

# The Machine Safety Life Cycle — A Process for Compliance, Safety and Productivity of Machines

Hazards are ever-present in the steel plant environment, and a heightened awareness and emphasis on safety is a necessary priority for our industry. This monthly column, coordinated by members of the AIST Safety & Health Technology Committee, focuses on procedures and practices to promote a safe working environment for everyone.

## Author

**Mark Eitzman**  
Sales Engineer/Safety and Project Manager, Integrated Mill Systems, Willoughby, Ohio, USA

There is a well-defined process to attain both regulatory compliance and an enterprise's acceptable level of risk in machine safety. Thanks to continuous updates to the global consensus standards, it can be applied to any manufacturing asset in the U.S. and the world. The process, often depicted as five steps, is commonly referred to as the machine safety life cycle. These steps are outlined in this article and should be present, in some form, in company policies and procedures for manufacturing safety for machines. This information can be used as a checklist to compare existing policies and procedures or can provide a framework from which to create them now. These five steps are shown in Fig. 1.<sup>1</sup>

The machine safety life cycle helps with compliance to OSHA's general duty clause which states: "OSH Act of 1970 SEC.5. Duties: (a) Each employer (1) shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees."

Further, executing on these steps helps companies to attain an acceptable level of risk as defined by the owner while striking a balance with productivity overall equipment effectiveness (OEE) and operations demands. This is done by defining risk reduction solutions that meet actual risk reduction requirements by following a systematic approach rather than assumed requirements or a universal or minimal level (i.e., all safety circuits shall be PLd/cat3 or higher).

From a broader perspective, the process documents the judgment and justification for the decisions made regarding risk reduction

efforts for known hazards, creating evidence that the best decision was made with the information available at that time. This will help in the event that this information may be used later following a safety incident and can help to protect the company image and brand equity. The best reason to follow these steps is that it is the best means to prevent a safety incident. The use of such a process can help the efforts to promote employee safety and corporate social responsibility. This, in turn, can enhance the ability to attract and retain a quality workforce by demonstrating a commitment to worker safety.

The following sections cover what is involved with each step of the machine safety life cycle, its purpose, and how each leads to and supports the steps to follow.

## Step One: The Team-Based Risk Assessment

Since all the following steps build on information in the risk assessment, Step One can be considered the most important foundational step. The purpose of a team-based risk assessment is to estimate and evaluate the risk to all of whom are affected by the machine, that is, operate, maintain or come in contact with the machine for any foreseeable manner or reason, including pedestrians and by-standers. Risk that is deemed acceptable is documented at this step and no further effort is needed. If the risk is unacceptable, the risk reduction methods to attain an acceptable level are outlined and used in the next step of the machine safety life cycle.

It is important to note that the term "risk assessment" may sometimes be

Comments are welcome.

If you have questions about this topic or other safety issues, please contact [safetyfirst@aist.org](mailto:safetyfirst@aist.org).

Please include your full name, company name, mailing address and email in all correspondence.

used as a label for something other or often less than what is defined by the standards as a risk assessment (presented later in Fig. 4).<sup>2</sup> Hazard assessments or machine safety audits may be called risk assessments, but usually do not include all of what is included in other steps. These lesser efforts may serve a purpose, such as helping to prioritize where full team-based risk assessments should be conducted, but those do not provide enough information for use in subsequent steps in the machine safety life cycle. Whether risk assessments are conducted internally or with outside resources, make sure that what is being done is as described in those steps.

The team-based risk assessment process includes the following steps.

**Step One** — Define the scope/machine/facility and gather the information about the asset(s), including:

- Machine life cycle phase(s) in scope (such as design, build, install, commission, setup, operate, decommission, demolition/removal).
- Production rates, cycle times, speed, forces, materials to be used.

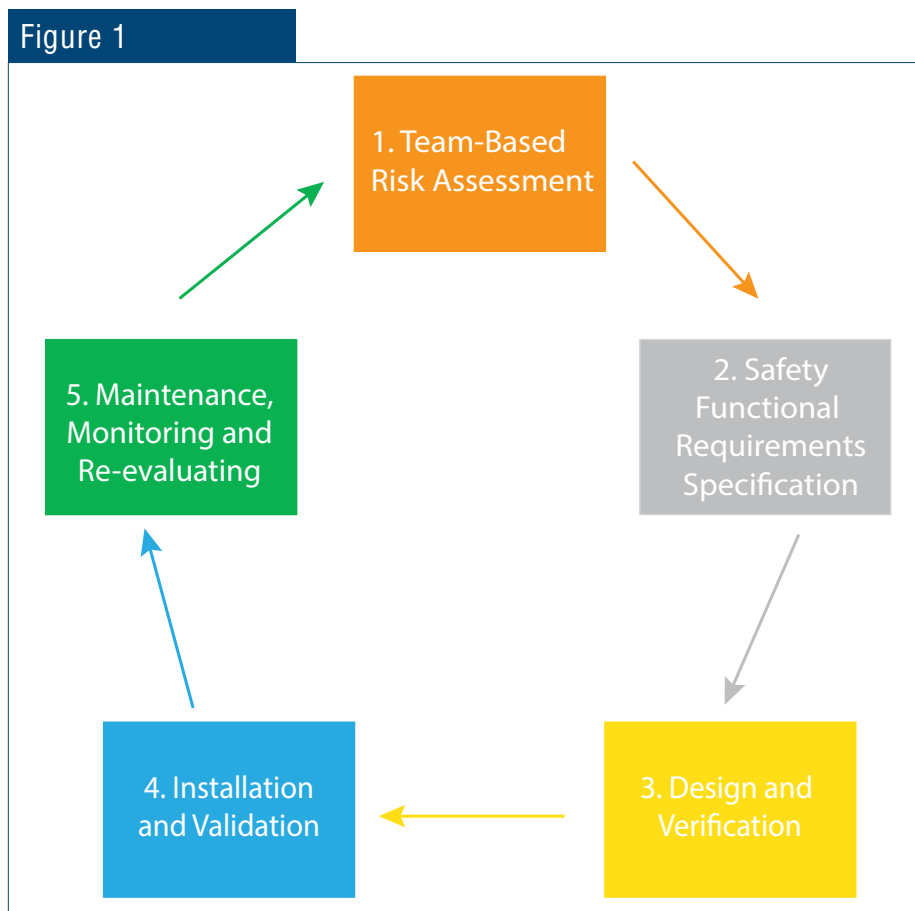
- Environmental limits (temperature, humidity, moisture, noise, location, lighting day and night).
- Other machines or equipment integrated or associated with the machine.
- All energy sources and lockout/tagout (LOTO) procedures.
- Products and materials to be process (type, sizes, grades, temperature, etc.).
- Define which material changes are the result of the process (type, sizes, grades, temperature, etc.).
- Anticipated tooling wear and anticipated maintenance tasks, times and intervals of mechanical, electrical, fluid power devices.
- Anticipated preventive maintenance tasks, times and intervals.
- Space required for installation, maintenance and operation.
- History of known safety incidents or similar assets.

**Step Two** — Identify all persons affected by the asset and the defined steps of each of their tasks under normal and foreseeable abnormal conditions/operations for each phase of the machine's life cycle. This includes bystanders and pedestrian traffic.

Next, identify all hazards that expose affected people or equipment to harm or damage during those tasks. The risk assessment documents will have a line item for each person/task/step/hazard.

**Step Three** — Estimate the risk for each person/task/step/hazard utilizing a method that considers severity and probability. Probability is estimated on the basis of exposure and avoidance. Fig. 4 refers to several risk estimating methods and Fig. 3<sup>1</sup> shows minimum risk reduction measures as a function of the risk level. The decision matrix results in estimated levels of risk such as negligible, low, medium, high and very high. Definitions of each rating are shown in Fig. 2.<sup>1</sup>

Risk estimation should be done from two perspectives — the initial risk and the existing risk. Initial risk estimation assumes no risk reduction methods are in place (such as machine



The machine safety life cycle is a continuous process where Step Five often leads to the need for Step One.

Figure 2

Severity of Injury	Exposure to the Hazard	Avoidance of the Hazard	Risk Level
S1 - Minor	E0 - Prevented		NEGLIGIBLE
	E1 - Low	A1 - Likely	
	E2 - High	A2/A3 - Not likely/ Not possible	LOW
S2 - Moderate	E0 - Prevented		MEDIUM
	E1 - Low	A1 - Likely	
	E2 - High	A2/A3 - Not likely/ Not possible	HIGH
S3 - Serious	E0 - Prevented		LOW
	E1 - Low		HIGH
	E2 - High	A1/A2 - Likely/Not likely	
			A3 - Not possible

Risk level decision matrix.

guards or personal protective equipment (PPE)) to provide an understanding of the underlying hazard. The existing risk can then be estimated with the current risk reduction methods in place.


**Step Four** — The responsible entity, typically the asset owner, evaluates the existing risk level of each person/task/step/hazard item and deems it either acceptable or unacceptable. If the existing risk is deemed acceptable, then this is documented and moves to the next person/task/step/hazard item. If it is unacceptable, then a future method to reduce the risk is proposed. This may include more than one method or layers, resulting in some residual risk. This residual risk is then estimated and evaluated and this effort is repeated until an acceptable risk level is obtained. All of this is documented and used in the next step in the machine safety life cycle.

The selected risk reduction methods are key to the risk assessment. There have been significant developments of products, technologies and techniques that provide an ever-increasing range of options. When selecting which of these methods is most feasible, the following should be considered:

- Existing safety culture.
- Regulatory obligations.
- Effectiveness and machine performance.
- Usability and productivity.
- Introduction of new hazards.
- Durability, maintainability and ability to clean.
- Ergonomic impact.
- Economic and technological feasibility.

The current standards provide further guidance on these options. Fig. 3 provides recommended methods

Figure 3

	Risk Reduction Measure	Risk Level				
		VERY HIGH	HIGH	MEDIUM	LOW	NEGLIGIBLE
 <p>Most Preferred</p> <p>Least Preferred</p>	Elimination	Use of one or a combination of these risk reduction measures are required as a primary means to reduce risks.				
	Substitution					
	Limit Interaction					
	Safeguarding/SRP/CS					
	Complementary Protective Measures	Use of one or a combination of these risk reduction measures may be used in conjunction with the above risk reduction measures but shall not be used as the primary risk reduction measure.				
	Warnings and Awareness Means					
	Administrative Controls					
	PPE					
		Any of the risk reduction measures that would reduce risks to an acceptable level may be used.				

Minimum risk reduction measures as a function of the risk level.

of risk reduction based on the results of the determined risk level from the decision tree. Fig. 4 provides good guidance on risk recommendations referred to as the Hazard Control Hierarchy.

A good understanding of these approaches is required in order to determine the expected risk reduction. The risk assessment should document a basic description of the method chosen for each person/task/step/hazard line item. The details of each future/proposed method will be defined in Step Two of the machine safety life cycle.

### Step Two: The Safety Functional Requirements Specification (SFRS)

The SFRS is an engineering study that defines the future risk reductions methods with enough detail for them to be designed and describes how they will be applied and used. This includes details such as:

- Operational sequence of the identified tasks.
- Definitions of the safety zones and span of control of e-stops and safety functions.
- Calculations such as the required machine response or stop time.
- Definitions of “safe state,” triggering events and means/conditions of reset.
- Exact dimensions and placement (safe distance) for fixed guards and movable guards with devices.
- Identification of each actuator or source of the hazardous energy associated with each hazard.

- Bill of material of the safety-rated parts of the control system (SRP/CS), made up of input, logic and actuator elements, and how they are to be connected (architected).
- The standards to which the solutions are being designed.

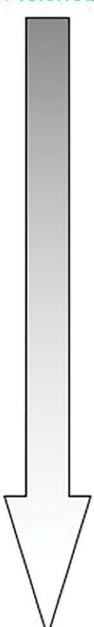
These risk reduction methods are grouped within ANSI B11.0 – 2020 into the following classifications:

- Inherently Safe by Design.
- Engineering Controls
- Administrative Controls.

The methods are then ranked in that order for preference and expected effectiveness. The partner standard to ANSI B11.0 – 2020 is ANSI B11.19 – 2019 Performance Requirements for Risk Reduction Measures: Safeguarding and other Means of Reducing Risk. ANSI B11.19 – 2019 provides the engineers with the current guidance on the requirements of these risk reduction methods and the proper application of contemporary technologies and products for each classification. These requirements, classifications and examples are shown in Fig. 4.

**Inherently Safe by Design** — Inherently safe by design are the means by which hazards are eliminated by changes to the asset’s design, process of use or materials used in the process. For example, these can include mechanical design changes that eliminate a pinch point. Another example would be changes to the

Figure 4

	Classification	Risk Reduction Measures	Examples
 <p>Most Preferred</p> <p>Least Preferred</p>	Inherently Safe by Design	Design Out (Elimination or Substitution)	<ul style="list-style-type: none"> <li>eliminate pinch points (increase clearance)</li> <li>intrinsically safe (energy containment)</li> <li>automated material handling (robots, conveyors, etc.)</li> <li>redesign the process to eliminate or reduce human interaction</li> <li>reduce force, speed, etc. through selection of inherently safe components</li> <li>substitute less hazardous chemicals</li> </ul>
		Engineering Controls	Guards, Control Functions and Devices
	Administrative Controls	Awareness Means	<ul style="list-style-type: none"> <li>lights, beacons, and strobes</li> <li>computer warnings</li> <li>signs and labels</li> <li>beepers, horns, and sirens</li> </ul>
		Information for Use (Training and Procedures)	<ul style="list-style-type: none"> <li>safe work procedures</li> <li>training</li> </ul>
		Administrative Safeguarding Methods	<ul style="list-style-type: none"> <li>safe-holding safeguarding method</li> </ul>
		Supervision	<ul style="list-style-type: none"> <li>supervisory control of configurable elements</li> </ul>
		Control of Hazardous Energy	<ul style="list-style-type: none"> <li>lockout / tagout</li> </ul>
		Tools	<ul style="list-style-type: none"> <li>workholding equipment</li> <li>hand tools</li> </ul>
Personal Protective Equipment (PPE)	<ul style="list-style-type: none"> <li>safety glasses and face shields</li> <li>ear plugs</li> <li>gloves</li> <li>protective footwear</li> <li>respirators</li> </ul>		

The Hazard Control Hierarchy.

process or task to limit or remove a person's exposure to a hazard, such as extending lubrication lines and zerk fittings outside of a hazardous area. Substituting less hazardous compounds used in a cleaning process would be another option.

**Engineering Controls** — Engineering controls include fixed guards or movable guards with control devices interlocked with safety-rated control systems. The SFRS would define guard dimensions and devices along with their exact placements. Detection and access control functional safety sequences would be defined to indicate how safety functions are triggered and reset as well as the machine's "safe state" and how fast this state needs to be attained.

All of these would take into account the defined task with the intent of minimal to no impact on the machine's operations. Methods such as these are "alternative means" to fixed guards and/or LOTO, both of which could impair the use, operation and productivity of the asset. An important aspect of the use of alternative means is that their use shall not increase risk over LOTO or fixed guards.

If an electric/electronic, hydraulic or pneumatic control circuit is to be used, the recommended performance level (PL) would have been determined by the estimated risk level in the risk assessment. PL is defined in ISO 13849-1 2008, Safety of Machinery — Safety-Related Parts of Control Systems Part 1: General Principles for Design. PL is analogous to safety integrity level (SIL). PL is covered in Step Three.

**Administrative Controls** — Administrative controls are reliant on proper human performance of actions and proper use of tools and devices that are meant to reduce risk. This inherently makes them the least preferred. This classification of risk reduction methods includes awareness means, training on procedures, safe-holding of an enabling switch/pendant, supervision, LOTO, tools and PPE. These methods can be used in combination with each other and/or with engineered controls for an accumulative effect in order to attain an acceptable level of risk.

Once the SFRS is complete, the design of solutions can be done more efficiently and accurately in the next step. The SFRS also reduces the probability of reengineering or designing during installation.

## Step Three: Design and Verification

The future risk reduction methods from the risk assessment are now ready to be engineered to the requirements in the SFRS. In this step, the solutions are engineered and then verified that the designs meet the requirements. If inherently safe by design methods are not feasible, then engineered controls and/or administrative controls may have been proposed. The administrative controls will be defined and documented as part of the information for use of the machine, such as LOTO procedures. If alternative means to guards or LOTO are to be used, this would involve engineered controls such as guards, control functions and devices.

When utilizing alternative means, the risk reduction methods may rely on controls or safety functions, and may have one or more SRP/CS (safety-rated part of the control system). These SRP/CS may include electrical/electronic, hydraulic and pneumatic technologies. These control circuits may be relied upon as the key method to reduce risk. Their integrity and reliability is vital and thus their engineering must be verified to ensure that it meets the performance and quality requirements of the application, based upon the risk level in the risk assessment. This will involve the entire solution (i.e., sensors/inputs, logic solver and actuators/power controllers and how these are connected/wired). This can be done manually, utilizing the formulas in ISO 13849-2 2018, Safety of Machinery — Safety-Related Parts of Control Systems Part 2: Validation.

**Table 1**

*Minimum Functional Safety PL and Structure Category of Design for the SRP/CS*

PFHd	Performance level
1:10,000	a
1:100,000	b
1:333,333	c
1:1,000,000	d
1:10,000,000	e

**Figure 5**

Risk Level	PL <sub>r</sub>	Structure Category
<b>NEGLIGIBLE</b> (see 6.5.3.1)	b	-
<b>LOW</b>	c	2
<b>MEDIUM</b>	d	2
<b>HIGH</b>	d	3
<b>VERY HIGH</b> (see 6.5.3.2)	e	4

*Minimum functional safety performance.*

Fortunately, there is an alternative: a software tool called SISTEMA (Safety Integrity Software Tool for the Evaluation of Machine Applications). SISTEMA is a tool produced by IFA (Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung) and is available as a free download from their website. SISTEMA not only incorporates algorithms using the formulas in ISO 13849-1,2, but also contains a database of information on the safety-rated products used in these circuits. Manufacturers of safety-rated electric, electronic, hydraulic and pneumatic control products submit performance and product life data to IFA and it is compiled into the SISTEMA library database. This data is used by SISTEMA software to calculate the PL of the combination of components that comprise the safety function. So, what is PL?

PL levels established the average probability of a failure to dangerous per-hour PFHd over a minimum time frame based on the anticipated number of operations per year. In other words, what is the average probability that the safety function could fail to a dangerous state? PL is a calculated rating for the entire safety function as well as the components of the SPR/CS. The PL level are expressed as A, B, C, D or E. This is shown in Table 1.

PL for the whole safety function (input + logic + output) is determined by the following attributes:

- Category — Wiring structure or architecture.
- Reliability — Mean time to dangerous failure (MTTFd) — average probability per hour to mean time to fail dangerous based on the anticipated number of operations per year as declared by the customer.
- Diagnostic coverage — Test or monitoring quality.

- Measures against common cause failure (CCF) on multi-channel systems.

Fig. 5 recommends a minimum PL level and category structure category based on the risk level from the risk assessment per Fig. 3 in that standards.

#### Step Four: Installation and Validation

Installation and commissioning of engineered controls should be done by qualified technicians that are experienced with the safety standards for guards, safety control functions and devices. Today, more and more safety controls are seamlessly integrated into the main controls system and machine designs. Thus, a growing number of machine builders and controls systems integrators have the engineering talent for machine safety controls.

Once engineering controls are installed, they are to be validated to ensure that they meet the requirements of the SFRS. Validation will be conducted on the actual machinery, with power applied, through the systematic testing of each safety function in all modes of operation, including reasonably foreseeable abnormal operations. Common faults should be injected into the safety circuits such as short circuits and broken wiring connections to show that the safety functions fail or fault to a safe condition. Any corrections needed to meet the SFRS and the acceptable level of risk as per the risk assessment are done now and reverified and revalidated. Each reaction to each validation test of the solutions is documented. These documents can be quite valuable if proof of intent and fulfillment of due diligence is required in the future. They are also helpful if changes are made after commissioning.

#### Step Five: Maintenance, Monitor, Reevaluating and Continuous Improvement

It is recommended by the consensus standards that the safety solutions' functionality and performance be reviewed and tested periodically, at least annually. This includes LOTO for the maintenance tasks, and the safety functions (alternative means) for the minor servicing tasks. This is to ensure that, over time, the safety functions still meet the required performance level (PLr), as operations, procedures and machine performance will likely change the way people are affected by the machine. Further, changes in standards and regulations may also play a factor in determining whether a known risk, once considered acceptable, may later become unacceptable. Thus, safety solutions should be a vital aspect of a company's management of change procedures.

The concepts of Industry 4.0 (digitization) can help with the management of change. It is increasingly more common for operational and quality data to be collected from control systems. Including the safety data in the enterprise's digitization plan is then quite simple. With contemporary and integrated safety control systems, the data generated by the specific tags in the SRP/CS can be collected, formatted and presented to those who can make use of it in a way that may improve both safety and operations.

The concept is that real-time data, such as time-stamps and duration of e-stops, as well as tripping of safety gates and light curtains, can be contextualized into information about how the safety solutions, and thus the machine, are actually being used. This can be compared to its anticipated use, or it can help to determine if the safety solution is reducing productivity. Once analyzed, this becomes knowledge that can spot areas of improvement, misuse or even abuse. Taking appropriate action, such as the retraining of operators or reengineering of the solutions can have benefits to both safety and operations.

#### Conclusion

Following these five steps of the machine safety life cycle can help manufacturers attain regulatory compliance as well as improve productivity and efficiencies. More importantly, this process can help to improve the work environment and contribute to the fulfillment of corporate social responsibility.

#### References

1. RIA TR R15.306-2016, Robotic Industries Association, a division of A3, [https://www.robotics.org/bookstore-prod.cfm?category\\_id=118&product\\_id=434](https://www.robotics.org/bookstore-prod.cfm?category_id=118&product_id=434).
2. Reprinted from ANSI B11.0-2020 with permission from B11 Standards Inc. ◆