Functional Safety of Machinery: EN ISO 13849-1
Stewart Robinson
TÜV SÜD Product Service
Overview of the presentation

- Defining Safety Functions
- Avoidance of Systematic Failures
- Defining Performance Levels Required
- Verifying Performance Levels Achieved
  - SRP/CS Architectures
  - Component reliability
  - Diagnostic Coverage
- Common Cause Failures
References

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO 13849-1
June 2008

ISO 13849-1:2006

Functional Safety of Machinery: EN ISO 13849

BGIA Report 2/2008e

Functional safety of machine controls – Application of EN ISO 13849 –
Two new functional standards are available for use in the machinery sector.

Source: BGIA Report 2/2008e
Which standard to use?

- **EN 62061**
  - Safety of Machinery: Functional safety of electrical, electronic and programmable electronic control systems
  - Technology specific
  - Covers all levels of complexity

- **EN ISO 13849-1**
  - Safety of machinery — Safety-related parts of control systems Part 1: General principles for design
  - Is a replacement for EN 954-1
  - Not technology specific, can be used for any energy source.
  - Can also be used for Programmable Systems (Safety PLC’s)
EN ISO 13849-1

Proven methods:
- Safety functions
- Risk chart
- Categories

New concepts:
- Quantification: component reliability and test quality
- Common cause failure

Source: BGIA Report 2/2008e
Overall Risk Estimation/Risk Reduction

Figure 1

EN ISO 13849-1
Risk estimation – general principles

Risk related to the identified hazard

\[ \text{Severity of the possible harm (Se)} \]

Risk related to the identified hazard = Severity of the possible harm (Se)

\[ \begin{align*}
\text{Probability of occurrence of that harm} \\
\text{Frequency and duration of exposure (Fr)} \\
\text{Probability of occurrence of a hazardous event (Pr)} \\
\text{Probability of avoiding or limiting harm (Av)}
\end{align*} \]

12/12/2012
Risk Reduction

Source: BGIA Report 2/2008e
What is a Safety Related Control System?

- A control system in a machine should be regarded as being safety-related if it contributes to reducing any risk to an acceptable level or if it is required to function correctly to maintain or achieve safety.
Systematic failure

• Failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors
  – the safety requirements specification,
  – the design, manufacture, installation, operation of the hardware, and
  – the design, implementation, etc., of the software.
• Further information can be found in EN ISO 13849-1, in particular in Annex G
Frequency of Failures

Out of control
Why control systems go wrong and how to prevent failure?

(Out of control, 2nd edition 2003, Health & Safety Executive HSE – UK)
Specifying requirements

EN ISO 13849-1

• 4.2.2 – For each safety function the characteristics and the required performance level shall be specified

• 4.3 Determination of required performance level (PLr)
  – For each selected safety function to be carried out by a SRP/CS, a required performance level (PLr) shall be determined and documented (see Annex A for guidance on determining PLr).
Safety Functions - Examples

- Safety related stop function initiated by safeguard
- Local control function
- Hold to run
- Enabling device
- Muting function
- Prevention of unexpected start up
- Control modes and mode selection
- Emergency stop
EN ISO 13849-1 Annex A risk graph
Risk Graph Parameters

- **Severity of Injury.**
  - S1 Slight injury, (bruise).
  - S2 Severe injury, (Amputation or death).

- **Frequency of exposure to injury.**
  - F1 Seldom.
  - F2 Frequent to continuous (Frequent to continuous are not defined in the standard).

- **Possibility of avoiding the hazard.**
  - P1 Possible.
  - P2 Less possible.
    - Based on the speed of approach of the hazard and the ability of the operator to avoid the hazard. If the operator can avoid the hazard then you would choose P1.
<table>
<thead>
<tr>
<th>PL</th>
<th>Average probability of dangerous failure per hour 1/h</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>$\geq 10^{-5} \text{ to } &lt; 10^{-4}$</td>
</tr>
<tr>
<td>b</td>
<td>$\geq 3 \times 10^{-6} \text{ to } &lt; 10^{-5}$</td>
</tr>
<tr>
<td>c</td>
<td>$\geq 10^{-6} \text{ to } &lt; 3 \times 10^{-6}$</td>
</tr>
<tr>
<td>d</td>
<td>$\geq 10^{-7} \text{ to } &lt; 10^{-6}$</td>
</tr>
<tr>
<td>e</td>
<td>$\geq 10^{-8} \text{ to } &lt; 10^{-7}$</td>
</tr>
</tbody>
</table>
## PL and SIL

<table>
<thead>
<tr>
<th>EN ISO 13849-1 Performance Level (PL)</th>
<th>Average probability of a dangerous failure per hour [1/h]</th>
<th>EN 62061 Safety Integrity Level (SIL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>$\geq 10^{-5}$ to $&lt; 10^{-4}$</td>
<td>no special safety requirements</td>
</tr>
<tr>
<td>b</td>
<td>$\geq 3 \times 10^{-6}$ to $&lt; 10^{-5}$</td>
<td>1</td>
</tr>
<tr>
<td>c</td>
<td>$\geq 10^{-6}$ 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>
EN ISO 13849-1 Clause 4.7

- Verification that achieved PL meets PLr
  - For each individual safety function the PL of the related SRP/CS shall match the required performance level (PLr) determined according to 4.3
  - The PL of the different SRP/CS which are part of a safety function shall be greater than or equal to the required performance level (PLr) of this safety function.
Factors to establish PL

• The Performance Level achieved depends on:
  – The architectures of the SRP/CS
    • Categories
  – The reliability of components
    • Mean Time To Dangerous Failure (MTTFd)
  – The effectiveness of error detection
    • Diagnostic Coverage (DC)
Designated Architectures

- Clause 6 describes “designated architectures” as categories (B, 1 – 4). Categories state the required behaviour of a SRP/CS in respect of it’s resistance to faults etc.
<table>
<thead>
<tr>
<th>B</th>
<th>SRP/CS shall be designed in accordance with relevant standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SRP/CS shall use well tried components and principles. No protection against faults.</td>
</tr>
<tr>
<td>2</td>
<td>SRP/CS shall use well tried principles and functions shall be “checked at suitable intervals”. Testing rate better than 100 times demand rate. No protection against faults.</td>
</tr>
<tr>
<td>3</td>
<td>SRP/CS shall be designed, so that: a single fault in any of these parts does not lead to the loss of the safety function; and whenever reasonably practicable the single fault is detected.</td>
</tr>
<tr>
<td>4</td>
<td>SRP/CS shall be designed, so that: a single fault in any of these parts does not lead to a loss of the safety function; and the single fault is detected at or before the next demand upon the safety function. If this is not possible, then an accumulation of faults shall not lead to a loss of the safety function.</td>
</tr>
</tbody>
</table>
Categories
Structure / Category

Cat B & Cat 1

Cat 2

Cat 4
Architecture - Categories 1 & 2

I Input \[\rightarrow\] L Logic \[\rightarrow\] O Output

Interconnection

Type 2 L/C

Test rate?

Functional Safety of Machinery: EN ISO 13849-1

12/12/2012
Architectures - Categories 3 & 4

Interconnection
Monitoring (reasonably practicable fault detection)
Cross monitoring (reasonably practicable fault detection)

Interconnection
Monitoring
Cross monitoring

I1 Input → L1 Logic → O1 Output
I2 Input → L2 Logic → O2 Output

MC1

I1 Input → L1 Logic → O1 Output
I2 Input → L2 Logic → O2 Output

TÜV SÜD Product Service
12/12/2012
Functional Safety of Machinery: EN ISO 13849-1
Slide 25
Combinations of Categories

Cat. B/1?

Cat. 1

Cat. 1?

Cat. 3/4

Cat. 3?

Cat. 2

Cat. 4

Cat. 1/2

Cat. 4

Cat. 4

Cat. 4
Component reliability - MTTFd

Mean time to dangerous failure, MTTF\textsubscript{d}

The MTTF assumes the fact that every system will fail if you just wait long enough

<table>
<thead>
<tr>
<th>Assessment</th>
<th>MTTF\textsubscript{d}</th>
</tr>
</thead>
<tbody>
<tr>
<td>low</td>
<td>3 years ≤ MTTF\textsubscript{d} &lt; 10 years</td>
</tr>
<tr>
<td>medium</td>
<td>10 years ≤ MTTF\textsubscript{d} &lt; 30 years</td>
</tr>
<tr>
<td>high</td>
<td>30 years ≤ MTTF\textsubscript{d} &lt; 100 years</td>
</tr>
</tbody>
</table>
• EN ISO 13849-1, Clause 4.5.2
• For the estimation of MTTFd of a component, the hierarchical procedure for finding data shall be, in the order given:
  – a) use manufacturer’s data;
  – b) use methods in Annexes C and D;
  – c) choose ten years.
• What do we do if no data is available?
### Good Engineering Practices

<table>
<thead>
<tr>
<th>Component Type</th>
<th>Basic and well-tried safety principles to EN ISO 13849-2:2003</th>
<th>Other relevant standards</th>
<th>Typical values: $MTTF_d$ (years) $B_{10d}$ (cycles) or fault exclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mechanical components</td>
<td>Tables A.1 and A.2</td>
<td>—</td>
<td>$MTTF_d = 150$</td>
</tr>
<tr>
<td>Hydraulic components</td>
<td>Tables C.1 and C.2</td>
<td>EN 982</td>
<td>$MTTF_d = 150$</td>
</tr>
<tr>
<td>Pneumatic components</td>
<td>Tables B.1 and B.2</td>
<td>EN 983</td>
<td>$B_{10d} = 20,000,000$</td>
</tr>
<tr>
<td>Relays and contactor relays with negligible load</td>
<td>Tables D.1 and D.2</td>
<td>EN 50205 IEC 61810 IEC 60947</td>
<td>$B_{10d} = 20,000,000$</td>
</tr>
<tr>
<td>Relays and contactor relays with maximum load</td>
<td>Tables D.1 and D.2</td>
<td>EN 50205 IEC 61810 IEC 60947</td>
<td>$B_{10d} = 400,000$</td>
</tr>
<tr>
<td>Proximity switches with negligible load</td>
<td>Tables D.1 and D.2</td>
<td>IEC 60947 EN 1088</td>
<td>$B_{10d} = 20,000,000$</td>
</tr>
<tr>
<td>Proximity switches with maximum load</td>
<td>Tables D.1 and D.2</td>
<td>IEC 60947 EN 1088</td>
<td>$B_{10d} = 400,000$</td>
</tr>
</tbody>
</table>

Source: BGIA Report 2/2008e

EN ISO 13849-1 Annex C
MTTFd = \frac{B10_d}{0.1 \times n_{op}}

Where \( B10_d \) = mean number of cycles until 10% of the components fail dangerously

\( n_{op} \) = number of operations per year

\[ n_{op} = \frac{d_{op} \times h_{op} \times 3600 \text{ s/h}}{t_{cycle}} \]

Where \( d_{op} \) = number of operating days per year
\( h_{op} \) = number of operating hours per day
\( t_{cycle} \) = cycle time in seconds
Diagnostic Coverage is the fractional decrease in the probability of dangerous hardware failures, resulting from the use of automatic diagnostic tests.

This is determined using the following equation

\[ \text{DC} = \frac{\sum \lambda_{DD}}{\sum \lambda_{D_{\text{total}}}} \]

\( \lambda_{DD} \) is the probability of detected dangerous failures.
\( \lambda_{D_{\text{total}}} \) is the probability of total dangerous failures.
## EN ISO 13849-1 Diagnostic Coverage

### Library of DC Measures

#### SISTEMA default library

<table>
<thead>
<tr>
<th>Description</th>
<th>DC</th>
<th>dependant on</th>
<th>not sufficient for PLs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MEASURES FROM ISO 13849-1:2006, ISO 13849-2:2003, TABLE E.1</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Input devices</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyclic test stimulus by dynamic change of the input signals</td>
<td>90</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Plausibility check, e.g. use of normally open and normally closed mechanical linked contacts</td>
<td>99</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Cross monitoring of inputs without dynamic test</td>
<td>0 - 99</td>
<td>depending on how often a signal change is done by the application</td>
<td></td>
</tr>
<tr>
<td>Cross monitoring of input signals with dynamic test if short circuits are not detectable (for multiple I/O)</td>
<td>90</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Cross monitoring of input signals and intermediate results within the logic (L), and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)</td>
<td>99</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)</td>
<td>90 - 99</td>
<td>depending on the application</td>
<td></td>
</tr>
<tr>
<td>Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)</td>
<td>99</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Fault detection by the process</td>
<td>0 - 99</td>
<td>depending on the application</td>
<td></td>
</tr>
<tr>
<td>Monitoring some characteristics of the sensor (response time, range of analogue signals, e.g. electrical resistance, capacitance)</td>
<td>60</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>
DCavg in accordance with EN ISO 13849-1

Determine the $\text{DC}_{\text{avg}}$, (diagnostic coverage)

Formula for $\text{DC}_{\text{avg}}$

$$
\text{DC}_{\text{avg}} = \frac{\text{DC}_1}{\frac{1}{\text{MTTF}_{d_1}}} + \frac{\text{DC}_2}{\frac{1}{\text{MTTF}_{d_2}}} + \ldots + \frac{\text{DC}_N}{\frac{1}{\text{MTTF}_{d_N}}}
$$

Where $d_1$, $d_2$ and $d_N$ represent the separate parts of the SRP/CS.
Diagnostic coverage is divided into 4 levels.

<table>
<thead>
<tr>
<th>Denotation</th>
<th>Range of DC</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>DC &lt; 60%</td>
</tr>
<tr>
<td>Low</td>
<td>60% ≤ DC &lt; 90%</td>
</tr>
<tr>
<td>Medium</td>
<td>90% ≤ DC &lt; 99%</td>
</tr>
<tr>
<td>High</td>
<td>99% ≤ DC</td>
</tr>
</tbody>
</table>
Relationship - PL and Cat, DC, MTTFd

- Cat B: DC\textsubscript{avg} = 0
- Cat 1: DC\textsubscript{avg} = 0
- Cat 2: DC\textsubscript{avg} = low
- Cat 3: DC\textsubscript{avg} = low
- Cat 4: DC\textsubscript{avg} = high

Legend:
- MTTF\textsubscript{d} = low
- MTTF\textsubscript{d} = medium
- MTTF\textsubscript{d} = high

MTTF\textsubscript{d} = medium

DC\textsubscript{avg} = med.
### Table K.1 — Numerical representation of Figure 5

<table>
<thead>
<tr>
<th>MTTF&lt;sub&gt;d&lt;/sub&gt; for each channel years</th>
<th>Cat. B PL</th>
<th>Cat. 1 PL</th>
<th>Cat. 2 PL</th>
<th>Cat. 2 PL</th>
<th>Cat. 3 PL</th>
<th>Cat. 3 PL</th>
<th>Cat. 4 PL</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>7.61 × 10⁻⁶ b</td>
<td>4.53 × 10⁻⁶ b</td>
<td>3.01 × 10⁻⁶ b</td>
<td>1.82 × 10⁻⁶ c</td>
<td>7.44 × 10⁻⁷ d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>7.13 × 10⁻⁶ b</td>
<td>4.21 × 10⁻⁶ b</td>
<td>2.77 × 10⁻⁶ b</td>
<td>1.67 × 10⁻⁶ c</td>
<td>6.76 × 10⁻⁷ d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>6.34 × 10⁻⁶ b</td>
<td>3.68 × 10⁻⁶ b</td>
<td>2.37 × 10⁻⁶ b</td>
<td>1.41 × 10⁻⁶ c</td>
<td>5.67 × 10⁻⁷ d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>5.71 × 10⁻⁶ b</td>
<td>3.26 × 10⁻⁶ b</td>
<td>2.06 × 10⁻⁶ b</td>
<td>1.22 × 10⁻⁶ c</td>
<td>4.85 × 10⁻⁷ d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>5.19 × 10⁻⁶ b</td>
<td>2.93 × 10⁻⁶ c</td>
<td>1.82 × 10⁻⁶ c</td>
<td>1.07 × 10⁻⁶ c</td>
<td>4.21 × 10⁻⁷ d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>4.76 × 10⁻⁶ b</td>
<td>2.65 × 10⁻⁶ c</td>
<td>1.62 × 10⁻⁶ c</td>
<td>9.47 × 10⁻⁷ d</td>
<td>3.70 × 10⁻⁷ d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>4.23 × 10⁻⁶ b</td>
<td>2.32 × 10⁻⁶ c</td>
<td>1.39 × 10⁻⁶ c</td>
<td>8.04 × 10⁻⁷ d</td>
<td>3.10 × 10⁻⁷ d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>3.80 × 10⁻⁶ b</td>
<td>2.06 × 10⁻⁶ c</td>
<td>1.21 × 10⁻⁶ c</td>
<td>6.94 × 10⁻⁷ d</td>
<td>2.65 × 10⁻⁷ d</td>
<td>9.54 × 10⁻⁸ e</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>3.46 × 10⁻⁶ b</td>
<td>1.85 × 10⁻⁶ c</td>
<td>1.06 × 10⁻⁶ c</td>
<td>5.94 × 10⁻⁷ d</td>
<td>2.30 × 10⁻⁷ d</td>
<td>8.57 × 10⁻⁸ e</td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>3.17 × 10⁻⁶ b</td>
<td>1.67 × 10⁻⁶ c</td>
<td>9.39 × 10⁻⁷ d</td>
<td>5.16 × 10⁻⁷ d</td>
<td>2.01 × 10⁻⁷ d</td>
<td>7.77 × 10⁻⁸ e</td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>2.93 × 10⁻⁶ c</td>
<td>1.53 × 10⁻⁶ c</td>
<td>8.40 × 10⁻⁷ d</td>
<td>4.53 × 10⁻⁷ d</td>
<td>1.78 × 10⁻⁷ d</td>
<td>7.11 × 10⁻⁸ e</td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>2.65 × 10⁻⁶ c</td>
<td>1.37 × 10⁻⁶ c</td>
<td>7.34 × 10⁻⁷ d</td>
<td>3.87 × 10⁻⁷ d</td>
<td>1.54 × 10⁻⁷ d</td>
<td>6.37 × 10⁻⁸ e</td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>2.43 × 10⁻⁶ c</td>
<td>1.24 × 10⁻⁶ c</td>
<td>6.49 × 10⁻⁷ d</td>
<td>3.55 × 10⁻⁷ d</td>
<td>1.34 × 10⁻⁷ d</td>
<td>5.76 × 10⁻⁸ e</td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>2.24 × 10⁻⁶ c</td>
<td>1.13 × 10⁻⁶ c</td>
<td>5.80 × 10⁻⁷ d</td>
<td>2.93 × 10⁻⁷ d</td>
<td>1.19 × 10⁻⁷ d</td>
<td>5.26 × 10⁻⁸ e</td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>2.04 × 10⁻⁶ c</td>
<td>1.02 × 10⁻⁶ c</td>
<td>5.10 × 10⁻⁷ d</td>
<td>2.52 × 10⁻⁷ d</td>
<td>1.03 × 10⁻⁷ d</td>
<td>4.73 × 10⁻⁸ e</td>
<td></td>
</tr>
<tr>
<td>62</td>
<td>1.84 × 10⁻⁶ c</td>
<td>9.06 × 10⁻⁷ d</td>
<td>4.43 × 10⁻⁷ d</td>
<td>2.13 × 10⁻⁷ d</td>
<td>8.84 × 10⁻⁸ e</td>
<td>4.22 × 10⁻⁸ e</td>
<td></td>
</tr>
<tr>
<td>68</td>
<td>1.68 × 10⁻⁶ c</td>
<td>8.17 × 10⁻⁷ d</td>
<td>3.90 × 10⁻⁷ d</td>
<td>1.84 × 10⁻⁷ d</td>
<td>7.68 × 10⁻⁸ e</td>
<td>3.80 × 10⁻⁸ e</td>
<td></td>
</tr>
<tr>
<td>75</td>
<td>1.52 × 10⁻⁶ c</td>
<td>7.31 × 10⁻⁷ d</td>
<td>3.40 × 10⁻⁷ d</td>
<td>1.57 × 10⁻⁷ d</td>
<td>6.62 × 10⁻⁸ e</td>
<td>3.41 × 10⁻⁸ e</td>
<td></td>
</tr>
<tr>
<td>82</td>
<td>1.39 × 10⁻⁶ c</td>
<td>6.61 × 10⁻⁷ d</td>
<td>3.01 × 10⁻⁷ d</td>
<td>1.35 × 10⁻⁷ d</td>
<td>5.79 × 10⁻⁸ e</td>
<td>3.08 × 10⁻⁸ e</td>
<td></td>
</tr>
<tr>
<td>91</td>
<td>1.25 × 10⁻⁶ c</td>
<td>5.88 × 10⁻⁷ d</td>
<td>2.61 × 10⁻⁷ d</td>
<td>1.14 × 10⁻⁷ d</td>
<td>4.94 × 10⁻⁸ e</td>
<td>2.74 × 10⁻⁸ e</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>1.14 × 10⁻⁶ c</td>
<td>5.28 × 10⁻⁷ d</td>
<td>2.29 × 10⁻⁷ d</td>
<td>1.01 × 10⁻⁷ d</td>
<td>4.29 × 10⁻⁸ e</td>
<td>2.47 × 10⁻⁸ e</td>
<td></td>
</tr>
</tbody>
</table>

*Average probability of a dangerous failure per hour (1/h) and corresponding performance level (PL)*

- MTTF<sub>d</sub>: Mean Time To Failure of each channel
- Cat. B: Category B
- Cat. 1: Category 1
- Cat. 2: Category 2
- Cat. 3: Category 3
- Cat. 4: Category 4
- PL: Performance Level

*Source: Functional Safety of Machinery: EN ISO 13849-1*
## EN ISO 13849-1 - Common Cause Failure

### Library of CCF Measures

<table>
<thead>
<tr>
<th>No.</th>
<th>Measure against CCF</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Physical separation between signal paths: separation in wiring / piping, sufficient clearances and creep age distances on printed-circuit boards.</td>
<td>15</td>
</tr>
<tr>
<td>2</td>
<td>Different technologies / design or physical principles are used, for example: first channel programmable electronic and second channel hardwired, kind of initiation, pressure and temperature. Measuring of distance and pressure, digital and analog. Components of different manufactures</td>
<td>20</td>
</tr>
<tr>
<td>3.1</td>
<td>Protection against over-voltage, over-pressure, over-current, etc.</td>
<td>15</td>
</tr>
<tr>
<td>3.2</td>
<td>Components used are well-tried</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>Are the results of a failure mode and effect analysis taken into account to avoid common-cause-failures in design.</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>Have designers / maintainers been trained to understand the causes and consequences of common cause failures?</td>
<td>5</td>
</tr>
<tr>
<td>6.1</td>
<td>Prevention of contamination and electromagnetic compatibility (EMC) against CCF in accordance with appropriate standards. Fluidic systems: filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, e.g. in compliance with the component manufacturers requirements concerning purity of the pressure medium. Electric systems: Has the system been checked for electromagnetic immunity, e.g. as specified in relevant standards against CCF? For combined fluidic and electric systems, both aspects should be considered.</td>
<td>25</td>
</tr>
<tr>
<td>6.2</td>
<td>Other influences. Have the requirements for immunity to all relevant environmental influences such as temperature, shock, vibration, humidity (e.g. as specified in relevant standards) been considered?</td>
<td>10</td>
</tr>
</tbody>
</table>
The $PFH_D$ of the Function is the sum of the $PFH_D$ of each of the SRP/CS (subsystems) that make up the Function.

\[
PFH_{D_{total}} = PFH_{D_{ss1}} + PFH_{D_{ss2}} + PFH_{D_{ss3}} + \ldots + PFH_{D_{ssn}}
\]
Example 1

- Low complexity
8.2.10 Safe stopping of a PLC-driven drive with emergency stop – Category 3 – PL c (Example 10)

Figure 8.19: Stopping of a PLC-driven frequency inverter drive following a stop or emergency stop command

Source: BGIA Report 2/2008e
Thank you for listening

For more information contact:

+44 (0)1642 345637
machinery@tuv-sud.co.uk

www.tuv-sud.co.uk/machinery