Basics of Functional Safety in Process Industry

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

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
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!

**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
History of functional safety standards

- **Accidents**
  - 1974: Flixborough (U.K.) – vapor cloud explosion
  - 1976: Seveso (Italy) – TCDD cloud
  - 1984: Bhopal (India) – MIC cloud (U.S. company)
  - 1999: Piper Alpha (U.K.) – oil platform fire

- **Law / rules**
  - 1982: Seveso directive (EC)
  - 1984: CIMAH (HSE) – U.K.
  - 1992: PSM / PSA (OSHA) – U.S.
  - 1999: Seveso directive II (EC)

- **Standards**
  - 1974: SEVESO directive
  - 1999: DIN Germany
  - 1996: ISA S84 U.S.
  - 1999/2003: IEC 61508/61511

---

**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: SIL 1 to SIL 4.
**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 61513
  - Nuclear Sector
- EN 50128
  - Railway Apps.
- IEC 61511
  - Process Industry
- IEC 60601
  - Other Sectors
- IEC 60601
  - 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

<table>
<thead>
<tr>
<th>No.</th>
<th>Step</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Concept</td>
</tr>
<tr>
<td>2</td>
<td>Overall scope definition</td>
</tr>
<tr>
<td>3</td>
<td>Hazard and risk analysis</td>
</tr>
<tr>
<td>4</td>
<td>Overall safety requirements</td>
</tr>
<tr>
<td>5</td>
<td>Overall Safety requirements allocation</td>
</tr>
<tr>
<td>6</td>
<td>E/E/PE system safety requirements specification</td>
</tr>
<tr>
<td>7</td>
<td>Overall installation &amp; commissioning planning</td>
</tr>
<tr>
<td>8</td>
<td>Overall operation &amp; maintenance planning</td>
</tr>
<tr>
<td>9</td>
<td>Overall safety validation</td>
</tr>
<tr>
<td>10</td>
<td>Decommissioning or disposal</td>
</tr>
<tr>
<td>11</td>
<td>Back to appropriate overall safety lifecycle phase</td>
</tr>
<tr>
<td>12</td>
<td>Other risk reduction measures specification and Realisation</td>
</tr>
</tbody>
</table>

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

---

### Overall Safety Lifecycle

<table>
<thead>
<tr>
<th>No.</th>
<th>Step</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Concept</td>
</tr>
<tr>
<td>2</td>
<td>Overall scope definition</td>
</tr>
<tr>
<td>3</td>
<td>Hazard and risk analysis</td>
</tr>
<tr>
<td>4</td>
<td>Overall safety requirements</td>
</tr>
<tr>
<td>5</td>
<td>Overall Safety requirements allocation</td>
</tr>
<tr>
<td>6</td>
<td>E/E/PE system safety requirements specification</td>
</tr>
<tr>
<td>7</td>
<td>Overall installation &amp; commissioning planning</td>
</tr>
<tr>
<td>8</td>
<td>Overall operation &amp; maintenance planning</td>
</tr>
<tr>
<td>9</td>
<td>Overall safety validation</td>
</tr>
<tr>
<td>10</td>
<td>Decommissioning or disposal</td>
</tr>
<tr>
<td>11</td>
<td>Back to appropriate overall safety lifecycle phase</td>
</tr>
<tr>
<td>12</td>
<td>Other risk reduction measures specification and Realisation</td>
</tr>
</tbody>
</table>

Source: IEC 61508-1 ED2.0 2010 Fig. 2
What is a Hazardous Situation?

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

What is a Risk?

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

(IEC 61508-4, 3.1.6)
Example (oil storage)

Let's have a look at this Control valve. How can it fail?

Is there a risk?
### Failure modes of control valve

<table>
<thead>
<tr>
<th>Failure</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sticky</td>
<td>Loss of control</td>
</tr>
<tr>
<td>Cavitation</td>
<td>Damage</td>
</tr>
<tr>
<td>Passing</td>
<td>Integrity HSE</td>
</tr>
<tr>
<td>Leaking gland</td>
<td>Spill small HSE</td>
</tr>
<tr>
<td>Noise</td>
<td>Damage valve</td>
</tr>
<tr>
<td>Corrosion</td>
<td>Major leak</td>
</tr>
<tr>
<td>Closing</td>
<td>Spurious Trip (random error)</td>
</tr>
<tr>
<td>Not closing</td>
<td>Hazard (HSE)</td>
</tr>
</tbody>
</table>

### Example (oil storage)

<table>
<thead>
<tr>
<th>No</th>
<th>Guideword</th>
<th>Deviation</th>
<th>Reason</th>
<th>Effect/Impact</th>
<th>Take action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>High</td>
<td>High level</td>
<td>Stuck open</td>
<td>High Level</td>
<td>High level protection</td>
</tr>
<tr>
<td>2.</td>
<td>High</td>
<td>High level</td>
<td>Defective level control</td>
<td>High Level</td>
<td>High level protection</td>
</tr>
</tbody>
</table>
Result, HAZOP for High Level protection
Example (oil storage)

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)

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
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)

<table>
<thead>
<tr>
<th>Demand mode</th>
<th>SIL Safety Integrity Levels</th>
<th>RRF Risk reduction factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL 1</td>
<td>100 to 10</td>
<td></td>
</tr>
<tr>
<td>SIL 2</td>
<td>1000 to 100</td>
<td></td>
</tr>
<tr>
<td>SIL 3</td>
<td>10000 to 1000</td>
<td></td>
</tr>
<tr>
<td>SIL 4</td>
<td>100000 to 10000</td>
<td></td>
</tr>
</tbody>
</table>

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).
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

Demands on the system architecture
(acc. – IEC 61511)

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

<table>
<thead>
<tr>
<th>SIL</th>
<th>minimum hardware fault tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>It sets out specific requirements. See IEC 61508</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>HFT</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1001</td>
<td>HFT = 0&lt;br&gt;The reaction is triggered and the sensor detects a dangerous state. (no DFT)&lt;br&gt;High probability of a dangerous failure</td>
</tr>
<tr>
<td>1002</td>
<td>HFT = 1&lt;br&gt;The reaction is triggered when one of the two sensors detects a dangerous state. (DFT)&lt;br&gt;Significant reduction of the probability of a dangerous defect</td>
</tr>
<tr>
<td>2002</td>
<td>HFT = 0&lt;br&gt;The reaction takes place when both sensors detect a dangerous condition. (SFT)&lt;br&gt;Lower probability of a random error, which means we have a higher availability of the plant&lt;br&gt;Higher probability of a dangerous failure</td>
</tr>
<tr>
<td>2003</td>
<td>HFT = 1&lt;br&gt;The reaction takes place when two of the three sensors detect a dangerous condition. (DFT)&lt;br&gt;Very high reduction of the probability of a dangerous failure</td>
</tr>
</tbody>
</table>
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.

Example (demand mode)
Protective function: Tank with overfill protection

HFT = 0
1oo1 for each device in the safety loop
**Demands from IEC standards**

1. **Hardware Fault Tolerance**

2. **Safe Failure Fraction**

---

**Failure rate including diagnosis**

**How devices fail?**

- Total failure rate $\lambda_{\text{Total}}$
  - Safe failure $\lambda_S$
    - Safe detected ($\lambda_{SD}$)
    - Safe undetected ($\lambda_{SU}$)
  - Dangerous failure $\lambda_D$
    - Dangerous detected ($\lambda_{DD}$)
    - Dangerous undetected ($\lambda_{DU}$)

Only for devices with constant failure rate

$$\text{MTBF} = \frac{1}{\lambda}$$

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

Architectural constraints
Hardware safety integrity

<table>
<thead>
<tr>
<th>Safe Failure Fraction (SFF)</th>
<th>Hardware Fault Tolerance (HFT)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Typ A</strong></td>
<td><strong>Typ B</strong></td>
</tr>
<tr>
<td>---</td>
<td>N = 0</td>
</tr>
<tr>
<td>0% ... &lt; 60%</td>
<td>---</td>
</tr>
<tr>
<td>60% ... &lt; 90%</td>
<td>SIL1</td>
</tr>
<tr>
<td>90% ... &lt; 99%</td>
<td>SIL2</td>
</tr>
<tr>
<td>≥ 90%</td>
<td>SIL3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>N = 1</th>
<th>N = 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0% ... &lt; 60%</td>
<td>SIL1</td>
<td>SIL2</td>
</tr>
<tr>
<td>60% ... &lt; 90%</td>
<td>SIL2</td>
<td>SIL3</td>
</tr>
<tr>
<td>90% ... &lt; 99%</td>
<td>SIL3</td>
<td>SIL4</td>
</tr>
<tr>
<td>≥ 90%</td>
<td>SIL4</td>
<td>SIL4</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Safe Failure Fraction (SFF)</th>
<th>Hardware Fault Tolerance (HFT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Typ A</td>
<td>Typ B</td>
</tr>
<tr>
<td>N = 0</td>
<td>N = 1</td>
</tr>
<tr>
<td>0% ...&lt; 60%</td>
<td>SIL1</td>
</tr>
<tr>
<td>60% ...&lt; 90%</td>
<td>SIL1</td>
</tr>
<tr>
<td>90% ...&lt; 99%</td>
<td>SIL2</td>
</tr>
<tr>
<td>≥ 90%</td>
<td>SIL3</td>
</tr>
<tr>
<td>≥ 99%</td>
<td>SIL4</td>
</tr>
</tbody>
</table>

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

Conclusion:
Redundancy requirements depend on the suitability of the individual components.

Question: Is this solution good enough?

SFF Consideration: (demand mode, PFD)
Protective function: Tank with overfill protection (Redundancy)

HFT_{SE} = 1
Solution of hardware fault tolerance

- Level switch (Vibration)
- Redundant Equipment
- Oil storage tank
- TK 001

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.

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.
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

<table>
<thead>
<tr>
<th>SIL Safety Integrity Level</th>
<th>PFD Probability of failure on demand</th>
<th>RRF Risk Reduction Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL 4</td>
<td>&gt;=10^{-5} to &lt;10^{-4}</td>
<td>100000 to 10000</td>
</tr>
<tr>
<td>SIL 3</td>
<td>&gt;=10^{-4} to &lt;10^{-3}</td>
<td>10000 to 1000</td>
</tr>
<tr>
<td>SIL 2</td>
<td>&gt;=10^{-3} to &lt;10^{-2}</td>
<td>1000 to 100</td>
</tr>
<tr>
<td>SIL 1</td>
<td>&gt;=10^{-2} to &lt;10^{-1}</td>
<td>100 to 10</td>
</tr>
</tbody>
</table>

PFD -> predominant in process industry!
SIL defines required loop PFD

SIL → PFD target for the SIF

\[ \text{PFD}_{\text{SIF}} = \text{PFD}_{\text{sensor(s)}} + \text{PFD}_{\text{logic solver}} + \text{PFD}_{\text{final element(s)}} \]

Safety manual

Extract datasheet / safety manual

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

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

<table>
<thead>
<tr>
<th>λd</th>
<th>λsu</th>
<th>λdd</th>
<th>λsu</th>
<th>SFF</th>
<th>DoP</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2.34 x 10^{-3}</td>
<td>5.46 x 10^{-6}</td>
<td>4.49 x 10^{-6}</td>
<td>95%</td>
<td>93%</td>
</tr>
</tbody>
</table>

0.23 FIT | 546 FIT | 42 FIT | 96%

\[ \text{PFD}_{\text{avg}} = 2.77 \times 10^{-4} \]

\[ \text{DoP}_{\text{avg}} = 9.67 \times 10^{-6} \]

Portion of the device on the entire loop of 10%
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 $PFD_{\text{avg}}(T_{\text{PROOF}}) = 1$ year

$PFD_{\text{SIF}} = PFD_{\text{Sensor}} + PFD_{\text{Isolator}} + PFD_{\text{PLC}} + PFD_{\text{Isolator$'}} + PFD_{\text{Actuator}}$

$PFD_{\text{SIF}} = 1.9*10^{-4} + 2.7*10^{-4} + 1*10^{-6} + 3.2*10^{-4} + 1.1*10^{-3}$
$PFD_{\text{SIF}} = 0,001881 = \sim 1.9*10^{-3}$

SIL 2 requirement is achieved at $T_{\text{PROOF}} = 1$ Year $\Rightarrow PFD_{\text{aim}} \geq 10^{-3} \ldots < 10^{-2}$
Design and verification of safety features

- Specification, including the required SIL
- Selection of appropriate equipment / defining the architecture
- Verification of the architecture requirements acc. HFT
- Hardware design Verified

Verification of the required probability of failure (PFD)

HFT requirements + SIL ok?

no

PFD requirements + SIL ok?

no

yes

PFD simplify acc. (ISA 84.00.01-2004)

1oo1

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

1oo2

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

1oo3

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

2oo3

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

2oo4

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

\( \lambda_{DU} \) = Proportion of dangerous undetected faults

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

TI = Interval between manual functional testing of component
Example Test frequency Calculations

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.

<table>
<thead>
<tr>
<th>Sensor</th>
<th>Final Element</th>
<th>Logic</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>Alarm</td>
<td>No</td>
</tr>
<tr>
<td>SIL1</td>
<td>1oo1</td>
<td>1oo1</td>
</tr>
<tr>
<td>SIL2</td>
<td>1oo1</td>
<td>1oo2</td>
</tr>
<tr>
<td>SIL3</td>
<td>1oo2</td>
<td>1oo2</td>
</tr>
</tbody>
</table>

SIL 1 loop test frequency calculation

Solution

PFD loop < 10⁻²

PFD_{loop} = PFD_{sensor} + PFD_{valve} + PFD_{final element}

\[ 10^{-4} = \frac{1}{2} \times \lambda_{dc(SE)} \times T + PFD_{valve} + \frac{1}{2} \times \lambda_{dc(FF)} \times T \]

\[ 10^{-4} = \frac{1}{2} \times \frac{1}{MTBF_{(SE)}} \times T + PFD_{valve} + \frac{1}{2} \times \frac{1}{MTBF_{(FF)}} \times T \]

\[ 10^{-4} = \frac{1}{2} \times \frac{1}{60\text{years}} \times T + \frac{1}{2} \times \frac{1}{30\text{years}} \times T \]

\[ T = 4 \text{ years} \]
Process risk

Required overall risk reduction

Analysed Process Risk

Risk Reduction

Hazard Rate

Risk without any Protection

Reduction

Tolerable Risk ??

Consequence

Demand

DCS
Exercise

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?

SIL 3 loop test frequency calculation

Solution

PFD loop < 10⁻³

\[ PFD_{loop} = PFD_{sensor} + PFD_{valve} + PFD_{final} \]

\[ 10^{-3} = \frac{1}{4} \cdot \lambda_{sensor}^2 \cdot T^2 + \frac{1}{4} \cdot \lambda_{valve}^2 \cdot T^2 + \frac{1}{4} \cdot \lambda_{final}^2 \cdot T^2 \]

\[ 10^{-3} = \frac{1}{4} \cdot \frac{1}{MTBF_{sensor}^2} \cdot T^2 + \frac{1}{4} \cdot \frac{1}{MTBF_{valve}^2} \cdot T^2 + \frac{1}{4} \cdot \frac{1}{900\text{ years}} \cdot T^2 \]

\[ T = \sqrt{\frac{10^{-3}}{3.3 \times 10^{-4}}} \]

\[ T = 1.7\text{ years} \]

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

if \( T = 0.85\text{ years} \), PFD is \( 0.25\times 10^{-3} \)
PFD simplify acc. (ISA 84.00.01-2004)

1001 \[ PFD_{\text{avg}} = \left[ \lambda_{DU} \times \frac{T_I}{2} \right] \]

1002 \[ PFD_{\text{avg}} = \left[ \left( \frac{\lambda_{DU}}{3} \right)^2 \times \frac{T_I}{2} \right] + \left[ \beta \times \lambda_{DU} \times \frac{T_I}{2} \right] \]

1003 \[ PFD_{\text{avg}} = \left[ \left( \frac{\lambda_{DU}}{4} \right)^3 \times \frac{T_I}{2} \right] + \left[ \beta \times \lambda_{DU} \times \frac{T_I}{2} \right] \]

2003 \[ PFD_{\text{avg}} = \left[ \left( \frac{\lambda_{DU}}{2} \right)^2 \times T_I \right] + \left[ \beta \times \lambda_{DU} \times T_I \right] \]

2004 \[ PFD_{\text{avg}} = \left[ \left( \frac{\lambda_{DU}}{3} \right)^3 \times T_I \right] + \left[ \beta \times \lambda_{DU} \times T_I \right] \]

\( \lambda_{DU} \) = Proportion of dangerous undetected faults
\( \beta \) = Error that impacts on more than one channel of a redundant system (Common Cause)
\( T_I \) = Interval between manual functional testing of component

Formulas IEC 61508-6

<table>
<thead>
<tr>
<th>Architecture with low demand rate</th>
<th>High demand or continuous mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1oo1 [ PFD_{H} = \frac{\lambda_{DU}}{\lambda_{DU} + \lambda_{MR}} \times \frac{1}{\bar{MTTR}} ]</td>
<td>( PFD_{H} = \lambda_{DU} )</td>
</tr>
<tr>
<td>1oo2 [ PFD_{H} = \left[ \lambda_{DU} \times \lambda_{MR} \times \frac{1}{\bar{MTTR}} \right] ]</td>
<td>( PFD_{H} = \lambda_{DU} \times \lambda_{MR} \times \frac{1}{\bar{MTTR}} )</td>
</tr>
<tr>
<td>2oo3 [ PFD_{H} = \left[ \lambda_{DU} \times \lambda_{MR} \times \frac{1}{\bar{MTTR}} \right] ]</td>
<td>( PFD_{H} = \lambda_{DU} \times \lambda_{MR} \times \frac{1}{\bar{MTTR}} )</td>
</tr>
<tr>
<td>1oo2D [ PFD_{H} = \left[ \lambda_{DU} \times \lambda_{MR} \times \frac{1}{\bar{MTTR}} \right] ]</td>
<td>( PFD_{H} = \lambda_{DU} \times \lambda_{MR} \times \frac{1}{\bar{MTTR}} )</td>
</tr>
</tbody>
</table>
Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDF</td>
<td>Cumulative Distribution Function</td>
</tr>
<tr>
<td>Electrical/electrical/programmable electronic systems (E/E/PES)</td>
<td>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, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities.</td>
</tr>
<tr>
<td>Equipment under control (EUC)</td>
<td>Failure Mode Effect (and Criticality) Analysis</td>
</tr>
<tr>
<td>ESD</td>
<td>Event Tree Analysis</td>
</tr>
<tr>
<td>ETA</td>
<td>Fault Tree Analysis</td>
</tr>
<tr>
<td>EMECA</td>
<td>Failure Mode Effect and Diagnostics Analysis</td>
</tr>
<tr>
<td>FIT</td>
<td>Hazardous situation which results in harm</td>
</tr>
<tr>
<td>FTA</td>
<td>HAZard and OPerability study</td>
</tr>
<tr>
<td>Hazardous event</td>
<td>Hardware Failure Tolerance</td>
</tr>
<tr>
<td>HAZOP</td>
<td>IEC 61508</td>
</tr>
<tr>
<td>HFT</td>
<td>IEC 61511</td>
</tr>
<tr>
<td>IEC/EN 61508</td>
<td>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.</td>
</tr>
<tr>
<td>IEC/EN 61511</td>
<td></td>
</tr>
<tr>
<td>LDM</td>
<td></td>
</tr>
</tbody>
</table>

Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MooN</td>
<td>M out of N channels</td>
</tr>
<tr>
<td>MTBF</td>
<td>Mean Time between Failures</td>
</tr>
<tr>
<td>MTTF</td>
<td>Mean Time to Failure</td>
</tr>
<tr>
<td>MTRR</td>
<td>Mean Time to Repair</td>
</tr>
<tr>
<td>PDF</td>
<td>Probability Density Function</td>
</tr>
<tr>
<td>PFD</td>
<td>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.</td>
</tr>
<tr>
<td>PFD avg</td>
<td>Average Probability of Failure on Demand</td>
</tr>
<tr>
<td>PFH</td>
<td>Probability of dangerous Failure per Hour</td>
</tr>
<tr>
<td>Risk</td>
<td>Combination of the probability of occurrence of harm and the severity of that harm. Calculated as the product between incident frequency and incident severity</td>
</tr>
<tr>
<td>SFF</td>
<td>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.</td>
</tr>
<tr>
<td>SIF</td>
<td>Safety Instrumented Function</td>
</tr>
</tbody>
</table>
# Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIS</td>
<td>Safety Instrumented System – A SIS (Safety system) comprises one or more safety functions; for each of these safety functions there is a SIL requirement.</td>
</tr>
<tr>
<td>SIL</td>
<td>Safety Integrity Level – 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.</td>
</tr>
<tr>
<td>SLC</td>
<td>Safety Life Cycle – Covers all aspects of safety, including the initial conception, design, implementation, installation, commissioning, validation, maintenance and decommissioning of the risk-reducing measures.</td>
</tr>
<tr>
<td>Safety</td>
<td>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.</td>
</tr>
<tr>
<td>Safety function</td>
<td>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 EU, in respect of a specific hazardous event.</td>
</tr>
<tr>
<td>Tolerable risk</td>
<td>Risk, which is accepted in a given context based upon the current values of society.</td>
</tr>
</tbody>
</table>