ELECTRO-PNEUMATICS AND

SAFETY OF MACHINERY

NEW MACHINERY DIRECTIVE 2006/42/EC
STANDARDS EN/IEC 62061 - EN ISO 13849-1
Principle of the safety of machinery:

To guarantee the safety and health of persons exposed to the installation, operation, adjustment and maintenance of machinery.

Development of the standards

Three key concepts for the design of machinery and their safety functions have emerged from the implementation of the new Machinery Directive 2006/42/EC:

- A risk analysis prior to design
- A particular consideration of the quantitative aspect of the safety functions in addition to the qualitative approach
- The use of performance levels (PL)

Risk evaluation:

The manufacturer or supplier of a machine must see to it that a risk evaluation is conducted to determine the health and safety requirements for persons involved in its operation. The machine must then be designed and constructed in accordance with the results of the risk evaluation.
The products’ reliability data (MTTF, MTTF\textsubscript{d}, B\textsubscript{10}, B\textsubscript{10d}…) gained from reliability tests under standard conditions can be downloaded in the SISTEMA format from our website www.asconumatics.eu.

Actuators (pneumatic cylinders) are not taken into consideration in the calculation of performance levels (PL). Since actuators are not an integral part of the control systems, they do not fall under EN ISO 13849-1 requirements. Manufacturers are, however, required to integrate the risks related to a failure of the actuator into their risk evaluation (EN ISO 14121 and EN ISO 12100).
**Risk Evaluation**

**“Good engineering practice + probabilistic calculations”**

**Construction and risk evaluation of machines**

- **EN ISO 12100**
  - Safety of machinery
  - Basic concepts, general principles for design

- **EN 1050 (EN ISO 14121-1)**
  - Safety of machinery
  - Risk assessment - Part 1: Principles

- Functional and safety-relevant requirements for safety-related control systems

**Design and construction of safety-related control systems for machines**

- **EN/IEC 62061**
  - Design and construction of safety-related control systems for machines

- **EN ISO 13849-1**
  - Electrical safety aspect

**Functional description:**

- **Starting point for estimation of risk**

<table>
<thead>
<tr>
<th>Effects</th>
<th>Severity S</th>
<th>Class</th>
<th>Frequency and/or duration of exposure F</th>
<th>Probability of occurrence O</th>
<th>Probability of damage P</th>
</tr>
</thead>
<tbody>
<tr>
<td>Death, loss of eye or arm</td>
<td>4</td>
<td>SL 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Permanent, loss of fingers</td>
<td>3</td>
<td>SL 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reversible, medical treatment</td>
<td>2</td>
<td>SL 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reversible, first aid</td>
<td>1</td>
<td>SL 3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Safety integrity levels SIL 1, 2, 3**

Any architecture

- **A** → Series arrangement w/o diagnostic function
- **B** → Parallel arrangement w/o diagnostic function
- **C** → Series arrangement with diagnostic function
- **D** → Parallel arrangement with diagnostic function

**Performance levels PL a, b, c, d, e**

Designated architecture (categories)

- **B, 1** → Series arrangement w/o diagnostic function
- **2** → Series arrangement with diagnostic function
- **3, 4** → Parallel arrangement with diagnostic function
Survey of the safety functions of a machine:
- Functional specifications to determine dangerous malfunction
- Safety-related specifications

Select a system architecture among types:
- A, B, C or D

Category B, 1, 2, 3 or 4

Select the system components involved in the safety functions:
- Taking their reliability data into account
  - MTTF, MTTF_d, B_{10d}, B_{100d}, etc.

Specify the diagnostic means for each component to ensure the required DC (Diagnostic Coverage):
- CCF (Common Cause Failure)
- Software
- Architectural requirements
- System integrity

Specify the other requirements:
- CCF
- Software
- Architectural requirements
- System integrity

Create a reliability model or graph for each function to support the different calculations:

Calculate:
- \( \lambda_d \)
- MTTF_d

Derive the safety performance level achievable by the system from:
- SIL EN/IEC 62061
- PL ISO 13849-1

Reliability data for components from manufacturers, standards, databases etc.

MTTF_d : Mean time to dangerous failure – Value expressed in years

\[
\begin{array}{|c|c|}
\hline
\text{Rating for each channel} & \text{MTTF_d} \\
\hline
\text{Low} & 3 \text{ years} < \text{MTTF_d} < 10 \text{ years} \\
\text{Medium} & 10 \text{ years} < \text{MTTF_d} < 30 \text{ years} \\
\text{High} & 30 \text{ years} < \text{MTTF_d} < 100 \text{ years} \\
\hline
\end{array}
\]

B_{10d} : Number of cycles after which 10% of a random sample of wearing components fail dangerously – Value expressed in number of cycles.

DC : Diagnostic Coverage

\[
\begin{array}{|c|c|c|c|}
\hline
\text{None} & \text{Low} & \text{Medium} & \text{High} \\
\hline
\text{DC} < 60\% & 60\% < \text{DC} < 90\% & 90\% < \text{DC} < 99\% & 99\% < \text{DC} \\
\hline
\end{array}
\]

CCF : Common Cause Failure. Measures to be taken to prevent a given cause (and its effect) from concurrently disabling the multiple channels of a safety circuit.

Mission time T_{10} : In line with “good engineering practice” as recommended in EN ISO 13849-1, components attaining this value must be replaced (precautionary principle).
For your safety

Only the pneumatic part is described in the form of a subsystem in these examples. Other safety-related components (e.g. protective devices, electrical logic elements) must be added to ensure the safety function is complete.

The examples shown here only relate to the stopping of hazardous movements. In pneumatics, safety measures concerning the interruption of energy sources, the evacuation of potential energy (pressure contained in a part of the circuit), and a “progressive” start-up after an unexpected shutdown should not be omitted.

To attain a PL = c, category 1 architecture

- **Safety function**: Stopping of the potentially hazardous movement of cylinder 1A.

- **Functional description**:
  - **Categories B and 1**: Input 'I': not represented
  - **Logic element 'L':** not represented, PLC

- **Calculation of the probability of dangerous failure**:

<table>
<thead>
<tr>
<th>Safety function</th>
<th>Working hours / day</th>
<th>Working days / year</th>
<th>Cycles / year</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 cycle = 5 s</td>
<td>16h</td>
<td>240</td>
<td>2 764 800 cycles</td>
</tr>
</tbody>
</table>

By limiting the valve’s operating time to 47 years, this corresponds to a PL = c
To attain a PL = c, category 2 architecture

- **Safety function**: Stopping of the potentially hazardous movement of cylinder 1A.
- **Functional description**:

<table>
<thead>
<tr>
<th>Category</th>
<th>Input signal</th>
<th>Output signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diagnostics</td>
<td>I</td>
<td>L</td>
</tr>
</tbody>
</table>

**Stop of cylinder ensured by:**

- **Output O**: Valve 1V1B

**Diagnostics ensured by:**

- Cross-monitoring in L1 of the supply status coherence of coils 1V1Ba and 1V1Bb and the limit switches 1S1

**0V1**: Energy isolating valve: ensures the system is exhausted in case of loop failure.

**Calculation of the probability of dangerous failure**:

<table>
<thead>
<tr>
<th>Safety function</th>
<th>Working hours / day</th>
<th>Working days / year</th>
<th>Cycles / year</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 cycle = 5 s</td>
<td>16h</td>
<td>240 days</td>
<td>2 764 800 cycles</td>
</tr>
</tbody>
</table>

\[ B_{10d} \text{ (valve 1V1B - series 542)} = 44 912 670 \text{ cycles}, \text{ i.e. an operating time of 16.2 ans,} \]
\[ \text{MTTF}_{d} = 162 \text{ years “high”} \]
\[ \text{MTTF}_{d} \text{ (sensors 1S1)} = 45 000 000 \text{ h,} \]
\[ \text{i.e. 11 718 years “high”} \]

The case study shows:

- DC (Diagnostic Coverage) = 60% “low”.

By limiting the valve’s operating time to 16.2 years, this corresponds to a PL=c for the safety loop.
To attain a PL = d, category 3 architecture

- **Safety function**: Stopping of the potentially hazardous movement of cylinder 1A.
- **Functional description**:

  ![Diagram](image)

  Inputs ‘I1’ and ‘I2’: not represented
  Logic elements ‘L1’ and ‘L2’: not represented, PLC

<table>
<thead>
<tr>
<th>Stop of cylinder ensured by:</th>
<th>Comparison in L1 of the supply status of coils 1V1Ba and 1V1Bb and the limit switches 1S1</th>
<th>Cross-monitoring of L1/L2 status coherence within the PLC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output O1: Valve 1V1B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Output O2: Valve 2V1 controlling the rod lock 2Z1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pressure switch 2S1 for transmission of signal to L2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

  **0V1B**: Energy isolating valve: ensures the system is exhausted

- **Calculation of the probability of dangerous failure**:

<table>
<thead>
<tr>
<th>Safety function</th>
<th>Working hours / day</th>
<th>Working days / year</th>
<th>Cycles / year</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 cycle = 10 s</td>
<td>16 h</td>
<td>240 days</td>
<td>1 382 400 cycles</td>
</tr>
</tbody>
</table>

  \[B_{10d} \text{ (valve 1V1B - series 542)} = 44 912 670 \text{ cycles}, i.e. an operating time of 32.4 years, MTTFd = 324 years “high”\]

  \[B_{10d} \text{ (valve 2V1 - series 520)} = 10 000 000 \text{ cycles}, i.e. an operating time of 7.23 years, MTTFd = 72.3 years “high”\]

  \[B_{10d} \text{ (pressure switch 2S1, dynamic rod lock 2Z1)} = 4 000 000 \text{ cycles}, i.e. a mission time of T10 = 2.89 years, MTTFd = 28.9 years “medium”\]

  \[MTTF_{d} \text{ (sensors 1S1)} = 45 000 000 h, i.e. 11 718 years “high”\]

  The case study shows:

  \[DC \text{ (1V1B)} = 60\% “low”, DC \text{ (2V1)} = 99\% “high”, DC^{+} \text{ (2Z1)} = 75\% i.e. for channel O2, DC = 78\% “low”\].

  **PL**: Performance levels
  - MTTF\(_r\) rating for each channel = low
  - MTTF\(_r\) rating for each channel = medium
  - MTTF\(_r\) rating for each channel = high

  *“Good engineering practice” methods associate this type of component with a low-to-medium DC to cover any of the component’s drift failures.*

By limiting the operating time of the pressure switch and rod lock to 2.89 years, this corresponds to a PL = d for the safety loop.
To attain a PL = d, category 3 architecture

- **Safety function**: Stopping of the potentially hazardous movement of cylinder 1A.
- **Functional description**:

**Input signal**
- I1
- I2

**Diagnostics**
- L1
- L2

**Output signal**
- O1
- O2

Inputs ‘I1’ and ‘I2’: not represented
Logic elements ‘L1’ and ‘L2’: not represented, PLC

---

### Stop of cylinder ensured by:

<table>
<thead>
<tr>
<th>Output O1: Valve 1V1B</th>
<th>Diagnostics ensured by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comparison in L1 of the supply status of coils 1V1Ba and 1V1Bb and the limit switches 1S1</td>
<td>Pressure switch 2S1 for transmission of signal to L2</td>
</tr>
</tbody>
</table>

| Output O2: Valve 2V1 controlling the two 2/2 “cylinder stop” valves used as braking units | Cross-monitoring of L1/L2 status coherence within the PLC |

---

**0V1B**: Energy isolating valve: ensures the system is exhausted.

**Calculation of the probability of dangerous failure**:

<table>
<thead>
<tr>
<th>Safety function</th>
<th>Working hours / day</th>
<th>Working days / year</th>
<th>Cycles / year</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 cycle = 10 s</td>
<td>16h</td>
<td>240 days</td>
<td>1 382 400 cycles</td>
</tr>
</tbody>
</table>

**B_{10d} (valve 1V1B - series 542) = 44 912 670 cycles**, i.e. an operating time of 32.4 years, **MTTF_d = 324 years “high”**

**B_{10d} (valve 2V1 - series 520) = 10 000 000 cycles**, i.e. an operating time of 7.23 years, **MTTF_d = 72.3 years “high”**

**B_{10d} (pressure switch 2S1) = 4 000 000 cycles**, i.e. a mission time of T10 = 2.89 years, **MTTF_d = 28.9 years “medium”**

**B_{10d} (2/2 cylinder stop valves 2V3, 2V2) = 60 000 000 h**, i.e. **MTTF_d = 434 years “high”**

---

*“Good engineering practice” methods associate this type of component with a low-to-medium DC to cover any of the component’s drift failures.*