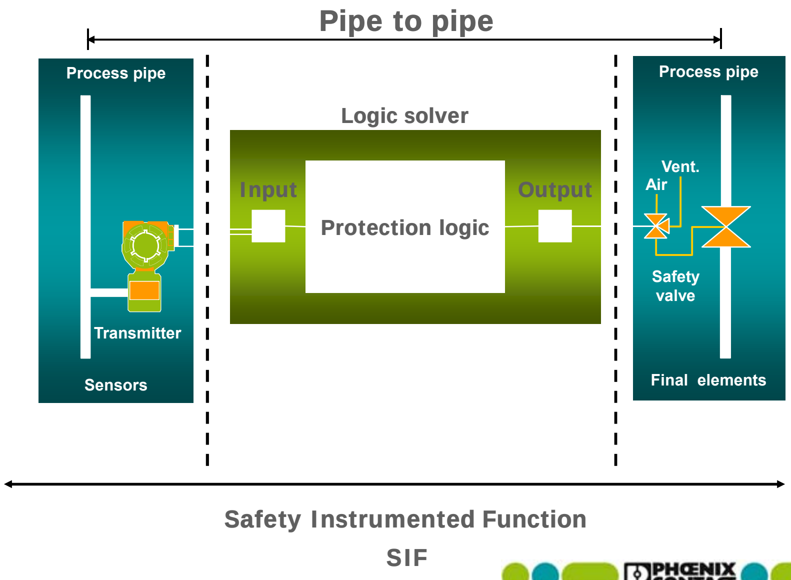
Safety Integrity Levels (SIL)

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).

Pipe to pipe



AGENDA

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

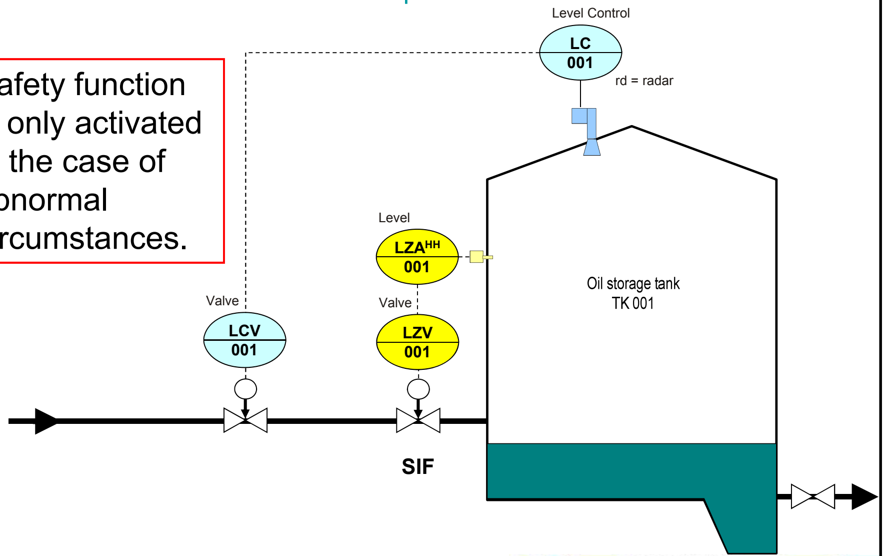
Error types

- The malfunction of a safety function may result from:
  - Systematic errors, e.g.:
    - Measuring range not suitable for the application
    - Emergency shut-down design incorrect
    - Operating temperature of the sensor not according to safety manual
    - Sensor liner not suitable for process fluid
  - Non systematic, random errors e.g.:
    - Hardware fault in electronics
    - Sensor error

Example (demand mode, PFD)

Protective function: Tank with overfill protection

Safety function is only activated in the case of abnormal circumstances.



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

HFT
(Hardware Fault Tolerance)

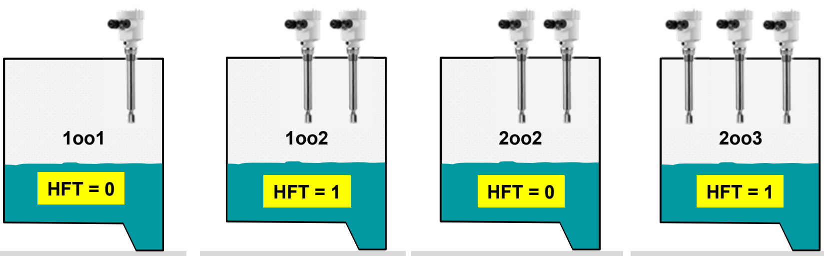
- The HFT of a device indicates the quality of a safety function:

  HFT = 0 Single-channel use.
  A single fault may cause a safety loss.

  HFT = 1 Redundant version.
  At least two hardware faults must occur at the same time to cause a safety loss.

- Through proved operation as well as different safety requirements the value of the needed HFT can be reduced by ‘1‘ according to IEC 61511

HFT examples



1oo1	1oo2	2oo2	2oo3
The reaction is triggered and the sensor detects a dangerous state. (no DFT)	The reaction is triggered when one of the two sensors detects a dangerous state. (DFT)	The reaction takes place when both sensors detect a dangerous condition. (SFT)	The reaction takes place when two of the three sensors detect a dangerous condition. (DFT)
High probability of a dangerous failure	Significant reduction of the probability of a dangerous defect	Lower probability of a random error, which means we have a higher availability of the plant Higher probability of a dangerous failure	Very high reduction of the probability of a dangerous failure

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.

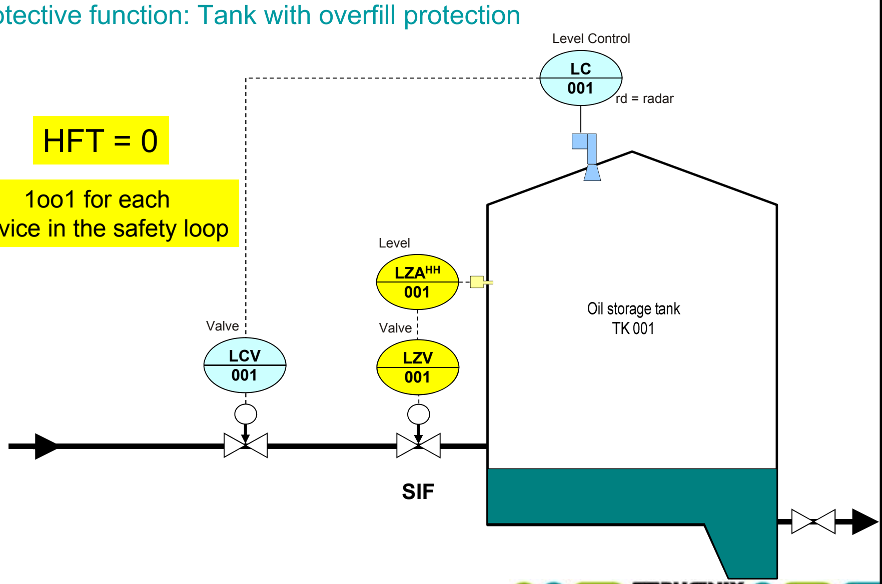
33 Basics of Functional Safety in Process Industry

Example (demand mode)

Protective function: Tank with overfill protection

HFT = 0

1oo1 for each
device in the safety loop



34 Basics of Functional Safety in Process Industry

Demands from IEC standards

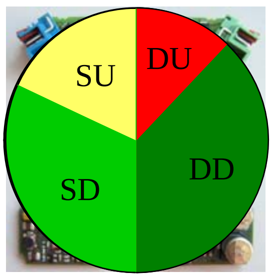
1. Hardware Fault Tolerance

2. Safe Failure Fraction

PHOENIX CONTACT
INSPIRING INNOVATIONS

Failure rate including diagnosis

How devices fail?



Total failure rate λ_{Total}

- Safe failure λ_S
  - Safe detected (λ_{SD})
  - Safe undetected (λ_{SU})
- Dangerous failure λ_D
  - Dangerous detected (λ_{DD})
  - **Dangerous undetected (λ_{DU})**

Only for devices with constant failure rate

MTBF = 1 / λ

acc. IEC 61508 Teil 7 D.2.3.2

PHOENIX CONTACT
INSPIRING INNOVATIONS

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

37 Basics of Functional Safety in Process Industry

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.

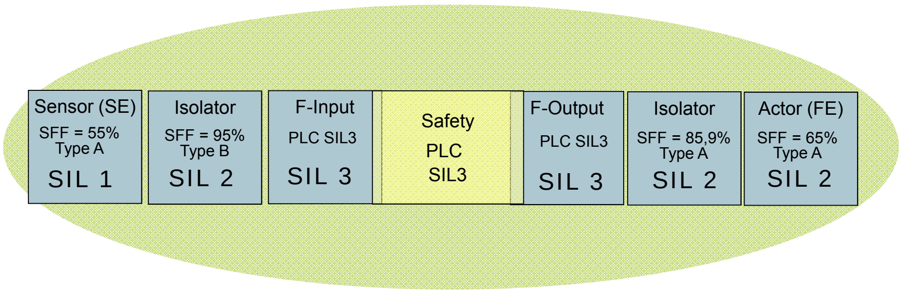
The behaviour of “complex” (type B) devices under fault conditions cannot be completely determined. The failure mode of at least one component is not well defined. Such components are e. g. microprocessors.

38 Basics of Functional Safety in Process Industry

PHOENIX CONTACT INSPIRING INNOVATIONS

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

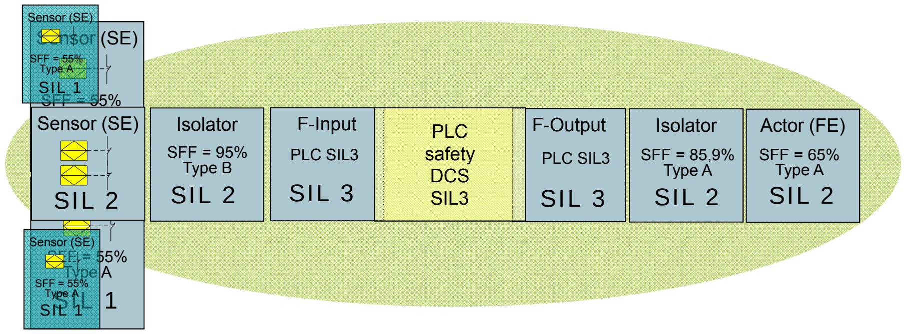
IEC 61508 Teil 2, Kap. 7.4.3.1.1 / Tab. 2&3

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.

SFF Consideration

Qualification of the individual components



SFF analysis of all components:

SFF component now allows SIL 2

Conclusion:

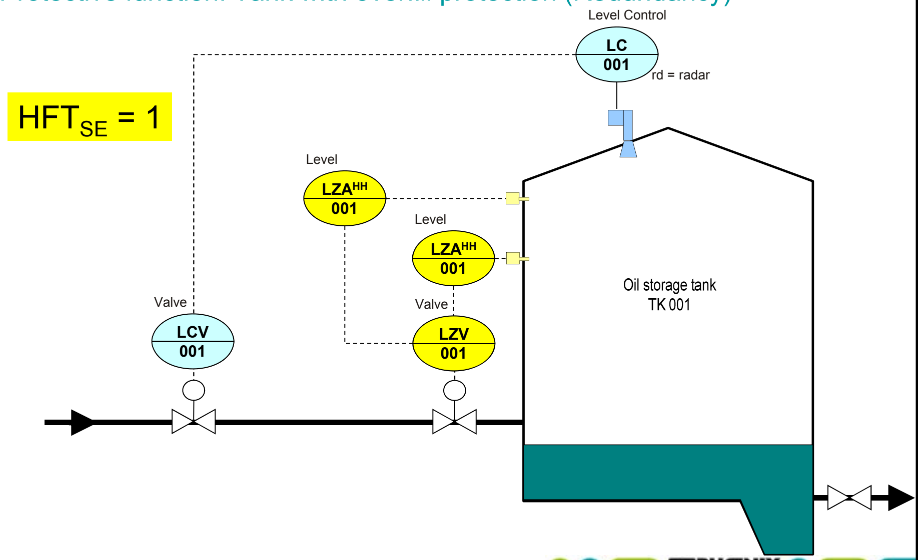
Redundancy requirements depend on the suitability of the individual components.

Question: Is this solution good enough?

PHOENIX CONTACT INSPIRING INNOVATIONS

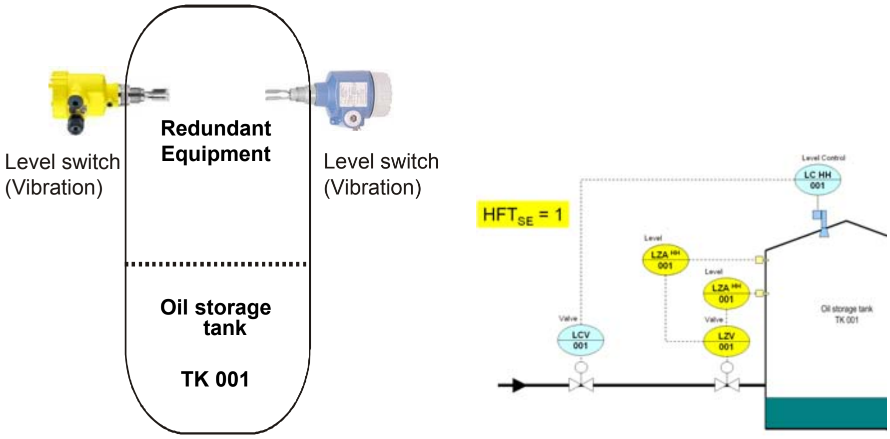
SFF Consideration: (demand mode, PFD)

Protective function: Tank with overfill protection (Redundancy)



PHOENIX CONTACT INSPIRING INNOVATIONS

Solution of hardware fault tolerance



Redundancy

What is redundancy?

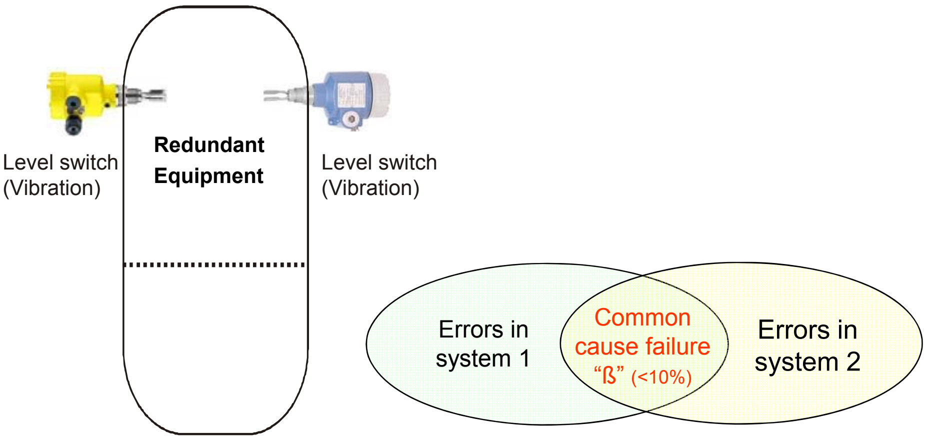
Definition:

- 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

Examples of redundancy

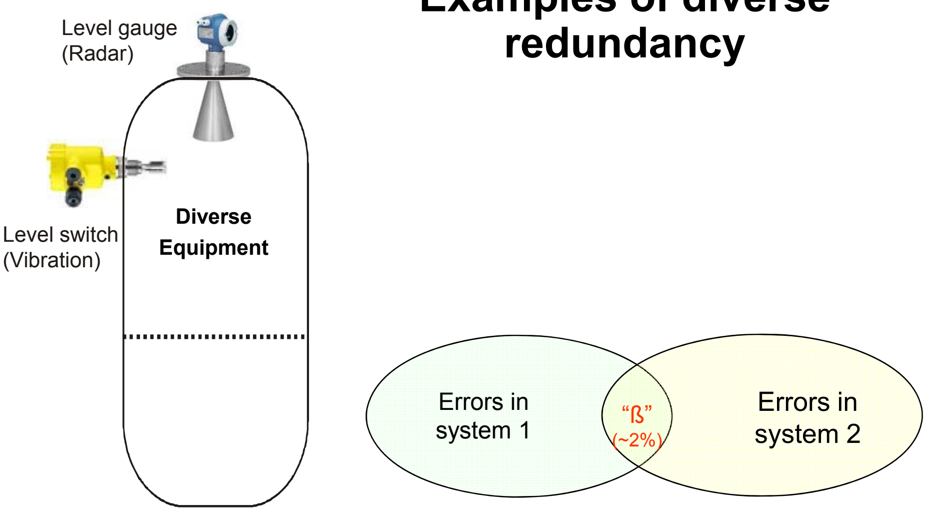


The beta factor is the failure rate for the simultaneous failure of two or more channels following an incident with a common cause.

45 | Basics of Functional Safety in Process Industry

PHOENIX CONTACT INSPIRING INNOVATIONS

Examples of diverse redundancy



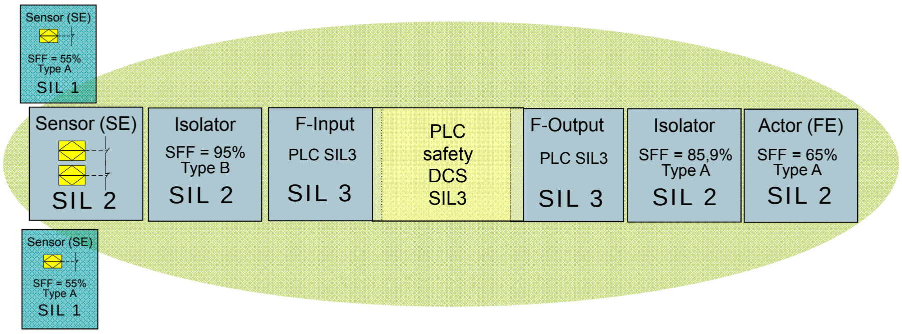
The beta factor is the failure rate for the simultaneous failure of two or more channels following an incident with a common cause.

46 | Basics of Functional Safety in Process Industry

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.

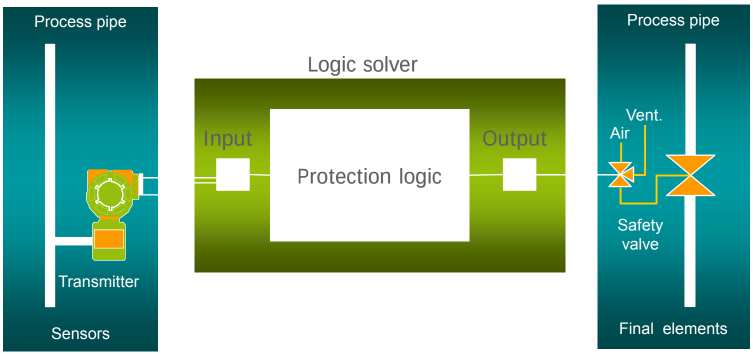
From an architectural view required SIL achieved, but ….

Safety Integrity Levels

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!

SIL defines required loop PFD



SIL → PFD $_{target}$ **for the SIF**

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

49 Basics of Functional Safety in Process Industry

Safety manual

Extract datasheet / safety manual

MACX MCR(-EX)-T-UIREL-UP(-SP)

Type B-device (acc. EN 61508-2)
Architectural 1oo1d
HFT = 0

λsd	λsu	λdd	λdu	SFF
0	234 FIT	548 FIT	42 FIT	95%

T[PROOF] =	1 Jahr	2 Jahre	5 Jahre
PFD_{avg} =	2,77 x 10^{-4}	4,49 x 10^{-4}	9,67 x 10^{-4}

Portion of the device on the entire loop of 10%

Appendix - Safety-related applications (SIL 2)

A1.2.1 Failure rates: MACX MCR-(EX)-T-UIREL-UP(-SP)

Input: RTD 4-wire connection method
Output: Switching output 2 and 3 (redundant)

- Type B device (according to EN 61508-2)
- Safety Integrity Level (SIL) 2
- HFT = 0
- 1oo1d architecture

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF	DC_D
0	2.34 * 10^{-7}	5.48* 10^{-7}	0.42 * 10^{-7}	95%	93 %
0 FIT	234 FIT	548 FIT	42 FIT		

The total failure rate is: 1.34 * 10^{-6}

The MTBF (Mean Time Between Failures) is therefore: 85 years.

The probability of a dangerous failure per hour for "continuous demand" mode and the average probability of failure of the specified function for "low demand" mode are determined from the error rate:

PFD_{avg} values

T[PROOF] =	1 year	2 years	5 years
PFD_{avg} =	2.77 * 10^{-4}	4.49 * 10^{-4}	9.67 * 10^{-4}

PFH* = 4.2 * 10^{-8}/h

The calculation is performed assuming a checking interval (T_{PROOF}) of 1 year and a repair time (MTTR) of 24 hours, a test coverage (CPT) of 95% and a life time (LT) of 10 years.

On the basis of the value determined for the average probability of failure **PFD_{avg}**, the checking interval can be increased to up to 5 years.

50 Basics of Functional Safety in Process Industry

Question

When the achieved PFD of a SIF is: 0.006, for the whole function, this SIF falls in the category

SIL 1
SIL 2
SIL 3
SIL 4
Choose!

SIL 2: 0,001 < **0,006** < 0,010
SIL 2: $1*10^{-3}$ < **$6*10^{-3}$** < $10*10^{-3}$

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

SIF
Safety Instrumented Function

Sensor (SE)	Isolator	F-Input	Safety PLC	F-Output	Isolator	Actor (FE)
SFF = 83%	SFF = 85%		SFF = 99%		SFF = 83%	SFF = 65%
Typ A	Typ A				Typ A	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**

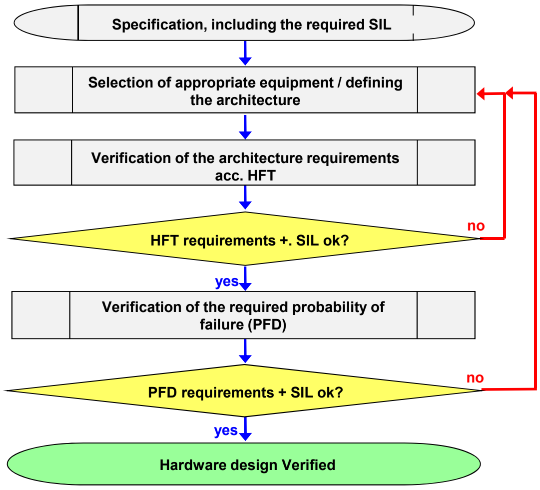
$PFD_{SIF} = PFD_{Sensor} + PFD_{Isolator} + PFD_{PLC} + PFD_{Isolator} + PFD_{Actuator}$

$PFD_{SIF} = 1,9*10^{-4} + 2,7*10^{-4} + 1*10^{-6} + 3,2*10^{-4} + 1,1*10^{-3}$
$PFD_{SIF} = 0,001881 \;\; = \sim 1,9*10^{-3}$

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

Design and verification of safety features



53 | Basics of Functional Safety in Process Industry

PHOENIX CONTACT INSPIRING INNOVATIONS

PFD simplify acc. (ISA 84.00.01-2004)

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

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

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

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

54 Basics of Functional Safety in Process Industry

PHOENIX CONTACT INSPIRING INNOVATIONS

Example Test frequency Calculations

	Sensor	Final Element	LogicS
a	Alarm	No	DCS
SIL1	1oo1	1oo1	IPS
SIL2	1oo1	1oo2	IPS
SIL3	1oo2	1oo2	IPS

Calculate the Test interval for a SIL 1 safety application, with:

- a sensor, MTBF of 60 years,
- a safety valve, MTBF of 30 years,
- an IPS (Instrumented Protective System = PLC) with a PFD of 1E-6, which is tested once every 10 years,
- all equipment is proven in use.

PHOENIX CONTACT INSPIRING INNOVATIONS

SIL 1 loop test frequency calculation

Solution

$$\text{PFD loop} < 10^{-1}$$

$$\text{PFD}_{\text{loop}} = \text{PFD}_{\text{sensor}} + \text{PFD}_{\text{solver}} + \text{PFD}_{\text{final element}}$$

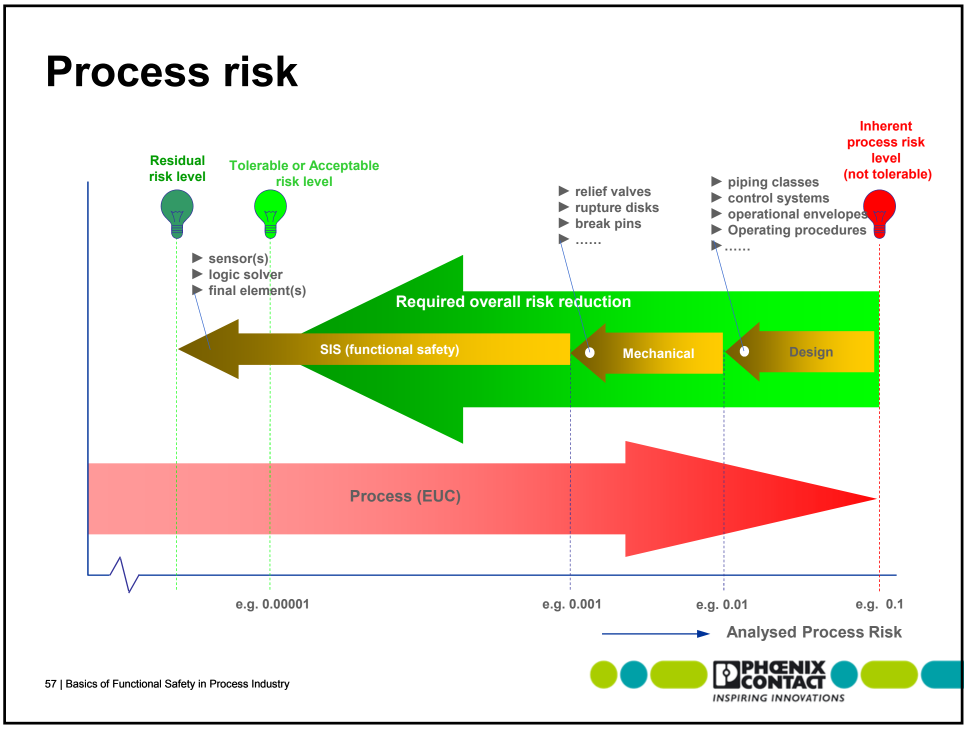
$$10^{-1} = \frac{1}{2} * \lambda_{\text{du (SE)}} * T + \text{PFD}_{\text{solver}} + \frac{1}{2} * \lambda_{\text{du (FE)}} * T$$

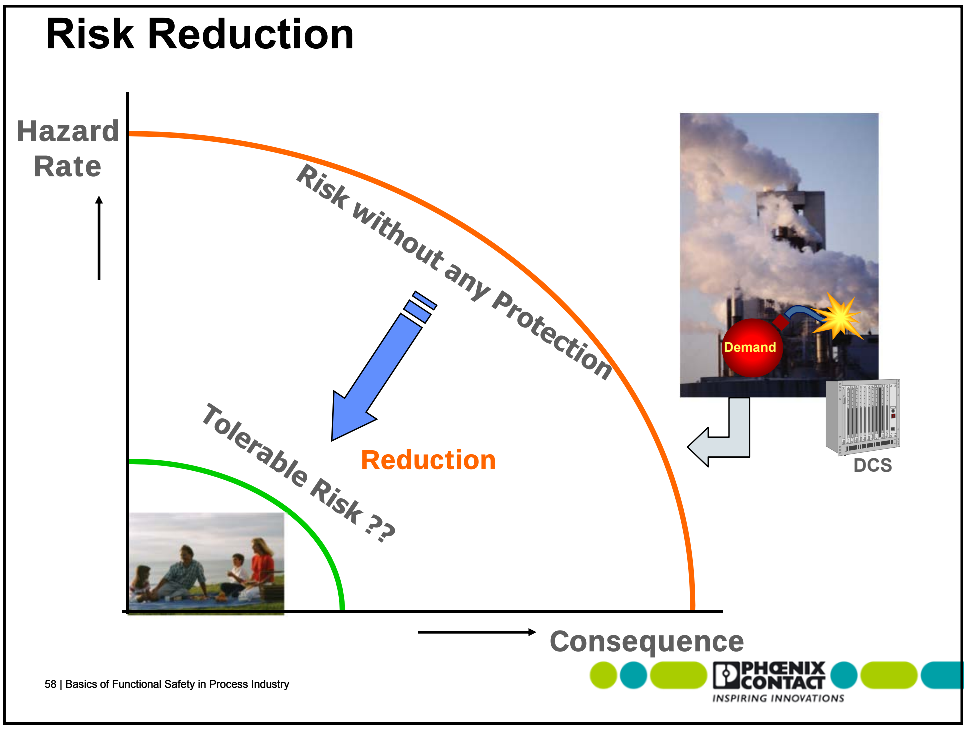
$$10^{-1} = \frac{1}{2} * \frac{1}{MTBF_{(SE)}} * T + \text{PFD}_{\text{solver}} + \frac{1}{2} * \frac{1}{MTBF_{(FE)}} * T$$

$$10^{-1} = \frac{1}{2} * \frac{1}{60\,years} * T + \cancel{10^{-6}} + \frac{1}{2} * \frac{1}{30\,years} * T$$

$$T = 4\,years$$

PHOENIX CONTACT INSPIRING INNOVATIONS


Process risk
Residual risk level
Tolerable or Acceptable risk level
Inherent process risk level (not tolerable)
sensor(s)
logic solver
final element(s)
relief valves
rupture disks
break pins
......
piping classes
control systems
operational envelopes
Operating procedures
......
Required overall risk reduction
SIS (functional safety)
Mechanical
Design
Process (EUC)
e.g. 0.00001
e.g. 0.001
e.g. 0.01
e.g. 0.1
Analysed Process Risk
57 | Basics of Functional Safety in Process Industry
INSPIRING INNOVATIONS


Risk Reduction
Hazard Rate
Risk without any Protection
Reduction
Tolerable Risk ??
Demand
DCS
Consequence
58 | Basics of Functional Safety in Process Industry
INSPIRING INNOVATIONS

5

Exercise

	Sensor	Final Element	LogicS
a	Alarm	No	DCS
SIL1	1oo1	1oo1	IPS
SIL2	1oo1	1oo2	IPS
SIL3	1oo2	1oo2	IPS

- Calculate the Test interval for a SIL 3 dangerous fault tolerant system, with a MTBF of 70 years for the sensor element, 30 years for the valve and an IPS with a PFD of 1E-6, which is tested once every 10 years. (All equipment is proven in use.)

- What happens to the PFD, if the test interval is doubled ?

5

SIL 3 loop test frequency calculation

Solution

$$\text{PFD loop} < 10^{-3}$$

$$\text{PFD}_{\text{loop}} = \text{PFD}_{\text{sensor}} + \text{PFD}_{\text{solver}} + \text{PFD}_{\text{final element}}$$

$$10^{-3} = \frac{1}{4} * \lambda^2_{\text{du (SE)}} * T^2 + \text{PFD}_{\text{solver}} + \frac{1}{4} * \lambda^2_{\text{du (FE)}} * T^2$$

$$10^{-3} = \frac{1}{4} * \frac{1^2}{MTBF^2_{(SE)}} * T^2 + \text{PFD}_{\text{solver}} + \frac{1}{4} * \frac{1^2}{MTBF^2_{(FE)}} * T^2$$

$$10^{-3} = \frac{1}{4} * \frac{1}{4900\, years} * T^2 + \cancel{10^{-6}} + \frac{1}{4} * \frac{1}{900\, years} * T^2$$

$$T = \sqrt{\frac{10^{-3}}{3.3 * 10^{-4}}}$$

$T = 1.7\, years$

if $\text{T} = 3.5$ years, PFD is $4 * 10^{-3}$ (Max SIL 2)

if $\text{T} = 0.85$ years, PFD is $0.25 * 10^{-3}$

PFD simplify acc. (ISA 84.00.01-2004)

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

61 Basics of Functional Safety in Process Industry

Formulas IEC 61508-6

	Mode	
Architecture	**with low demand rate**	**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	$PFD_G = 2(1-\beta)\lambda_{DU}((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU} + \lambda_{SD}) t_{CE}' t_{GE}' + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU}\left(\frac{T_1}{2} + MTTR\right)$ $t_{CE}' = \frac{\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) + (\lambda_{DD} + \lambda_{SD}) MTTR}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}}$ $t_{GE}' = \frac{\lambda_{DU}\left(\frac{T_1}{3} + MTTR\right) + (\lambda_{DD} + \lambda_{SD}) MTTR}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}}$	$PFH_G = 2(1-\beta)\lambda_{DU}((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU} + \lambda_{SD}) t_{CE}' + \beta_D \lambda_{DD} + \beta \lambda_{DU}$ $t_{CE}' = \frac{\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) + (\lambda_{DD} + \lambda_{SD}) MTTR}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}}$

62 Basics of Functional Safety in Process Industry

Definitions

Term	Description
CDF	Cumulative Distribution Function
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	Emergency Shut-Down
ETA	Event Tree Analysis
FME(C)A	Failure Mode Effect (and Criticality) Analysis
FMEDA	Failure Mode Effect and Diagnostics Analysis
FIT	Failures in Time
FTA	Fault Tree Analysis
Hazardous event	hazardous situation which results in harm
HAZOP	HAZard and OPerability study
HFT	Hardware Failure Tolerance
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	Low Demand Mode – 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.

63 Basics of Functional Safety in Process Industry

Definitions

MooN	M out of N channels
MTBF	Mean Time between Failures
MTTF	Mean Time to Failure
MTTR	Mean Time to Repair
PDF	Probability Density Function
PFD	Probability of Failure on Demand – 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}	Average Probability of Failure on Demand
PFH	Probability of dangerous Failure per Hour
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	Safe Failure Fraction – 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	Safety Instrumented Function

64 Basics of Functional Safety in Process Industry

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.

PHOENIX CONTACT
INSPIRING INNOVATIONS