Ten Fingers and Ten Toes: Applying Machinery Safety Principles in a Process Plant

Lauren J. Caldwell, PE(SC), CFSP, CMSE®
aeSolutions
Greenville, SC
lauren.caldwell@aesolutions.com

Prepared for Presentation at
American Institute of Chemical Engineers
2023 Spring Meeting and 19th Global Congress on Process Safety
Houston, TX
March 12 – March 15, 2023

Ten Fingers and Ten Toes: Applying Machinery Safety Principles in a Process Plant

Lauren J. Caldwell
aeSolutions
Greenville, SC
lauren.caldwell@aesolutions.com

Keywords: Machinery Safety, Risk Assessment, Interlocks, Hazard Identification and Risk Analysis, Compliance with Standards, Health, Safety and the Environment

Abstract

When performing risk assessments on process equipment, are you reviewing machinery as well? Bag dump stations, conveyors, and various vendor-packaged machinery provided with E-Stops are sometimes evaluated in a Process Hazards Analysis (PHA), but they tend to be reviewed at a high level. Because they do not have process flow, they may not be viewed as having traditional process safety hazards. Machines still have hazards, and there is a need for a deeper dive with respect to machinery-related hazards.

Did you know that machinery E-Stops fall under OSHA's General Duty Clause? In an interpretation letter from April 28, 1999, OSHA noted, "If a serious injury could result from an improperly-designed or installed emergency stop device, a citation under the OSH Act's General Duty Clause could be issued." This brings the question – how should machinery without process flow be addressed?

There are separate standards available for evaluating machinery hazards and designing their safeguards appropriately: ISO 12100, IEC 62061, and ISO 13849. Fortunately, functional safety of machinery follows a similar workflow to the process safety lifecycle. Similar to identifying risk gaps in a Process Hazards Analysis (PHA), we can identify risk gaps for machinery. We can define risk targets, determine how to best close the risk gaps, specify a design, and verify the risk has been adequately addressed.

This paper will present a practical example application to demonstrate machinery safety risk reduction in accordance with machinery safety standards for machinery common to chemical process plants.

1 Introduction

Several years ago, in the United States of America (USA), Dust Hazard Analyses (DHA) came to the forefront of process safety risk analysis discussions. Performing a hazard analysis on a dust collection system was not a new concept. It was covered as part of a standard process hazards analysis (PHA), with guidance from the National Fire Protection Association (NFPA). The fairly new standard, NFPA 652, addressed hazards unique to dust. Chapter 7 of the standard requires the DHA methodology for existing facilities or those implementing significant modifications.[1] As seen with the evolution of the DHA, sometimes a specific attribute of a hazard analysis requires specialized knowledge and tools.

Machinery safety is one of these areas, requiring a specialized risk assessment method and design analysis methods. Internationally, the International Organization for Standardization (ISO) and International Electrochemical Commission (IEC) standards drive regulation. In the USA, the Occupational Health and Safety Administration (OSHA) sets and enforces standards. Standards are approved and published by the American National Standards Institute (ANSI). While OSHA does not list extensive machinery safety regulations, it does list machine guarding requirements for 6 main types of equipment: woodworking machinery, abrasive wheel machinery, mills and calendars (rubber and plastics industries), mechanical power presses, forging machines, and mechanical power-transmission apparatus.[2] In an interpretation letter from April 28, 1999, OSHA notes that:

> If a serious injury could result from an improperly-design or installed emergency stop device, a citation under the OSH Act's General Duty Clause could be issued.[3]

Failure to mitigate the risks associated with machinery falls under the General Duty Clause. Emergency Stops (E-Stops) represent just one type of machinery safeguarding available. Knowing the General Duty Clause can be cited, are we paying enough attention to conveyors, box dumpers, cutter machines, and other common machinery during our normal process risk assessments? This is not to cast doubt on the abilities of all the talented PHA facilitators of the world. It's not that these risk assessments cannot be led by the same facilitator that leads the PHA. We cannot be honest without realizing additional knowledge is needed for classifying machinery-associated risks.

Let us then consider a "machinery safety risk assessment" (MSRA) in the future. Machinery safety is less about process flow and more about human interaction with the machinery. Machinery hazards are sufficiently different from process hazards that machinery warrants a different risk assessment methodology. Risks are then eliminated through design or the risk of hazards are reduced through protective measures. The resulting machine safety functions have a safety lifecycle that is very similar to that of safety instrumented functions (SIFs) in the process safety lifecycle following IEC 61511, which many PSM covered plants are already familiar with.[4] There are specific standards for handling the design of machinery safety functions. This paper walks through an overview of a machinery safety lifecycle that can be found in chemical process plants to help us keep all ten fingers and all ten toes.

In the USA, the American National Standards Institute is the recognized organization providing the guidance for machinery safety safeguarding in the ANSI B11 standards. Due to broad international applicability, this paper refers to the international standards.

2 Machinery Safety Risk Assessment (MSRA)

2.1 Hazard identification

For the presented example, consider a Pastillator machine. In simplistic terms, by someone who is by no means a Pastillator expert, a Pastillator looks like a long conveyor. The product is fed onto a belt in the form of droplets. The product is cooled by cooling water sprayed against the underside of the belt, and product droplets solidify into pastilles. Along the machine there are various hot surfaces exceeding 140°F that have been insulated or guarded.

A process hazards analysis is recommended to capture the hazards of liquid flow to and through the Pastillator. To address hazards around machinery regarding rotating equipment, entanglement, crushing, and shearing, consider a machinery safety risk assessment. The Pastillator also has various pinch, nip points, and shearing points along the length of the machine.

At one end of the Pastillator, there is a Feed Tank. The Feed Tank has a flat top hinged lid. The tank is fed with a feed pump. Although there is a high-level switch, operators open the lid twice daily to visually verify the liquid level of the product. The tank is fitted with a mixer. The operator does not normally open the tank while the mixer is in operation.

The moving mixer inside poses the risk of an entanglement hazard. This could cause an irreversible injury, such as amputation of fingers or arms. The operator is protected when the lid is closed during operation, as they cannot contact the mixer. Consider that currently, there is no interlock on the tank lid. The mixer does not stop when the lid is opened, which exposes the operator to the entanglement hazard.

Understanding the hazardous scenario is the first step. Next, move into quantifying the risk and identifying the safeguarding requirements associated with designing a safe machine interaction.

2.2 Risk quantification

Annex A of ISO 13849-1 provides guidance on one methodology for ranking the risk associated with the hazardous scenario.[5] The method presented is a risk graph with a binary ranking matrix. This binary approach is simplistic and provides an estimate for quantification of risk. The risk graph is shown in Figure 1 below.

Severity of Injury		
S1	Minor	Normally Reversible
S2	Severe	Normally Irreversible
Frequency of Exposure		
F1	Seldom	<5% of operating time, or <1 occurrence per 15 minutes
F2	Frequent	>5% of operating time, or >1 occurrence per 15 minutes
Possibility of Avoidance		
P1	Possible	Realistic chance of avoiding hazard
P2	Impossible	No realistic chance of avoiding hazard

Figure 1: Risk Ranking Parameters, ISO 13849-1

Consider the example hazardous scenario: the operator opens the lid of the tank twice per day and is exposed to the risk of entanglement due to the mixer. The mixer is located at the top of the tank, and it is not possible for the operator to anticipate the position of the mixing arm prior to opening the lid; therefore, the operator is immediately exposed to the hazard.

The severity of injury is first examined and divided into minor injuries (normally reversible) and severe injuries (normally irreversible) or death. A laceration that will heal as part of the normal healing process is considered a minor injury. An example of a severe injury is an amputation.

S2 – Severe injury is selected for the example scenario.

The operator's duration and frequency of exposure to the hazard are considered for the next parameter. If the operator is frequently exposed to the hazard, F2 (frequent) should be selected. An infrequent exposure would be approximately less than 5% of the operating time.

F1 – Seldom is selected for the example scenario.

Finally, the possibility of avoiding the hazard is considered. This parameter also considers the probability of occurrence of the hazardous event. The rule of thumb for this parameter is to select P2 (impossible). P1 (possible) can be selected if there is a genuine chance of avoiding the hazard.

P2 – Impossible to avoid is selected for the example scenario, as the mixer is located near the lid of the tank, it is not possible for operator to anticipate the position of the mixer and likely would not be possible to avoid.

Utilizing the risk ranking matrix from ISO 13849-1 (see Figure 2: Risk Matrix & Performance Level Required, ISO 13849-1), we can determine the required risk quantification and performance level requirements for the safeguard that is selected to mitigate this hazardous scenario. S2, F1, and P2 yield a high level of risk, with a performance level (PL) requirement of PLd. Mapping to Figure 2, the risk correlates to an unacceptable level and therefore requires mitigation by safeguarding.

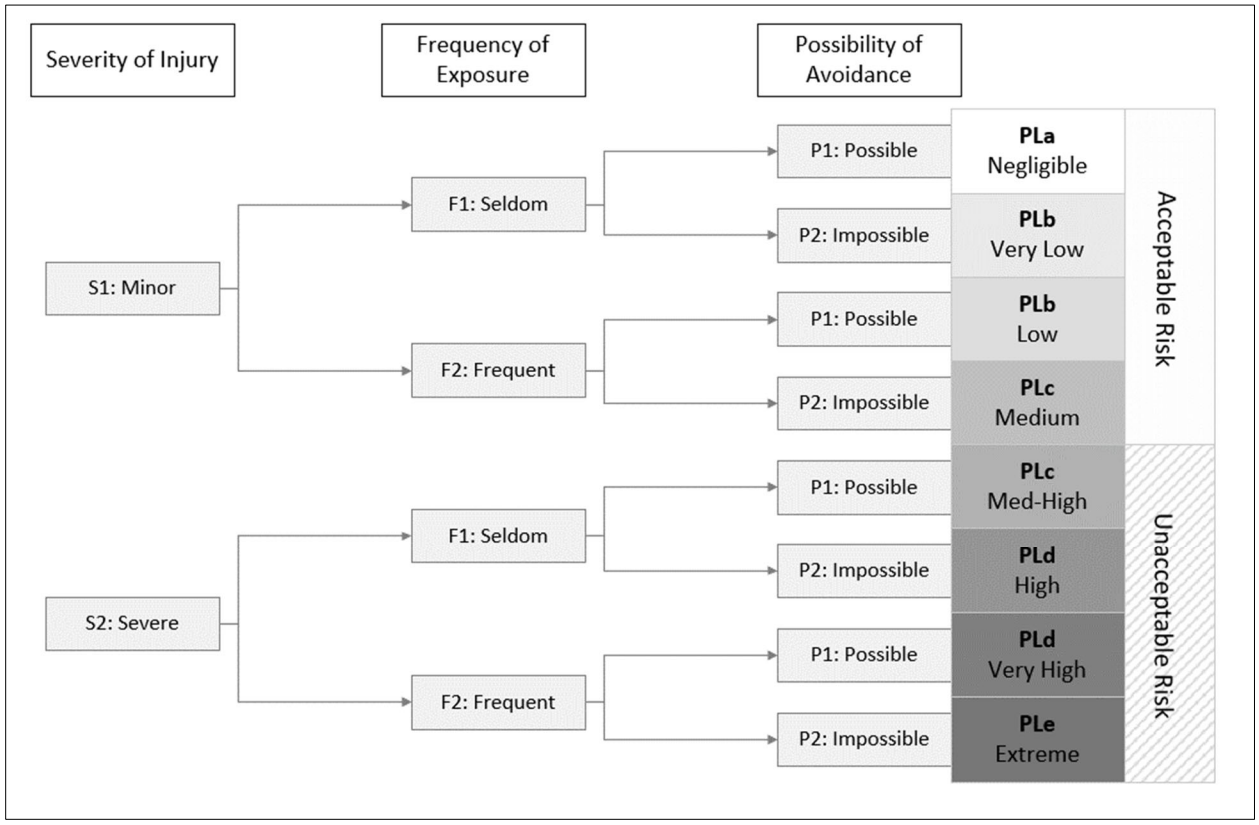


Figure 2: Risk Ranking & Performance Level Required, ISO 13849-1

2.3 Safeguard Selection

The only existing safeguards around this scenario are administrative, which are not considered for further risk reduction credit. The team recommends interlocking the Feed Tank lid so that upon opening, the agitator will stop prior to the chance for entanglement. Per the risk ranking matrix, the new interlock will need to meet the requirements for PLd per ISO 13849-1. The lid should be interlocked to stop the rotating equipment (the agitator) as quickly as possible.

Figure 3 demonstrates the MSRA documenting the safeguard selection and the risk levels achieved by the safeguard. It is determined that an interlocking switch on the lid of the Feed Tank that stops the agitator will be sufficient to reduce the risk of injury to an acceptable level.

				Risk Ranking without Safeguards								Risk Ranking prior to Recommendations and Corrective Actions			Risk Ranking post Recommendations and Corrective Actions	
Scenario	**Hazard**	**Operational Mode**	**Task**	**Severity of Injury**	**Frequency of Exposure**	**Possibility of Avoidance**	**Risk Ranking**	**Acceptable?**	**Safeguard Selection**	**PLr (PL required)**	**Existing Safeguard Description**	**Risk Ranking**	**Acceptable?**	**Recommendations and Corrective Actions**	**Risk Ranking**	**Acceptable?**
Scenario 1	Entanglement hazard	All	Opening tank lid for visual level verification	S2	F1	P2	**High**	**N**	[Proposed] Interlocking Guard	PLd	Administrative measures only (Personal Protectice Equipment, Safe Work Procedures)	**High**	**N**	Interlock the Feed Tank lid to stop the agitator upon opening; Verify interlock meets requirements of PLd per ISO 13849-1	**Neg.**	**Y**

Figure 3: MSRA Safeguard Selection and Requirements

For further examples of hazards, hazardous situations, and hazardous events pertaining to machinery, ISO 12100 is available.[6] Annex B of this standard groups types of hazards and their potential consequences. For example, the potential consequences for rotating or moving elements are noted as severing and entanglement. This standard is an excellent resource to review and reference for a machinery safety risk assessment.

The Pastillator design includes physical guarding around rotating equipment as well as rope pull switches along either side of the machine. Tension on the safety-rated rope switch from any angle will E-Stop the machine. These E-Stop pull rope switches around the machinery are considered during the risk assessment for general pinching, nipping, or shearing along the length of the Pastillator machine. For E-Stops, in particular, the standard ISO 13850 is considered. Per this standard, the minimum performance level* required is PLc.[7] During the risk assessment, the team does not determine a need for a higher PL than this. ISO 13850 requires the safety-related parts of the emergency stop to comply with machinery safety standards ISO 13849-1 and/or IEC 62061.[8] The team recommends that the currently installed rope pull switches be verified for compliance with ISO 13850 requirements for E-Stops.

*Note that ISO 13850 gives the alternate performance target of SIL 1 per IEC 62061

3 Design to Meet the Target PL

To meet the required performance level of PLd, an interlocking switch will be installed on the Feed Tank lid. The plant has a coded magnet safety switch already available and would like to use it if feasible. There is currently no safety relay, and the single agitator motor contactor is for general-purpose use.

First, the designer considers whether the lid will need to be locked. In many cases, a locking hatch or locking lid is required to prevent the hazard. Will the agitator stop in time upon opening the lid to prevent an entanglement hazard? An additional option could be to install a gate with an

interlocked switch around the Feed Tank to stop the agitator. This would allow additional time to reach the hazard for motors with a longer rundown time.

For this example, 2 standards were reviewed for guidance in determining speed of approach (walking speed and upper limb movement) and the minimum safety distances required. The standards are ISO 13855 for safe stopping distances and orientation relative to the hazard and ISO 13857 for establishing the minimum safety distances required to prevent the hazard from being reached.[9,10] It was determined that the Feed Tank agitator would stop quickly enough upon immediate removal of power to use the coded magnet safety switch alone. A locking switch or gate around the Feed Tank will not be utilized.

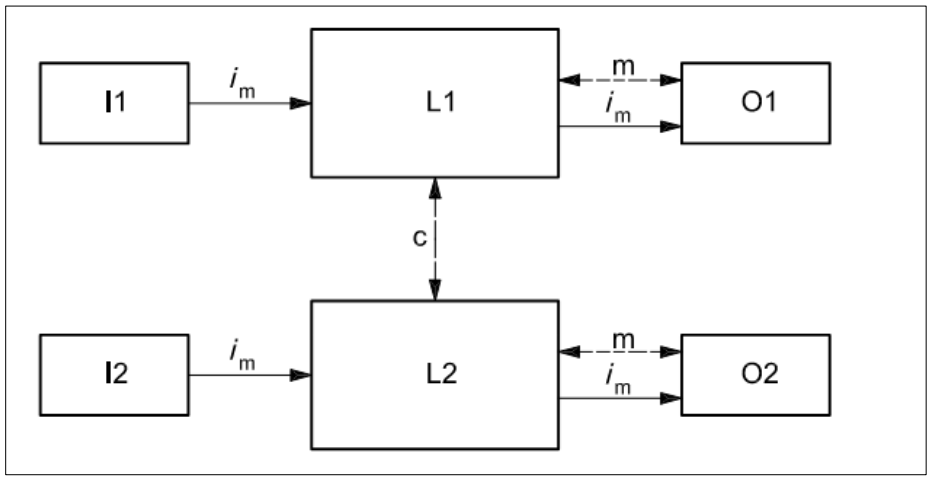
The chosen coded magnet safety switch also is a well-tried model with manufacturer safety data available. It is a dual-channel safety switch with an actuator. The switch has 2 normally closed contacts. With dual-channel usage and wiring per manufacturer requirements, the manufacturer claims that the switch is capable of reaching up to Category 4, PLe per ISO 13849-1.

A safety relay will be installed to monitor and trip the safety interlock. The selected safety relay is a well-tried model with manufacturer safety data available. The device is capable of wire breakage and earth leakage detection. The manufacturer claims the device is capable of reaching up to Category 4, PLe per ISO 13849-1. The safety relay will monitor the feedback contacts from the motor contactors and will trip on detection of a fault.

The existing single motor contactor rated for general-purpose use will not be adequate for achieving the target PLd. To strengthen the safety integrity of this circuit, a well-tried safety-rated motor contactor is selected.

Is this single motor contactor adequate, or is a second motor contactor required? ISO 13849-1 describes acceptable architectures or “Categories”. Safety circuits can be configured per ISO 13849-1 in Category b, 1, 2, 3, or 4. If the failure rate data is sufficiently low, then the single contactor could be used in a Category 2 configuration. This would require a test output channel with a second means of shutting down the agitator.

For this example, a test output channel will not be used. The target architecture will then be a Category 3. The structure for Category 3 per ISO 13849-1 is illustrated in Figure 4.



Key

i_m	interconnecting means
c	cross monitoring
I1, I2	input device, e.g. sensor
L1, L2	logic
m	monitoring
O1, O2	output device, e.g. main contactor

Figure 4: Designated Architecture for Category 3 per ISO 13849-1

With this structure, redundancy is required. It is worth noting that this redundancy can be achieved in some cases using a single device equipped with internal redundancy. The safety relay has internal redundancy, and as noted previously, it is capable of reaching up to Category 4. For this example, the design is targeting meeting a minimum of Category 3 architecture and its requirements. Refer to the block diagram shown in Figure 5.

Achieving Category 3 does mean that some form of diagnostic coverage is required. For the safety switch, the requirement for diagnostic coverage is fulfilled by cross-monitoring at the safety monitor. Also, there is fault detection by the process whenever the lid is opened twice daily. The diagnostic coverage is assumed as 90% (“medium”). To reduce common cause failures for this dual-channeled switch, the designers specify individual shielded twisted pairs on each channel between the switch and the safety monitor. The dangerous mean time to failure ($MTTF_D$) provided by the manufacturer for the switch is “high,” which corresponds to a “low” failure rate.

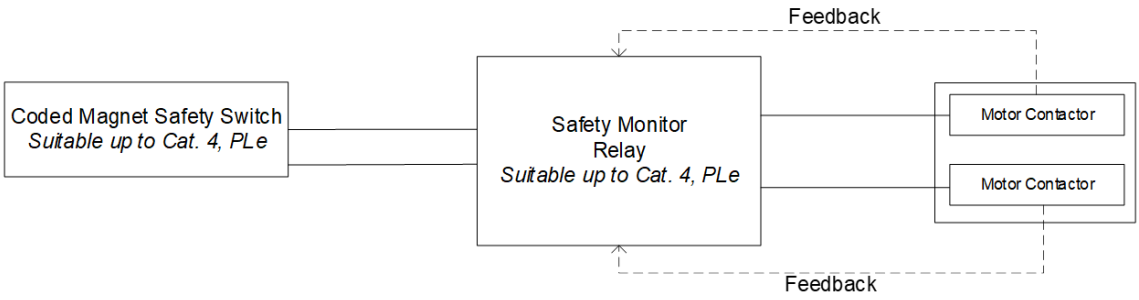


Figure 5: Selected Architecture for Meeting Category 3 per ISO 13849-1

The safety monitor is specified to ensure its dipswitch is set to include cross monitoring. The dangerous mean time to failure ($MTTF_D$) provided by the manufacturer for the safety monitor is "high".

The motor contactors are each equipped with a mirror contact. This is a normally closed contact that cannot physically be closed simultaneously with a normally open main contact. They are mechanically linked, where even in the case of a welded main contact, the mirror contact cannot close. The motor contactor is suitable in application up to Category 4, PLe depending on the configuration. To achieve the minimum Category 3 target for this safety interlock, the motor contactors will include a feedback loop of the mirror contacts to the safety monitor for monitoring. The dangerous mean time to failure provided by the manufacturer for the motor contactors is "high." To reduce common cause failures, installation will need to ensure sufficient separation in wiring (for example, for the prevention of electromagnetic coupling and induced noise). The motor contactors will use separate cables and have short runs within the control cabinet.

To verify the target of PLd is met, the component parameters are entered into the ISO 13849-1 verification software SISTEMA.[11] The structure of the calculation includes dual channels for the switch and the motor contactors (Figure 6).

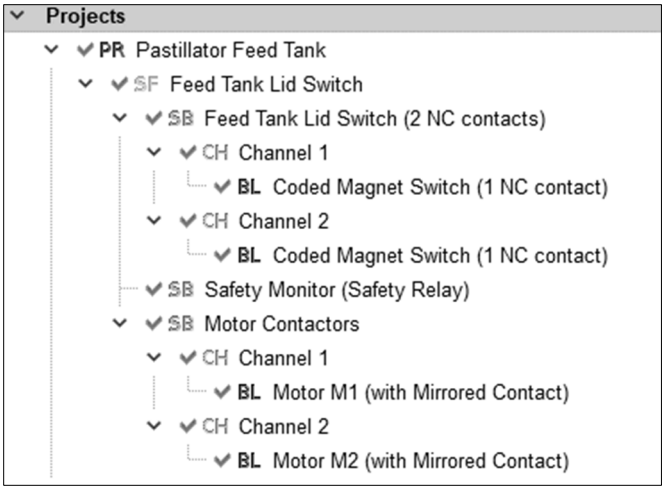


Figure 6: PL Verification Calculation Structure in SISTEMA

While there is a single switch, it is used per the manufacturer in dual-channel wiring (1 normally closed contact per channel). The calculation achieves the target Performance Level, PLd (Figure 7).

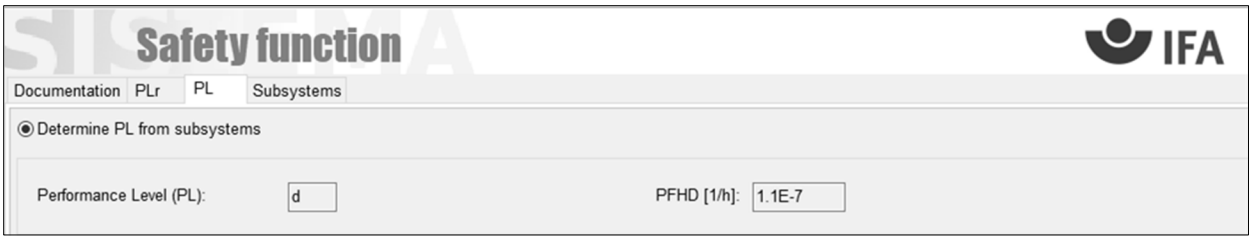


Figure 7: Performance Level Achieved in SISTEMA

4 Safety Requirements Specification

ISO 13849-1 requires that a safety requirements specification (SRS) shall be available for each safety function. Concurrently with the safety function initial design, the SRS is compiled. Ideally, PL verification calculations are performed *after* the SRS, but realistically draft calculations are helpful *during* the early SRS phase for narrowing down component selections.

The requirements that shall be documented as part of the SRS are listed in the standard. It includes documenting the required performance level as well as other machinery operating characteristics necessary for achieving safe operation of the control system. This step is very similar to creating a safety requirements specification for a process safety SIF.

Beyond simply knowing the structure of the safety function and what components will be used, the SRS helps fill in the gap with details. Will the machinery safety function need to be active at all times? Will the safety function still trip if the machine is in a Maintenance Mode, or is the safety function disabled? Is the equipment located in a hazardous (classified) area? How often will the safety function be activated?

A software SRS is required when a programmable safety relay or a safety programmable logic controller (PLC) is used. The software is additionally required to be validated during software validation testing. In this example, the safety monitor is non-programmable, and a software SRS is not required.

The requirements determined during the design process are documented in the SRS to define the safety function. In addition to the boundary conditions specified below in Figure 7, Clause 5 of ISO 13849-1 can be followed for further requirements.

Requirement	Description
Safety Function (SF) identification	SF-01 Feed Tank Lid Switch
Task and Machine Interactions	Opening tank lid for visual level verification
Type of Function	Safety-related Stop Function
SF Control Function Description	Agitator motor must be shut down when the lid of Feed Tank is opened.
Hazard	Entanglement – Operator contact with rotating agitator
Fault Considerations	Trip function (de-energize agitator motor) upon detection of fault. Motor de-energizes upon loss of power to the machine.
Frequency of Operation	Every 12 hours
Required reaction time	The motor must stop (stand still) within 0.5 seconds

Figure 8: Safety Requirements Specification Excerpt for Safety Function

After the safety function is designed and analyzed, the system is implemented. It can then be tested or validated as part of the machinery safety lifecycle. Validation ensures that the safety requirements specifications made during design have been followed. Guidance for the validation process is provided in ISO 13849-2.[12]

5 Conclusion

In conclusion, we've identified that machinery requires a different risk assessment methodology and outlined key design and analysis considerations for machinery safety functions. While both machinery safety lifecycles and process safety lifecycles have a similar look and feel at a conceptual level in the chemical process industries, they are very different activities. This requires different skillsets, knowledge, and possibly team members to be involved. Where process fluids are flowing, comply with PHA methodologies and IEC 61511 or other standards as necessary. Where machinery E-Stops, light curtains, switches, and stopping rotating equipment occur, consider a machinery safety risk assessment. There are already established standards for machinery. Next time, why not take advantage of these tools instead of forcing machinery into a chemical process-colored box?

References

[1] NFPA 652*, Standard on the Fundamentals of Combustible Dust*. National Fire Protection Association; 2019.

[2] United States Department of Labor. *1910 Subpart O - Machinery and Machine Guarding*. Occupational Safety and Health Administration; 2004. Accessed January 4, 2023. https://www.osha.gov/laws-regs/regulations/standardnumber/1910/1910SubpartO

[3] United States Department of Labor. *Clarification of under voltage protection on metal-working equipment and emergency stop devices.* Occupational Safety and Health Administration. Published April 28, 1999. Accessed January 4, 2023. https://www.osha.gov/laws-regs/standardinterpretations/1999-04-28

[4] IEC 61511-1*, Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Application Programming Requirements*. IEC; 2016.

[5] ISO 13849-1:2015*, Safety of Machinery – Safety-Related Parts of Control Systems – Part 1: General Principles for Design*. International Organization for Standardization; 2015.

[6] ISO 12100:2010*, Safety of Machinery — General Principles for Design — Risk Assessment and Risk Reduction*. International Organization for Standardization; 2010.

[7] ISO 13850:2015*, Safety of Machinery - Emergency Stop Function – Principles for Design*. International Organization for Standardization; 2015.

[8] IEC 62061*, Safety of Machinery - Functional Safety of Safety-Related Control Systems*. IEC; 2021.

[9] ISO 13855:2010*, Safety of Machinery — Positioning of Safeguards with Respect to the Approach Speeds of Parts of the Human Body*. International Organization for Standardization; 2010.

[10] ISO 13857:2019*, Safety of Machinery – Safety Distances to Prevent Hazard Zones Being Reached by Upper and Lower Limbs*. International Organization for Standardization; 2019.

[11] *Safety Integrity Software Tool for the Evaluation of Machine Applications* [Computer Software]. Version 2.0.8. Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA); 2018.

[12] ISO 13849-2:2012*, Safety of Machinery — Safety-Related Parts of Control Systems — Part 2: Validation*. International Organization for Standardization; 2012