Rockwell Automation On The Move
May 16-17 2018   Milwaukee, WI

CT433 - Machine Safety
Performance Level Selection and Design Realization

Jon Riemer
Solution Architect – Safety & Security
Functional Safety Engineer – TUV Rheinland

PUBLIC
Goals

- 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 ≥ PL)
7. Validation – The Safety Control System meets the requirements of the SRS
8. Review the Risk Assessment to ensure all Safety Functions are analyzed
Risk Assessment

- Risk Assessment is the basis of risk reduction
- 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

- 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

---

### Item ID | User/Task | Hazard / Failure mode | Initial Assessment Severity/Probability | Risk Level | Risk Reduction Methods | Comments
--- | --- | --- | --- | --- | --- | ---
1 | Operator: Normal Operation | Mechanical: Friction abrasion by material conveyed under conveyor belt | Minor/Likely | Low | Safeguard: Mechanical guarding around sleeve and locked interlocked door for operator access. | Minor/Remote, Negligible
2 | Operator: Normal Operation | Mechanical: Friction abrasion by bottle fed side belt | Minor/Likely | Low | Safeguard: Mechanical guarding around sleeve and locked interlocked door for operator access. Administrative: Warning labels and operating procedures. | Minor/Remote, Negligible
3 | Operator: Normal Operation | Mechanical: Entanglement and crush with sleeve feeder index roll | Serious/Likely | High | Safeguard: Mechanical guarding around sleeve and locked interlocked door for operator access. Administrative: Warning labels and operating procedures. | Serious/Remote, Low
4 | Operator: Normal Operation | Mechanical: Cut by the sleeve cutting knife | Serious/Likely | High | Safeguard: Mechanical guarding around sleeve and locked interlocked door for operator access. Administrative: Warning labels and operating procedures. | Serious/Remote, Low
5 | Operator: Normal Operation | Mechanical: Entanglement and crush with sleeve feeder belt drive, drive side | Serious/Likely | High | Safeguard: Mechanical guarding around sleeve drive side belt and non-locking interlocked door for operator access. Administrative: Warning labels and operating procedures. | Serious/Remote, Low
6 | Operator: Abnormal Operation | Hazardous situation due to unforeseen circumstances in the sleeveing zone | Serious/Likely | High | Safeguard: Emergency Stop function, Administrative: Provide warning labels and operating procedures. | Serious/Remote, Low
7 | Operator: Abnormal Operation | Hazardous situation due to unforeseen malfunction of vacuum pump | Minor/Unlikely | Low | Safeguard: Emergency Stop function, Administrative: Provide warning labels and operating procedures. | Minor/Remote, Negligible

---

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_r) 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_r)
7. Validation – The Safety Control System meets the requirements of the SRS
8. Review the Risk Assessment to ensure all Safety Functions are analyzed
1 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 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 sweeper 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 sweeper 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 sweeper 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 sweeper 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 sweeper 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>

- 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
Identify Complementary Safety Functions

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

<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>
</tr>
</thead>
<tbody>
<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>
</tr>
<tr>
<td>8</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>Safeguard: Emergency Stop function. Administrative: Provide warning labels and operating procedures.</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
2 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
- Provides the pass/fail criteria for future verification and validation activities
- See handout Annex A for a sample
Specify Safety Requirements (SRS)

- Detail each safety function

### 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: PLb</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 = 17,520/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 Sleeper 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 (PL<sub>r</sub>)

- Severity and probability data from the Risk Assessment is needed
- ISO 13849-1, Annex A shows how to use a risk graph scoring technique to identify one of four 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 (PL<sub>r</sub>)

- Each safety function must have a PL<sub>r</sub> based upon Risk Assessment
- PL<sub>r</sub> may vary depending upon Safety Function risk scoring

<table>
<thead>
<tr>
<th>SF</th>
<th>Safety Function Description</th>
<th>PL&lt;sub&gt;r&lt;/sub&gt;</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>
Typical Input, Logic and Output SRP/CS devices

- E-Stop buttons
- Interlock Switches
- Light Curtains
- Limit Switches
- Safety Relays
- Safety PLCs
- Contactors
- Safe Torque Off Drive
- Relays
- Solenoid Valves

- Develop a block diagram for each safety function
- Identify devices and assign them to Input/Logic/Output subsystems
### Safety Function Description

<table>
<thead>
<tr>
<th>SF</th>
<th>Safety Function Description</th>
<th>PL&lt;sub&gt;f&lt;/sub&gt;</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>

**Diagram:**

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

- **SF5**
  - I: Hazards Safe State Feedback
  - L: Safety Relay
  - O: Guard Door Unlock Solenoid

- **SF9**
  - I: E-Stop Pushbutton
  - L: Safety Relay
  - O: Sleeve Feeder Servo

- **SF11**
  - I: E-Stop Pushbutton
  - L: Safety Relay
  - O: Vacuum Pump Contactor
Design and Technical Realization

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

- **Shared**

<table>
<thead>
<tr>
<th>Component</th>
<th>Nops</th>
</tr>
</thead>
<tbody>
<tr>
<td>SF3 Guard Door Switch</td>
<td>17,520</td>
</tr>
<tr>
<td>SF11 E-Stop Pushbutton</td>
<td>465</td>
</tr>
<tr>
<td>SF9 E-Stop Pushbutton</td>
<td>100</td>
</tr>
<tr>
<td>SF5 Hazards Safe State Feedback</td>
<td>17,520</td>
</tr>
<tr>
<td>SF11 E-Stop Pushbutton</td>
<td>100</td>
</tr>
<tr>
<td>SF5 Guard Door Unlock Solenoid</td>
<td>17,520</td>
</tr>
</tbody>
</table>

Nops = 100
Nops = 17,520
Nops = 465
Nops = 17,620
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 PL_r 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.

- Interlock Switch
- Contactor
- Locking Interlock Switch
- Safety Relay
- Emergency Stop
- Drive
- Servo
- Safety Relay
- Emergency Stop
4 Design and Technical Realization

- Identify safety data for each safety function device

![Diagram showing safety devices]

<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</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</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>Button</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety</td>
<td>440R-D22R2</td>
<td>1</td>
<td>Guardmaster Dual Input Safety Relay (Di), 2 Dual Channel Universal Inputs, 1 N.C. SAuxiliary Output</td>
<td>SIL3, PLe, Cat. 4, PFHd = 4.35E-9</td>
</tr>
<tr>
<td>Relay</td>
<td></td>
<td></td>
<td></td>
<td></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, Pld, 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.

<table>
<thead>
<tr>
<th>Probability</th>
<th>Dangerous Failure (PFH$_D$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>$1 / 10,000$</td>
</tr>
<tr>
<td>b</td>
<td>$1 / 100,000$</td>
</tr>
<tr>
<td>c</td>
<td>$1 / 1,000,000$</td>
</tr>
<tr>
<td>d</td>
<td>$1 / 10,000,000$</td>
</tr>
<tr>
<td>e</td>
<td>$1 / 100,000,000$</td>
</tr>
</tbody>
</table>
5 Evaluate the Performance Level (PL)

- Most systems have both electronic and electro-mechanical 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
5 PL Variables: CATEGORY

Cat 1
Guard Interlock Switch
Contactor
Motor

Cat 2
Guard Interlock Switch
Safety Contactor
Motor

Cat 3
Guard Interlock Switch
Safety Monitoring Relay with start up check
Safety Contactor 1
Safety Contactor 2
Motor

Cat 4
Guard Interlock Switch With Monitor
OSSD
Safety Contactor 1
Safety Contactor 2
Motor

Test 100x demand rate

Safety Monitoring Relay with start up 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: \( PFH_D = 4.29 \times 10^{-8} / PLe \)

E-Stop Button: \( PFH_D = 4.29 \times 10^{-8} / PLe \)

Contactor: \( PFH_D = 1.14 \times 10^{-6} / PLc \)
Evaluate the Performance Level (PL)

- The total $PFH_D$ for each safety function is calculated by adding the $PFH_d$ values for each safety device.
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>
<thead>
<tr>
<th>Safety Function Description</th>
<th>From: Risk Assessment</th>
<th>PLr - ISO 13849-1, Annex A</th>
<th>PL Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td>SF3 Protectivestop and prevention of restart of the sleeve feeder when the guard door 1 (op side) is opened</td>
<td>Severity/Probability, Risk Level</td>
<td>Severity, Frequency of Exposure, Possibility of Avoidance</td>
<td>PL Calculation</td>
</tr>
<tr>
<td>SF9 Emergency stop 1 (op side) of the sleeve feeder when the emergency stop push button is pressed</td>
<td>Severity/Probability, Risk Level</td>
<td>Severity, Frequency of Exposure, Possibility of Avoidance</td>
<td>PL Calculation</td>
</tr>
<tr>
<td>SF11 Emergency stop 1 (op side) of vacuum pump when the emergency stop push button is pressed</td>
<td>Severity/Probability, Risk Level</td>
<td>Severity, Frequency of Exposure, Possibility of Avoidance</td>
<td>PL Calculation</td>
</tr>
</tbody>
</table>
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 and device libraries can be downloaded here.
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
8 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 sleever 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 sleever 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 sleever 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 sleever 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 sleever drive side belt and non-locked interlocked door for operator access. Administrative: Warning labels and operating procedures.</td>
<td>Serious/Remote</td>
<td>Low</td>
</tr>
</tbody>
</table>
Questions?
Thank you for your time and attention!