Introduction to Functional Safety
Focus: ISO 13849-1

Dave Rasmussen
Functional Safety Engineer
(TÜV Rheinland, #4188/11, Machinery)
North America Safety Manager

PUBLIC INFORMATION
Agenda

- Standards – Global and North America
- ISO 13849-1
- Performance Levels – 6 Steps
- SISTEMA
- Rockwell Automation Verification Tools
- Mechanical – Cat and PL
OSHA CFR 1910 Standards

Question: What OSHA standards apply to machine guarding of production equipment?

- **CFR 1910.147 – Lockout / Tagout Standard**
  - Applies when employees perform maintenance and service to production equipment
  - Requires that unexpected energization of equipment be prevented by removing all energy from a machine and locking the energy sources in the off-state whenever an employee must place any part of their body in a potentially hazardous location

- **CFR 1910 Subpart O – Machine Guarding Standards**
  - Applies when employees operate and work around equipment that is in the production state
  - Requires that employers provide safeguarding of hazards that could cause injury or illness to employees

- **Exception to Lockout/Tagout**
  - Applies when employees perform “minor servicing” to equipment
  - Requires that employers provide effective “alternative measures” to safeguard employees
Relationship of OSHA Standards

**Machine Maintenance**
- **Regulation:** Lockout / Tagout per CFR 1910.147
- **Requirement:** Release stored energy
- **Tasks:** Isolation of Mechanical / Electrical Equipment for Service and Maintenance

**Production Operation**
- **Regulation:** Machine Guarding per CFR 1910 Subpart O
- **Requirement:** Protect operators from machine production hazards
- **Tasks:** Operator Interaction for Regular Machine Production

**Minor Servicing Exception**
- **Regulation:** Machine Guarding per Subpart O
- **Requirement:** Protect operators from machine production hazards when performing minor servicing
- **Tasks:** Minor servicing such as clearing minor jams, minor tool changes & adjustments, exchange of work piece, etc.

*Minor servicing must be **routine, repetitive and integral** to the operation*
OSHA lists National Consensus, that provide guidance

https://www.osha.gov/SLTC/robotics/
https://www.osha.gov/Publications/Mach_SafeGuard/chapt5.html

National Consensus

Note: These are NOT OSHA regulations. However, they do provide guidance from their originating organizations related to worker protection.

American National Standards Institute (ANSI)

- R15.06-1999, Industrial Robots and Robot Systems - Safety Requirements
EN/ISO and OSHA/ANSI Standards Hierarchy Comparison

- **European Machine Directive 2006/42/EC**
- **OSHA Machine Safety 1910.xxx**
- **Safety of Machinery– General Principles of Design and Risk Assessment ANSI/ISO 12100**
- **Safety of Machinery– General Principles of Design and Risk Assessment ANSI/ISO 12100**
- **Machine Safety - safety-related parts of control systems EN/ISO 13849-1 PL a-e**
- **Machine Safety - Functional safety of control systems IEC 62061 SIL 1-3**
- **Performance Criteria for Safe Guarding ANSI B11.19**
- **Machine Safety - Electrical equipment of machines IEC 60204-1**
- **Electrical equipment of machines ANSI/NFPA 79**

Control Reliable
Harmonization: ANSI/RIA 15.06-2012


- Harmonization of standards
  - ANSI: American Nation Standards Institute
  - RIA: Robotic Industries Association
  - ISO: International Organization of Standardization

- True Global Robotics Safety Standard
  - No added North American Material
History of Development

RIA 15.06-1999

ISO 10218-2011

RIA 15.06-2012
Major Shifts

- Risk Assessment Required
- Terminology
- Safeguarding Dimensions
- Clearance Dimensions
- Collaborative robot applications (4 types)
  - Safety-rated monitored stop
  - Hand-guided (automatic, not teach/manual)
  - Power and force limited
  - Speed & separation limited
- Safety Control Circuitry transitions to Functional Safety
- References ISO standards (including ISO 14119)
Machine Directive

Machinery Official Journal (OJ) – Published Standards

- Free download search “Machinery OJ”
- Assumption of Conformity – all relevant harmonized standards and directives are obeyed

<table>
<thead>
<tr>
<th>BS EN ISO 13849-1:2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>BS – British Standard</td>
</tr>
<tr>
<td>EN – European Norm</td>
</tr>
<tr>
<td>ISO – International Standards Organization</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CEN</th>
<th>Reference and title of the harmonized standard (and reference document)</th>
<th>First publication OJ</th>
<th>Reference of superseded standard</th>
<th>Date of cessation of presumption of conformity of superseded standard</th>
</tr>
</thead>
</table>
ISO Standard Development

Development of ISO 13849 – Technical Committee 199

- Like United Nations
  - One Country = One Vote
  - ANSI gets one vote, BSI gets one vote

- Ex: Rockwell → ANSI → ISO
Agenda

- Standards – Global and North America
- ISO 13849-1
- Performance Levels – 6 Steps
- SISTEMA
- Rockwell Automation Verification Tools
- Mechanical – Cat and PL
Choose a Relevant Safety Standard

BS EN ISO 13849-1:2008
Safety of machinery - Safety-related parts of control systems
Part 1: General principles for design
# EN 954 vs. EN/ISO 13849

## EN 954 vs. EN/ISO 13849

<table>
<thead>
<tr>
<th>Structure (Categories)</th>
<th>Qualitative</th>
<th>Quantitative</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTTF&lt;sub&gt;d&lt;/sub&gt;</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Diagnostic Coverage (DC)</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Common Cause Failures (CCF)</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Software</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Systematic Failure</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Behavior Under Fault conditions</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Environmental</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

**EN 954** was basically a **Qualitative** approach. **Time & Component Reliability** are **Quantitative** aspects which must now be considered when developing a safety control system using **EN/ISO 13849-1**.
ISO 13849-1

Thumb through:
98 pages in 30 minutes
Functional Safety Design Process - the “Safety Life Cycle”

1. Assessment

2. Functional Requirements

3. Selection, Design & Verification

4. Installation & Validation

5. Operate, Maintain & Improve

The Machinery Safety Lifecycle is a defined process that is followed to ensure that proper safety practices have been implemented!
Risk Assessment Process
ISO12100

Risk Assessment: Determine the Level of Safety Required

Risk Assessment Process 13849-1 Annex A

Machine Characteristics/Limits

- Hazard Identification
- Risk Estimation
- Risk Evaluation

Risk Reduction

OK: Risk Tolerable

Too High

S = Severity
F = Frequency or Duration of Exposure
P = Avoidance Probability

S1 → F1 → P1 → a
S1 → F2 → P2 → b
S1 → F1 → P1 → c
S1 → F2 → P2 → d
S2 → F1 → P1 → e
S2 → F2 → P2 → d
Possible Mitigation Techniques

Hierarchy of Protective Measures

- Design it out
- Fixed enclosing guard
- Monitoring Access / Interlocked Gates
- Awareness Means, Training and Procedures (Administrative)
- Personal protective equipment

Most Effective

Least Effective
For each safety function, the characteristics (see Clause 5) and the required performance level shall be specified and documented in the safety requirements specification. (13849-1 4.2.2)

- **Safety Function** - function of the machine whose failure can result in an immediate increase of the risk(s)

- System components include
  - Input
  - Logic
  - Output
Safety Function Details - Input

The guard door closed safety interlock is connected to a pair of pulse tested safety inputs of a 1734-IB8S module. The I/O module is connected via CIP Safety over an EtherNet/IP network to the GuardLogix safety controller.

The operation of the guard door locking solenoid is controlled by a pulse tested output from a 1734-OB8S output module. The status of the solenoid lock is monitored with a pulse tested safety input of a 1734-IB8S module.

The safety code in the safety processor monitors the status of the safety input using a pre-certified safety instruction named Dual Channel Stop Test and Lock (DCSTL). When the safety gate is closed and locked with no faults detected on the input modules, the safety circuit can be reset. The guard door will only unlock when all hazardous conditions in a safety zone have been controlled. A zone lockout condition shall also unlock the guard door.

<table>
<thead>
<tr>
<th>Catalog Number</th>
<th>Description</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>440G-T27259</td>
<td>TLS-GD2 Safety Switch</td>
<td>1</td>
</tr>
<tr>
<td>1734-AENTR</td>
<td>24V DC Ethernet Adapter – Dual Port</td>
<td>1</td>
</tr>
<tr>
<td>1734-TB</td>
<td>Module Base with Removable IEC Screw Terminals</td>
<td>4</td>
</tr>
<tr>
<td>1734-IB8S</td>
<td>Safety Input Module</td>
<td>1</td>
</tr>
<tr>
<td>1734-OB8S</td>
<td>Safety Output Module</td>
<td>1</td>
</tr>
</tbody>
</table>
Hazardous motion is prevented by the drive Safe Torque Off (STO). The PowerFlex 525 STO inputs are connected to a pair of pulse tested outputs on the 1734-OB8S output module. The I/O module is connected via CIP Safety over an EtherNet/IP network to the GuardLogix safety controller. The safety code uses a block called Configurable Redundant Output (CROUT) to control outputs connected to the drive STO inputs. There is no hardwired feedback for the PowerFlex 525 STO, so the CROUT shall use the output as feedback. The status of the STO is obtained via EtherNet/IP and shall be included in the zone safety Reset signal logic to verify operation.

Where a Cat0 stop is required by the risk assessment the STO inputs will be removed upon actuation of the safeguard.

Where a Cat1 stop is required by the risk assessment the drive will be issued a fast stop command upon actuation of the safeguard, followed by a time delayed removal of STO inputs. The time delay will be based on normal running conditions, and shall allow the drive time to stop the load.

When all safeguard conditions are satisfied, no faults are detected on the safety zone, and the reset push button is pressed, the controller then issues an output signal to the safety output module to switch ON a pair of outputs to energize the STO.
### Zone Specific Details:

<table>
<thead>
<tr>
<th>Name</th>
<th>Quantity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Level</td>
<td>Cat3/PLd</td>
<td>Prescribed by RIA 15.06-2012</td>
</tr>
<tr>
<td>E-stops</td>
<td>2</td>
<td>Robot, Front</td>
</tr>
<tr>
<td>Lockout</td>
<td></td>
<td>Energy source locations defined by customer LOTO policy</td>
</tr>
<tr>
<td>Guarding</td>
<td>Lockout All</td>
<td>Perimeter barrier guarding encloses the entire area</td>
</tr>
<tr>
<td>Guard Doors</td>
<td>1</td>
<td>Locking guard door switch</td>
</tr>
<tr>
<td>Light Curtains</td>
<td></td>
<td>NA</td>
</tr>
<tr>
<td>Entry Keys</td>
<td>1</td>
<td>ProSafe Key</td>
</tr>
<tr>
<td>Safe-Off Drives</td>
<td>1</td>
<td>Grinder – PowerFlex 525</td>
</tr>
<tr>
<td>Safety Contactors</td>
<td>1</td>
<td>Robot safety interface contacts - redundant</td>
</tr>
<tr>
<td>Pneumatics</td>
<td></td>
<td>NA</td>
</tr>
<tr>
<td>Hydraulics</td>
<td></td>
<td>NA</td>
</tr>
<tr>
<td>Zero Speed</td>
<td>1</td>
<td>Grinder Time Delay, based on tested stop rate</td>
</tr>
<tr>
<td>Reset</td>
<td></td>
<td>Machine Reset PB or HMI</td>
</tr>
<tr>
<td>Gravitational</td>
<td></td>
<td>NA</td>
</tr>
<tr>
<td>General Operation</td>
<td></td>
<td>Cat1 stop required per risk assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Estop, Guard Door open or unlocked issues a Cat1 stop</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access key will issue a cycle stop, followed by a Cat1 stop.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Estop ok, Guard Door closed and locked, access key in run position along with</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a reset will enable safety circuit.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guard Door will remain locked until grinder has reached zero speed.</td>
</tr>
<tr>
<td>Notes:</td>
<td></td>
<td>Conveyors 1 and 2 to be safeguarded by customer, and user warning signs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>regarding maintained power</td>
</tr>
</tbody>
</table>
My assessment & requirements spec sure made this easy!

Design considerations:
- What mitigation technique should I use?
- What circuit structure should I use?
- What safety products should I use?
- What type of control system should I use?
- What type of special operations do I need?
- Where are all of my safety devices?
- What kind of interactions are needed for auxiliary machines?
- What kind of diagnostics do I need?
- Should I use hardwiring or networked systems?
How do I verify my design!

Design verification:
- Review safety system design
- Compile product safety and reliability data
- Estimate number of operations
- Calculate Performance Level

\[
\text{MTTF}_d = \frac{2}{3} \left( \frac{1}{\text{MTTF}_{d1}} + \frac{1}{\text{MTTF}_{d2}} \right)
\]

\[
\text{DC}_{\text{avg}} = \frac{\text{DC}_1}{\text{MTTF}_{d1}} + \frac{\text{DC}_2}{\text{MTTF}_{d2}} + \ldots + \frac{\text{DC}_N}{\text{MTTF}_{dN}}
\]
How is my safety system installed?

Installation:
- Verify installation of safety components per functional specification
- Verify wiring methods and grounding
- Confirm signage and labeling
- Confirm wiring per electrical schematics
How do I validate my safety system?

Validation:
- Specific instructions regarding the validation of each safety function
  - Normal operation test:
    - safety input, logic, output
  - Abnormal operation test
    - Shorting wires, breaking connections, removing wires, etc.

ISO 13849-2 Part 2: Validation
How do I operate my machine?

- Training for all personnel that will be interacting with the machine.
- The training should include:
  - Intended use
  - Safety system components training
  - Normal operation
  - Safety system operation
How do I maintain my safety system?

- Periodic testing should be done to verify proper system functionality.
- Machine modifications that affect safety require validation of the safety function
  - Program changes
  - Safety system use
  - Hardware or software changes
  - Machinery changes

Should the safety-related software be subsequently modified, it shall be revalidated on an appropriate scale. ISO 13849-2, 9.5
Agenda

Standards – Global and North America

ISO 13849-1

Performance Levels – 6 Steps

SISTEMA

Rockwell Automation Verification Tools

Mechanical – Cat and PL
6 Steps to Performance Level

There are six basic steps required to determine the Performance Level.

**Step 1** – Determine the required performance level (PLr)

**Step 2** – Identify the SRP/CS Components & Design Block Diagram

**Step 3** – Evaluate the Performance Level (PL)

  **Step 3a** - Category
  **Step 3b** - Mean Time to Dangerous Failure (MTTFd)
  **Step 3c** - Diagnostic Coverage (DC)
  **Step 3d** - Common Cause Failure (CCF)

**Step 4** – Develop Safety-Related Software (If Required)

**Step 5** – Verification of Performance Level (PL \(\geq\) PLr)

**Step 6** – Validation that all requirements are met
Step 1
Required Performance Level (PLr)

The Risk Assessment determines Required Performance Level (PLr)

Choose the most suitable combination of:

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

<table>
<thead>
<tr>
<th>Performance level</th>
<th>NOT COVERED</th>
<th>NOT COVERED</th>
<th>NOT COVERED</th>
<th>NOT COVERED</th>
<th>NOT COVERED</th>
<th>NOT COVERED</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>e</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Designated architecture</th>
<th>Designated architecture</th>
<th>Designated architecture</th>
<th>Designated architecture</th>
<th>Designated architecture</th>
<th>Designated architecture</th>
<th>Designated architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cat B</td>
<td>Cat 1</td>
<td>Cat 2</td>
<td>Cat 2</td>
<td>Cat 3</td>
<td>Cat 3</td>
<td>Cat 4</td>
</tr>
<tr>
<td>DC_{avg} &lt;60%</td>
<td>DC_{avg} &lt;60%</td>
<td>DC_{avg} 60%&lt;90%</td>
<td>DC_{avg} 90%&lt;99%</td>
<td>DC_{avg} 60%&lt;90%</td>
<td>DC_{avg} 90%&lt;99%</td>
<td>DC_{avg} 99%</td>
</tr>
</tbody>
</table>

Key:
- Green: MTTFd of each channel = from 3 years to <10 years
- Yellow: MTTFd of each channel = from 10 years to <30 years
- Red: MTTFd of each channel = from 30 years to <100 years

Copyright © 2014 Rockwell Automation, Inc. All Rights Reserved.
Step 2
Identify Component & Block Diagram

- Typical safety function diagram:

  Sensing element          Control element          Final Element
  INPUT                   LOGIC SOLVING                 OUTPUT

- The machine designer shall select an architecture that will meet the needs of the safety function.
  - Cat B, 1, 2, 3 or 4
Step 3
Evaluate the Performance Level

Safety categories (same as in EN 954-1)

| B | 1 | 2 | 3 | 4 |

Reliability of the HW: MTTF_d

Quality of the diagnostic measures: DC (cat. 2 and higher)

Sufficient measures against Common Cause Failures (CCF)

Performance Level (PL) acc. to EN ISO 13849-1

a b c d e

Measures to avoid systematical failures (QM)
The structure and behavior of the safety function under fault conditions

Designated Architecture Category B

Requirements

• Basic Safety principles
• Withstand expected influences

Behavior under fault conditions
A fault can cause a loss of the safety function.

Typical implementation

Designed to product standards e.g. IEC 60947-5-2 (not specific safety standards)

Designed for environment and electrical safety aspects e.g., IEC 60204-1
Step 3a
Structure Category 1

The structure and behavior of the safety function under fault conditions

Designated Architecture Category 1

Requirements

- Category B
- Well tried components
- Well tried safety principles

Behavior under fault conditions

A fault can cause a loss of the safety function.

Typical implementation

- Input device
- Logic
- Output device

- Contactor
- Guard interlock switch
- Motor
- Machine Control
Step 3a
Safety Principles and Components

- Safety system design begins with the use of ‘well tried’ engineering principles and ‘well tried’ components.

<table>
<thead>
<tr>
<th>Basic Safety Principles (Cat. B)</th>
<th>Well Tried Safety Principles (Cat. 1 – 4)</th>
<th>Well Tried Components (Cat. 1 – 4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed per Instructions</td>
<td>Use Mechanically Linked Contacts</td>
<td>Direct Opening Switches</td>
</tr>
<tr>
<td>Voltage &amp; Current Ratings</td>
<td>Redundant Devices</td>
<td>E-Stop Devices</td>
</tr>
<tr>
<td>Environmental Conditions</td>
<td>Diverse Technologies</td>
<td>Fuses/Circuit Breakers</td>
</tr>
<tr>
<td>N.C. Inputs &amp; N.O. Outputs</td>
<td>Monitoring/Diagnostics</td>
<td>Contactors</td>
</tr>
<tr>
<td>Transient Suppression</td>
<td>Limitation of Energy</td>
<td>Mechanically Linked Contacts</td>
</tr>
<tr>
<td>No Unexpected Start-up</td>
<td>Over-Dimensioning (Factor of 2)</td>
<td>Auxiliary Contactor/Relay</td>
</tr>
<tr>
<td>Secure Mounting of Devices</td>
<td>No Undefined States</td>
<td>Interlocks</td>
</tr>
<tr>
<td>Control Circuit Protection</td>
<td>Separation of Safety &amp; Non-Safety</td>
<td>Temperature/Pressure Switches</td>
</tr>
<tr>
<td>Proper Grounding</td>
<td>Fail-to-Safe Operation</td>
<td>Programmable Controller</td>
</tr>
</tbody>
</table>
Step 3a
Structure Category 2

The structure and behavior of the safety function under fault conditions

Designated Architecture Category 2

Requirements

- Category B
- Well tried safety principles
- Single fault does cause a loss of safety function
- Functional check at start up and periodically (on/off check)

Behavior under fault conditions
A fault occurring between the checks can cause a loss of the safety function.

Typical implementation

![Diagram of typical implementation]
Step 3a
Structure Category 3

The structure and behavior of the safety function under fault conditions

Designated Architecture Category 3

Requirements

- Category B
- Well tried safety principles
- Single fault does not cause a loss of safety function
- Where practicable that fault should be detected

Behavior under fault conditions

Accumulation of undetected faults can cause a loss of the safety function.

Typical implementation

- Machine Control
- Contactors with mechanically linked contacts
- Motor
- Safety monitoring relay
- Guard interlock switches
- Contactor monitoring
- Machine Control
**Step 3a**
**Structure Category 4**

The structure and behavior of the safety function under fault conditions

### Designated Architecture Category 4

- Input device → Logic → Monitoring → Output device
- Input device → Logic → Monitoring → Output device

### Requirements

- Category B
- Well tried safety principles
- Single fault does not cause a loss of safety function
- An accumulation of faults does not cause a loss of safety function

### Behavior under fault conditions

Faults will be detected in time to prevent a loss of safety function

### Typical implementation

- Contactors with mechanically linked contacts
- Guard interlock switches
- Contactor monitoring relays
- Machine Control
- Motor
Step 3a  
Structure – Fault Exclusion

The structure and behavior of the safety function under fault conditions

Designated Architecture Categories B, 1, 2, 3 & 4

Fault exclusion

Clause 7.3 deals with Fault Exclusion. It states:

*It is not always possible to evaluate safety related parts of control systems without assuming that certain faults can be excluded.....*

*Fault exclusion is a compromise between the technical safety requirements and the theoretical possibility of occurrence of a fault.*

Fault exclusion can be based on:

• the technical improbability of the occurrence of some faults.
• generally accepted technical experience, independent of the considered application, and
• technical requirements related to the application and the specific hazard

*If faults are excluded, a detailed justification shall be given in the technical documentation.*

Example list of excludable in annex of ISO 13849-2

• Example
  – *short between conductors belonging to different sheathed wires or cable conduit can be excluded.*
Step 3b
Mean Time to Dangerous Failure (MTTFd)

- MTTFd = Mean Time to dangerous Failure
- Average value of the operating time without dangerous failure in one channel
- Statistical value, no guaranteed lifetime!

\[
\frac{1}{MTTF_d} = \sum \lambda_D = \sum \frac{1}{MTTF_{di}}
\]

<table>
<thead>
<tr>
<th>Denotation of MTTF(_d) of each channel</th>
<th>Range of MTTF(_d) of each channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>3 years (\leq) MTTFd &lt; 10 years</td>
</tr>
<tr>
<td>Medium</td>
<td>10 years (\leq) MTTFd &lt; 30 years</td>
</tr>
<tr>
<td>High</td>
<td>30 years (\leq) MTTFd &lt; 100 years</td>
</tr>
</tbody>
</table>
Step 3c
Diagnostic Coverage (DC)

```
 DC = Detected Dangerous Failures
     -----------------------------
     All Dangerous Failures
```

Examples are given in Annex E of EN ISO 13849

Measure of the effectiveness of the fault detection
Step 3c Diagnostic Coverage (DC)

- The Diagnostic Coverage for the individual “Input-Logic-Output” blocks are first determined.
- The individual values are then averaged for the entire safety channel.

\[
DC_{avg} = 73.3\%
\]

<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 &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>
Step 3d
Common Cause Failure

- Failure which is the result of one or more events and which causes simultaneous failures of two or more separate channels in a multi-channel system, leading to the failure of a safety-related control function.

Table F1 of Annex F
Gives a scoring process of measures against CCF

<table>
<thead>
<tr>
<th>Number</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>
</tbody>
</table>

Add up scores, must be >= 65
Step 4
Requirements for Software Development

- **Software safety requirements (ISO 13848-1:2006, Clause 4.6)**
  - All lifecycle activities of safety-related embedded or **application software** (RSLogix 5000) shall primarily consider the avoidance of faults introduced during the software lifecycle. The main objective of the following requirements is to have readable, understandable, testable and maintainable software.

![Figure 6 – Simplified V-model of software safety lifecycle](image-url)
Verify PL of the design ≥ PLr
### Step 5
Verification: PFH\(_d\) Equivalent (Annex K)

<table>
<thead>
<tr>
<th>MTTF(_d) 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. 2</th>
<th>PL</th>
<th>Cat. 2</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(_{avg}) = none</td>
<td>DC(_{avg}) = none</td>
<td>DC(_{avg}) = low</td>
<td>DC(_{avg}) = medium</td>
<td>DC(_{avg}) = low</td>
<td>DC(_{avg}) = medium</td>
<td>DC(_{avg}) = high</td>
<td>DC(_{avg}) = high</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>7,61 \times 10^{-6}</td>
<td>b</td>
<td>4,53 \times 10^{-6}</td>
<td>b</td>
<td>3,01 \times 10^{-6}</td>
<td>b</td>
<td>1,82 \times 10^{-6}</td>
<td>b</td>
<td>7,44 \times 10^{-7}</td>
<td>d</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>7,13 \times 10^{-6}</td>
<td>b</td>
<td>4,21 \times 10^{-6}</td>
<td>b</td>
<td>2,77 \times 10^{-6}</td>
<td>c</td>
<td>1,67 \times 10^{-6}</td>
<td>c</td>
<td>6,76 \times 10^{-7}</td>
<td>d</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>6,34 \times 10^{-6}</td>
<td>b</td>
<td>3,68 \times 10^{-6}</td>
<td>b</td>
<td>2,37 \times 10^{-6}</td>
<td>c</td>
<td>1,41 \times 10^{-6}</td>
<td>c</td>
<td>5,67 \times 10^{-7}</td>
<td>d</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>5,71 \times 10^{-6}</td>
<td>b</td>
<td>3,26 \times 10^{-6}</td>
<td>b</td>
<td>2,06 \times 10^{-6}</td>
<td>c</td>
<td>1,22 \times 10^{-6}</td>
<td>c</td>
<td>4,85 \times 10^{-7}</td>
<td>d</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>5,19 \times 10^{-6}</td>
<td>b</td>
<td>2,93 \times 10^{-6}</td>
<td>c</td>
<td>1,82 \times 10^{-6}</td>
<td>c</td>
<td>1,07 \times 10^{-6}</td>
<td>c</td>
<td>4,21 \times 10^{-7}</td>
<td>d</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>4,76 \times 10^{-6}</td>
<td>b</td>
<td>2,65 \times 10^{-6}</td>
<td>c</td>
<td>1,62 \times 10^{-6}</td>
<td>c</td>
<td>9,47 \times 10^{-7}</td>
<td>d</td>
<td>3,70 \times 10^{-7}</td>
<td>d</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>4,23 \times 10^{-6}</td>
<td>b</td>
<td>2,32 \times 10^{-6}</td>
<td>c</td>
<td>1,39 \times 10^{-6}</td>
<td>c</td>
<td>8,04 \times 10^{-7}</td>
<td>d</td>
<td>3,10 \times 10^{-7}</td>
<td>d</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>3,80 \times 10^{-6}</td>
<td>b</td>
<td>2,06 \times 10^{-6}</td>
<td>c</td>
<td>1,21 \times 10^{-6}</td>
<td>c</td>
<td>6,94 \times 10^{-7}</td>
<td>d</td>
<td>2,65 \times 10^{-7}</td>
<td>d</td>
<td>9,54 \times 10^{-8}</td>
<td>e</td>
<td></td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>3,46 \times 10^{-6}</td>
<td>b</td>
<td>1,85 \times 10^{-6}</td>
<td>c</td>
<td>1,06 \times 10^{-6}</td>
<td>c</td>
<td>5,94 \times 10^{-7}</td>
<td>d</td>
<td>2,30 \times 10^{-7}</td>
<td>d</td>
<td>8,57 \times 10^{-8}</td>
<td>e</td>
<td></td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>3,17 \times 10^{-6}</td>
<td>b</td>
<td>1,67 \times 10^{-6}</td>
<td>c</td>
<td>9,39 \times 10^{-7}</td>
<td>d</td>
<td>5,16 \times 10^{-7}</td>
<td>d</td>
<td>2,01 \times 10^{-7}</td>
<td>d</td>
<td>7,77 \times 10^{-8}</td>
<td>e</td>
<td></td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>2,93 \times 10^{-6}</td>
<td>c</td>
<td>1,53 \times 10^{-6}</td>
<td>c</td>
<td>8,40 \times 10^{-7}</td>
<td>d</td>
<td>4,53 \times 10^{-7}</td>
<td>d</td>
<td>1,78 \times 10^{-7}</td>
<td>d</td>
<td>7,11 \times 10^{-8}</td>
<td>e</td>
<td></td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>2,65 \times 10^{-6}</td>
<td>c</td>
<td>1,37 \times 10^{-6}</td>
<td>c</td>
<td>7,34 \times 10^{-7}</td>
<td>d</td>
<td>3,87 \times 10^{-7}</td>
<td>d</td>
<td>1,54 \times 10^{-7}</td>
<td>d</td>
<td>6,37 \times 10^{-8}</td>
<td>e</td>
<td></td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>2,43 \times 10^{-6}</td>
<td>c</td>
<td>1,24 \times 10^{-6}</td>
<td>c</td>
<td>6,49 \times 10^{-7}</td>
<td>d</td>
<td>3,35 \times 10^{-7}</td>
<td>d</td>
<td>1,34 \times 10^{-7}</td>
<td>d</td>
<td>5,76 \times 10^{-8}</td>
<td>e</td>
<td></td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>2,24 \times 10^{-6}</td>
<td>c</td>
<td>1,13 \times 10^{-6}</td>
<td>c</td>
<td>5,80 \times 10^{-7}</td>
<td>d</td>
<td>2,93 \times 10^{-7}</td>
<td>d</td>
<td>1,19 \times 10^{-7}</td>
<td>d</td>
<td>5,26 \times 10^{-8}</td>
<td>e</td>
<td></td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>2,04 \times 10^{-6}</td>
<td>c</td>
<td>1,02 \times 10^{-6}</td>
<td>c</td>
<td>5,10 \times 10^{-7}</td>
<td>d</td>
<td>2,52 \times 10^{-7}</td>
<td>d</td>
<td>1,03 \times 10^{-7}</td>
<td>d</td>
<td>4,73 \times 10^{-8}</td>
<td>e</td>
<td></td>
<td></td>
</tr>
<tr>
<td>62</td>
<td>1,84 \times 10^{-6}</td>
<td>c</td>
<td>9,06 \times 10^{-7}</td>
<td>d</td>
<td>4,43 \times 10^{-7}</td>
<td>d</td>
<td>2,13 \times 10^{-7}</td>
<td>d</td>
<td>8,84 \times 10^{-8}</td>
<td>e</td>
<td>4,22 \times 10^{-8}</td>
<td>e</td>
<td></td>
<td></td>
</tr>
<tr>
<td>68</td>
<td>1,68 \times 10^{-6}</td>
<td>c</td>
<td>8,17 \times 10^{-7}</td>
<td>d</td>
<td>3,90 \times 10^{-7}</td>
<td>d</td>
<td>1,84 \times 10^{-7}</td>
<td>d</td>
<td>7,68 \times 10^{-8}</td>
<td>e</td>
<td>3,80 \times 10^{-8}</td>
<td>e</td>
<td></td>
<td></td>
</tr>
<tr>
<td>75</td>
<td>1,52 \times 10^{-6}</td>
<td>c</td>
<td>7,31 \times 10^{-7}</td>
<td>d</td>
<td>3,40 \times 10^{-7}</td>
<td>d</td>
<td>1,57 \times 10^{-7}</td>
<td>d</td>
<td>6,62 \times 10^{-8}</td>
<td>e</td>
<td>3,41 \times 10^{-8}</td>
<td>e</td>
<td></td>
<td></td>
</tr>
<tr>
<td>82</td>
<td>1,39 \times 10^{-6}</td>
<td>c</td>
<td>6,61 \times 10^{-7}</td>
<td>d</td>
<td>3,01 \times 10^{-7}</td>
<td>d</td>
<td>1,35 \times 10^{-7}</td>
<td>d</td>
<td>5,79 \times 10^{-8}</td>
<td>e</td>
<td>3,08 \times 10^{-8}</td>
<td>e</td>
<td></td>
<td></td>
</tr>
<tr>
<td>91</td>
<td>1,25 \times 10^{-6}</td>
<td>c</td>
<td>5,88 \times 10^{-7}</td>
<td>d</td>
<td>2,61 \times 10^{-7}</td>
<td>d</td>
<td>1,14 \times 10^{-7}</td>
<td>d</td>
<td>4,94 \times 10^{-8}</td>
<td>e</td>
<td>2,74 \times 10^{-8}</td>
<td>e</td>
<td></td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>1,14 \times 10^{-6}</td>
<td>c</td>
<td>5,28 \times 10^{-7}</td>
<td>d</td>
<td>2,29 \times 10^{-7}</td>
<td>d</td>
<td>1,01 \times 10^{-7}</td>
<td>d</td>
<td>4,29 \times 10^{-8}</td>
<td>e</td>
<td>2,47 \times 10^{-8}</td>
<td>e</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Step 5
Relationship between PL and SIL

You can convert a ‘simple circuit’ calculated in ISO 13848 and apply it to IEC 62061 by using the chart below.

<table>
<thead>
<tr>
<th>Performance level (PL)</th>
<th>Average probability of a dangerous failure per hour [1/h]</th>
<th>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>

Combining Table 3 and 4 from ISO 13849-1:2006
Step 6
Validation

- Validation is an evaluated inspection (including analysis and testing) of the safety functions and categories of SRP/CS. Validation requires fault injection and is typically done off-line.

- Goal:
  - Proof that the SRP/CS comply to the overall safety requirements of the machinery, proof that the requirements of EN ISO 13849-1 are fulfilled.

- Method:
  - Analysis and testing according to the validation plan

- Validation requirements are defined in ISO 13849-2

<table>
<thead>
<tr>
<th>Test Step</th>
<th>Validation</th>
<th>Pass/Fail</th>
<th>Changes/Modifications</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Step 6
Validation Documentation

Documents required for validation:

- Specification of the expected performance, of the safety functions and categories
- Drawings and specifications
  - Block diagram with functional description of the blocks
  - Circuit diagram including interfaces/connections
- Functional description of the circuit diagram
- Time sequence diagram(s) for switching components, signals relevant for safety
- Component lists with item designations, rated values, tolerances etc.
- Analysis of all relevant faults, including the justification of any excluded faults
6 Steps to Performance Level

There are six basic steps required to determine the Performance Level.

Step 1 – Determine the required performance level (PLr)

Step 2 – Identify the SRP/CS Components & Design Block Diagram

Step 3 – Evaluate the Performance Level (PL)
  Step 3a - Category
  Step 3b - Mean Time to Dangerous Failure (MTTFd)
  Step 3c - Diagnostic Coverage (DC)
  Step 3d - Common Cause Failure (CCF)

Step 4 – Develop Safety-Related Software (If Required)

Step 5 – Verification of Performance Level (PL ≥ PLr)

Step 6 – Validation that all requirements are met
Parse the Safety Function Definition

- Monitoring of area in front of AGV through one laser scanner
- Logic controller switches contactors K1 & K2 if laser scanner has been actuated
- Contactors K1 & K2 switch off power for brake
- AGV starts braking (Emergency stop)

From risk analysis:

$$PL_r = PL d$$
Parse the Safety Function Block Diagram

- Cat =
- MTTF_d =
- DC =
- CCF =
- PL =

- Cat =
- MTTF_d =
- DC =
- CCF =
- PL =

- Cat =
- MTTF_d =
- DC =
- CCF =
- PL =
Parse the Safety Function
Device Information

- Laserscanner: from manufacturer
  Cat 3, MTTF_d = 43 a,

  DC = 90 %, PL d

- Logic controller: from manufacturer
  Cat 3, MTTF_d = 40 a,

  DC = 90 %, PL d

- Contactors: EN ISO 13849-1 (Tab. C.1)
  \[ B_{10d} = 2,000,000 \]

- Application specific:
  - average operating time per day: 24 h/day
  - average operating time per year: 365 days/year

Average number of Demands: 1/day, mean time between two demands: 24 Hrs = 86,400s
Parse the Safety Function
Number of Operations and MTTF\textsubscript{d}

\begin{itemize}
  \item \textbf{\underline{$n_{\text{op}}$ Contactor}}:
    \begin{itemize}
      \item $n_{\text{op}} = 365 \text{ [d/a]} \times 24 \text{ [h/d]} \times 3,600 \text{ [s/h]} / 86,400 \text{ [s]}
      \item = 365 \text{ Actuations/Year}
    \end{itemize}

  \item \textbf{\underline{MTTF\textsubscript{d} Contactor}}
    \begin{itemize}
      \item MTTF\textsubscript{d} = 2,000,000 / (0.1 \times 365 \text{ [1/a]}) = 54,800 \text{ a}
    \end{itemize}
\end{itemize}
Parse the Safety Function Diagnostic Coverage

• **Laserscanner:**
  - $DC_{LS} = \text{medium} \ (\geq \ 90 \ %)$

• **Logic controller:**
  - $DC_L = \text{medium} \ (\geq \ 90 \ %)$

• **Contactor**
  - Direct monitoring (monitoring of electromechanical devices by mechanically linked contact element): $DC_{Contactor} = 99 \ %$
Parse the Safety Function Subsystem Maximum PL

• Laserscanner:
  - Information from manufacturer max. PL d

• Logic controller:
  - Information from manufacturer max. PL d

• Contactors
  - Cat 4, 2-channel (2 contactors), MTTF_d = high, DC_{contactors} = 99 %, measures against common cause are sufficient max. PL e
Parse the Safety Function
Simplified Method PL

Safety function:
If object detected
+ Actuate laserscanner outputs
+ Processing of outputs through logic controller
+ Initiate braking through K1, K2.

- Cat 3
- MTTF<sub>d</sub> = 43 y
- DC = 90 %
- PL = d

- Cat 3
- MTTF<sub>d</sub> = 40 y
- DC = 90 %
- PL = d

- Cat 4
- MTTF<sub>d</sub> = 54,800 y
- DC = 99 %
- PL = e

- Evaluation according to simplified method:
  2 subsystems with minimum PL d ->
  overall PL = d
Parse the Safety Function System - MTTF<sub>d</sub>

- Calculation of the entire MTTF<sub>d</sub>:

\[
\frac{1}{MTTF_d} = \frac{1}{MTTF_{d\_LS}} + \frac{1}{MTTF_{d\_L}} + \frac{1}{MTTF_{d\_K1}}
\]

\[
MTTF_d = 21 \text{y}
\]

- MTTF<sub>dChannel2</sub> = MTTF<sub>dChannel1</sub> = MTTF<sub>d</sub> = 21 y

No symmetrisation required because both channels have the same structure.

- Acc. to table 5 the MTTF<sub>d</sub> can be classified as "medium" (10 y ≤ MTTF<sub>d</sub> ≤ 30 y)
Parse the Safety Function System – Diagnostic Coverage

- Calculation of the average diagnostic coverage:

\[
DC_{avg} = \frac{DC_{LS}}{MTTF_{d_{LS}}} + \frac{DC_{L}}{MTTF_{d_{L}}} + \frac{DC_{K}}{MTTF_{d_{K}}} \quad = \quad 90\% 
\]

- Acc. to table 6 the \( DC_{avg} \) can be classified as “medium”
Parse the Safety Function System – PL

- Category for all subsystems: minimum 3
- $DC_{avg} = \text{medium}$
- $MTTF_d = \text{medium}$
- Measures against common cause faults have been sufficiently applied.

- Achieved Performance Level: d
- Required Performance Level: d
Parse the Safety Function System – Analysis Summary

Safety function:
If object detected
+ Actuate laserscanner outputs
+ Processing of outputs through logic controller
+ Initiate braking through K1, K2.

Overall Circuit
- CAT = 3
- MTTF_d = High
- DC = Med
- PL = d
- CCF = considered
- PLr = d

- CAT = 3
- MTTF_d = 40 y
- DC = 90%
- CCF = 65
- PL = d

- CAT = 4
- MTTF_d = 54,800 y
- DC = 99%
- CCF = 65
- PL = e

- CAT = 3
- MTTF_d = 43 y
- DC = 90%
- CCF = 65
- PL = d
Probability of Dangerous Failures / Hour
Sum of PFHd

SafeZone:
Cat3, PLd
PFHd = 4.46e-7 (1/hr)

SmartGuard 600:
Cat4, PLe
PFHd = 3.89e-10 (1/hr)

System:
Cat4, PLd
PFHd = 4.71e-7 (1/hr)

Table 3 ➔ PLd

Table K.1:
PFHd = 2.47e-8 (1/hr)

Safety function:
- If object detected
- Actuate laserscanner outputs
- Processing of outputs through logic controller
- Initiate braking through K1, K2.

LS — L — CCF

• CAT = 4
• MTTFd = 54,800 y
• DC = 99 %
• CCF = 65
• PL = e
Agenda

Standards – Global and North America

ISO 13849-1

Performance Levels – 6 Steps

SISTEMA

Rockwell Automation Verification Tools

Mechanical – Cat and PL
Introduction to SISTEMA

- What is SISTEMA and its role?
  - SISTEMA – Safety Integrity Software Tool for the Evaluation of Machine Applications
  - The SISTEMA software utility provides developers and testers of safety-related machine controls with comprehensive support in the evaluation of SRP/CS in the context of ISO 13849-1.
  - The tool enables you to model the structure of the safety-related control components based upon the designated architectures.
  - SISTEMA is a free software tool designed by Germany’s IFA (Institute for Occupational Safety & Health).
  - The tool offers automated calculation of a safety function’s attained PL by using product data provided by safety product manufacturer.

- Who are SISTEMA’s intended users?
  - Machine builders and system designers who need to apply ISO 13849-1.

SISTEMA simplifies the PL calculation of a safety function for customers if they have access to the appropriate vendor product data.
What are the benefits of using SISTEMA vs. manually calculating PL?

- Relevant parameters such as the risk parameters for determining the required Performance Level (PLr), the category of the SRP/CS, measures against Common Cause Failures (CCF) on multi-channel systems, the average component quality (MTTFd) and the average test quality (DCavg) of components and blocks, are entered in a systematic manner.
- Users are spared time-consuming calculations and table lookups.
- Users can assess system design changes with little effort.
- Software allows for PDF report generation.
- Software indicates when a condition of ISO 13849:1 is not satisfied and when limit values are exceeded.
- Software is developed by IFA, a well-respected, neutral government authority on Functional Safety in machinery.
- Software allows use of vendor-created product data libraries to further simplify PL calculations.
The Report:

![Image of SISTEMA software interface]

**PROJECT STATUS**

- **Status:** yellow
- **Note:** There are warnings with yellow status listed for this project (or it's subordinate basic elements). Please consider these hints.

**OVERVIEW**

- **Projectname:** XBB2 project
- **Machine:** X robot access gate - Also other hazard points like SISTEMA version 1.0.5
- **Author:** Dines
- **Standard version:** ISO 13849-1:2006, ISO 13849-2

**Safety functions:**

- **SP** Name: guard door interlocking system
  - **Type:** Safety-related stop function initiated by safeguard
  - **PL:** e
  - **PLe:** d
  - **Subsystems:**
    - **SB** Name: Safety PLC: SmartGuard 600 Foodfiller
      - **PL:** e
      - **DCarg [%]:** not relevant
      - **MTTFd [a]:** not relevant
      - **COF Points:** not relevant
      - **Category:** 4
Agenda

Standards – Global and North America

ISO 13849-1

Performance Levels – 6 Steps

SISTEMA

Rockwell Automation Verification Tools

Mechanical – Cat and PL
NEW Safety Return-On-Investment Tool
Find out how to quantify the savings and productivity gains from safety investments. The Rockwell Automation Safety Return-On-Investment Tool accounts for improved safety, reduced claims, improved productivity, and other issues unique to safety applications.

NEW Safety Functions
The Safety Functions Program is building block approach to designing safety systems. Each building block has a complete documentation package that includes a description of each safety function, an electrical schematic, a bill of material, a SISTEMA verification calculation and a verification and validation plan.

NEW Safety Automation Builder
The Safety Automation Builder software package that allows users to import images of their machines. Users can identify hazardous access points and the associated hazards in order to develop a list of safety products that will be used to mitigate the risk. This gives the customer a complete drawing, a bill of material and SISTEMA calculation.

EXISTING Safety Connected Components Building Blocks
The Connected Components Building Blocks provide users with pre-designed safety solutions that have panel drawings, wiring diagrams, programs, HMI screens and start-up manuals make the design and integration of safety systems quick and easy.

EXISTING Safety Solutions Toolkit
The Safety Solutions Toolkit is a tool that presents all safety-related product launches, presentations, videos & animations, literature, event archives, and many other additional resources that the Rockwell Automation Safety Solutions program provides.

EXISTING Safety Accelerator Toolkit
The Safety Accelerator Toolkit provides easy to use system design, programming, and diagnostic tools to assist you in the rapid development and deployment of your safety systems using GuardLogix, Compact GuardLogix, or SmartGuard 600 Controllers, Guard I/O, and Safety Devices. The toolkit includes a risk assessment and system design guide, hardware selection guide, CAD drawings, safety logic routines, and operator status and diagnostic faceplates.

New Pro-Safe Trapped Key Builder
The Pro-safe Trapped Key Builder tool allows you to build safety solutions using a broad range of trapped key switches and devices that can isolate pneumatic, hydraulic and electrical sources in a systematic repeatable process. Pro-safe builder is linked to ProposalWorks to allow users to generate complete Bills of Materials (BOM).
Tools
Safety Functions Library

• Safety Functions include GSR relay and GuardLogix solutions
• Safety Functions Including:
  • E-stop
  • Light Curtains
  • Two hand control
  • Enabling Switch
  • Guard-locking switches
  • Door interlocks
  • Safe Limited Speed

http://literature.rockwellautomation.com
Search: safety-at <keyword>
Tools
Safety Functions Library

Each safety function includes:

- System descriptions of operations
- Bill of material
- Electrical drawings
- SISTEMA calculations
- Verification & validation plans

Bill of Materials:

<table>
<thead>
<tr>
<th>Device ID</th>
<th>Qty</th>
<th>Catalog Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ES1, ES2</td>
<td>2</td>
<td>800FP-MT44PX02</td>
<td>800F Non-Illuminated Mushroom Operators, Twist to Release, 40mm, Round Plastic (Type 4/4X/13, IP66), Red, 2 N.C. Contacts</td>
</tr>
<tr>
<td>ES1, ES2</td>
<td>2</td>
<td>800F-15YE112</td>
<td>800F Legend Plate, 60mm Round, English: EMERGENCY STOP, Yellow with Black Legend Text</td>
</tr>
<tr>
<td>SR1</td>
<td>1</td>
<td>440R-D22R2</td>
<td>Guardmaster Safety Relay, 2 Dual Channel Universal Inputs, 1 N.C. Solid State Auxiliary Outputs</td>
</tr>
<tr>
<td>K1, K2</td>
<td>2</td>
<td>100S-C09DJ14C</td>
<td>MCS 100S-C Safety Contactor, 9A, 24V DC (w/Integrated Diode)</td>
</tr>
<tr>
<td>Reset</td>
<td>1</td>
<td>800FP-F6PX10</td>
<td>800F Push Button - Plastic, Flush, Blue, No Legend, Plastic Latch Mount, 1 N.O. Contact</td>
</tr>
<tr>
<td>Reset</td>
<td>1</td>
<td>800F-11WE186</td>
<td>800F Legend Plate, 30 X 40mm Std., 2 Piece Snap-In (Plate and Frame), English: RESET, White with Black Legend Text</td>
</tr>
</tbody>
</table>

Wiring Diagram:
Tools
Safety Automation Builder

**Software tool to plan safety systems and select products to achieve a specified performance level. Populates SISTEMA projects directly for performance level verification of each safety function and generates project documentation.**

- Use SAB to:
  - layout machine hazards and access points
  - define safety functions and select safety products
  - export data to SISTEMA for analysis*

- Outputs of SAB include:
  - Bill of Material
  - conceptual safety layout drawings
  - SISTEMA project files*

* SAB and SISTEMA tools must be used in conjunction with each other to provide this output

**SAB is based on global standard EN ISO 13849-1.**
Risk Assessment

Determines (PLr)

Identification of Safety Functions (SF)

Specification of Characteristics of each SF

Determination of Required PLr… For each SF

Design Verification

Confirms PLr Achieved
Tools
Safety Automation Builder - Benefits

Available as a free download from the Rockwell Automation website. It guides manufacturers through the safety-system design process by providing options for layout, safety performance level (PL) analysis based on ISO 13849-1 using IFA’s SISTEMA tool, and product selection using Allen-Bradley safety-automation products.

Hazard or Risk Assessment
Functional Requirements

ProposalWorks

Time & Documentation
Agenda

- Standards – Global and North America
- ISO 13849-1
- Performance Levels – 6 Steps
- SISTEMA
- Rockwell Automation Verification Tools
- Mechanical – Cat and PL
Mechanical Components – Cat and PL

As most of the references in Tables 8 and 9 relate to electrical standards, the applicable requirements will need to be adapted in the case of other technologies (e.g. hydraulic, pneumatic).

ISO 13849-1, 5.1 Specification of Safety functions

- **Safety Function** - function of the machine whose failure can result in an immediate increase of the risk(s)
Mechanical Components – Cat and PL

Pneumatic:

- ANSI B11.TR6 – Section 6.4 Pneumatic Systems

Use manufacture data or default data for PL calculations
Hydraulic:

- ANSI B11.TR6 – Section 6.5 Hydraulic Systems

- Use manufacture data or default data for PL calculations

Table C.1 — International Standards dealing with MTTF<sub>d</sub> or B<sub>10d</sub> for components

<table>
<thead>
<tr>
<th>Basic and well-tried safety principles according to ISO 13849-2:2003</th>
<th>Other relevant standards</th>
<th>Typical values: MTTF&lt;sub&gt;d&lt;/sub&gt; (years) B&lt;sub&gt;10d&lt;/sub&gt; (cycles)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hydraulic components</td>
<td>Tables C.1 and C.2</td>
<td>EN 982</td>
</tr>
</tbody>
</table>
Hydraulic Example:

Risk Assessment Hazard:
Potential burns - Contact with leaking hot melt adhesive due to trapped hydraulic pressure
Cat Reg = Cat2
Global Machine Safety Standards

Focus: ISO 13849-1