Safety Categories, Performance Levels and SILs for Machine Safety Control Systems

Raj Sohal, P.Eng., CHSC
Project Manager
Stantec Consulting Ltd
Outline

• Understanding Risk and its approach towards selection of safety control systems.

• IEC 62061 Approach to Functional Safety based on the SIL assignments.

• ISO 13849 Approach to SRP/CS based on the Performance Levels Requirements.

• Comparing the two approaches.
Machine Safety Control System

• Safety-related parts of control systems (SRP/CS), including the design of software including firmware.

• Parts of machinery control systems that are assigned to provide safety functions are called (SRP/CS).

• The ability of SRP/CS to perform a safety function depends on the specific design criteria and specified behaviors under fault conditions.

ISO-13849-1:2015(E)
Why Safety Control System?

• What's the risk - How do we define it?
• How to determine the risk?
• What criteria do we use?
• How do the risk levels lead to the determination of SRP/CS?
• How to justify the design of the SRP/CS?
• Can we ultimately eliminate the risk?
What's The Risk? How Do We Define It?

• Risk is a function of severity of harm and probability of occurrence of that harm.
• Various risk scoring systems, whether qualitative or quantitative, are used to characterize how these risk factors combine to determine a risk level.
• Using a task-based risk assessment methodology for robots, robot systems and cells.

RIA TR R15.306 and ISO 14121
Performance - Current Standards

• IEC 62061:2005
  – Safety of Machinery - Functional safety of safety-related electrical, electronic and programmable electronic control system

• ISO 13849-1:2015(E)
  – Safety of Machinery – Safety related part of the control system

These two standards address functional safety in similar but different methods. The designer may choose to use either of the two standards.
Performance - Requirement

For robots (type – C Standard), safety-related parts of control systems shall specifically be designed so that they comply with:

– PL=d with structure category 3 as described in ISO 13849-1:2006, OR

– SIL 2 with a hardware fault tolerance of 1 with a proof test interval of not less than 20 years, as described in IEC 62061:2005.
Factors For Design Of SRP/CS

ISO 13849 Approach:

- The ability of SRP/CS to perform a safety function is allocated by one of five levels, called performance levels (PL).
- Design and facilitate the assessment of achieved PL, based on the five levels of categorization of structures according to specific design criteria called category levels.
Factors For Design Of SRP/CS

IEC 62061 Approach:

– The safety integrity requirements for each SRCF shall be derived from the risk assessment to ensure the necessary risk reduction can be achieved.

– Safety integrity requirement is expressed as a target failure value for the probability of dangerous failure per hour of each SRCF.

– The safety integrity requirements for each SRCF shall be specified in terms of a SIL.
IEC 62061 - Terminology

• Safety Related Control Function (SRCF)
  – Control function implemented by SRECS.

• Safety Integrity Level (SIL)
  – Discrete level (one out of a possible three) for specifying the safety integrity requirements of the safety-related control functions to be allocated to the SRECS.

• Probability of Dangerous Failure per hour (PFHd)
  – Average probability of dangerous failure within 1 h.
IEC 62061 – Terminology Cont’d

• Safe Failure Fraction (SFF)
  – Fraction of overall failure rate that does not result in dangerous failure.

• Common Cause Failure (CCF)
  – Failure resulting in coincidental failures of two or more separate channels in a redundant architecture subsystem.

• Diagnostic Coverage (DC)
  – Decrease in probability of dangerous hardware failure, resulting from automatic diagnostic tests.
• Hardware Fault Tolerance
  – In relation to hardware safety integrity, the ability of the component or hardwired subsystem to be able to perform the required safety function during one or more dangerous faults.
  – Tolerance of 1 means that dangerous failure of one of the two components/subsystem does not prevent the safety function being performed.
Risk Estimation Parameters

• **Severity (Se)**
  - Severity of injury or damage to health can be estimated by taking into account reversible injuries, irreversible injuries and death.

• **Consequences**

  | Irreversible: death, losing an eye or arm | 4 |
  | Irreversible: severely broken limb(s), losing a finger(s) | 3 |
  | Reversible: requiring medical treatment | 2 |
  | Reversible: requiring first aid | 1 |
Risk Estimation Parameters

• Probability of Occurrence of Harm
  – Each of the three parameters ($Fr$, $Pr$ and $Av$) should be estimated independently.
  – Use worst-case assumptions to ensure that SRCF(s) are not incorrectly assigned a lower SIL than is necessary.

• Frequency and Duration of Exposure ($Fr$)
  – Frequency of Exposure            Duration $> 10$ min
    $\leq 1$ h                       5
    $> 1$ h to $\leq 1$ day          5
    $> 1$ day to $\leq 2$ weeks      4
    $> 2$ weeks to $\leq 1$ year     3
    $> 1$ year                       2
Risk Estimation Parameters

- Probability of Occurrence of a Hazardous Event (Pr)
  - estimated by taking into account predictability of machine behavior in different modes of use
  - e.g. normal operation, maintenance, fault finding

- Probability (Pr) Classification
  - Probability of Occurrence   Probability (Pr)
    Very high                   5
    Likely                      4
    Possible                    3
    Rarely                      2
    Negligible                  1
Risk Estimation Parameters

• Probability of Avoiding or Limiting Harm (Av)
  – Estimated by taking into account sudden, fast or slow speed of appearance of the hazardous event.
    
    | Class       | Score |
    |-------------|-------|
    | Impossible  | 5     |
    | Rarely      | 3     |
    | Probable    | 1     |

• Class of Probability of Harm (Cl)
  – For a specific hazard, calculate the Class (Cl) by adding Fr, Pr and Av
  – e.g. \( Cl = Fr + Pr + Av \)
# Risk Estimation Parameters

<table>
<thead>
<tr>
<th>Severity (Se)</th>
<th>Class (CI)</th>
<th>3-4</th>
<th>5-7</th>
<th>8-10</th>
<th>11-13</th>
<th>14-15</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>SIL 2</td>
<td>SIL 2</td>
<td>SIL 2</td>
<td>SIL 3</td>
<td>SIL 3</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>OM</td>
<td>SIL 1</td>
<td>SIL 2</td>
<td>SIL 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>OM</td>
<td>OM</td>
<td>SIL 1</td>
<td>SIL 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>OM</td>
<td>SIL 1</td>
<td></td>
</tr>
</tbody>
</table>
Risk Estimation Parameters

• Black boxes with assigned SIL levels are mandatory.

• Grey boxes with no SIL level assigned means recommended other measures.

• A specific hazard with Se=3, Fr=4 and Pr=5 and an Av=5 will be:
  - CI = Fr + Pr + Av
  - CI=4+5+5 =14 for Se of 3
  - Which leads to SIL=3
IEC 62061 – Target Failure Rates

• The safety integrity requirements for each SRCF shall be specified in terms of a SIL.
• A SIL is expressed as a target failure value for the probability of dangerous failure per hour of each SRCF.

<table>
<thead>
<tr>
<th>SIL LEVEL</th>
<th>PFH $d$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>$\geq 10^{-8}$ to $&lt; 10^{-7}$</td>
</tr>
<tr>
<td>2</td>
<td>$\geq 10^{-7}$ to $&lt; 10^{-6}$</td>
</tr>
<tr>
<td>1</td>
<td>$\geq 10^{-6}$ to $&lt; 10^{-5}$</td>
</tr>
</tbody>
</table>
IEC 62061 – Safety Performance

Factors effecting Probability of Dangerous Failures per Hour (PFHD)

- Architecture of the subsystem
- Failure rate (\( \lambda \)) of individual components in the subsystems
- Proof test interval (T1) of the individual component provided by the manufacturer
- Diagnostic Test interval (T2) - number of intended operations per hour of the individual component
- Common Cause Failures (\( \beta \)) as per table F.1, Annex F IEC 62061
- Diagnostic Coverage (DC) as per Table E.1, ISO 13849-1:2015(E)
IEC 62061 – Architectures

• Basic subsystem architecture A: Zero fault tolerant without diagnostic coverage,
  \[ \lambda_{DssA} = \lambda_{De1} + \lambda_{Den} \]
  \[ PFH_{DssA} = \lambda_{DssA} \times 1h \]

• Any dangerous failure of the subsystem causes a failure of the SRCF.
$\lambda_{DssA} = \lambda_{De1} + ... + \lambda_{Den}$  \hspace{1cm} (A)

$PFH_{DssA} = \lambda_{DssA} \times 1h$

Figure 6 – Subsystem A logical representation
IEC 62061 – Architectures

- Basic subsystem architecture B: single fault tolerant without diagnostic coverage
  \[
  \lambda_{DssB} = (1 - \theta)^2 \times \lambda_{De1} \times \lambda_{De2} \times T \times 1 + \theta \times (\lambda_{De1} + \lambda_{De2})/2
  \]
  \[
  PFH_{DssB} = \lambda_{DssB} \times 1h
  \]

- Any single failure of the subsystem does not cause a failure of the SRCF.
IEC 62061 – Architectures

Figure 7 – Subsystem B logical representation
IEC 62061 – Architectures

• Basic subsystem architecture C: Zero fault tolerant with diagnostic coverage

\[ \lambda_{DssC} = \lambda_{De1} (1 - DC_1) + \ldots + \lambda_{Den} (1 - DC_n) \]

\[ PFH_{DssC} = \lambda_{DssC} \times 1h \]

• Any undetected dangerous fault of the subsystem element leads to dangerous failure of the SRCF.

Section 6.7.8.2.4 IEC 62061:2005
IEC 62061 – Architectures

\[ \lambda_{DssC} = \lambda_{De1} (1 - DC_1) + \ldots + \lambda_{Den} (1 - DC_n) \]  

\( PFH_{DssC} = \lambda_{DssC} \times 1h \)
IEC 62061 – Architectures

• Basic subsystem architecture D: single fault tolerant with diagnostic coverage

\[
\lambda_{DssD} = (1 - \theta)^2 \left\{ \left[ \lambda_{De1} \times \lambda_{De2} \times (DC_1 + DC_2) \right] \times T_2/2 + \left[ \lambda_{De1} \times \lambda_{De2} \times (2 - DC_1 - DC_2) \right] \times T_1/2 \right\} + \theta \times \left( \lambda_{De1} + \lambda_{De2} \right)/2
\]

\[
PFH_{DssD} = \lambda_{DssD} \times 1h
\]

• A single failure of any of the subsystem elements does cause a loss of the SRCF.
IEC 62061 – Architectures

Diagram:
- Subsystem D
  - Subsystem element \( \lambda_{de1} \)
  - Diagnostic function(s)
  - Subsystem element \( \lambda_{de2} \)
  - Common cause failure
IEC 62061 – Safety Performance

What about Failure Rates ($\lambda$) for Electromechanical components????
IEC 62061 – Safety Performance

\[ \lambda = 0.1 \times \frac{C}{B_{10}} \]

- \( C \) = Number of operating cycles per hour
- \( B_{10} \) = Number of cycles until 10% of the components fail (provided by the manufacturer)

\[ \lambda = \lambda_s + \lambda_d \]

Where
- \( \lambda_s \) = rate of safe failure
- \( \lambda_d \) = rate of dangerous failure

Note 1: Where a detailed analysis of each failure mode is not possible, a division of failures into 50% safe, 50% dangerous is generally accepted.

Note 1 Per IEC 61508-6; 2010
IEC 62061 – Safety Performance

FOR EXAMPLE:

• Safety Gate Switch: $B_{10}$ value of 1 million and the gate switch is opened once every hour.

• Dangerous Failure rate ($\lambda_d$) per hour is:
  Failure Rate $\lambda = 0.1 \times (1) / 1,000,000 = 1 \times 10^{-7}$
  Thus $\lambda_d = 0.5 \times \lambda = 5 \times 10^{-8} / h.$
ISO 13849 - Terminology

• Safety – Related Part of a Control System
  – SRP/CS, part of a control system that responds to safety-related input signals and generates safety-related outputs.

• Categories (B, 1, 2, 3, & 4)
  – Classification of the safety-related parts of a control system with respect to their resistance to faults. In other words, this refers to the type of circuit architecture used to achieve a performance level.

• MTTF d
  – mean time to dangerous failure.
ISO 13849 – Terminology Cont’d

• **Diagnostic Coverage (DC)**
  – Measure of diagnostic level (for Input/Logic/Output) which may be determined as the ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures.

• **Common Cause Failure (CCF)**
  – Measure of failures of different items resulting from a single event, where these failures are not consequences of each other.
ISO 13849 - Performance Levels

• The ability of safety-related parts of control systems to perform a safety function under foreseeable conditions is allocated by one of five levels, called performance levels (PL).

• These performance levels are defined in terms of probability of dangerous failure per hour.
ISO 13849 - Performance Levels

The probability of dangerous failure of the safety function depends on:

- The extent of fault detection mechanisms [diagnostic coverage (DC)];
- Reliability of components [mean time to dangerous failure (MTTFd)];
- Common cause failure (CCF); and
- Design process, operating stress, environmental conditions and operation procedures.
## ISO 13849 - Performance Levels

<table>
<thead>
<tr>
<th>PL</th>
<th>PFH ( d ) (1/h)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>( \geq 10^{-5} ) to ( &lt; 10^{-4} )</td>
</tr>
<tr>
<td>b</td>
<td>( \geq 3 \times 10^{-6} ) to ( &lt; 10^{-5} )</td>
</tr>
<tr>
<td>c</td>
<td>( \geq 10^{-6} ) to ( &lt; 3 \times 10^{-6} )</td>
</tr>
<tr>
<td>d</td>
<td>( \geq 10^{-7} ) to ( &lt; 10^{-6} )</td>
</tr>
<tr>
<td>e</td>
<td>( \geq 10^{-8} ) to ( &lt; 10^{-7} )</td>
</tr>
</tbody>
</table>

*Table 2 of ISO 13849-1:2005(E)*
Risk Determination Criteria (Robots)

Table 8 of TR R15.306-2015
## Risk Levels Leading To SRP/CS (Robots)

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Minimum SRP/CS requirements</th>
<th>Structure Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEGLIGIBLE (see 5.6.1)</td>
<td>c</td>
<td>1</td>
</tr>
<tr>
<td>LOW</td>
<td>c</td>
<td>2</td>
</tr>
<tr>
<td>MEDIUM</td>
<td>d</td>
<td>2</td>
</tr>
<tr>
<td>HIGH</td>
<td>d</td>
<td>3</td>
</tr>
<tr>
<td>VERY HIGH (see 5.6.2)</td>
<td>e</td>
<td>4</td>
</tr>
</tbody>
</table>
Risk Levels Leading To SRP/CS (Generic)

Figure A.1 ISO 13849-1:2015 (E)
Risk Levels Leading To SRP/CS (Generic)

- Severity of Injury S1 and S2
  - S1 (normally reversible) & S2 (normally irreversible)

- Frequency and/or Exposure Times to Hazards, F1 and F2
  - F1 (infrequent exposure) & F2 (frequent and continuous exposure)

- Possibility of Avoidance Hazard, P1 and P2 and Probability of Occurrence.
  - P1 (possible) & P2 (scarcely possible)
ISO 13849 - Category Levels

Category B:

- The SRP/CS is designed using basic safety principles
- No DC avg required
- MTTFd can be low to medium
- Maximum PL achievable with Category B is PL=b
- CCF not relevant
- When fault occurs it can lead to loss of safety function
ISO 13849 - Category Levels

Category 1:

- The SRP/CS is designed using well-tried safety components and well-tried safety principles
- No DC avg required
- MTTFd of each channel shall be high
- Maximum PL achievable with Category 1 is PL=c
- CCF not relevant
- When fault occurs it can lead to loss of safety function
ISO 13849 - Category Levels

Category 2:

- The SRP/CS is designed using well-tried safety principles
- DC avg required is at least low
- MTTFd of each channel shall be low to high (depending on PLr)
- Maximum PL achievable with Category 2 is PL=d
- Measure against CCF shall be applied
- When fault occurs it can lead to loss of safety function between checks, (but checked during start-up and new cycles)
ISO 13849 - Category Levels

Category 2 Architecture

Input → Logic → Output

Logic → Test equipment(TE) → Output of TE
ISO 13849 - Category Levels

Category 3:

- The SRP/CS is designed using well-tried safety principles
- DC avg required is at least be low to high
- MTTFd of each channel shall be low to high (depending on PLr)
- Maximum PL achievable with Category 3 is PL=d
- Measure against CCF shall be applied
- When fault occurs, it does not lead to loss of safety function, but accumulation of undetected fault can lead to loss of safety function
ISO 13849 - Category Levels

Category 3 Architecture

- Input 1
- Logic 1
- Output 1
- Input 2
- Logic 2
- Output 2

Cross Monitoring
ISO 13849 - Category Levels

Category 4:

- The SRP/CS is designed using well-tried safety principles
- DC avg shall be high
- MTTF of each channel shall be high
- Maximum PL achievable with Category 4 is PL=e
- Measure against CCF shall be applied
- A single fault does not lead to loss of safety function
- Accumulation of undetected faults does not lead to loss of safety function
ISO 13849 - Category Levels

Category 4 Architecture

Input 1 → Logic 1 → Output 1

Cross Monitoring

Input 2 → Logic 2 → Output 2
ISO 13849 - Diagnostic Coverage

<table>
<thead>
<tr>
<th>Denotation</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>NONE</td>
<td>DC &lt; 60%</td>
</tr>
<tr>
<td>LOW</td>
<td>60% ≤ DC ≤ 90%</td>
</tr>
<tr>
<td>MEDIUM</td>
<td>90% ≤ DC ≤ 99%</td>
</tr>
<tr>
<td>HIGH</td>
<td>99% ≤ DC</td>
</tr>
</tbody>
</table>
# ISO 13849 - Evaluating PL

<table>
<thead>
<tr>
<th>Category</th>
<th>B</th>
<th>1</th>
<th>2</th>
<th>2</th>
<th>3</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTTF d of each Channel</td>
<td>None</td>
<td>None</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
<td>high</td>
</tr>
</tbody>
</table>

| Low       | a  | N/A | a  | b  | b  | c  | N/A |
| Medium    | b  | N/A | b  | c  | c  | d  | N/A |
| High      | N/A | c   | c  | d  | d  | d  | e  |

*Table 6 of ISO 13849-1:2005(E)*
## ISO 13849 – CCF Assignment

<table>
<thead>
<tr>
<th>No</th>
<th>Measure against CCF</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Separation/ Segregation</td>
<td>15</td>
</tr>
<tr>
<td>2</td>
<td>Diversity</td>
<td>20</td>
</tr>
<tr>
<td>3</td>
<td>Design/ Application/Experience</td>
<td>20</td>
</tr>
<tr>
<td>4</td>
<td>Assessment/Analysis</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>Competence / Training</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>Environmental</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>Maximum achievable( Total)</td>
<td>100</td>
</tr>
</tbody>
</table>

Table F.1 ISO 13849-1:2015(E)
## ISO 13849 – CCF Assignment

<table>
<thead>
<tr>
<th>TOTAL SCORE</th>
<th>MEASURES FOR AVOIDING CCF</th>
</tr>
</thead>
<tbody>
<tr>
<td>≥ 65</td>
<td>MEETS THE REQUIREMENTS</td>
</tr>
<tr>
<td>&lt;65</td>
<td>PROCESS FAILED. CHOOSE ADDITIONAL MEASURES</td>
</tr>
</tbody>
</table>

*Table F.1 ISO 13849-1:2015(E)*
ISO 13849-Safety Performance

- What about **Mean Time to Dangerous Failure** (MTTF d) for individual components????
- e.g.: pneumatic, mechanical and electromechanically components.
ISO 13849-Safety Performance

• MTTFd for the components are calculated as:

\[ MTTF_d = \frac{B_{10d}}{0.1 \times n_{op}} \]

• Where \( B_{10d} \): is the mean number of cycles until 10% of the components fail dangerously.

• And \( n_{op} \): is the mean number of annual operations.
ISO 13849-Safety Performance

• MTTFd for complete channel is calculated as:

\[
\frac{1}{MTTF_d} = \sum_{i=1}^{N} \frac{1}{MTTF_{d_i}}
\]

• Where \( i_n \): is the number of individual components in the channel.
ISO 13849- Safety Performance

• What if different components are contributing to individual channel (redundant systems) for one output?
• Either use the minimum achieved MTTFd data of each channel, OR
• Calculate per below:

\[
MTTF_d = \frac{2}{3} \left( \frac{1}{MTTF_{d\ c1}} + \frac{1}{MTTF_{d\ c2}} - \frac{1}{MTTF_{d\ c1} + MTTF_{d\ c2}} \right)
\]
## ISO 13849 - Safety Performance

### Table K.1 ISO 13849-1:2015(E)

<table>
<thead>
<tr>
<th>MTTF₂ for each channel years</th>
<th>Cat. B PL DCₐvg = none</th>
<th>Cat. 1 PL DCₐvg = none</th>
<th>Cat. 2 PL DCₐvg = low</th>
<th>Cat. 3 PL DCₐvg = medium</th>
<th>Cat. 3 PL DCₐvg = low</th>
<th>Cat. 4 PL DCₐvg = high</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>3.80 x 10⁻⁵ a</td>
<td>2.58 x 10⁻⁵ a</td>
<td>1.99 x 10⁻⁵ a</td>
<td>1.26 x 10⁻⁵ a</td>
<td>6.09 x 10⁻⁶ b</td>
<td></td>
</tr>
<tr>
<td>3.3</td>
<td>3.46 x 10⁻⁵ a</td>
<td>2.33 x 10⁻⁵ a</td>
<td>1.79 x 10⁻⁵ a</td>
<td>1.13 x 10⁻⁵ a</td>
<td>5.11 x 10⁻⁶ b</td>
<td></td>
</tr>
<tr>
<td>3.6</td>
<td>3.17 x 10⁻⁵ a</td>
<td>2.13 x 10⁻⁵ a</td>
<td>1.62 x 10⁻⁵ a</td>
<td>1.03 x 10⁻⁵ a</td>
<td>4.86 x 10⁻⁶ b</td>
<td></td>
</tr>
<tr>
<td>3.9</td>
<td>2.93 x 10⁻⁵ a</td>
<td>1.05 x 10⁻⁵ a</td>
<td>1.48 x 10⁻⁵ a</td>
<td>9.37 x 10⁻⁶ b</td>
<td>4.40 x 10⁻⁶ b</td>
<td></td>
</tr>
<tr>
<td>4.3</td>
<td>2.65 x 10⁻⁵ a</td>
<td>1.76 x 10⁻⁵ a</td>
<td>1.33 x 10⁻⁵ a</td>
<td>8.39 x 10⁻⁶ b</td>
<td>3.89 x 10⁻⁶ b</td>
<td></td>
</tr>
<tr>
<td>4.7</td>
<td>2.43 x 10⁻⁵ a</td>
<td>1.60 x 10⁻⁵ a</td>
<td>1.20 x 10⁻⁵ a</td>
<td>7.58 x 10⁻⁶ b</td>
<td>3.48 x 10⁻⁶ b</td>
<td></td>
</tr>
<tr>
<td>5.1</td>
<td>2.24 x 10⁻⁵ a</td>
<td>1.47 x 10⁻⁵ a</td>
<td>1.10 x 10⁻⁵ a</td>
<td>6.91 x 10⁻⁶ b</td>
<td>3.15 x 10⁻⁶ b</td>
<td></td>
</tr>
<tr>
<td>5.6</td>
<td>2.04 x 10⁻⁵ a</td>
<td>1.33 x 10⁻⁵ a</td>
<td>9.87 x 10⁻⁶ b</td>
<td>6.21 x 10⁻⁶ b</td>
<td>2.80 x 10⁻⁶ c</td>
<td></td>
</tr>
<tr>
<td>6.2</td>
<td>1.84 x 10⁻⁵ a</td>
<td>1.19 x 10⁻⁵ a</td>
<td>8.80 x 10⁻⁶ b</td>
<td>5.33 x 10⁻⁶ b</td>
<td>2.47 x 10⁻⁶ c</td>
<td></td>
</tr>
<tr>
<td>6.8</td>
<td>1.68 x 10⁻⁵ a</td>
<td>1.08 x 10⁻⁵ a</td>
<td>7.93 x 10⁻⁶ b</td>
<td>4.98 x 10⁻⁶ b</td>
<td>2.20 x 10⁻⁶ c</td>
<td></td>
</tr>
<tr>
<td>7.5</td>
<td>1.52 x 10⁻⁵ a</td>
<td>9.75 x 10⁻⁶ b</td>
<td>7.10 x 10⁻⁶ b</td>
<td>4.45 x 10⁻⁶ b</td>
<td>1.95 x 10⁻⁶ c</td>
<td></td>
</tr>
<tr>
<td>8.2</td>
<td>1.39 x 10⁻⁵ a</td>
<td>8.87 x 10⁻⁶ b</td>
<td>6.43 x 10⁻⁶ b</td>
<td>4.02 x 10⁻⁶ b</td>
<td>1.74 x 10⁻⁶ c</td>
<td></td>
</tr>
<tr>
<td>9.1</td>
<td>1.25 x 10⁻⁵ a</td>
<td>7.94 x 10⁻⁶ b</td>
<td>5.71 x 10⁻⁶ b</td>
<td>3.57 x 10⁻⁶ b</td>
<td>1.53 x 10⁻⁶ c</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>1.16 x 10⁻⁵ a</td>
<td>7.18 x 10⁻⁶ b</td>
<td>5.14 x 10⁻⁶ b</td>
<td>3.21 x 10⁻⁶ b</td>
<td>1.36 x 10⁻⁶ c</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>1.04 x 10⁻⁵ a</td>
<td>6.64 x 10⁻⁶ b</td>
<td>4.53 x 10⁻⁶ b</td>
<td>2.81 x 10⁻⁶ c</td>
<td>1.18 x 10⁻⁶ c</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>9.51 x 10⁻⁶ b</td>
<td>5.84 x 10⁻⁶ b</td>
<td>4.04 x 10⁻⁶ b</td>
<td>2.49 x 10⁻⁶ c</td>
<td>1.04 x 10⁻⁶ c</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>8.78 x 10⁻⁶ b</td>
<td>5.33 x 10⁻⁶ b</td>
<td>3.64 x 10⁻⁶ b</td>
<td>2.23 x 10⁻⁶ c</td>
<td>9.21 x 10⁻⁷ d</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>7.61 x 10⁻⁶ b</td>
<td>4.53 x 10⁻⁶ b</td>
<td>3.01 x 10⁻⁶ b</td>
<td>1.82 x 10⁻⁶ c</td>
<td>7.44 x 10⁻⁷ d</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>7.13 x 10⁻⁶ b</td>
<td>4.21 x 10⁻⁶ b</td>
<td>2.77 x 10⁻⁶ c</td>
<td>1.67 x 10⁻⁶ c</td>
<td>6.76 x 10⁻⁷ d</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>6.34 x 10⁻⁶ b</td>
<td>3.68 x 10⁻⁶ b</td>
<td>2.37 x 10⁻⁶ c</td>
<td>1.41 x 10⁻⁶ c</td>
<td>5.67 x 10⁻⁷ d</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>5.71 x 10⁻⁶ b</td>
<td>3.26 x 10⁻⁶ b</td>
<td>2.06 x 10⁻⁶ c</td>
<td>1.22 x 10⁻⁶ c</td>
<td>4.85 x 10⁻⁷ d</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>5.19 x 10⁻⁶ b</td>
<td>2.93 x 10⁻⁶ b</td>
<td>1.82 x 10⁻⁶ c</td>
<td>1.07 x 10⁻⁶ c</td>
<td>4.21 x 10⁻⁷ d</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE 1** If for category 2 the demand rate is less than or equal to 1/25 of the test rate (see 4.5.4), then the PFH₂ values stated in the Table K.1 for category 2 multiplied by a factor of 1.1 can be used as a worst case estimate.

**NOTE 2** The calculating of the PFH₂ values was based on following DCₐvg:
- DCₐvg = low, calculated with 60 %
- DCₐvg = medium, calculated with 90 %
- DCₐvg = high, calculated with 99 %
## ISO 13849 - Safety Performance

### Table K.1 ISO 13849-1:2015(E)

<table>
<thead>
<tr>
<th>MTTF for each channel years</th>
<th>Cat. B</th>
<th>PL</th>
<th>Cat. 1</th>
<th>PL</th>
<th>Cat. 2</th>
<th>PL</th>
<th>Cat. 3</th>
<th>PL</th>
<th>Cat. 3</th>
<th>PL</th>
<th>Cat. 4</th>
<th>PL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DC&lt;sub&gt;avg&lt;/sub&gt; = none</td>
<td>DC&lt;sub&gt;avg&lt;/sub&gt; = low</td>
<td>DC&lt;sub&gt;avg&lt;/sub&gt; = medium</td>
<td>DC&lt;sub&gt;avg&lt;/sub&gt; = high</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>4.76 x 10^-6 b</td>
<td>2.65 x 10^-4 c</td>
<td>1.62 x 10^-6 c</td>
<td>9.47 x 10^-7 d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>4.23 x 10^-4 b</td>
<td>3.32 x 10^-5 c</td>
<td>1.39 x 10^-6 c</td>
<td>8.04 x 10^-7 d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>3.80 x 10^-6 b</td>
<td>2.06 x 10^-5 c</td>
<td>1.21 x 10^-5 c</td>
<td>6.94 x 10^-7 d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>3.46 x 10^-6 b</td>
<td>1.85 x 10^-6 c</td>
<td>1.06 x 10^-5 c</td>
<td>5.94 x 10^-7 d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>3.17 x 10^-5 b</td>
<td>1.67 x 10^-6 c</td>
<td>9.39 x 10^-7 d</td>
<td>5.16 x 10^-7 d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>2.93 x 10^-5 c</td>
<td>1.53 x 10^-7 c</td>
<td>8.40 x 10^-7 d</td>
<td>4.53 x 10^-7 d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>2.65 x 10^-5 c</td>
<td>1.37 x 10^-6 c</td>
<td>7.34 x 10^-7 d</td>
<td>3.87 x 10^-7 d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>2.43 x 10^-5 c</td>
<td>1.24 x 10^-6 c</td>
<td>6.49 x 10^-7 d</td>
<td>3.35 x 10^-7 d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>2.24 x 10^-5 c</td>
<td>1.13 x 10^-6 c</td>
<td>5.80 x 10^-7 d</td>
<td>2.93 x 10^-7 d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>2.04 x 10^-5 c</td>
<td>1.02 x 10^-6 c</td>
<td>5.10 x 10^-7 d</td>
<td>1.52 x 10^-7 d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>62</td>
<td>1.84 x 10^-5 c</td>
<td>9.06 x 10^-7 d</td>
<td>4.43 x 10^-7 d</td>
<td>2.13 x 10^-7 d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>68</td>
<td>1.60 x 10^-5 c</td>
<td>8.17 x 10^-7 d</td>
<td>3.90 x 10^-7 d</td>
<td>1.84 x 10^-7 d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>75</td>
<td>1.52 x 10^-5 c</td>
<td>7.31 x 10^-7 d</td>
<td>3.40 x 10^-7 d</td>
<td>1.57 x 10^-7 d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>82</td>
<td>1.39 x 10^-5 c</td>
<td>6.61 x 10^-7 d</td>
<td>3.01 x 10^-7 d</td>
<td>1.35 x 10^-7 d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>91</td>
<td>1.25 x 10^-5 c</td>
<td>5.88 x 10^-7 d</td>
<td>2.61 x 10^-7 d</td>
<td>1.14 x 10^-7 d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>1.14 x 10^-5 c</td>
<td>5.28 x 10^-7 d</td>
<td>2.29 x 10^-7 d</td>
<td>1.01 x 10^-7 d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NOTE 1:** If for category 2 the demand rate is less than or equal to 1/25 of the test rate (see 4.5.4), then the PFH<sub>E</sub> values stated in the Table K.1 for category 2 multiplied by a factor of 1.1 can be used as a worst case estimate.

**NOTE 2:** The calculating of the PFH<sub>E</sub> values was based on following DC<sub>avg</sub>:
- DC<sub>avg</sub> = low, calculated with 60 %
- DC<sub>avg</sub> = medium, calculated with 90 %
- DC<sub>avg</sub> = high, calculated with 99 %
Comparing The PLs, SILs And Category:

<table>
<thead>
<tr>
<th>Probability of dangerous failure per hour (PFH&lt;sub&gt;d&lt;/sub&gt;)</th>
<th>ISO 13849-1 Performance levels (PL)</th>
<th>IEC 62061 Safety integrity levels (SIL)</th>
<th>ISO 13849-1 Recommended Safety category</th>
</tr>
</thead>
<tbody>
<tr>
<td>10⁻⁵ &lt; PFH&lt;sub&gt;d&lt;/sub&gt; &lt; 10⁻⁴</td>
<td>A</td>
<td>N/A</td>
<td>b</td>
</tr>
<tr>
<td>3 x10⁻⁶ &lt; PFH&lt;sub&gt;d&lt;/sub&gt; &lt; 10⁻⁵</td>
<td>b</td>
<td>1</td>
<td>b</td>
</tr>
<tr>
<td>10⁻⁶ &lt; PFH&lt;sub&gt;d&lt;/sub&gt; &lt; 3x10⁻⁶</td>
<td>c</td>
<td>1</td>
<td>1 (~) or 2(*)</td>
</tr>
<tr>
<td>10⁻⁷ &lt; PFH&lt;sub&gt;d&lt;/sub&gt; &lt; 10⁻⁶</td>
<td>d</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>10⁻⁸ &lt; PFH&lt;sub&gt;d&lt;/sub&gt; &lt; 10⁻⁷</td>
<td>e</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

(*) = Well tried Safety principles, (~) = Well tried Safety Components
For robots (type – C Standard), safety-related parts of control systems shall specifically be designed so that they comply with:

- PL=d with structure category 3 as described in ISO 13849-1:2006, OR
- SIL 2 with a hardware fault tolerance of 1, with a proof test interval of not less than 20 years, as described in IEC 62061:2005.
Machine Safety Control System

By justifying the design per the required Performance levels and SILs, have we ultimately eliminated the risk?
Can The Risk Be Prevented?
Can The Risk Be Prevented?

• MAYBE

• However, we have reduced the risk to a reasonable level where we can comfortably say the hazardous situation can be prevented, provided...
  
  – End-user Safe Work Procedures for Production and Maintenance tasks, including Zero-Energy LOTO and Alternate Control Measures (ACM) for minor servicing tasks are documented and implemented in the workplace by trained, competent personnel.
At The End

YOU ARE THE KEY......

TO YOUR SAFETY

SmartSign.com • 800-952-1457 • S-4173

www.mysafetysign.com
Contact Information

Raj Sohal, P.Eng., CHSC
Stantec Consulting Ltd.
Waterloo, Ontario Canada

Telephone: +1 (519) 585-7397

raj.sohal@stantec.com