Introduction to Machine Safety Standards

Jon Riemer
Solution Architect – Safety & Security
Functional Safety Engineer (TÜV Rheinland)
Cyber Security Specialist (TÜV Rheinland)
Agenda

- Understand the big picture of machine safety
- ‘Connect the dots’ between Risk Assessment and safety control system design
- Work through the eight-step design process of ISO 13849-1

1. Use the Risk Assessment to Identify all Safety Functions
2. Specify each Safety Function – Safety Requirements Specification (SRS)
3. Determine the required Performance Level (PL) for each Safety Function
4. Design and technical realization of each Safety Function
5. Evaluate the Performance Level (PL) of each Safety Function
6. Verification of the PL for each Safety Function (PL ≥ PLe)
7. Validation – The Safety Control System meets the requirements of the SRS
8. Review the Risk Assessment to ensure all Safety Functions are analyzed
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

*Minor servicing must be routine, repetitive and integral to the operation*
OSHA Connection

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.

- R15.06-1999, Industrial Robots and Robot Systems - Safety Requirements
- ISO 10218-1:2006, Robots for Industrial Environments

OSHA encourages employers to abide by the more current industry consensus standards since those standards are more likely to be abreast of the state of the art than an applicable OSHA standard may be.
EN/ISO and OSHA/ANSI Standards Hierarchy Comparison

- 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
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
Machine Directive

Machinery Official Journal (OJ) – Published Standards

- Free download search “Machinery OJ”
  [Link](http://ec.europa.eu/enterprise/policies/european-standards/harmonised-standards/machinery/index_en.htm)
- Assumption of Conformity – all relevant harmonized standards and directives are obeyed

<table>
<thead>
<tr>
<th>ISO (1)</th>
<th>Reference and title of the harmonised 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 Note 1</th>
</tr>
</thead>
</table>

BS EN ISO 13849-1:2015

BS – British Standard
EN – European Norm
ISO – International Standards Organization
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

### Member responses - Votes by members

<table>
<thead>
<tr>
<th>Country (Member body)</th>
<th>Status</th>
<th>1a. Agree to add to work programme</th>
</tr>
</thead>
<tbody>
<tr>
<td>United Kingdom (BSI)</td>
<td>P</td>
<td>X</td>
</tr>
<tr>
<td>United States (ANSI)</td>
<td>P</td>
<td>X</td>
</tr>
<tr>
<td><strong>Sub-Total Question 1a</strong></td>
<td></td>
<td><strong>17</strong></td>
</tr>
</tbody>
</table>

### Member responses - Votes not cast (2)

<table>
<thead>
<tr>
<th>Country (Member body)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Philippines (SFS)</td>
<td></td>
</tr>
<tr>
<td>Russian Federation (GOST R)</td>
<td></td>
</tr>
</tbody>
</table>

### Ballot Information

- **Ballot reference:** ISO/TC 199 N 1106 – NWP Trapped key interlocking devices – Part 1
- **Ballot type:** NP
- **Ballot title:** Safety of machinery – Trapped key interlocking devices – Part 1
- **Opening date:** 2014-03-16
- **Closing date:** 2014-06-16
- **Note:** The enclosed New Work Item Proposal has been forwarded.
Functional Safety Design Process - the Safety Lifecycle

1. Assessment

2. Functional Requirements

3. Selection, Design & Verification

4. Installation & Validation

5. Operate, Maintain & Improve
Risk Definition

**RISK**

Is a function of

Severity of Harm

And

Probability of Occurrence

- Exposure of Person to Hazard
- Occurrence of Hazardous Event
- Possibility to Avoid or Limit Harm

Only changes with design

ANSI/ISO 12100: 2012; Figure 3
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
Risk Assessment

- Risk Assessment is the basis of risk reduction
- Process of risk analysis and risk evaluation
- A control system is a common risk reduction method
- When a control system is used, you must follow the iterative design process of the safety-related parts of a control system (SRP/CS)
- ISO 13849-1 is an iterative design process
Risk Assessment

- Risk assessment performed as if existing safeguards are NOT in place
- A comprehensive risk assessment includes all hazard types and tasks
- Task based risk assessment identifies hazards based upon real machine interaction
## Risk Assessment:

### RIA TR R15.306 – Tasked Based Risk Assessment Methodology

#### Severity of Injury

<table>
<thead>
<tr>
<th>Severe</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1 - Minor</td>
<td>E1 - Low</td>
<td>A1 - Likely</td>
<td>NEGLIGIBLE</td>
</tr>
<tr>
<td>S2 - Moderate</td>
<td>E1 - Low</td>
<td>A2/A3 - Not likely/possible</td>
<td>LOW</td>
</tr>
<tr>
<td>S3 - Serious</td>
<td>E2 - High</td>
<td>A1/A2 - Likely/Not likely</td>
<td>HIGH</td>
</tr>
</tbody>
</table>

#### Exposure to the Hazard

<table>
<thead>
<tr>
<th>SEVERITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>E0 - PREVENTED</td>
</tr>
<tr>
<td>E1 - LOW</td>
</tr>
<tr>
<td>E2 - HIGH</td>
</tr>
</tbody>
</table>

#### Avoidance of the Hazard

<table>
<thead>
<tr>
<th>LEVEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1 - LIKELY</td>
</tr>
<tr>
<td>A2/A3 - NOT LIKELY</td>
</tr>
<tr>
<td>A3 - NOT POSSIBLE</td>
</tr>
</tbody>
</table>

#### Risk Level

- **PLr**
- **PLc**
- **PLc**
- **PLd**
- **PLd**
- **PLE**

### Table:

<table>
<thead>
<tr>
<th>Factor</th>
<th>Rating</th>
<th>Criteria (Examples)</th>
<th>R1A TR R15.306 – Tasked Based Risk Assessment Methodology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Injury</td>
<td>Serious</td>
<td>Fatality, long-term disability, career-ending injury</td>
<td>NEGLIGIBLE</td>
</tr>
<tr>
<td>Injury</td>
<td>Moderate</td>
<td>Minor</td>
<td>LOW</td>
</tr>
<tr>
<td>Injury</td>
<td>Minor</td>
<td>Minor</td>
<td></td>
</tr>
<tr>
<td>Exposure</td>
<td>Prevent</td>
<td>Major</td>
<td>HIGH</td>
</tr>
<tr>
<td>Exposure</td>
<td>Minor</td>
<td>Minor</td>
<td></td>
</tr>
<tr>
<td>Avoidance</td>
<td>Not Likely</td>
<td>Not Likely</td>
<td></td>
</tr>
<tr>
<td>Avoidance</td>
<td>Likely</td>
<td>Likely</td>
<td></td>
</tr>
</tbody>
</table>

### Notes:

- **NEGLIGIBLE**
- **LOW**
- **MEDIUM**
- **HIGH**
- **VERY HIGH**

---

**PUBLIC**

Copyright © 2018 Rockwell Automation, Inc. All Rights Reserved. 2018 Rockwell Automation TechED™ Event #ROKTechED
Risk Assessment

- Use system architecture to identify hazard sources
- Five sources of mechanical hazards:
  1) Conveyor Belt
  2) Bottle Side Belt
  3) Sleeve Indexer
  4) Sleeve Cutter
  5) Vacuum Pump
- Other hazards sources:
  1) Pneumatics
  2) Hydraulics
  3) Gravitational
## Risk Assessment

- **Sources of Mechanical Hazard**
  - Conveyor Belt
  - Bottle Side Belt
  - Sleeve Indexer
  - Sleeve Cutter
  - Vacuum Pump

- Operator doing Normal Operating Tasks on the Machine

- Possible injuries the Operator may sustain and Risk Level for each

- Risk Reduction Methods are identified

---

### Risk Assessment Table

<table>
<thead>
<tr>
<th>Item ID</th>
<th>User/Task</th>
<th>Hazard/Failure mode</th>
<th>Initial Assessment Severity/Probability</th>
<th>Risk Level</th>
<th>Risk Reduction Methods Comments</th>
<th>Final Assessment Severity/Probability</th>
<th>Residual Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Operator: Normal Operation</td>
<td>Mechanical: Friction abrasion by material on conveyor belt</td>
<td>Minor/likely</td>
<td>Low</td>
<td>Administrative: Warning labels and operating procedures.</td>
<td>Minor/remote</td>
<td>Negligible</td>
</tr>
<tr>
<td>2</td>
<td>Operator: Normal Operation</td>
<td>Mechanical: Friction abrasion by bottle on side belt</td>
<td>Minor/likely</td>
<td>Low</td>
<td>Administrative: Warning labels and operating procedures.</td>
<td>Minor/remote</td>
<td>Negligible</td>
</tr>
<tr>
<td>3</td>
<td>Operator: Normal Operation</td>
<td>Mechanical: Entanglement and crush with sleeve feeder index roll</td>
<td>Serious/likely</td>
<td>High</td>
<td>Administrative: Warning labels and operating procedures.</td>
<td>Serious/remote</td>
<td>Low</td>
</tr>
<tr>
<td>4</td>
<td>Operator: Normal Operation</td>
<td>Mechanical: Cut by the sleeve cutting knife</td>
<td>Serious/likely</td>
<td>High</td>
<td>Administrative: Warning labels and operating procedures.</td>
<td>Serious/remote</td>
<td>Low</td>
</tr>
<tr>
<td>5</td>
<td>Operator: Normal Operation</td>
<td>Mechanical: Entanglement and crush with sleeve feeder belt drive, drive side</td>
<td>Serious/likely</td>
<td>High</td>
<td>Administrative: Warning labels and operating procedures.</td>
<td>Serious/remote</td>
<td>Low</td>
</tr>
<tr>
<td>6</td>
<td>Operator: Abnormal Operation</td>
<td>Hazardous situation due to unforeseen circumstances in the sleeving zone</td>
<td>Serious/likely</td>
<td>High</td>
<td>Safeguard: Emergency stop function. Administrative: Provide warning labels and operating procedures.</td>
<td>Serious/remote</td>
<td>Low</td>
</tr>
</tbody>
</table>

---

A Control System for Risk Reduction = Safety Function
ISO 13849-1 – Big Picture

**Goal:** Minimize Safety Control System Failures

**Hardware Integrity**
- Architecture
- Component Reliability
- Fault Detection and Reaction

Random hardware failure can be mathematically modeled as a Probability of Dangerous Failure per hour (PFH_D).

**Systematic Integrity**
- Design Quality Measures
- Project Management
- Specification and Documentation

Human error can be avoided during the hardware and software design, implementation, and operation of the system.
Overview of ISO 13849-1 Design Flow

1. Use the Risk Assessment to Identify all Safety Functions
2. Specify each Safety Function – Safety Requirements Specification (SRS)
3. Determine the required Performance Level (PL<sub>r</sub>) for each Safety Function
4. Design and technical realization of each Safety Function
5. Evaluate the Performance Level (PL) of each Safety Function
6. Verification of the PL for each Safety Function (PL ≥ PL<sub>r</sub>)
7. Validation – The Safety Control System meets the requirements of the SRS
8. Review the Risk Assessment to ensure all Safety Functions are analyzed
Identify Primary Safety Functions

- Safety Function = Control system for risk reduction
- List each hazardous energy source and triggering event possibility

<table>
<thead>
<tr>
<th>Item ID</th>
<th>User/Task</th>
<th>Hazard / Failure mode</th>
<th>Initial Assessment Severity/Probability</th>
<th>Risk Level</th>
<th>Risk Reduction Method(s) Comments</th>
<th>Final Assessment Severity/Probability</th>
<th>Residual Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Operator: Normal Operation</td>
<td>Mechanical: Friction abrasion by material conveyor belt</td>
<td>Minor/Likely</td>
<td>Low</td>
<td>Safeguard: Mechanical guarding around elevator and locked interlocked door for operator access. Administrative: Warning labels and operating procedures.</td>
<td>Minor/Remote</td>
<td>Negligible</td>
</tr>
<tr>
<td>2</td>
<td>Operator: Normal Operation</td>
<td>Mechanical: Friction abrasion by bottle feed side belt</td>
<td>Minor/Likely</td>
<td>Low</td>
<td>Safeguard: Mechanical guarding around elevator and locked interlocked door for operator access. Administrative: Warning labels and operating procedures.</td>
<td>Minor/Remote</td>
<td>Negligible</td>
</tr>
<tr>
<td>3</td>
<td>Operator: Normal Operation</td>
<td>Mechanical: Entanglement and crush with sleeve feeder index roll</td>
<td>Serious/Likely</td>
<td>High</td>
<td>Safeguard: Mechanical guarding around elevator and locked interlocked door for operator access. Administrative: Warning labels and operating procedures.</td>
<td>Serious/Remote</td>
<td>Low</td>
</tr>
<tr>
<td>4</td>
<td>Operator: Normal Operation</td>
<td>Mechanical: Cut by the knife cutting knife</td>
<td>Serious/Likely</td>
<td>High</td>
<td>Safeguard: Mechanical guarding around elevator and locked interlocked door for operator access. Administrative: Warning labels and operating procedures.</td>
<td>Serious/Remote</td>
<td>Low</td>
</tr>
<tr>
<td>5</td>
<td>Operator: Normal Operation</td>
<td>Mechanical: Entanglement and crush with sleeve feeder belt drive side</td>
<td>Serious/Likely</td>
<td>High</td>
<td>Safeguard: Mechanical guarding around elevator and locked interlocked door for operator access. Administrative: Warning labels and operating procedures.</td>
<td>Serious/Remote</td>
<td>Low</td>
</tr>
</tbody>
</table>

SF1: Guard Door 1 (op side) Protective stop and prevention of restart of the conveyor when opened
SF2: Guard Door 1 (op side) Protective stop and prevention of restart of the bottle feed belts when opened
SF3: Guard Door 1 (op side) Protective stop and prevention of restart of the sleeve feeder when opened
SF4: Guard Door 1 (op side) Protective stop and prevention of restart of the cutter when opened
SF5: Guard Door 1 (op side) Unlock with conditional time delayed unlock
SF6: Guard Door 2 (dr side) Protective stop and prevention of restart of the sleeve feeder opened
1 Identify Complementary Safety Functions

- Emergency Stop safety functions are complementary
- List each hazardous energy source

<table>
<thead>
<tr>
<th>Item</th>
<th>User/Task</th>
<th>Hazard / Failure mode</th>
<th>Initial Assessment Severity/Probability</th>
<th>Risk Level</th>
<th>Risk Reduction Methods Comments</th>
<th>Final Assessment Severity/Probability</th>
<th>Residual Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Operator: Abnormal Operation</td>
<td>Hazardous situation due to unforeseen circumstances in the sleeving zone</td>
<td>Serious/Likely</td>
<td>High</td>
<td>E-stop 1 (op side) Emergency Stop function. Administrative: Provide warning labels and operating procedures.</td>
<td>Serious/Remote</td>
<td>Low</td>
</tr>
<tr>
<td>3</td>
<td>Operator: Abnormal Operation</td>
<td>Hazardous situation due to unforeseen circumstances in the sleeve feeder drive belt area</td>
<td>Serious/Likely</td>
<td>High</td>
<td>E-stop 1 (dr side) Emergency Stop function. Administrative: Provide warning labels and operating procedures.</td>
<td>Serious/Remote</td>
<td>Low</td>
</tr>
</tbody>
</table>

SF7 Emergency Stop 1 (op side) of the conveyor when the emergency stop push button is pressed
SF8 Emergency Stop 1 (op side) of the bottle feed belts when the emergency stop push button is pressed
SF9 Emergency Stop 1 (op side) of the sleeve feeder when the emergency stop push button is pressed
SF10 Emergency Stop 1 (op side) of the cutter when the emergency stop push button is pressed
SF11 Emergency Stop 1 (op side) of vacuum pump when the emergency stop push button is pressed
SF12 Emergency Stop 2 (dr side) of the sleeve feeder when the emergency stop push button is pressed
Safety Requirements Specification (SRS)

- SRS describes the characteristics of the safety-related parts of a control system (SRP/CS)
- Needed for the design and technical realization of the control system
Specify Safety Requirements (SRS)

- Detail each safety function
- Provides the pass/fail criteria for future verification and validation activities
- Describe interaction with standard machine control
- Document unique behavior or requirements

### SF1: SAFETY FUNCTION SPECIFICATION

<table>
<thead>
<tr>
<th>Safety Function Name:</th>
<th>Guard Door 1 (op side) Protective stop and prevention of restart of the conveyor when opened</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Level Requirement (PLR):</td>
<td>Per ISO 13849-1 Annex A: PLe</td>
</tr>
<tr>
<td>Type of Safety Function:</td>
<td>Safety-related stop initiated by safeguard</td>
</tr>
<tr>
<td>Operating Modes:</td>
<td>Automatic &amp; Manual</td>
</tr>
<tr>
<td>Triggering Event:</td>
<td>Opening of the Guard Door</td>
</tr>
<tr>
<td>Safety Reaction:</td>
<td>Initiate a Category 0 Stop</td>
</tr>
<tr>
<td>Safe State:</td>
<td>Conveyor Stopped</td>
</tr>
<tr>
<td>Number of Operations:</td>
<td>2/ Hour @ 365 Days/Year = 17,320/Year</td>
</tr>
<tr>
<td>Fault Reaction:</td>
<td>Initiate an STO and annunciate the fault</td>
</tr>
<tr>
<td>Faults Considered and/or Excluded:</td>
<td>Broken Guard Door Switch Actuator</td>
</tr>
<tr>
<td>Response Time/Distance Consideration:</td>
<td>N/A – Locking Guard Door</td>
</tr>
</tbody>
</table>

The conveyor is exposed with a stop time of 1 second. A distance calculation is not applicable due to the minor injury potential.

**Safety Function Requirements:**

Opening of the guard door will initiate a Category 0 stop of the conveyor and prevent an unintended restart by removal of power to the motors via the drive STO feature. The stop time must not exceed 1 second. Upon closing of the door, motion of the conveyor and bottle feed belts will not resume until the reset pushbutton is pressed and released. Faults at the door interlock switch, wiring terminals or drive will be detected by the safety relay before the next safety demand and inhibit a reset of the safety function.

**Interface to Other Safety Functions:**

This will not degrade the Sleever feeder/cutter function and the Emergency Stop will override this safety function

**Verification/Validation Document Reference:**

TBD – Validation Document Page

**Other Document References:**

TBD – Electrical Print Numbers
3 Determine the Required PL (PLᵣ)

- Severity and probability data from the Risk Assessment is needed
- ISO 13849-1, Annex A
  - Risk Reduction by Safety Related Parts of the Control System
  - Shows a risk graph scoring technique to identify Performance Levels (a, b, c, d & e)
- As risk increases, safety performance of the control system must increase

S1 & S2 – Severity of Injury (Slight or Serious)
F1 & F2 – Frequency and/or Exposure (Seldom or Frequent)
P1 & P2 – Possibility of Avoidance (Possible or Not Possible)
Determine the Required PL (PLr)

- Each safety function must have a PLr based upon Risk Assessment
- PLr may vary depending upon Safety Function risk scoring

<table>
<thead>
<tr>
<th>SF</th>
<th>Safety Function Description</th>
<th>PLr</th>
</tr>
</thead>
<tbody>
<tr>
<td>SF1</td>
<td>Guard Door 1 (op side) Protective stop and prevention of restart of the conveyor when opened</td>
<td>b</td>
</tr>
<tr>
<td>SF2</td>
<td>Guard Door 1 (op side) Protective stop and prevention of restart of the bottle feed belts when opened</td>
<td>b</td>
</tr>
<tr>
<td>SF3</td>
<td>Guard Door 1 (op side) Protective stop and prevention of restart of the sleeve feeder when opened</td>
<td>d</td>
</tr>
<tr>
<td>SF4</td>
<td>Guard Door 1 (op side) Protective stop and prevention of restart of the cutter when opened</td>
<td>d</td>
</tr>
<tr>
<td>SF5</td>
<td>Guard Door 1 (op side) Unlock with conditional time delayed unlock</td>
<td>c</td>
</tr>
<tr>
<td>SF6</td>
<td>Guard Door 2 (dr side) Protective stop and prevention of restart of the sleeve feeder opened</td>
<td>d</td>
</tr>
<tr>
<td>SF7</td>
<td>Emergency Stop 1 (op side) of the conveyor when the emergency stop push button is pressed</td>
<td>b</td>
</tr>
<tr>
<td>SF8</td>
<td>Emergency Stop 1 (op side) of the bottle feed belts when the emergency stop push button is pressed</td>
<td>b</td>
</tr>
<tr>
<td>SF9</td>
<td>Emergency Stop 1 (op side) of the sleeve feeder when the emergency stop push button is pressed</td>
<td>d</td>
</tr>
<tr>
<td>SF10</td>
<td>Emergency Stop 1 (op side) of the cutter when the emergency stop push button is pressed</td>
<td>d</td>
</tr>
<tr>
<td>SF11</td>
<td>Emergency Stop 1 (op side) of vacuum pump when the emergency stop push button is pressed</td>
<td>a</td>
</tr>
<tr>
<td>SF12</td>
<td>Emergency Stop 2 (dr side) of the sleeve feeder when the emergency stop push button is pressed</td>
<td>c</td>
</tr>
</tbody>
</table>
Design and Technical Realization

- Typical Input, Logic and Output SRP/CS devices

![Diagram]

- Develop a block diagram for each safety function
- Identify devices and assign them to Input/Logic/Output subsystems
## Design and Technical Realization

<table>
<thead>
<tr>
<th>SF</th>
<th>Safety Function Description</th>
<th>PLr</th>
</tr>
</thead>
<tbody>
<tr>
<td>SF3</td>
<td>Guard Door 1 (op side) Protective stop and prevention of restart of the sleeve feeder when opened</td>
<td>d</td>
</tr>
<tr>
<td>SF5</td>
<td>Guard Door 1 (op side) Unlock with conditional time delayed unlock</td>
<td>c</td>
</tr>
<tr>
<td>SF9</td>
<td>Emergency Stop 1 (op side) of the sleeve feeder when the emergency stop push button is pressed</td>
<td>d</td>
</tr>
<tr>
<td>SF11</td>
<td>Emergency Stop 1 (op side) of vacuum pump when the emergency stop push button is pressed</td>
<td>a</td>
</tr>
</tbody>
</table>

**SF3**
- **I** Guard Door Switch
- **L** Safety Relay
- **O** Sleeve Feeder Servo

**SF5**
- **I** E-stop push button
- **L** Safety Relay
- **O** Guard Door Unlock Solenoid

**SF9**
- **I** E-stop push button
- **L** Safety Relay
- **O** Sleeve Feeder Servo

**SF11**
- **I** E-stop push button
- **L** Safety Relay
- **O** Vacuum Pump Contactor
4 Design and Technical Realization

- Estimate number of annual operation (Nops) of each electromechanical component
- Highlight any components shared by safety functions
- Nops must include any normal operation

- SF3
  - Guard Door Switch
  - Safety Relay
  - Sleeve Feeder Servo
  - Shared Nops = 17,620
  - Nops = 17,520

- SF5
  - Hazards Safe State Feedback
  - Safety Relay
  - Guard Door Unlock Solenoid
  - Nops = 17,520

- SF9
  - E-stop push button
  - Safety Relay
  - Sleeve Feeder Servo
  - Nops = 100

- SF11
  - E-stop push button
  - Safety Relay
  - Vacuum Pump Contactor
  - Nops = 465

- SF11
  - E-stop push button
  - Safety Relay
  - Vacuum Pump Contactor
  - Nops = 100
With safety functions defined and block diagrams created:

- Review safety functions for design optimization
  - Migrate electromechanical devices with solid state (remove Nops from equation)
    - Interlocks dry contact → OSSD
    - Contactors to Safe Torque Off drive
    - Electromechanical Safe Torque Off to solid-state Safe Torque Off
  - Choose safety logic level to optimize total cost of ownership:
    - Safety: Relay, Configurable Relay, PLC
  - Review power structure to determine cost-effective energy control
  - Hardware standardization will simplify design, verification, and validation
    - Exceeding PLr is common
    - Standardized hardware choices may allow combining of safety functions
4 Design and Technical Realization

- Specify bill of material for each Safety Function control system safety devices
4 Design and Technical Realization

- Identify safety data for each safety function device

![Diagrams showing SF3 and SF9 connections]

<table>
<thead>
<tr>
<th>Item ID</th>
<th>Part Number</th>
<th>Qty.</th>
<th>Part Description</th>
<th>Safety Data (SAFETY-SR001-EN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interlock Switch</td>
<td>440G-T27260</td>
<td>1</td>
<td>Guard Locking Switch - 440G TLS-GD2: Solenoid Voltage: 24V AC/DC, Contacts(Safety and Aux): 2 Normally Closed, 1 Normally Open, Actuator: Fully-Flex, Conduit Entry: M20 Conduit</td>
<td>B10d = 2.00E+6</td>
</tr>
<tr>
<td>E-Stop Button</td>
<td>800FP-MT44PX02</td>
<td>1</td>
<td>Emergency Stop Operator, 40mm Red Twist to Relase with 2 N.C. Contacts</td>
<td>B10d = 7.36E+5</td>
</tr>
<tr>
<td>Safety Relay</td>
<td>440R-D22R2</td>
<td>1</td>
<td>Guardmaster Dual Input Safety Relay (DI), 2 Dual Channel Universal Inputs, 1 N.C. Auxiliary Output</td>
<td>SIL3, PLe, Cat. 4, PFHd = 4.35E-9</td>
</tr>
<tr>
<td>Servo</td>
<td>2097-V34PR5-LM</td>
<td>2</td>
<td>Kinetix 350 Single Axis Ethernet/IP Servo Drive with STO, 480V AC Three-Phase, 2.0 kW</td>
<td>SIL2, Pla, Cat. 3, PFHd = 5.90E-10</td>
</tr>
</tbody>
</table>
Evaluate the Performance Level (PL)

- The Performance Level (PL) is a way to express the ability of an SRP/CS to perform a safety function under foreseeable conditions.

- Two aspects to safety design process:
  1. **Hardware Integrity (PFH_D)**
  2. **Systematic Integrity (Design Techniques)**

Both must be fulfilled to claim a PL for the safety function.
Evaluate the Performance Level (PL)

- Most systems have both electronic and electromechanical devices
- Using the manufacturer’s safety data makes the PFH_D calculation easier
- Sum up the device PFH_D numbers to get the total safety function PFH_D
- The PL is determined from ISO 13849-1, Table 2
PL Variables: CATEGORY

Cat 1
- Guard Interlock Switch
- Contactor
- Motor

Cat 2
- Guard Interlock Switch
- Safety Contactor
- Motor
- Safety Monitoring Relay with startup check
- Test 100x demand rate

Cat 3
- Guard Interlock Switch
- Safety Contactor 1
- Safety Contactor 2
- Motor
- Safety Monitoring Relay with startup check

Cat 4
- Guard Interlock Switch
- With Monitor
- OSSD
- Safety Contactor 1
- Safety Contactor 2
- Motor
- Safety Monitoring Relay with startup check
Evaluate the Performance Level (PL)

- Interlock Switch and E-stop have B10d data and will require the complete ISO 13849-1 calculation
- A summary of the calculations are shown in the table

Interlock Switch: \( \text{PFH}_D = 4.29E-08 / \text{PLe} \)
E-stop Button: \( \text{PFH}_D = 4.29E-08 / \text{PLe} \)
Contactor: \( \text{PFH}_D = 1.14E-06 / \text{PLc} \)
Evaluate the Performance Level (PL)

- The total PFH_d for each safety function is calculated by adding the PFHd values for each safety device.

### Safety Function 1:
- Cat. 3/PLd
- \( \text{PFH}_D = 4.78 \times 10^{-8} \)

### Safety Function 2:
- Cat. 3/PLd
- \( \text{PFH}_D = 4.89 \times 10^{-8} \)

### Safety Function 3:
- Cat. 1/PLc
- \( \text{PFH}_D = 1.18 \times 10^{-6} \)
### 6. Verification of the PL (PL ≥ PL_r)

- For each safety function, the PL of the SRP/CS shall meet or exceed the PL_r identified in Step 3

#### Table: Risk Assessment and PL Calculation

<table>
<thead>
<tr>
<th>SF</th>
<th>Safety Function Description</th>
<th>Severity/Probability</th>
<th>Risk Level</th>
<th>From: Risk Assessment</th>
<th>PLr - ISO 13849-1, Annex A</th>
<th>PL Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td>SF3</td>
<td>Protective stop and prevention of restart of the sleeve feeder when the guard door 1 (op side) is opened</td>
<td>Serious/Likely</td>
<td>High</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SF9</td>
<td>Emergency stop 1 (op side) of the sleeve feeder when the emergency stop push button is pressed</td>
<td>Serious/Likely</td>
<td>High</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SF11</td>
<td>Emergency stop 1 (op side) of vacuum pump when the emergency stop push button is pressed</td>
<td>Minor/Unlikely</td>
<td>Low</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Safety Function 1:**
  - Cat. 3/PLd
  - PFH_D = 4.78E-8

- **Safety Function 2:**
  - Cat. 3/PLd
  - PFH_D = 4.89E-8

- **Safety Function 3:**
  - Cat. 1/PLc
  - PFH_D = 1.18E-6
SISTEMA Software

- SISTEMA software supports SRP/CS designers with the calculation and documentation requirements of ISO 13849-1
- The tool enables modeling of the SRP/CS devices and safety functions
- Calculation of the safety device reliability values and total safety function Performance Level (PL)
- The SISTEMA software free online:
  
  
7 Validation – SRP/CS Meets the SRS

- SRP/CS shall be validated as a system
- ISO 13849-2 sets the requirements for validation and calls for a documented plan to confirm the requirements in the SRS are met
- Validation includes functional testing and fault injection to determine the system responds accordingly
- Use a checklist to document the validation of the SRP/CS
Verify all Safety Functions Analyzed

- The final step in the ISO 13849-1 design process is to review the Risk Assessment to ensure all Safety Functions have been identified and analyzed.
- The Functional Safety Design process is iterative.
- As changes are made, the risk assessment is used to review the impact to safety.

<table>
<thead>
<tr>
<th>Item ID</th>
<th>User/Task</th>
<th>Hazard/Failure mode</th>
<th>Initial Assessment Severity/Probability</th>
<th>Risk Level</th>
<th>Risk Reduction Methods Comments</th>
<th>Final Assessment Severity/Probability</th>
<th>Residual Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Operator: Normal Operation</td>
<td>Mechanical: Friction abrasion by material conveyor belt</td>
<td>Minor/Likely</td>
<td>Low</td>
<td>Safeguard: Mechanical guarding around s GW and locked interlocked door for operator access. Administrative: Warning labels and operating procedures.</td>
<td>Minor/Remote</td>
<td>Negligible</td>
</tr>
<tr>
<td>2</td>
<td>Operator: Normal Operation</td>
<td>Mechanical: Friction abrasion by bottle feed slide belt</td>
<td>Minor/Likely</td>
<td>Low</td>
<td>Safeguard: Mechanical guarding around s GW and locked interlocked door for operator access. Administrative: Warning labels and operating procedures.</td>
<td>Minor/Remote</td>
<td>Negligible</td>
</tr>
<tr>
<td>3</td>
<td>Operator: Normal Operation</td>
<td>Mechanical: Entanglement and crush with sleeve feeder index roll</td>
<td>Serious/Likely</td>
<td>High</td>
<td>Safeguard: Mechanical guarding around s GW and locked interlocked door for operator access. Administrative: Warning labels and operating procedures.</td>
<td>Serious/Remote</td>
<td>Low</td>
</tr>
<tr>
<td>4</td>
<td>Operator: Normal Operation</td>
<td>Mechanical: Cut by the sleeve cutting knife</td>
<td>Serious/Likely</td>
<td>High</td>
<td>Safeguard: Mechanical guarding around s GW and locked interlocked door for operator access. Administrative: Warning labels and operating procedures.</td>
<td>Serious/Remote</td>
<td>Low</td>
</tr>
<tr>
<td>5</td>
<td>Operator: Normal Operation</td>
<td>Mechanical: Entanglement and crush with sleeve feeder belt drive, drive side</td>
<td>Serious/Likely</td>
<td>High</td>
<td>Safeguard: Mechanical guarding around s GW drive side belt and non-locking interlocked door for operator access. Administrative: Warning labels and operating procedures.</td>
<td>Serious/Remote</td>
<td>Low</td>
</tr>
</tbody>
</table>
Share your Feedback
Please complete a session survey on the mobile app

- Download the Rockwell Automation Events App
- Select Rockwell Automation TechED™ and login
- Click on Session Surveys or Schedule in the main menu
  - Select the session you are attending
  - Click on the survey tab
  - Complete the survey and submit
Questions?