SICK
Sensor Intelligence.

Validation and Deployment Concerns to Maintain Acceptable Risk

Part 5 of 5 in a series addressing the primary milestones to a safe machine

Introduction

In order to ensure an acceptable level of residual risk has been achieved prior to deploying equipment for active service, it is imperative to implement one final series of steps. This stage is necessary to confirm that all risk reduction measures applied (design and build, technological, and organizational) are working together effectively to reduce the risk of all identified hazards to a tolerable level. This validation process must be documented to provide a written record of the current assumptions and decisions to aid future iterations of the risk assessment and risk reduction process.

Additionally, it must be acknowledged and accepted that the dynamics of the real world may – and probably will – eventually change the use of any machine. An effective change management program must therefore be in place to ensure that a process exists to catch even the slightest modifications, which could have a large impact to the overall level of safety of the equipment.

The concepts of final validation and documentation, combined with a recurring review process, will help maintain the lowest possible level of residual risk associated with the machine or process throughout the equipment lifecycle.

Types of Validation Steps

As part of the overall risk reduction process, protective measures are applied in a preferential order, as discussed in Part 3 of this series (*The Risk Reduction Process Utilizing a Hierarchy of Controls*). Typically, more than one measure is selected from the hierarchy to achieve an accumulated outcome of reducing the risk to an acceptable level. To ensure the effectiveness of the risk reduction strategy selected, however, each measure must be validated after it has been implemented. This validation process is intended to ensure that the initial goals have been fully achieved through proper selection, implementation, and execution of each protective measure.

The methods used to validate protective measures can vary depending on the type of measures applied, but often includes one or more of the following:

- Testing and verifying operation of safety devices and circuits
- Review of training
- Presence of warning labels
- Presence of lockout procedures and safe job procedures
- Functioning of complementary equipment

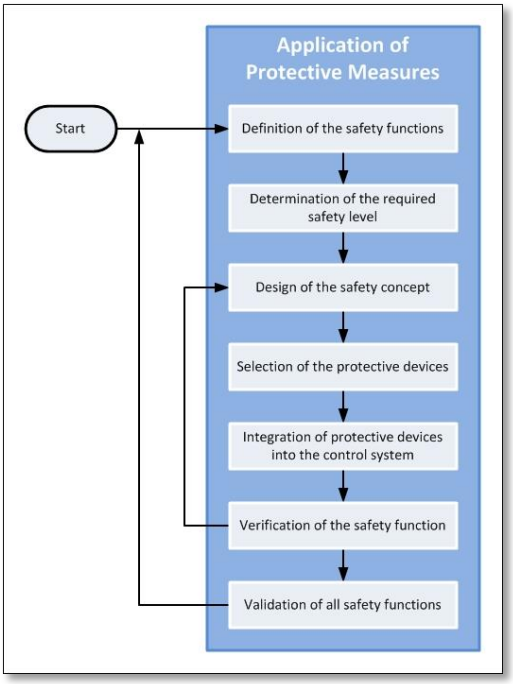

Figure 1: Application of Protective Measures

As discussed in Part 4 of this series (*Functional Safety for Machine Controls*), one of the key aspects of functional safety is to confirm that the specified performance for each safety function in the safety-related parts of control systems (SRP/CS) has been achieved. This is also an element of the overall validation which is performed after the protective measures are installed, as identified in Figure 1. Validation involves testing and analysis (for example, static, dynamic or failure analysis) to show that all parts interact correctly to perform the safety function and that unintended functions do not occur. Validation of the SRP/CS can include, but is not limited to, the following:

- The circuit was designed and implemented correctly
- The wiring was checked after installation and before commissioning
- The functionality of the safety system(s) was verified by the integrator and/or the user
- The safety device was functionally tested before commissioning

Ensure Safety during Validation

Testing of protective measures must not expose an individual to potential harm should the safeguard not provide the protection expected. Therefore, the validation process must be considered during the task and hazard analysis portion of the risk assessment.

The use of programmable control systems introduces an additional possibility to defeat or circumvent provisions to limit access if not properly applied or supervised. This is especially significant when remote access for the purposes of diagnostics or process correction are required. The organizational culture towards safety should also be considered, as it has bearing on the tendency to defeat or circumvent risk reduction measures. As reviewed in Part 3 of this series, there are many incentives to defeat or circumvent risk reduction measures, and all must be considered when validating the effectiveness of the protective measures applied.

Competence of Inspection and Validation Personnel

It is important that individuals conducting a validation or inspection are qualified and fully competent to perform the functional testing, evaluation and review necessary to determine if a protective measure is performing as intended. In some world regions or fields of study, determination of an individual or organization's competence can be established by certifications or other credentials that are maintained and up to date.

However in many specialized disciplines, there simply is no professional or educational program available to declare the qualifications of a person or organization. At other times, regulations or internal policies of an organization may require that an external entity perform such evaluations. In these cases, the following considerations should be made when evaluating the competence of the party providing validation or inspection services (the same criteria can be applied when evaluating potential resources to perform a risk assessment):

- Familiarity with applicable resources (regulations, standards, industry norms and best practices, etc.)
- Level of experience with the application, equipment, and protective measures
- Availability of resources
- Network of available resources and ability to draw on a larger pool of expertise to bring a high level of specialist skill
- Ability to provide an independent view and is resistant to undue influences
- Membership to professional and trade organizations
- Reputation / references

Commissioning

Many expectations exist which require equipment to be formally accepted or "signed off" prior to being placed into production. This process, commonly referred to as 'commissioning,' is the final opportunity for the user (employer) to verify all safety functions of the machinery. While near the end of the overall risk assessment process, as shown in Figure 2, commissioning (or validation of protective solutions) is one of the earliest opportunities afforded to the user to validate that the equipment supplier has effectively reduced all known risks to a tolerable level. Regardless of whether final commissioning takes place at the supplier or end user's facility, all potential hazards must be accounted for. If the commissioning and sign off occurs at a location other than the equipment's intended place of use, it important to also consider hazards which may arise from the intended environment, including clearances, accessibility, lighting and visibility, integration to other machines and/or processes, and so on.

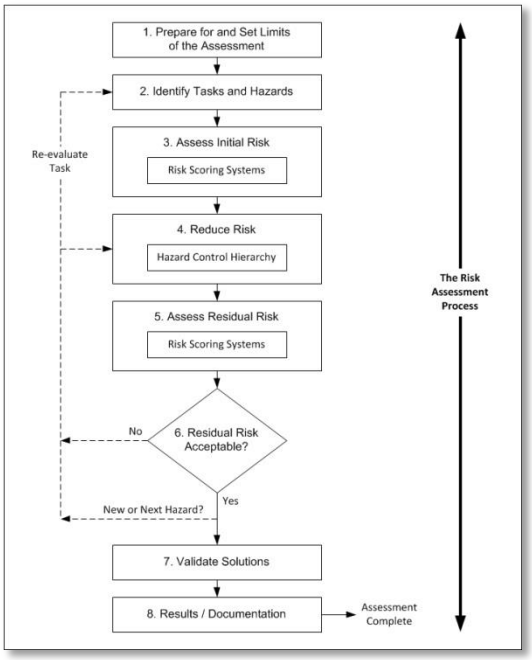

Figure 2: The Risk Assessment Process

Periodic Review (Assessment and Inspection)

As addressed in Part 2 of this series (*The Risk Assessment Process*), the process of ensuring safe equipment for use in the workplace is never ending; there are ongoing steps which continue throughout the lifecycle of the machine.

Necessity for Periodic Review

Following the initial commissioning of a machine prior to deployment, periodic inspections must be performed on equipment to ensure tolerable levels of residual risk are maintained. In all world regions, the machine user is in the best position to ensure that acceptable risk is maintained. In addition to implementing risk assessment as a continuous process, periodic reviews should occur that verify that protective measures (including safeguarding, complimentary protective measures, and administrative controls) are adequately maintained. Furthermore, the machinery supplier should inform the users of any need and methods to verify or re-verify the safety systems of the equipment.

A very useful and insightful document provided by the European Commission is the *Guidance on risk assessment at work*. This guide is intended primarily to help Member State of the European Economic Area (EEA) to fulfill the general obligations placed on employers by Article 6 of Directive 89/391/EEC on the introduction of measures to encourage improvements in the safety and health of workers at work (the OSH Framework Directive).

One of the valuable elements of this guide is an outline of the reasons why periodic review is required. Listed below are the reasons provided in the guide:

- The assessment might result in changes to the work process
- Precautionary measures introduced to reduce risk may affect the work process
- The assessment:
    - May no longer be applicable due to invalid data or information
    - Can be improved
    - Needs to be updated and revised
- The protective measures currently in place are insufficient or no longer adequate
- The result of the finding of an investigation of an accident or 'near miss'

Guidance in North America

In North America, the guidance for periodic and regular inspection is extremely subjective, as it is not clearly stipulated how often such inspection should occur. As an example, the A-type standard *ANSI B11.0-2010 – Safety of Machinery – General Requirements and Risk Assessment* provides the following guidance for operation and maintenance of industrial machinery in Clause 4.7:

> During the operation and maintenance of the machinery, the user shall ensure that the risk level is maintained at an acceptable level, as determined by the risk assessment and the appropriate machine-specific (C-level) standard.
>
> The user shall establish and follow a program of periodic and regular inspection and maintenance to ensure that all parts, auxiliary machinery, and safeguards are in a state of safe operating condition, adjustment and repair in accordance with the supplier information for operation and maintenance.

For more specific applications such as mechanical power presses, there is slightly more guidance, but it is still somewhat subjective. At the federal level, *OSHA 29 CFR 1910.217 – Mechanical power presses* stipulates requirements for general and direct inspections as follows:

> *1910.217(e)*
> Inspection, maintenance, and modification of presses -
>
> *1910.217(e)(1)*
> *Inspection and maintenance records*. The employer shall establish and follow an inspection program having a general component and a directed component.
>
> *1910.217(e)(1)(i)*
> Under the general component of the inspection program, the employer shall:
>
> *1910.217(e)(1)(i)(A)*
> Conduct periodic and regular inspections of each power press to ensure that all of its parts, auxiliary equipment, and safeguards, including the clutch/brake mechanism, antirepeat feature, and single-stroke mechanism, are in a safe operating condition and adjustment;
>
> *1910.217(e)(1)(i)(B)*
> Perform and complete necessary maintenance or repair, or both, before operating the press; and
>
> *1910.217(e)(1)(i)(C)*
> Maintain a certification record of each inspection, and each maintenance and repair task performed, under the general component of the inspection program that includes the date of the inspection,

maintenance, or repair work, the signature of the person who performed the inspection, maintenance, or repair work, and the serial number, or other identifier, of the power press inspected, maintained, and repaired.

1910.217(e)(1)(ii)
Under the directed component of the inspection program, the employer shall:

1910.217(e)(1)(ii)(A)
Inspect and test each press on a regular basis at least once a week to determine the condition of the clutch/brake mechanism, antirepeat feature, and single-stroke mechanism;

1910.217(e)(1)(ii)(B)
Perform and complete necessary maintenance or repair, or both, on the clutch/brake mechanism, antirepeat feature, and single-stroke mechanism before operating the press; and

1910.217(e)(1)(ii)(C)
Maintain a certification record of each maintenance task performed under the directed component of the inspection program that includes the date of the maintenance task, the signature of the person who performed the maintenance task, and the serial number, or other identifier, of the power press maintained.

Furthermore, the voluntary consensus standard *ANSI B11.1-2009 – Safety Requirements for Mechanical Power Presses* contains an entire clause (9.4 Inspection and maintenance) with program requirements. Clause 9.4 states in part:

Inspection and maintenance programs shall conform to the following requirements:

a) The user shall establish a systematic program of periodic and regular inspection of press production systems to ensure that all their parts, auxiliary equipment, and safeguarding are in safe operating condition and adjustment.

b) The user shall ensure that all scheduled inspections are performed.

c) Whenever an inspection uncovers a potentially hazardous condition, the user shall ensure that the press production system is removed from service and locked out until necessary adjustments or repairs have been scheduled and performed.

d) Inspection, testing, and maintenance shall be performed or supervised by an individual(s) that has the training or experience necessary to ensure that the inspection, testing, and maintenance is performed in a manner that results in the safe operation of the press.

The user shall document that press inspections are made as scheduled, and that any necessary follow-up repair work has been performed.

Additionally, ANSI B11.1 includes an informative annex (Annex K) with a sample press inspection report, checklist and maintenance record. This example includes recommendations for weekly, monthly, and semi-annual checks of various subsystems of a press, including pneumatic, electrical, lubrication and mechanical components.

Guidance in Europe

The general guidelines in Europe are not much clearer, as outlined in Article 5 of the Use of Work Equipment Directive (Directive 2009/104/EC – use of work equipment), stating:

Inspection of work equipment

1. The employer shall ensure that where the safety of work equipment depends on the installation conditions, it shall be subject to an initial inspection (after installation and before first being put into service) and an inspection after assembly at a new site or in a new location by competent persons within the meaning of national laws and/or practices, to ensure that the work equipment has been installed correctly and is operating properly.

2. In order to ensure that health and safety conditions are maintained and that deterioration liable to result in dangerous situations can be detected and remedied in good time, the employer shall ensure that work equipment exposed to conditions causing such deterioration is subject to:
    (a) periodic inspections and, where appropriate, testing by competent persons within the meaning of national laws and/or practices;
    (b) special inspections by competent persons within the meaning of national laws and/or practices each time that exceptional circumstances which are liable to jeopardise the safety of the work equipment have occurred, such as modification work, accidents, natural phenomena or prolonged periods of inactivity.

3. The results of inspections shall be recorded and kept at the disposal of the authorities concerned. They must be kept for a suitable period of time.

    When work equipment is used outside the undertaking it shall be accompanied by physical evidence that the last inspection has been carried out.

4. Member States shall determine the conditions under which such inspections are made.

While the time frame for 'periodic inspections' is again subjective, each Member State is required to comply with all directives of the European Parliament. Furthermore, each country is required to set forth specific guidelines, and they are given latitude to introduce requirements for protective measures that are more (but never less) stringent.

Some of the key legal requirements which apply to EEA Member States come from the Treaty on the Functioning of the European Union (the FEU Treaty), one of the two core functional treaties which lay out how the European Union (EU) operates. As shown in Figure 3, FEU Treaty Article 114 is intended to remove trade barriers within the EU (applying to equipment manufacturers) while Article 153 outlines consumer protection requirements (affecting machinery users).

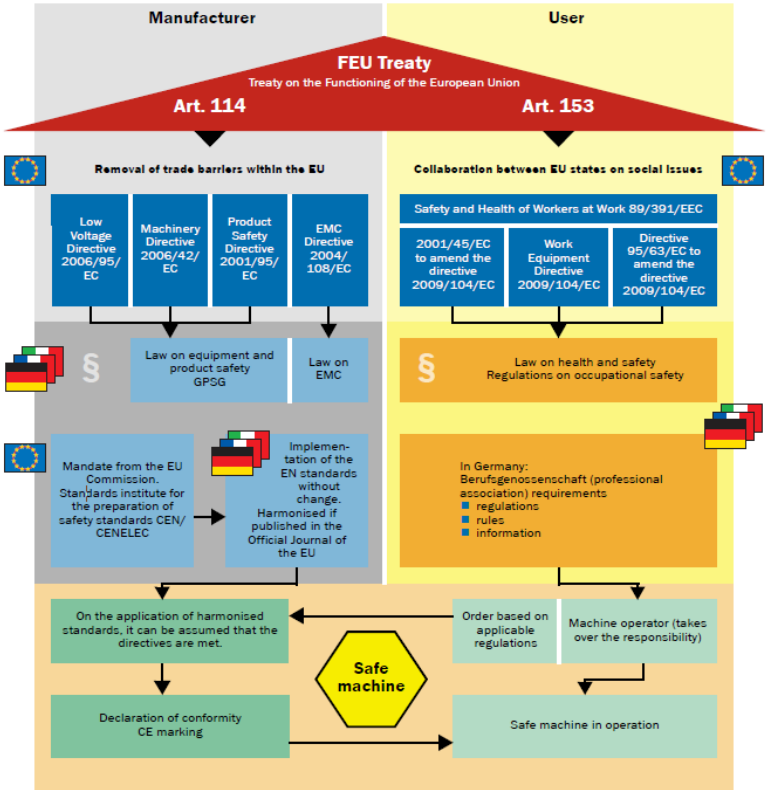

Figure 3: Key Aspects of the Treaty on the Functioning of the European Union (FEU Treaty)

As an example of how Member States implement their own specific requirements, the UK utilizes the Provision and Use of Work Equipment Regulations 1998 (PUWER). General requirements for inspection are provided in Part II, including:

6. Inspection

(1) Every employer shall ensure that, where the safety of work equipment depends on the installation conditions, it is inspected—
  (a) after installation and before being put into service for the first time; or
  (b) after assembly at a new site or in a new location,
  to ensure that it has been installed correctly and is safe to operate.

(2) Every employer shall ensure that work equipment exposed to conditions causing deterioration which is liable to result in dangerous situations is inspected—
  (a) at suitable intervals; and
  (b) each time that exceptional circumstances which are liable to jeopardise the safety of the work equipment have occurred,
  to ensure that health and safety conditions are maintained and that any deterioration can be detected and remedied in good time.

(3) Every employer shall ensure that the result of an inspection made under this regulation is recorded and kept until the next inspection under this regulation is recorded.

Again we see that there is not much specific guidance – until we arrive at Part IV for power presses. In this section of the PUWER requirements we find very specific guidelines for implementing the general requirements (above) to a historically hazardous classification of equipment. The clear requirements include:

32. Thorough examination of power presses, guards and protective devices

(4) For the purpose of ensuring that health and safety conditions are maintained, and that any deterioration can be detected and remedied in good time, every employer shall ensure that—
  (a) every power press is thoroughly examined, and its guards and protection devices are thoroughly examined when in position on that power press—
    (i) at least every 12 months, where it has fixed guards only; or
    (ii) at least every 6 months, in other cases; and
    (iii) each time that exceptional circumstances have occurred which are liable to jeopardise the safety of the power press or its guards or protection devices; and
  (b) any defect is remedied before the power press is used again.

33. Inspection of guards and protective devices

(2) Every employer shall ensure that a power press is not used after the expiration of the fourth hour of a working period unless its every guard and protection device has been inspected and tested while in position on the power press by a person appointed in writing by the employer who is—
  (a) competent; or
  (b) undergoing training for that purpose and acting under the immediate supervision of a competent person, and who has signed a certificate which complies with paragraph (3).

35. Keeping of Information

(1) Every employer shall ensure that the information in every report made pursuant to regulation 34(1) is kept available for inspection for 2 years after it is made.

(2) Every employer shall ensure that a certificate under regulation 33(1)(a)(ii) or (2)(b) is kept available for inspection—
  (a) at or near the power press to which it relates until superseded by a later certificate; and
  (b) after that, until 6 months have passed since it was signed.

Documentation

It is important for both the supplier and the end user to document the justification of the risk reduction measures selected by each. Details of any analyses that were undertaken and how stakeholder considerations were accounted for should be included in the documentation. Such record keeping is invaluable for monitoring progress of the overall risk management process, as well as for the defense of due diligence should something go wrong in the future.

Additionally, documentation is vital to keeping decision making about acceptable risk a rational process. Documentation aids in making acceptable risk decisions on similar machines and on future designs of the same machine type. Documentation provides a guideline and framework toward achieving risk reduction goals.

Content

The outcome of each risk assessment must be documented to demonstrate the procedure that has been followed, the hazards identified, and the protective measures applied to reduce risks to an acceptable level. Whether from the supplier or the user, the documentation should include the following, as applicable:

- The machinery for which the risk assessment has been made (for example, manufacturer, model, specifications, limits, intended use)
- Any relevant assumptions that have been made (for example, loads, strengths, safety [design] factors)
- The information on which risk assessment was based, including:
    - The data used and the sources (accident histories, experience gained from risk reduction applied to similar machinery, etc.)
    - The uncertainty associated with the data used and its impact on the risk assessment
- Names of the members of the risk assessment team
- Date(s) of the risk assessment
- The tasks, hazards and hazardous situations identified, as well as the hazardous events considered in the risk assessment
- Initial risks associated with the equipment
- The risk reduction measures implemented to eliminate identified hazards or to reduce risk, including the objectives to be achieved by each protective measure
    - NOTE: standards or other specifications used to select protective measures should be referenced
- Residual risks associated with the equipment
- The result of the risk assessment
- Any forms completed during the risk assessment
- The validation of risk reduction measures, including the responsible individual(s) and the date of validation
- The configuration report of the safety controller including a date and time stamp, if used
- Circuit validation documentation (i.e., SISTEMA or similar)

Furthermore, the information must be updated throughout the lifecycle of the equipment and a new risk assessment may be necessary as this information changes.

Supplier Guidelines

In most world regions (if not all), there are no regulations which “require” the supplier to deliver the risk assessment documentation together with the machine. In fact, many suppliers protect the information

contained in the risk assessment and consider the information to be a trade secret since much of the technical documentation is specific to the equipment and not public knowledge. However, more and more end users are requesting the risk assessment, while still others are mandating the information as part of the purchase agreement.

To prevent this discussion from becoming an intense negotiation between suppliers and their customers, suppliers must focus on providing the information outlined in the list above. Furthermore, the supplier documentation must also include recommendations for additional risk reduction measures to be implemented by the user, system integrator or other entities involved in machine utilization.

Retention of Documentation

At a minimum, the most recent risk assessment documentation must be retained for the life of the machine. While some organizations may have more stringent document retention policies, it is also considered best practice to maintain documentation prepared during earlier risk assessments of the same equipment. Preserving this information may prove to be beneficial in the long run if the equipment is ever reverted back to a previous state of use.

Guidelines in Europe

As part of Directive 2006/42/EC on machinery (more commonly referred to as the Machinery Directive), Annex VII outlines the required procedure for compiling a technical file as required for CE marking of completed or partly completed equipment. The technical file required by suppliers includes documentation of the risk assessment.

For end users, Directive 2009/104/EC – use of work equipment (the Use of Work Equipment Directive, above) applies. As shown in Article 5, section 3, documentation must always be producible as proof of the last inspection. This is again repeated in Article 6, section 3 of the PUWER (also above). Specific for press applications, Article 35 of the PUWER requires documentation to be maintained for 2 years following inspection, even when inspections are required every 6 or 12 months.

Requirements for Other High Risk Equipment

As we see above, there are sometimes specific requirements for specialized equipment such as presses. Unfortunately, such clear guidelines do not exist for other categories of industrial machinery. However, a case could be easily made that similar inspection and documentation guidelines could – and probably should – be applied to other (non-press) classifications of equipment with similar or higher levels of inherent risk as determined by a risk assessment.

Maintaining Tolerable Risk

As discussed in Part 3 of this series, determining when adequate risk reduction has been achieved is a subjective process. However, the process can be assisted by a rational review and assessment of the residual risk levels after protective measures have been applied. In order to ensure all protective measures are providing the expected level of risk reduction throughout the ongoing use of the equipment, each measure must be maintained as part of an effective change management process, as outlined in Part 2 of this series.

Conclusion

In order for all residual risks to be maintained at a level as low as reasonably practicable (ALARP), adequate commissioning and ongoing inspection is imperative, and these services must be performed at appropriate intervals by competent individuals. Furthermore, documentation of the pertinent information is vital to the overall safety program, as is retention of the appropriate documents. As necessary, any organization implementing or improving a comprehensive safety program should not hesitate to request assistance from outside resources to provide supplemental support in any of the areas where internal skills are not yet fully developed.

After discussion throughout all 5 parts of this series outlining the intricate aspects associated with machine safety, it is evident that implementing an effective machine safety program is not for the faint of heart. In Part 1, we reviewed the considerations associated with selecting and referencing applicable regulations and standards when implementing machine safeguarding requirements. Part 2 provided insight into the risk assessment process, as well as a review of the elements that comprise risk and some of the pitfalls which must be avoided. The logical and systematic methodology to reduce risk using a hierarchy of controls was detailed in Part 3. A high level discussion was then presented in Part 4 regarding safety functions and the functional safety requirements associated with those which interface to the machine control system. Lastly, this Part 5 of the series outlines the final measures necessary to confirm adequate risk has been achieved and maintained throughout the entire lifecycle of the equipment.

This white paper is meant as a guideline only and is accurate as of the time of publication. When implementing any safety measures, we recommend consulting with a safety professional.

For more information about validation and deployment concerns associated with maintaining acceptable levels of residual risk, contact SICK Safety Application Specialist Chris Soranno at chris.soranno@sick.com, or visit our web site at www.sickusa.com.