Safety-related parts of controls systems (SRP/CS)

The part of the control system of a machine that prevents a hazardous condition from occurring.

Safety Function

A function of a machine that reduces the risk presented by the machine to an acceptable level determined by the risk assessment.
Functional Safety

Safety Function
- If each safety function is executed according to the risk determined by the risk assessment, the machinery can be considered safe and functional safety is achieved.

Safety Integrity
- Safety integrity is the probability that safety related system will satisfactorily perform the required safety function under all stated conditions within a stated period of time when required to do so.

Basic Elements of a Safety Function
- Triggering Event
- Safety-related reaction
- Dangerous part of the machine
Safety Function Example

Requirements:
• The rotor cannot start until the guard is closed
• Opening the guard will cause the rotor to stop
• Closing the guard does not restart the machine
• The circuit that issues the stop command is required to meet the requirements of PLe/ Cat 4

Safety Function

The safety function is executed by all components which are involved in the safety function:
Control System Functional Safety Standards

- ISO 13849-1: Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design
- IEC 62061: Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems
- IEC 61511: Functional safety - Safety instrumented systems for the process industry sector

ISO 13849 and IEC 62061

Performance Level (PL) or Safety Integrity Level (SIL)

What’s the difference?
Performance Level (PL)  
ISO 13849

- Architecture of the system (Category)
- Reliability Data, Mean Time To Dangerous Failure (MTTFd)
- Protection against Common Cause Failure (CCF)
- Protection against systematic faults
- Environmental conditions
- Where relevant, specific requirements for software
Performance Level (PL) & Categories (Cat)

Designated Architecture Categories

Category B
- Basic safety principles
- Fault tolerance of zero

Input Device → Logic → Output Device

Designated Architecture Category B
Designated Architecture Categories

Category 1
- Basic safety principles
- Well tried safety components and principles
- Fault tolerance of zero – but the probability of occurrence is lower than for Category B

![Diagram of Designated Architecture Category 1]

Designated Architecture Categories

Category 2
- Basic safety principles
- Well tried safety components and principles
- Diagnostic monitoring via a functional test of the system or subsystem
- Fault tolerance of zero, the loss of the safety function is detected

![Diagram of Designated Architecture Category 2]
Designated Architecture Categories

**Category 3**
- Basic safety principles, Well tried safety components and principles
- Diagnostic Coverage at least 60%
- Fault tolerance of one, the single fault is detected
- Some but not all faults are detected
- Accumulation of undetected faults can lead to the loss of the safety function

![Designated Architecture Category 3](image)

---

Designated Architecture Categories

**Category 4**
- Basic safety principles
- Well tried safety components and principles
- Diagnostic Coverage at least 99%
- All single dangerous faults and dangerous combinations of faults must be detected

![Designated Architecture Category 4](image)
Graphical Determination of PL

PL

MTTF_s – Low
MTTF_s – Medium
MTTF_s – High

Cat. B
DC_{Cat} None
Cat. 1
DC_{Cat} None
Cat. 2
DC_{Cat} Low
Cat. 3
DC_{Cat} Medium
Cat. 4
DC_{Cat} High

SISTEMA

• Safety Integrity Software Tool for the Evaluation of Machine Applications
• Developed by the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA)
• Automates calculation of the attained Performance Level from the safety-related parts of a machine’s control system to ISO 13849
### Safety Integrity Level (SIL)
**IEC 62061**

<table>
<thead>
<tr>
<th>Element for SIL Consideration</th>
<th>Symbol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probability of Dangerous Failure per Hour</td>
<td>$PFH_{op}$</td>
</tr>
<tr>
<td>Hardware Fault Tolerance</td>
<td>HFT</td>
</tr>
<tr>
<td>Safe Failure Fraction</td>
<td>SFF</td>
</tr>
<tr>
<td>Proof Test Interval</td>
<td>$T_1$</td>
</tr>
<tr>
<td>Diagnostic Test Interval</td>
<td>$T_2$</td>
</tr>
<tr>
<td>Susceptibility to Common Cause Failures</td>
<td>$\beta$</td>
</tr>
<tr>
<td>Diagnostic Coverage</td>
<td>DC</td>
</tr>
</tbody>
</table>

### PL / PFHd / SIL

<table>
<thead>
<tr>
<th>PL (Performance Level)</th>
<th>$PFH_{op}$ (Probability of dangerous failure per hour)</th>
<th>SIL (Safety Integrity Level)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>$\geq 10^5$ to $&lt;10^4$</td>
<td>None</td>
</tr>
<tr>
<td>b</td>
<td>$\geq 2 \times 10^5$ to $&lt;10^5$</td>
<td>1</td>
</tr>
<tr>
<td>c</td>
<td>$\geq 10^4$ to $&lt;3 \times 10^6$</td>
<td>1</td>
</tr>
<tr>
<td>d</td>
<td>$\geq 10^7$ to $&lt;10^6$</td>
<td>2</td>
</tr>
<tr>
<td>e</td>
<td>$\geq 10^8$ to $&lt;10^7$</td>
<td>3</td>
</tr>
</tbody>
</table>
Questions?