W09 - Safety Risk Assessments
Determining Machine Safety Performance Levels and Safety Integrity Levels

Mike Duta & Derek Jones
November 2012
Functional Safety

Safety that depends on equipment functioning correctly

What is functional safety?:
Risk reduction due to the correct operation of the Safety Control System that is made up of:

- Task Analysis
- Risk Assessment
- Safety Requirement Specification
- Design & Implementation
- Validation
- Management, Competencies and Organization
Functional Safety Standards

“Generic” Electrical Control Systems

IEC 61508

“Process” Electrical Control Systems

IEC 61511

“Machinery” Electrical Control Systems

IEC 62061

“Machinery” Control Systems (All technologies)

ISO 13849-1

“Automotive” Road vehicles – Functional safety

ISO 26262

SIL

PL

ASIL
EU Legislation

Machinery Directive

"Aim: Harmonization"

EN ISO 13849 (i.e. Standards)

"Each Country: Adoption"

NF EN ISO 13849 France
DIN EN ISO 13849 Germany
UNI EN ISO 13849 Italy
ÖNORM EN ISO 13849 Austria

CE - Information
Directives vs. Standards

Directive = Law:

- Low Voltage Directive 2006/95/CE (Low Voltage Directive)
- ATEX Directive 94/9/EC (Classified Area – Explosives)
- Work Equipment Directive 89/655/EEC
- Framework Directive "worker protection" 89/391/EEC
- Essential Health and Safety Requirements

Standards (European Norms) = Technical Rules

- Standards contain compliance assumptions:
  - EN ISO 12100– Risk Reduction and Risk Assessment methodology
  - EN 62061, EN ISO 13849..... – Functional safety of control systems

CE - Information
Common Essential Health and Safety Requirements

Machinery Directive

2006/42/EC

EHSR’s

Directive on "the use of work equipment" UWED

EHSR’s – Essential Health and Safety Requirements

CE - Information
Machinery Directive - 2006/42/EC

For best info see:
http://ec.europa.eu/enterprise/mechanical_equipment/machinery/index.htm

- Clear requirement for Risk Assessment at design stage
- Full Quality Assurance Scheme for Annex IV machines
- No Certificate of Adequacy option for Annex IV
- Clarification and relevance updated
- Covers partly completed machinery

Guide to Application of the Machinery Directive
In the Machinery Directive, Annex I – the general principles for conformance are communicated

- A Risk Assessment must be carried out to determine the health and safety requirements which apply to the machinery.
  - On Initial machines, the machine concept must be developed prior to the initial risk assessment being performed – this would be an iterative process in the beginning stages of the project
  - The machinery must then be designed and constructed taking into account the results of the risk assessment

**Steps Outlined for a Risk Assessment:**

- Determine the limits of the machinery –
  (intended use and reasonably foreseeable misuse)
- Identify the hazards
- Estimate the Risks
- Evaluate the risk with a view for determining if risk reduction is required
- Eliminate the hazard or reduce the risks by the application of protective measures
Essential Health and Safety Requirements are comprised of 1 main section and 5 supplementary sections

- These sections outline requirements for the application and functional performance of the systems / machine / documentation

**Essential Health and Safety Requirements - (Main Section)**

**Supplementary Essential Health and Safety Requirements:**

- For certain categories of machinery
- To offset hazards due to the mobility of machinery
- To offset hazards due to lifting operations
- For Machinery intended for underground work
- For Machinery presenting particular hazards due to the lifting of persons
EHSR’s cover topics such as these (not all inclusive – see Annex I)

- Definitions
- Principles of Safety Integration
- Materials utilized to construct machinery
- Lighting
- Ergonomics
- Control Systems (Safety and Reliability) – General and specific requirements
- Control Devices
- Starting & Stopping of the machinery
- Selection of Control Modes
- Failure mode considerations – component failure, machine breakup, etc.
- Risks related to a list of many aspects of the use of the machinery
- Guarding requirements
- Maintenance
- Information for use / Marking of machinery
Essential Heath and Safety Requirements (EHSR’s)

- To meet the EHSR’s – there are standards.
  (See List in the Official European Journal) – Part of resources
  **EN Harmonized European Standards**
  - These standards are common to all EEA countries and are produced by the European Standardization Organizations CEN and CENELEC. Their use is voluntary but designing and manufacturing equipment to them is the most direct way of demonstrating compliance with the EHSR’s.

- There are 3 types of Standards:
  - **Type A. Standards**: Cover aspects applicable to all types of machines.
  - **Type B. Standards**: Subdivided into 2 groups.
    - Type B1 STANDARDS: Cover particular safety and ergonomic aspects of machinery.
    - Type B2 STANDARDS: Cover safety components and protective devices.
  - **Type C. Standards**: Cover specific types or groups of machines.
Standards - EN, ISO and IEC

**EXAMPLES**

**Type A**

**Type B**
- **EN ISO 13849-1** - Safety related parts of control systems
- **EN ISO 13850** - Emergency stop function
- **EN / IEC 62061** - Functional safety of electrical control systems
- **EN / IEC 60204-1** - Safety of machinery. Electrical Equipment
- **EN 574 / ISO 13851** – Two hand controls

**Type C**
- **EN ISO 2860** - Earth Moving Machinery
- **EN ISO 8230** - Safety requirements for dry-cleaning machines
Standards for Functional Safety

Other safety type standards

EN ISO 14122 - Safety of machinery. Means of access to machinery
ISO 14120 EN 953 - Safety of machinery -- Guards
EN 614-2 - Safety of machinery. Ergonomic design
etc., etc., etc..

EN ISO 12100

EN ISO 13849
IEC 62061

EN ISO 13849-1 & 2
IEC 62061-1
ISO 23849

EN 60204
EN 61508
EN ISO 13849
IEC/EN 62061

Figure 1 – Relationship of IEC 62061 to other relevant standards
EN ISO 12100: 2010 - Safety of machinery -- General principles for design -- Risk Assessment and Risk Reduction
Methodology using:

- Safety related control functions
- System-based approach

Qualitative Index of Safety: Safety Integrity Level (PL or SIL)
- PL/SIL assessment methodology
- Architecture orientated
- Quantitative indication of safety reliability
- Requirements for avoidance control of systematic failures
Basic terminology, methodology and Technical principles

- Hazard types: Mechanical, electrical, thermal, noise, vibration, radiation, materials and substances, ergonomic, slips trips and falls, environment.

- Risk reduction

- Protective measures

- Inherently safe design measures

- Provisions for maintainability

- Preventing electrical hazards

- Minimizing the probability of failure of safety functions

- Safeguarding and protective measures

- Signals, signs and warning devices

- Indexes to more specific B type standards

EN ISO 12100 provides the frame work for the design of the risk reduction elements:
Time to use our brains!
EN ISO 12100: Safety of Machinery – Risk Assessment and Risk Reduction

- General principles
- Risk estimation
- Checklists of hazard types, hazardous events and hazardous situations

See ISO TR 14121-2 for worked examples of methodologies
Define the Machine Characteristics and Limits (LOM)

(1) Hazard Identification

(2) Risk Estimation

(3) Risk Evaluation

- Acceptable
- Unacceptable

Risk Reduction

Next Hazard

Risk Analysis

Risk Assessment

Risk Tolerable

Fundamental Process
An Example
The Starting Point – Risk Assessment

EN ISO 12100 Safety of machinery — General principles for design — Risk assessment and risk reduction
OSHA 29 CFR 1910 Subpart O - Machinery and Machine Guarding
ANSI B11.0-2010 - Safety of Machinery; General Requirements and Risk Assessment
CSA Z434-04 – Safeguarding of machinery
ISO 10218-1&2: Safety requirements for industrial robots

<table>
<thead>
<tr>
<th>Task Analysis</th>
<th>Hazard Identification</th>
<th>Risk Estimation</th>
<th>Risk Evaluation</th>
</tr>
</thead>
</table>

Table A.19 — Example of a completed hybrid method form

ISO 10218-1&2: Safety requirements for industrial robots
Risk Assessment and Risk Reduction

Hierarchy of measures for risk reduction

• Inherently safe design measures
• Safeguarding and protective measures
• Information for use / training / PPE etc.
• Personal Protective Equipment
Protective Measures and Safety Related Control Systems - EN ISO 13849-1

Protective measures
hazards that will be addressed by a safety related control system

Requirements for access into robot enclosure

• Cleaning
• Teaching
• Maintenance
Protective Measures and Safety Related Control Systems - EN ISO 13849-1

Functional requirements specification

1. **Automatic mode** – Lock the guard door when closed unless power is OFF and motion is stopped.

2. **Automatic Mode** - Isolate power if guard door is not closed.

3. **Teach Mode** - Allow power for robot teaching only with **safe limited speed** conditions and with **local control enabling** **device** activated and **guard door open**
1 – **Automatic mode** - Lock the guard door when closed unless power is OFF and motion is stopped.

### EN ISO 13849-1 Recommendations for its Practical Use

<table>
<thead>
<tr>
<th>Robot axis <strong>power</strong> status</th>
<th>Robot axis <strong>motion</strong> status</th>
<th>Release of <strong>stored energy</strong></th>
<th>Lock release request</th>
<th>Robot in home position</th>
<th>Guard unlock Command Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ON</td>
<td>NOT STOPPED</td>
<td>NOT RELEASED</td>
<td></td>
<td></td>
<td>OFF</td>
</tr>
<tr>
<td>ON</td>
<td>NOT STOPPED</td>
<td>RELEASED</td>
<td></td>
<td></td>
<td>OFF</td>
</tr>
<tr>
<td>ON</td>
<td>STOPPED</td>
<td>NOT RELEASED</td>
<td></td>
<td></td>
<td>OFF</td>
</tr>
<tr>
<td>ON</td>
<td>STOPPED</td>
<td>RELEASED</td>
<td></td>
<td></td>
<td>OFF</td>
</tr>
<tr>
<td>OFF</td>
<td>NOT STOPPED</td>
<td>NOT RELEASED</td>
<td></td>
<td></td>
<td>OFF</td>
</tr>
<tr>
<td>OFF</td>
<td>NOT STOPPED</td>
<td>RELEASED</td>
<td></td>
<td></td>
<td>OFF</td>
</tr>
<tr>
<td>OFF</td>
<td>STOPPED</td>
<td>NOT RELEASED</td>
<td></td>
<td></td>
<td>OFF</td>
</tr>
<tr>
<td>OFF</td>
<td>STOPPED</td>
<td>RELEASED</td>
<td></td>
<td></td>
<td>ON</td>
</tr>
</tbody>
</table>
EN ISO 13849-1 Recommendations for its Practical Use

<table>
<thead>
<tr>
<th>Guard Door Status</th>
<th>Guard Lock Status</th>
<th>Output Actuators Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPEN</td>
<td>UNLOCKED</td>
<td>OFF</td>
</tr>
<tr>
<td>OPEN</td>
<td>LOCKED</td>
<td>OFF</td>
</tr>
<tr>
<td>CLOSED</td>
<td>UNLOCKED</td>
<td>OFF</td>
</tr>
<tr>
<td>CLOSED</td>
<td>LOCKED</td>
<td>ON</td>
</tr>
</tbody>
</table>

2 - Automatic Operation Mode - Isolate power if guard door is not closed and locked
<table>
<thead>
<tr>
<th>Safe Speed</th>
<th>Guard Door Status</th>
<th>Manual Local Control Priority Enabled</th>
<th>Output Actuators Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>CLOSED</td>
<td>NO</td>
<td>OFF</td>
</tr>
<tr>
<td>NO</td>
<td>CLOSED</td>
<td>YES</td>
<td>OFF</td>
</tr>
<tr>
<td>NO</td>
<td>OPEN</td>
<td>NO</td>
<td>OFF</td>
</tr>
<tr>
<td>NO</td>
<td>OPEN</td>
<td>YES</td>
<td>OFF</td>
</tr>
<tr>
<td>YES</td>
<td>CLOSED</td>
<td>NO</td>
<td>OFF</td>
</tr>
<tr>
<td>YES</td>
<td>CLOSED</td>
<td>YES</td>
<td>OFF</td>
</tr>
<tr>
<td>YES</td>
<td>OPEN</td>
<td>NO</td>
<td>OFF</td>
</tr>
<tr>
<td>YES</td>
<td>OPEN</td>
<td>YES</td>
<td>ON</td>
</tr>
</tbody>
</table>

3 - Teach Mode - Allow power for robot teaching only with safe limited speed conditions and with local control enabling device activated and guard door open
EN ISO 13849-1 Recommendations for its Practical Use

What is the required Performance Level (PL)?

<table>
<thead>
<tr>
<th>Safe Speed</th>
<th>Guard Door Status</th>
<th>Manual Local Control Priority Enabled</th>
<th>Output Actuators Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>CLOSED</td>
<td>NO</td>
<td>OFF</td>
</tr>
<tr>
<td>NO</td>
<td>CLOSED</td>
<td>YES</td>
<td>OFF</td>
</tr>
<tr>
<td>NO</td>
<td>OPEN</td>
<td>NO</td>
<td>OFF</td>
</tr>
<tr>
<td>NO</td>
<td>OPEN</td>
<td>YES</td>
<td>OFF</td>
</tr>
<tr>
<td>YES</td>
<td>CLOSED</td>
<td>NO</td>
<td>OFF</td>
</tr>
<tr>
<td>YES</td>
<td>CLOSED</td>
<td>YES</td>
<td>OFF</td>
</tr>
<tr>
<td>YES</td>
<td>OPEN</td>
<td>NO</td>
<td>OFF</td>
</tr>
<tr>
<td>YES</td>
<td>OPEN</td>
<td>YES</td>
<td>ON</td>
</tr>
</tbody>
</table>

Teach Mode Safety Function: Allow power for robot teaching only with safe limited speed conditions and with local control enabling device activated and guard door open.

Safety Related Electrical Control System: Safe Limited Speed

Fully decompose the safety function.
Decomposition of Teach mode safety function

**Teach Mode Safety Function:** Allow power for robot teaching only with **safe limited speed** conditions and with **local control enabling device** activated and **guard door open**

<table>
<thead>
<tr>
<th>Safe Speed</th>
<th>Guard Door Status</th>
<th>Manual Local Control Priority Enabled</th>
<th>Output Actuators Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>CLOSED</td>
<td>NO</td>
<td>OFF</td>
</tr>
<tr>
<td>NO</td>
<td>CLOSED</td>
<td>YES</td>
<td>OFF</td>
</tr>
<tr>
<td>NO</td>
<td>OPEN</td>
<td>NO</td>
<td>OFF</td>
</tr>
<tr>
<td>NO</td>
<td>OPEN</td>
<td>YES</td>
<td>OFF</td>
</tr>
<tr>
<td>YES</td>
<td>CLOSED</td>
<td>NO</td>
<td>OFF</td>
</tr>
<tr>
<td>YES</td>
<td>CLOSED</td>
<td>YES</td>
<td>OFF</td>
</tr>
<tr>
<td>YES</td>
<td>OPEN</td>
<td>NO</td>
<td>OFF</td>
</tr>
<tr>
<td>YES</td>
<td>OPEN</td>
<td>YES</td>
<td>ON</td>
</tr>
</tbody>
</table>

*a - Safe Limited Speed  
b - Enabling function  
c - Guard door closed sensing*
What is the required Performance Level (PLr)?

<table>
<thead>
<tr>
<th>Safe Speed</th>
<th>Guard Door Status</th>
<th>Manual Local Control Priority Enabled</th>
<th>Output Actuators Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>CLOSED</td>
<td>NO</td>
<td>OFF</td>
</tr>
<tr>
<td>NO</td>
<td>CLOSED</td>
<td>YES</td>
<td>OFF</td>
</tr>
<tr>
<td>NO</td>
<td>OPEN</td>
<td>NO</td>
<td>OFF</td>
</tr>
<tr>
<td>NO</td>
<td>OPEN</td>
<td>YES</td>
<td>OFF</td>
</tr>
<tr>
<td>YES</td>
<td>CLOSED</td>
<td>NO</td>
<td>OFF</td>
</tr>
<tr>
<td>YES</td>
<td>CLOSED</td>
<td>YES</td>
<td>OFF</td>
</tr>
<tr>
<td>YES</td>
<td>OPEN</td>
<td>NO</td>
<td>OFF</td>
</tr>
<tr>
<td>YES</td>
<td>OPEN</td>
<td>YES</td>
<td>ON</td>
</tr>
</tbody>
</table>

Teach Mode Safety Function 1: Safe Limited Speed.

Safety Related Electrical Control System: Safe Limited Speed

Shaft Encoders

Safe Speed Sensing

Logic Solving

Output Actuation

Safe Speed Control Unit

Contactors
EN ISO 13849-1 - PL allocation

EN ISO 13849-1
risk graph

PLr allocation for each safety function

For example PLr for safe limited speed function
= PL?
Then we choose the most suitable combination of

Structure (Category), Reliability (MTTFd) and Diagnostics (DC)

To achieve that Performance Level (PL)

Key
PL performance level
1 MTTFd of each channel = low
2 MTTFd of each channel = medium
3 MTTFd of each channel = high
EN ISO 13849-1 Safety of Machinery – Safety Related Parts of Control Systems

See annex K

Shaft Encoders
Safe Speed Control Unit
Contactors

Safety Related Electrical Control System: Safe Limited Speed

---

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

<table>
<thead>
<tr>
<th>t</th>
<th>PL</th>
<th>Cat. 2</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>= none</td>
<td>DC&lt;sub&gt;avg&lt;/sub&gt; = low</td>
<td>Cat. 2</td>
<td>DC&lt;sub&gt;avg&lt;/sub&gt; = medium</td>
<td>Cat. 3</td>
<td>DC&lt;sub&gt;avg&lt;/sub&gt; = low</td>
<td>Cat. 3</td>
<td>DC&lt;sub&gt;avg&lt;/sub&gt; = medium</td>
<td>Cat. 4</td>
<td>DC&lt;sub&gt;avg&lt;/sub&gt; = high</td>
<td></td>
</tr>
<tr>
<td>≤ 10&lt;sup&gt;-6&lt;/sup&gt;</td>
<td>b</td>
<td>1,67 × 10&lt;sup&gt;-6&lt;/sup&gt;</td>
<td>c</td>
<td>9,39 × 10&lt;sup&gt;-7&lt;/sup&gt;</td>
<td>d</td>
<td>5,16 × 10&lt;sup&gt;-7&lt;/sup&gt;</td>
<td>d</td>
<td>2,01 × 10&lt;sup&gt;-7&lt;/sup&gt;</td>
<td>d</td>
<td>7,77 × 10&lt;sup&gt;-8&lt;/sup&gt;</td>
<td>e</td>
</tr>
<tr>
<td>&lt; 10&lt;sup&gt;-6&lt;/sup&gt;</td>
<td>c</td>
<td>1,53 × 10&lt;sup&gt;-6&lt;/sup&gt;</td>
<td>c</td>
<td>8,40 × 10&lt;sup&gt;-7&lt;/sup&gt;</td>
<td>d</td>
<td>4,53 × 10&lt;sup&gt;-7&lt;/sup&gt;</td>
<td>d</td>
<td>1,78 × 10&lt;sup&gt;-7&lt;/sup&gt;</td>
<td>d</td>
<td>7,11 × 10&lt;sup&gt;-8&lt;/sup&gt;</td>
<td>e</td>
</tr>
<tr>
<td></td>
<td>c</td>
<td>1,53 × 10&lt;sup&gt;-6&lt;/sup&gt;</td>
<td>c</td>
<td>7,34 × 10&lt;sup&gt;-7&lt;/sup&gt;</td>
<td>d</td>
<td>3,87 × 10&lt;sup&gt;-7&lt;/sup&gt;</td>
<td>d</td>
<td>1,54 × 10&lt;sup&gt;-7&lt;/sup&gt;</td>
<td>d</td>
<td>6,37 × 10&lt;sup&gt;-8&lt;/sup&gt;</td>
<td>e</td>
</tr>
<tr>
<td></td>
<td>c</td>
<td>6,49 × 10&lt;sup&gt;-7&lt;/sup&gt;</td>
<td>d</td>
<td>5,80 × 10&lt;sup&gt;-7&lt;/sup&gt;</td>
<td>d</td>
<td>1,34 × 10&lt;sup&gt;-7&lt;/sup&gt;</td>
<td>d</td>
<td>5,76 × 10&lt;sup&gt;-8&lt;/sup&gt;</td>
<td>e</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c</td>
<td>6,49 × 10&lt;sup&gt;-7&lt;/sup&gt;</td>
<td>d</td>
<td>5,10 × 10&lt;sup&gt;-7&lt;/sup&gt;</td>
<td>d</td>
<td>1,19 × 10&lt;sup&gt;-7&lt;/sup&gt;</td>
<td>d</td>
<td>5,26 × 10&lt;sup&gt;-8&lt;/sup&gt;</td>
<td>e</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d</td>
<td>4,43 × 10&lt;sup&gt;-7&lt;/sup&gt;</td>
<td>d</td>
<td>2,93 × 10&lt;sup&gt;-7&lt;/sup&gt;</td>
<td>d</td>
<td>4,73 × 10&lt;sup&gt;-8&lt;/sup&gt;</td>
<td>e</td>
<td>4,22 × 10&lt;sup&gt;-8&lt;/sup&gt;</td>
<td>e</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d</td>
<td>3,90 × 10&lt;sup&gt;-7&lt;/sup&gt;</td>
<td>d</td>
<td>2,52 × 10&lt;sup&gt;-7&lt;/sup&gt;</td>
<td>d</td>
<td>3,80 × 10&lt;sup&gt;-8&lt;/sup&gt;</td>
<td>e</td>
<td>3,41 × 10&lt;sup&gt;-8&lt;/sup&gt;</td>
<td>e</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d</td>
<td>3,40 × 10&lt;sup&gt;-7&lt;/sup&gt;</td>
<td>d</td>
<td>1,84 × 10&lt;sup&gt;-7&lt;/sup&gt;</td>
<td>d</td>
<td>6,62 × 10&lt;sup&gt;-8&lt;/sup&gt;</td>
<td>e</td>
<td>3,41 × 10&lt;sup&gt;-8&lt;/sup&gt;</td>
<td>e</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d</td>
<td>1,57 × 10&lt;sup&gt;-7&lt;/sup&gt;</td>
<td>d</td>
<td>8,84 × 10&lt;sup&gt;-8&lt;/sup&gt;</td>
<td>e</td>
<td>4,22 × 10&lt;sup&gt;-8&lt;/sup&gt;</td>
<td>e</td>
<td>3,80 × 10&lt;sup&gt;-8&lt;/sup&gt;</td>
<td>e</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d</td>
<td>1,57 × 10&lt;sup&gt;-7&lt;/sup&gt;</td>
<td>d</td>
<td>4,22 × 10&lt;sup&gt;-8&lt;/sup&gt;</td>
<td>e</td>
<td>3,80 × 10&lt;sup&gt;-8&lt;/sup&gt;</td>
<td>e</td>
<td>3,41 × 10&lt;sup&gt;-8&lt;/sup&gt;</td>
<td>e</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
EN ISO 13849-1 Recommendations for its Practical Use

Safety Related Electrical Control System: Safe Limited Speed

MTTFd of Channel 1

MTTFd of Channel 2

PFHd or MTTFd at Subsystem level
EN ISO 13849-1 Recommendations for its Practical Use

I.3.2 Quantification of MTTF_d for each channel, DC^avg, common

The values for MTTF_d for each channel, DC^avg and common cause fail according to annexes C, D, E and F, or to be given by the manufacturer according to the method of D.1 yields for the MTTF_d of one channel:

\[
\frac{1}{MTTF_d} = \frac{1}{MTTF_{SW1A}} + \frac{1}{MTTF_{K1A}} = \frac{1}{20 \text{ years}} + \frac{1}{50 \text{ years}} = 0.07 \text{ years}^{-1}
\]

E.2 Estimation of average DC (DC^avg)

In many systems, several measures for fault detection might parts of the SRP/CS and have different DC. For an estimation of average, DC for the whole SRP/CS performing the safety function DC may be determined as the ratio between the failure rate of total dangerous failures. According to this definition an average of the following formula:

\[
DC^avg = \frac{DC_1 \times MTTF_{d1} + DC_2 \times MTTF_{d2} + \ldots + DC_N \times MTTF_{dN}}{MTTF_{d1} + MTTF_{d2} + \ldots + MTTF_{dN}}
\]

In the second channel SW2, PLC and CC are contributing to MTTF_d. For these three components as well as for RS a MTTF_d of 20 years is assumed to be given by the manufacturer. The parts count method of D.1 yields for the MTTF_d of the second channel:

\[
\frac{1}{MTTF_{d,C2}} = \frac{1}{MTTF_{d,SW2}} + \frac{1}{MTTF_{d,PLC}} + \frac{1}{MTTF_{d,CC}} = \frac{1}{20 \text{ years}} + \frac{1}{20 \text{ years}} + \frac{1}{20 \text{ years}} = 0.15 \text{ years}^{-1}
\]

which leads to MTTF_d = 6.7 years for the channel.

Because both channels have different MTTF_d, the formula above can be used to calculate a substitutional value for a single-channel MTTF_d of a symmetrical SRP/CS system. This formula yields MTTF_d = 20 years or "medium" for the channel according to Table 5.

DC

In control circuit B, four of the associated parts are tested by the PLC: SW2 and K1B are read back by the PLC, the PLC performs self-tests and the CC is read back via RS by the PLC. The related DC of every tested part are:

1) DC_{SW2} = 99 \%, due to monitoring of input signals without dynamic test, see Table E.1 (third row of input device part),

2) DC_{K1B} = 99 \%, "high", due to normally open and normally closed mechanically linked contacts, see Table E.1 (second row of input device part),

3) DC_{PLC} = 30 \%, due to low effectiveness of self-tests (it is assumed that the manufacturer has calculated this value itself), and

4) DC_{CC} = 90 \%, "medium", redundant shut-off path with monitoring of the actuator by control logic, see Table E.1 (sixth row of input device part) — if the PLC monitors a failure of CC, it is able to stop the motion with the safe implementation (additional shut-off path).

For an estimation of the PL, an average DC value (DC^avg) is needed as input for Figure 5.

\[
DC^avg = \frac{DC_{SW2} \times MTTF_{d,SW2} + DC_{K1B} \times MTTF_{d,K1B} + DC_{PLC} \times MTTF_{d,PLC} + DC_{CC} \times MTTF_{d,CC}}{MTTF_{d,SW2} + MTTF_{d,K1B} + MTTF_{d,PLC} + MTTF_{d,CC}}
\]

\[
= \frac{0.99 \times 20y + 0.9\times 30y + 0.3 \times 20y + 0.6 \times 20y}{20y + 30y + 20y + 20y} = 0.123 - 67.1 \%
\]
SISTEMA (available in multiple languages)

- PL Calculation software for EN ISO 13849-1
- Free to use
- Data Libraries available
- Independent
- Maintained
Where can you download SISTEMA and Data?

IEC 62061 – Machinery safety related E/E/PE control systems

IEC EN 62061 risk chart

Safety Integrity Level
SIL allocation for each safety function

For example safe limited speed function = SIL?
IEC 62061 – Machinery safety related E/E/PE control systems

SIL 3 required for the Safety Function: Teach mode – Safe limited speed

<table>
<thead>
<tr>
<th>Safety integrity level</th>
<th>Probability of a dangerous Failure per Hour ($PFH_D$)</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>

<table>
<thead>
<tr>
<th>Safe failure fraction</th>
<th>Hardware fault tolerance (see Note 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
</tr>
<tr>
<td>&lt; 60 %</td>
<td>Not allowed (for exceptions see Note 3)</td>
</tr>
<tr>
<td>60 % – &lt; 90 %</td>
<td>SIL1</td>
</tr>
<tr>
<td>90 % – &lt; 99 %</td>
<td>SIL2</td>
</tr>
<tr>
<td>≥ 99 %</td>
<td>SIL3</td>
</tr>
</tbody>
</table>

Shaft Encoders
Safe Speed Control Unit
Contactors
Safety Related Electrical Control System: Safe Limited Speed
SIL 3 required for the Safety Function: Teach mode – Safe limited speed

Subsystems:
- Subsystem 1:
  - SIL CL = 3
  - PFH\_D = 4.3 \times 10^{-8}
- Subsystem 2:
  - SIL CL = 3
  - PFH\_D = 3.38 \times 10^{-9}
- Subsystem 3:
  - SIL CL = 3
  - PFH\_D = 1.50 \times 10^{-9}

Total PFH\_D = 4.788 \times 10^{-8}

SIL achieved = 3
The real world - HRN
From Risk assessment to PL
The real world - HRN
From Risk assessment to PL

Risk Assessment of overall machine

Hazard Identities

HRN (Hazard rating number)

Qualitative information

Map HRN to ISO13849 / IEC 62061 Risk Graph

Risk Reduction of overall machine

Differently safe design of machine and its control system

Guards & protective devices

Information & PPE

Safety Functional Requirement

PLr / SIL Safety Integrity Requirement

Design of safety Function(s)

ISO 13849-1
Or
IEC 62061
SISTEMA

Did I increase or reduce The original HRN?
Severity? Probability?
Risk Assessment of overall machine
- Hazard Identities
- HRN (Hazard rating number)
- Qualitative information

Risk Reduction of overall machine
- By inherently safe design of machine and its control system
- Guards & protective devices
- Information & PPE

Map HRN to ISO13849 / IEC 62061
- Risk Graph

Safety Functional Requirement
- PLr / SIL Safety Integrity Requirement

Did I increase or reduce The original HRN? Severity? Probability?

Design of safety Function(s)
- ISO 13849-1
- Or
- IEC 62061
- SISTEMA
Thank you for participating