Basis for Machine Safeguarding Requirements

White Paper

KENEXIS

>> DISCLAIMER

CAUTION *— Kenexis white papers necessarily address problems of a general nature. Kenexis is not undertaking to meet the duties of employers, manufacturers, or suppliers to warn and properly train and equip their employees and others exposed concerning health and safety risks and precautions, nor undertaking their obligations under local, state, or federal laws. The use of this white paper may involve hazardous materials, operations, or equipment. The white paper cannot anticipate all possible applications or address all possible safety issues associated with use in hazardous conditions. The user of this white paper must exercise sound professional judgment concerning its use and applicability under the user's particular circumstances. The user must also consider the applicability of any governmental regulator limitations and established safety and health practices before implementing this technical report.*

Additionally, implementation of the technical report may require use of techniques, processes, or materials covered by patent rights. Kenexis will not be responsible for identifying any patents that may require a license before implementation of the white paper or for investigating the validity or scope of any patents brought to its attention. The user should carefully investigate relevant patents before using the technical report for the user's intended application.

This white paper is for informational purposes only. KENEXIS MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

While some information contained in this white paper appears legal in nature, Kenexis and its employees are not attorneys and do not purport to provide legal advice. All legal considerations for project work executed by readers of this white paper should be reviewed, as required, by licensed legal counsel retained by such readers.

>> INTRODUCTION

Industry has applied instrumentation and control devices for the purpose of safeguarding people, equipment, and business for almost as long as instrumentation and control has been used. In the "wet" process industries these devices and systems have been employed to detect out of control conditions in the process and take mitigative action to move the process to a safe state. In the "discrete" manufacturing industries instrumentation and controls have been used to prevent personnel from exposing themselves to sources of danger, such as hazardous motion, by either interlocking barriers to prevent access to the hazard while it is present or remove power from the hazard when personnel come into close proximity.

There is now a large number of guidance documents for the implementation of safety instrumentation and the determination of which documents apply to which application projects has become difficult.

As industry matured and instrumentation and control systems evolved and became more standardized, regulators and industry groups promulgated standard practices and regulation that define how these systems should be implemented. This web of regulations[1] and standards was built from the perspective end use, as opposed to the instrumentation and controls that are employed in the safety functionality. As a result, there is now a large number of guidance documents for the implementation of safety instrumentation and the determination of which documents apply to which application projects has become difficult. This situation is further exacerbated by the fact that much of the engineering for these protective instrumented systems is being performed by outside engineering contractors and systems integrators who do not have an end user's perspective on the equipment under control. In fact, these outside contractors often perform projects using a common set of equipment (for instance, a limit switch de-energizing a motor starter) where the basis, in standards, for the design varies from client to client and even from project to project for a single client.

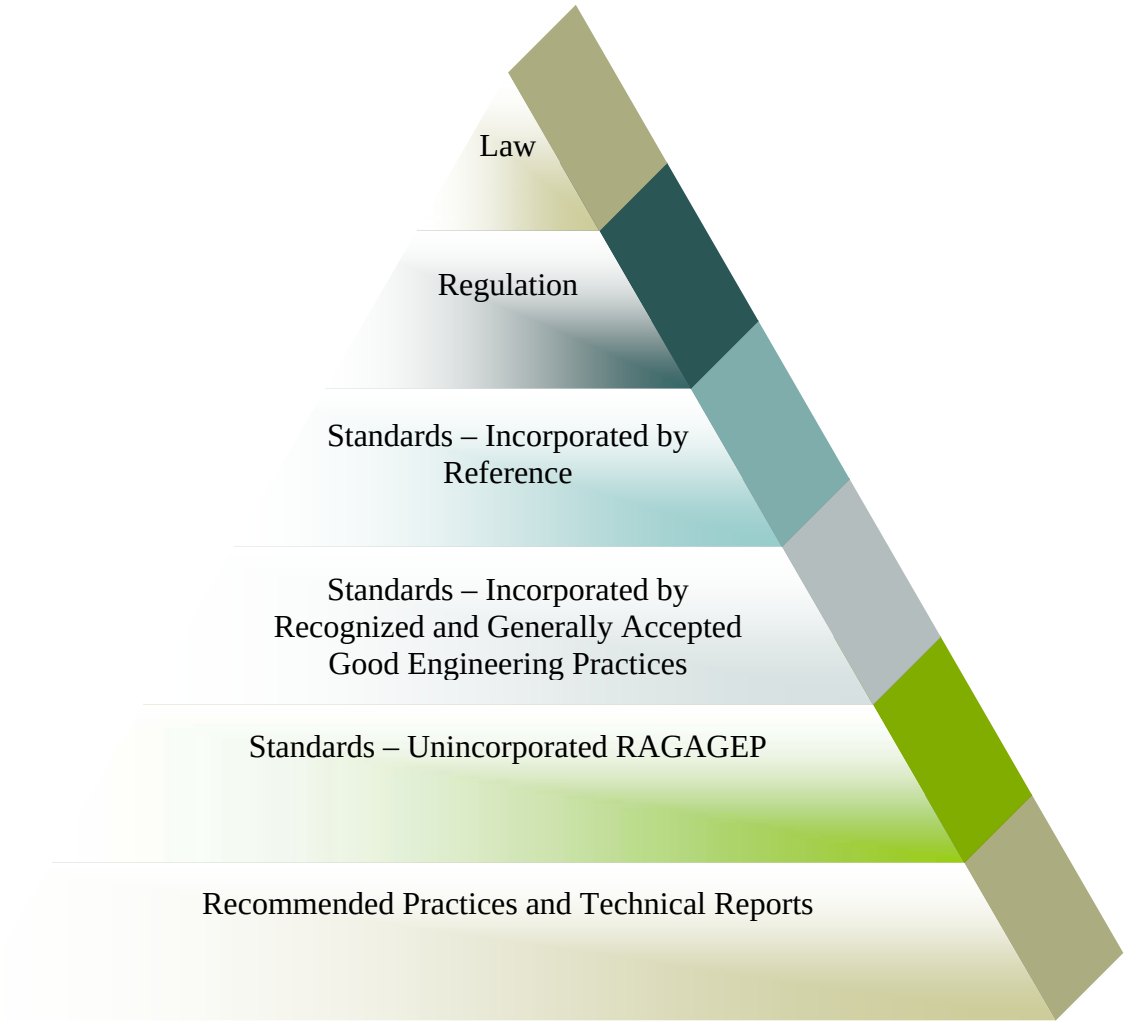
The purpose of this white paper is to assist end users, engineering contractors, and systems integration firms to determine which standards and regulations apply to the systems they are designing. The paper does this by providing an overview of the standards and regulations that apply to safety instrumentation and a process for determining which of those will apply to a specific project by analyzing the nature of the equipment under control (EUC) and the level of risk reduction that is required of the instrumented systems that are being proposed for protection.

[1] This white paper focuses on regulations and standards that are applicable in the United States of America. While the general concepts contained in this paper may be valid on a global basis, the specific laws, regulations, and standards that should be implemented as a result of the analysis of systems contained in this white paper will vary from country to country.

2.0 Standards and Regulations for Safety Instrumentation

Industry is driven to implement systems that safeguard their people, equipment and business for reasons that are financial, moral, and legal. The financial aspects can be considered utilizing cost-benefit analysis calculations and the moral aspects are a function and the culture of the companies and employees implementing the designs. The regulatory framework, on the other hand, is common to all companies, and is the focus of this white paper.

Figure 1 – Hierarchy of Rules and Guidance (U.S.)



In the United States, rules that govern the details of how business and commerce is transacted are based on a hierarchy of priority. At the highest level of the priority is legislation – or laws. Legislation is the set of rules that are enacted by elected representatives in the legislative branch of government and enforced by the executive branch of government. This legislation can be written and enforced at the federal, state, or local level.

The need to comply with legislation is well understood and respected due to the immediate and potentially severe nature of not doing so, and the degree of enforcement of these rules. In the US, at the federal level, all legislation can be found in the United States Code (USC).

The next level down in the hierarchy is regulation. Regulations are more detailed rules that are developed by government agencies that specialize in a certain industry or discipline. Regulatory agencies and the rules that they create are created by legislative acts, and carry the full weight of law. For instance, the regulatory agency of most importance to the implementation of protective instrumentation is the Occupational Safety and Health Administration (OSHA). OSHA was created through an act of federal legislation called the Occupation Safety and Health Act of 1970 (29 USC 661). Legislators can further direct regulatory agencies to take specific actions through new legislation. For instance, in 1900 OSHA was directed to create new rules to prevent the accidental release of highly hazardous chemicals resulting in the Process Safety Management regulation of 1992 (29 CFR 1910.119). This new set of rules was required by the Clean Air Act Amendments Legislation.

Regulations are contained in the Code of Federal Regulations (CFR). These rules essentially have the weight of law because the legislators who created the regulatory agencies also gave them the power to not only write rules but also enforce them (and levy punishments including fines and imprisonment). While regulations do not have the same level of immediacy that legislation does, their importance and the need to comply is well understood. Furthermore, enforcement actions stemming from inspections and audits by regulatory agencies have increased awareness and improved compliance.

The "requirement" to use standards is not as direct as the "requirement" to follow laws and regulations, but it is still present.

Standards are guidance documents that are prepared by industry groups. These documents describe the details of the implementation of equipment and design procedures for a specific area of interest. For instance, the Instrumentation, Systems, and Automation Society publishes standards for the implementation of safety instrumented systems in the Process Industries, and the American Society of Mechanical Engineers (ASME) publishes standards for the implementation of boilers, pressure vessels, and piping systems. The "requirement" to use standards is not as direct as the "requirement" to follow laws and regulations, but it is still present.

Standards have different degrees of enforceability depending on what position regulators and legislators take regarding their adoption. Some standards are "incorporated by reference" into either legislation or regulation. One common example of "incorporation by reference" is state adoption of the ASME boiler and pressure vessel codes. Some states (referred to as Code States) have written laws the mandate that the boiler and pressure vessel code be followed. In essence, this statement turns the standard into law. The previous example was based on incorporation through legislation, but incorporation through regulation is also sometimes done.

Even if standards are not incorporated by reference, their use may still be required through legislative and regulatory incorporation of recognized and generally accepted good engineering practices (RAGAGEP). In situations where regulators do not desire to write specific rules and elect to allow

industry to provide solutions through the consensus-based standards process, they often "require" that RAGAGEP be used as the basis for the regulated activity. This is a particularly common approach when there are competing industry standards, many of which are applicable or when the scope of the regulation and the large number of applicable standards makes incorporation by reference impractical. When legislation or a regulation incorporates RAGAGEP as a basis for the regulated activity, it is the responsibility of the end user to determine which standards are applicable to the systems that they are working with. In the eyes of the regulators, most industry consensus-based standards are considered RAGAGEP. If an industry consensus-based standard is available for the performance of a regulated activity and an end-user elects not to employ that standard, then it will be incumbent upon them to – in the case of an audit or other legal proceeding – to demonstrate that their approach meets the intention of the regulation or legislation, and may also be required to demonstrate how their alternative approach is 'as good or better' than the industry standard. In essence, if an industry standard is available for a regulated activity it should be implemented unless the user has another superior approach. Simply ignoring the standard is not a reasonable option.

The lowest level of the hierarchy is the recommended practice and technical report. Where a standard is developed by an industry group using the consensus process and represents the lowest level of conformance that should be implemented by a reasonable practitioner, a best practice or technical report often represents an optimum method that is not absolutely required. In some cases, best practices and technical reports are issued without following the rigorous consensus process, and thus may not represent a comprehensive cross-section of the issuing body's membership.

3.0 Legislation and Regulation for Protective Instrumentation

Design, implementation, operation, maintenance, and testing of protective instrumented systems – particularly those that are critical to personnel safety – are regulated activities. The regulations governing these activities are primarily issued by OSHA. The specific regulations of concern are a function of the equipment under control (EUC) and not necessarily a function of the instrumentation that is used. As mentioned previously, an identical set of instruments can be employed on two processes, and be governed by completely different rules depending on the nature of the EUC. The two major delineations for protective instrumentation regulations are machine EUC and process EUC.

The specific regulations pertaining the protective instrumentation are shown below.

EUC	Regulator	Citation	Description
Machines – Machine Tools (Discrete Manufacturing)	OSHA	29 CFR 1910.211-219	Machinery and Machine Guarding
Process Industries ("wet" processes)	OSHA	29 CFR 1910.119	Process Safety Management (PSM)

While it is fairly clear from the descriptions of the regulations which set of rules will apply to a particular process, there are a large number of facilities where the distinction is not so clear, and multiple regulations may be applicable for an equipment item. Some examples of typical areas of confusion include the following.

- What regulation is applicable to safeguarding of extruded polymer cutting devices in a polypropylene production facility? While most of the plant is a "wet" process and covered by the OSHA PSM rule, the portion of the plant that handles finished product and cuts polymer strands into small pellets is more appropriately considered a "machine tool".

- What regulation is applicable to the manual shutdown of pump? Is a pump shutdown an emergency stop that should be designed in accordance with NFPA 79 (implying relevance of CFR 1910.211-219)? Or process shutdown as per ISA 84.00.01-2004 (implying relevance of CFR 1910.119)? Or not safety critical? The design basis for a pump manual shutoff will vary depending on the intention of the shutoff and the intention of the pump, and may be required to meet multiple standards.

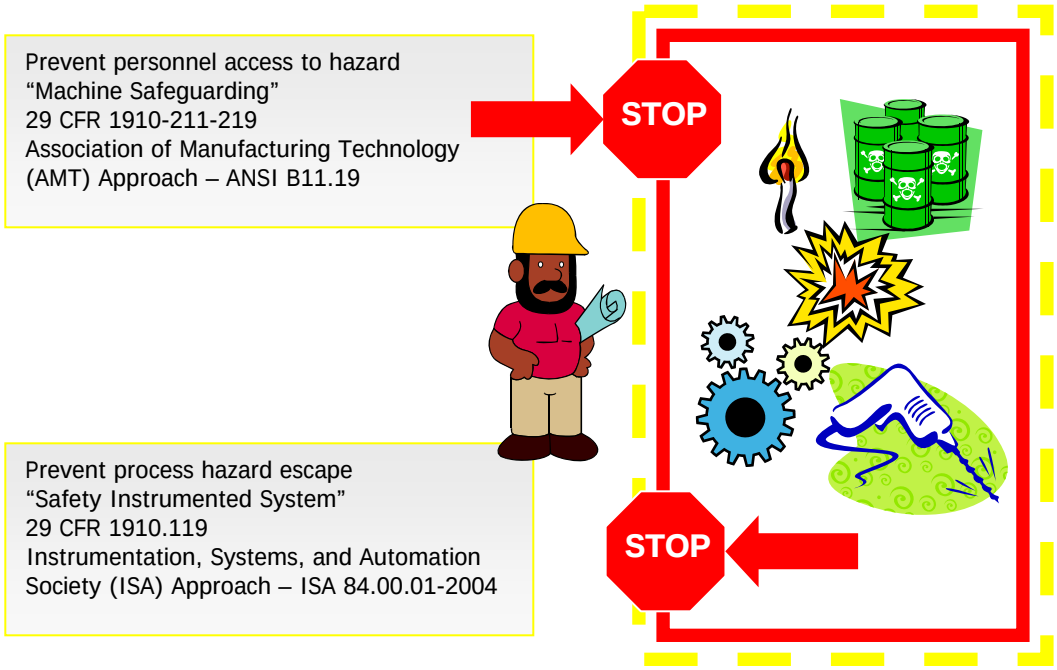
The process for determining which standard will be applicable begins with a definition of the EUC and an assessment of the hazard that is intended to be prevented by an instrumented protective function. The determination of whether a machine safeguarding approach (as developed by the Association for Manufacturing Technology (AMT) industry group) or the safety instrumented system approach (as developed by the Instrumentation, Systems, and Automation Society (ISA) industry group) is the appropriate one is performed by considering the nature of the hazard and the mechanism by which a person can be exposed to that hazard, as demonstrated in *Figure 2*.

For each protective instrumented function the intention of the standard must be considered. Generally, there are two intentions for protective instrumented systems. If one considers an industrial process, it may contain hazards – such as high pressures, high temperatures, toxic materials, pinch points, and hazardous motion. These hazards are separated from the personnel that are operating the industrial process with a hazard/personnel barrier, which might be piping that contains a process fluid or a fence the separates personnel from hazardous motion.

Protective instrumented functions whose intention is to prevent breech of the hazard/personnel barrier by preventing the personnel from crossing

the barrier until a safe condition exists are considered "machine safeguarding" and are typically designed in accordance with CFR 1910.211-219 regulations and the AMT standards approach[2]. Protective instrumented functions whose intention is to prevent breech of the hazard/personnel barrier by uncontrolled conditions in the process (e.g., high pressures causing pipe rupture and release of process material to the atmosphere) are considered "safety instrumented systems" that are typically designed in accordance with CFR 1910.119 regulations and the ISA standards approach.

Figure 2 – Protective Instrumentation Intention and Design Basis



Once the intention of the protective instrumented function is defined, the standards that should be used as a design basis will follow as a direct result. Furthermore, the requirement to follow standards is also clear for both paths. For the regulated activity of machine safeguarding, the regulations (29 CFR 1910.212 – General Requirements for all Machines – a. Machine Guarding, 3. Point of operation guarding) clearly state that use of standards is required, and thus is incorporated by reference.

> *ii. The point of operation of machines, whose operation exposes an employee to injury, shall be guarded.* ***The guarding device shall be in conformity with any appropriate standards*** *therefore and in the absence of applicable specific standards , shall be so designed*

[2] The standards that are referenced in this paper for machine safeguarding are the U.S. standards on this subject. There are other equivalent European standards, most prominently EN-954. While the European standards are not directly applicable they are of interest to US practitioners because many equipment vendors have their equipment certified to the European standards, and thus application to equipment in the US will require cross-correlation of the requirements between the two approaches.

and constructed as to prevent the operator from having any part of his body in the danger zone during the operating cycle.

The case is similar in process applications. The applicable regulation [29 CFR 1910.119 (d)(3)(ii)] clearly incorporates applicable standards, by referring to RAGAGEP, in several places, including the section shown below.

The employer shall document that equipment [specifically including safety systems, e.g., interlocks, detection, or suppression systems (d)(3)(i)(H)] complies with recognized and generally accepted good engineering practices.

4.0 Standards for Protective Instrumentation

Depending specifically on the regulation that has 'jurisdiction' for the application under design, and generally on the intention of the protective instrumented function – as shown in *Figure 2* – the standards that should be employed and that are considered RAGAGEP will change. There are two sets of standards that will need to be considered when using either approach. The first set is the application specific standards and the second set is the instrumentation and control specific standards.

The application specific standards describe the requirements for a specific process or machine. For instance, if you are designing a boiler, you would want to base your design on National Fire Protection Association (NFPA) standard 85, or if designing a mechanical power press, you would want to base your design on ANSI B11.1. These application specific standards provide guidance specifically on what protective instrumentation should be implemented (or at least considered). A list of application specific standards is presented in *Table 1* for the process industries and in *Table 2* for the machine industries. The lists are only a selection of the most common standards. It would not be possible to list every available standard due to the large amount and continually evolving nature of these standards.

Table 1 – Application Standards – Process Industries - Selected

Standard Number	Title
NFPA 85	Boiler and Combustion Systems Hazards Code
NFPA 86	Standard for Ovens and Furnaces
API 14C	Recommended Practice for Analysis, Design, Installation, and Testing for Basic Surface Safety Systems for Offshore Production Platforms
API 556	Instrumentation and Control Systems for Fired Heaters and Steam Generators

API 616	Gas Turbines for Petroleum, Chemical, and Gas Industry Services
API 617	Axial and Centrifugal Compressors and Expander-Compressors for Petroleum, Chemical and Gas Industry Services
API 618	Reciprocating Compressors for Petroleum, Chemical, and Gas Industry Services
API 619	Rotary-Type Positive Displacement Compressors for Petroleum, Petrochemical and Natural Gas Industries

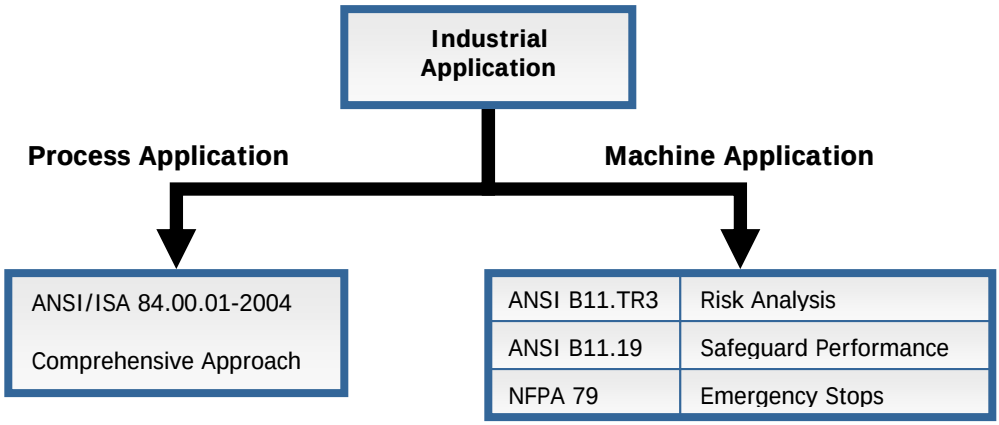
Table 2 – Application Standards – Machine Industries – Selected

Standard Number	Title
ANSI B11.1	Mechanical Power Presses
ANSI B11.2	Hydraulic Power Presses
ANSI B11.3	Power Press Brakes
ANSI B11.4	Shears
ANSI B11.5	Iron Workers
ANSI B11.6	Lathes
ANSI B11.7	Cold Headers and Cold Formers
ANSI B11.8	Drilling, Milling, and Boring Machines
ANSI B11.9	Grinding Machines
ANSI B11.10	Metal Sawing Machines
ANSI B11.11	Gear Cutting Machines
ANSI B11.12	Roll Forming and Roll Bending Machines
ANSI B11.13	Single- and Multiple-Spindle Automatic Screw/Bar and Chucking Machines
ANSI B11.14	Coil Slitting Machines/Equipment
ANSI B11.15	Pipe, Tube, and Shape Bending Machines
ANSI B11.17	Horizontal Hydraulic Extrusion Presses
ANSI B11.18	Machinery and Machine Systems for the Processing of Coiled Strip, Sheet, and Plate
ANSI B11.19	Machine Tools, Safeguarding
ANSI B11.20	Manufacturing Systems/Cells
ANSI B15.1	Power Transmission Apparatus
ANSI B19.1	Air Compressor Systems
ANSI B19.3	Compressors for Process Industries
ANSI B20.1	Conveyors and Related Equipment
ANSI B24.1	Forging Machinery
ANSI B28.6	Rubber Machinery, Hose
ANSI B28.7	Rubber Machinery, Hose
ANSI B28.8	Rubber Machinery, Hose
ANSI B28.9	Rubber Machinery, Hose
ANSI B28.10	Rubber Machinery, Endless Belt
ANSI B30.16	Overhead Hoists
ANSI B151.1	Plastics Injection Molding Machinery, Horizontal
ANSI B151.2	Plastics Machinery, Film Casting
ANSI B151.3	Plastics Machinery, Screen Changers
ANSI B151.4	Plastics Machinery, Blown Film Takeoff &Auxiliary Equipment
ANSI B151.5	Plastics Machinery, Film & Sheet Winding
ANSI B151.6	Plastics Machinery, Slit Tape & Monofilament Post extrusion Equipment
ANSI B151.7	Plastics & Rubber Extrusion Machinery
ANSI B151.11	Plastics Machinery, Granulators, Pelletizers, & Dicers

ANSI B151.15	Plastics Machinery, Extrusion Blow Molding
ANSI B151.21-1986	Plastics Machinery, Injection Blow Molding
ANSI B151.25	Plastics Machinery, Injection Molding
ANSI B152.2	Permanent-Mold Casting Machines (Other than Gray Iron)
ANSI B153.1	Automotive Lifts
ANSI B155.1	Packaging Machinery
ANSI B169.1	Envelope Manufacturing Machinery
ANSI B176	Copper-Alloy Diecasting
ANSI B177.2	Printing Ink Vertical Post Mixers
ANSI/RIA R15.06	Industrial Robots and Robot Systems
ANSI Z8.1	Commercial Laundry & Dry-Cleaning Equipment
ANSI Z241.1	Foundry, Sand Prep., Molding, & Core-Making
ANSI Z241.2	Foundry, Melting & Pouring of Metals
ANSI Z241.3	Foundry, Cleaning & Finishing of Castings
ANSI Z245.1	Refuse Collecting & Compacting Equipment
ANSI Z245.3	Stability of Refuse Bins
ANSI Z245.5	Bailing Equipment
ANSI Z268.1	Metal Scrap Processing Equipment

Instrumentation and control specific standards set general requirements for all the equipment that is used to perform the automatic protective actions, and apply regardless of the specific. These standards are a function of the safeguarding approach that is used, i.e., either the AMT machine safeguarding approach or the ISA safety instrumented system approach. *Figure 3* demonstrates the standards related to each scenario.

Figure 3 – Protective Instrumentation Standards



For process industry applications, the foundation of design is the ISA 84.00.01 standard (ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod) Functional Safety: Safety Instrumented Systems for the Process Industries Sector – Part 1: Framework, Definitions, System, Hardware, and Software Requirements). This standard provides a comprehensive basis for all facets of the design lifecycle from risk analysis, through design, all the way to implementation and functional testing.

For machine industry applications, a group of standards – when combined – forms a complete basis for machine safeguard design. These standards are as follows:

- ANSI B11.TR3-2000 Risk Assessment and Risk Reduction – A Guide to Estimate, Evaluate and Reduce Risks Associated with Machine Tools
- ANSI B11.19-2003 Performance Criteria for Safeguarding
- NFPA 79 – 2002 Electrical Standard for Industrial Machinery

The B11.TR3 standard is the starting point for assessing machine guarding functions. This standard provides a framework for performing risk assessments that identify where machine safeguards are required and then to assign a target level of performance to those safeguards. The B11.19 standard provides performance criteria for machine safeguards including both instrumented and non-instrumented means. The NFPA 79 standard provides specific guidance on a number of electrical issues related to machines, including key requirements regarding emergency stop switches including where they are necessary and how they should be designed, maintained, installed, and tested.

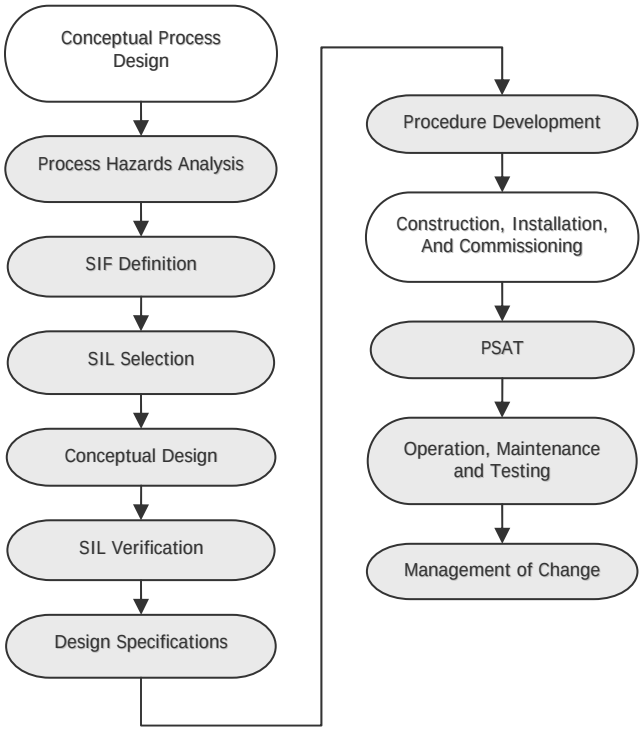
5.0 What the Standards Require

Both the ISA 84 standard for process industry applications and the ANSI B11 series of standards for machine applications provide a design lifecycle or series of steps, which if completed properly, will yield a functionally safe system. While the two approaches differ in terms of the type of performance target that is set and how the various levels of safety are achieved, they have a similar lifecycle. In general, the lifecycle includes the following tasks.

- Identification of the required protective functions
- Risk analysis to establish performance targets
- Design in accordance with the performance targets
- Verification that the performance targets have been achieved.

Figure 4 presents the lifecycle that is applicable to process industry applications.

Figure 4 – Process Industry Applications Lifecycle



The ISA 84 standard begins by requiring that a process hazards analysis of the process EUC by performed in order to identify hazards that require safeguarding through instrumented means. These functions are defined in terms of inputs, outputs and logic, and the assigned a target for performance. In the ISA 84 paradigm, the performance target is the Safety Integrity Level (SIL). SIL is a category that is primarily defined by the average probability of failure on demand of the function under consideration. The SIL levels and their corresponding ranges of failure on demand are shown in the following table.

Table 3 – Safety Integrity Levels

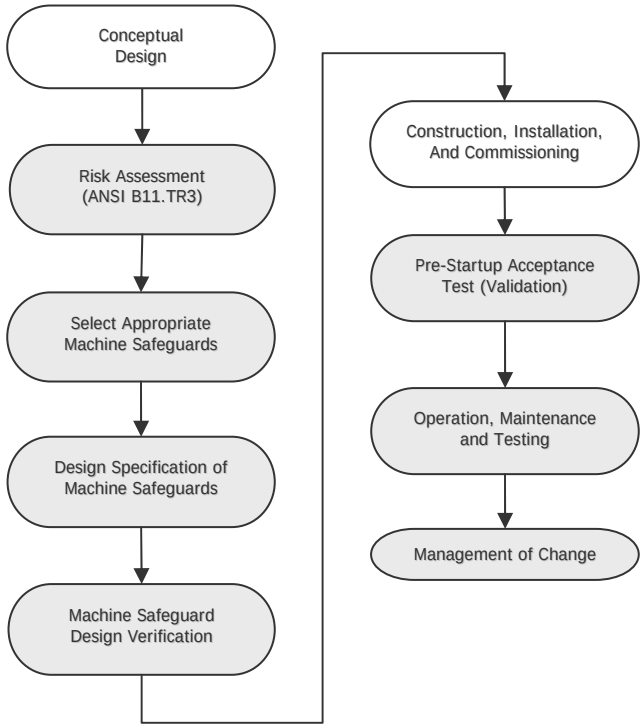
SIL	Average Probability of Failure on Demand
4	10^{-4} to 10^{-5}
3	10^{-3} to 10^{-4}
2	10^{-2} to 10^{-3}
1	10^{-1} to 10^{-2}

Based on the risk analysis a SIL is chosen that is sufficiently high to provide an amount of risk reduction that is required to meet the risk tolerance of the end user. Once the SIL target is chosen, the function is designed. The design required to meet the SIL is a function of the equipment selected, the level of diagnostics, the voting architecture and the testing philosophy. All of these components combined determine the average probability of failure on demand. After the design is complete a

verification step is performed. The verification step confirms that the target SIL level is achieved, through the use of quantitative reliability engineering calculations.

Figure 5 presents the lifecycle that is appropriate to machine industry applications.

Figure 5 – Machine Industry Applications Lifecycle



Machine safeguard design should also begin with an analysis of the hazards presented by the EUC. This analysis should be done in conformance with ANSI B11.TR3 and OSHA guidance for hazard assessments. Risk analysis is a two step process.

1. Identify the hazards the are presented by the application

2. Assess the level of risk presented by the hazards in order to set an appropriate performance target for the safeguards that are employed.

Identification of hazards can be done utilizing one of two common approaches; machine hazard assessment or job safety analysis (JSA). Machine hazard assessment involves an experienced analyst visually inspecting a machine and its appurtenances for the purpose of identifying points-of-operation and motion hazards that should be safeguarded. JSA is a structured brainstorming exercise performed by a team of persons familiar with the machine, including operations, maintenance, engineering, and safety – along with an experienced facilitator. The JSA reviews all tasks that are associated with the machine and makes recommendations

for additional safeguarding measures if the risk is high. JSA is an OSHA recommended process that is much more comprehensive as it can identify hazards of a more general nature and will produce recommendations and findings that are more comprehensive than machine hazard assessment due to the way that the study is conducted.

The results of these studies eventually lead to a list of safeguards that are recommended for implementation. The next step in the process is to perform an assessment of the magnitude of the risk that those hazards present. This risk assessment considers several factors typically including: severity of harm, probability of occurrence of harm, and exposure to a hazard. The result of the risk analysis is that for every protective instrumented function that has been recommended, a performance target is selected that will determine the level of integrity that the safeguard will provide and sets certain criteria for how the design will be implemented. An example of risk analysis criteria from ANSI B11.TR3 is shown in *Table 4.*

Table 4 – Risk Assessment Criteria (based on ANSI B11.TR3)

Probability of Occurrence of Harm	**Severity of Harm**			
	Catastrophic	**Serious**	**Moderate**	**Minor**
Very Likely	High	High	High	Medium
Likely	High	High	Medium	Low
Unlikely	Medium	Medium	Low	Negligible
Remote	Low	Low	Negligible	Negligible

Risk Estimate	**Safeguard Circuit Performance**
High	Control Reliable
Medium	Single Channel with Monitoring
Low	Single Channel
Negligible	Simple

Unlike process industry applications, risk assessment may not be required or even desired for all functions. The need for risk assessment is determined by the applicable EUC specific standard. Some standards allow the risk assessment approach, some do not and stipulate safeguard circuit performance regardless of the level of risk, and some standards do not address the issue. For instance, ANSI/RIA 15.06 for robots states that either a risk assessment shall be performed to determine circuit performance targets, or if an assessment is not performed all circuits shall be Control Reliable. The ANSI B11.1 standard for mechanical power presses, on the other hand does, not recognize risk assessment and requires that all safeguards comply with requirements that essentially make them Control Reliable. The key lesson for setting performance targets for machine safeguarding circuits is that the application specific standard will dictate whether or not risk assessment is allowed to de-rate low risk functions to designs less stringent than control-reliable. If the application specific standard does not address the required level of circuit performance, then defaulting to the more general guidance in B11.TR3

would imply that the risk assessment approach is appropriate. Looking at it another way, it is clear that all circuits shall be designed as control reliable unless a risk assessment has been performed and indicates that a less stringent design is acceptable – unless the application specific standard precludes this approach.

In the AMT machine safeguarding paradigm, the performance targets are categories. These categories are listed in *Table 5*.

Table 5 – Machine Safeguard Categories[3] (AMT Approach)

Category	Requirements
Control Reliable	Control reliable safety circuitry shall be designed, constructed, and applied such that any single component failure shall not prevent the stopping action of the robot. These circuits shall be hardware based or comply with [rules for safe programmable systems], and include automatic monitoring at the system level. a) The monitoring shall generate a stop signal if a fault is detected. A warning shall be provided if a hazard remains after cessation of motion; b) Following a detection of a fault, a safe state shall be maintained until the fault is cleared. c) Common mode failures shall be taken into account when the probability of such a failure occurring is significant. d) The single fault should be detected at time of failure. If not practicable, the failure shall be detected at the next demand upon the safety function.
Single Channel with Monitoring	Single channel with monitoring safety circuits shall include the requirements for single channel, shall be safety rated, and shall be checked (preferably automatically) at suitable intervals. a) The check of the safety functions shall be performed 1) At machine start-up, and 2) Periodically during operation; b) The check shall either 1) Allow operation if not faults have been detected, or 2) Generate a stop signal if a fault is detected. A warning shall be provided if a hazard remains after cessation of motion; c) The check itself shall not cause hazardous motion d) Following detection of a fault, a safe state shall be maintained until the fault is cleared.
Single Channel	Single channel safety circuits shall be hardware based or comply with [rules for safe programmable systems], include components which should be safety rated, be used in compliance with manufacturers' recommendations and proven circuit designs (e.g., a single channel electro-mechanical positive break device which signals a stop in a de-energized state.)
Simple	Simple safety circuits shall be designed and constructed using accepted single channel circuitry, and may be programmable.

After the performance target is selected the design is accomplished in accordance with the requirements of the target. The final design of each

[3] The category definitions that are presented in Table 4 are based on information in the ANSI/RIA 15.06 Standard – American National Standard for Industrial Robots and Robot Systems – Safety Requirements.

safeguard is then verified against the requirements its category, through a combination of review and testing.

In the machine safeguarding paradigm, emergency stop circuits are also a consideration. As completely described in NFPA 79, all machines (specifically machine tools) are required to be fitted with emergency stop switch(es) in appropriate quantity and location. The purpose of an emergency stop is to allow any personnel that may become entangled in a machine to manually stop its operation to prevent or minimize any harm that they may sustain due to such entanglement. Emergency stop switches for such purposes shall be designed in accordance with NFPA 79 and other stop switches related to wet process shutdowns or non safety critical stopping need not be.

6.0 Procedure for Selecting Design Basis Standards

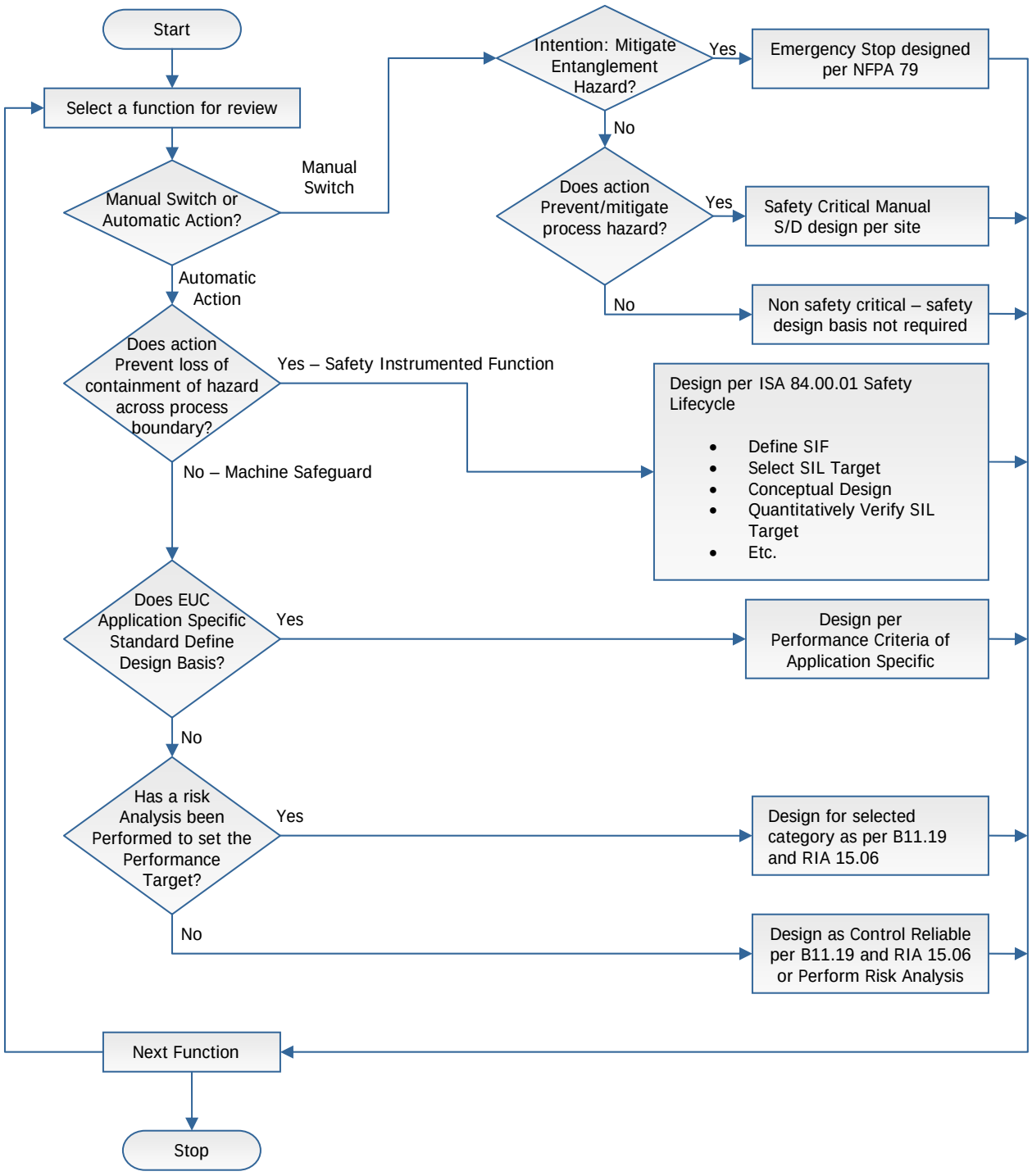
The following procedure provides guidance on how to analyze a proposed instrumented protective function (including manual shutdowns) to determine how its design basis should be developed in terms of which standards are applicable and what and how its performance criteria should be developed. *Figure 6* provides a flow chart overview of the process.

The process begins with a list of protective instrumented functions that are to be reviewed in order to determine what their safety design basis will be. Even before reaching this point a decision will have to be made for every control function to determine whether it is a basic process control function or a protective function. A good rule of thumb for making this determination is as follows:

> A Basic Process Control or Indication Function is a function that provides routine indication and action (typically modulating) that keeps the process parameters inside their normal operating limits. Basic Process Control functions can include discrete on-off actions that are performed on a regular basis (whether automatic or manual) where widely variable process conditions cause continuous throttling control to be impractical (e.g., storm sump).
>
> A Protective Function is a function that is used when the process is out of its normal operating range due to failure of normal controls (automatic, manual, mechanical, etc.) or an abnormal condition, causing a non-routine action (typically on-off and not modulating) that is not the primary means of keeping the process in the normal operating range. The action may be automatic or require manual intervention and typically moves the process to a predetermined state that is different than the normal operating condition.

The design basis selection flowchart is performed once for each protective function on the list for review.

Figure 6 – Safety Instrumentation Design Basis Standard Determination



The function is analyzed to determine whether it is an automatic action, or is the result of a manually operated switch. If a protective function is a manually operated switch, it may be an emergency stop (as elaborated in NFPA 79). The determination of whether or not a stop is an NFPA 79 Emergency Stop is a function of its intention. NFPA 79 addresses machine tools, and the associated hazards of entanglement in the point of operation or motion hazards of that machine. If the purpose of the stop is to address some other hazard, then it is not an NFPA 79 Emergency Stop. Consider a pump that is on the outlet of a vessel pump liquefied petroleum gas. Furthermore, assume that the pump has a completely enclosed drive and coupling system that is not accessible during normal operation. It is very common that this pump might be fitted with a shutdown switch. In this case, the intention of the switch is not to address entanglement hazards (as there are none) but to allow stopping of the pump from a remote location in the situation where there is a fire at the pump, and a remote stop will aid in firefighting. While this pump has a safety critical shut off switch, it is not an NFPA 79 Emergency Stop. For safety critical shutoff switches that are not NFPA 79 Emergency Stops, the design basis will usually be set by individual company practices, as there is no “process industry” standard for safety related shutoff circuit design.

If a protective function is automatic, the hazard that is being prevented is then considered. If the hazard the is being prevented is a loss of process control resulting in loss of containment and breech of the hazard / personnel barrier caused by conditions in the process, then the protective function is a safety instrumented function. Safety instrumented functions should be designed in accordance with the ISA 84.00.01 safety lifecycle. If the intention of the protective function is to prevent a person from crossing the hazard / personnel barrier and entangling himself in a point of operation, motion , or other hazard, then the function is a Machine Safeguard and should be designed in accordance with the appropriate AMT standards.

The appropriate AMT standards and final design target selection will be a function of the EUC. First, the appropriate application specific standard should be identified (see Table 2 for an overview of some of these standards). If an application specific standard is available for the EUC, it should be reviewed to determine if that standard stipulates the performance targets and/or design basis for any protective functions that are required to be employed.

If either there is no application specific standard or the application specific standard does not provide instrumented protective function performance targets or design criteria, then the user should revert to the risk analysis approach as demonstrated in ANSI B11.TR3 and ANSI/RIA 15.06. Using this approach the user has two options. If a risk analysis is performed and demonstrates that the risk is suitably low, then the performance criteria for the safeguard under consideration can be set at the level that is appropriate for the risk. If a risk analysis is not performed, all safeguards should be designed in accordance with the strictest performance target, which is Control Reliable.

7.0 CONCLUSION

Developing a design for protective functions is a complex process that is regulated by government agencies.

Industry has employed instrumentation and control systems in a protective capacity for almost as long as instrumentation and control systems have been used. Developing a design for protective functions is a complex process that is regulated by government agencies. Ensuring that protective functions are being designed properly requires a thoughtful analysis of the Equipment Under Control (EUC), legislation and regulations affecting the EUC, consensus standards written to address the legislation and regulations, and the intention of the functions that are being designed. The data, figures, and information presented in this white paper will serve as a useful tool and starting point in the analysis of instrumented protective functions, for the purpose of defining the appropriate design basis and performance targets for these systems.

8.0 REFERENCES

Association for Manufacturing Technology, ANSI B11.19 – American National Standard for Machine Tools – Performance Criteria for Safeguarding, McLean, VA, 2003

Association for Manufacturing Technology, ANSI B11.TR3 – Risk Assessment and Risk Reduction – A Guide to Estimate, Evaluate and Reduce Risk Associated with Machine Tools, McLean, VA, 2000

Marszal, Edward and Scharpf, Eric, *Safety Integrity Level Selection with Layer of Protection Analysis*, Instrumentation Systems and Automation Society, Research Triangle Park, NC, 2002.

National Fire Protection Agency, NFPA 79: Electrical Standard for Industrial Machinery, Quincy, MA, 2002.

Occupational Safety and Health Administration (OSHA), Process Safety Management, 29 CFR 1910.119, 1992

Occupational Safety and Health Administration (OSHA), Machinery and Machine Guarding, 29 CFR 1910.212-219

Robotic Industries Association, ANSI/RIA 15.06 – American National Standard for Industrial Robots and Robot Systems – Safety Requirements, Ann Arbor, MI, 1999.

Instrumentation, Systems, and Automation Society, ISA 84.00.01 (IEC 61511 Modified) – Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Software Requirements, Research Triangle Park, NC, 2004

About the Authors

Edward M. Marszal, PE, CFSE
President, Kenexis
edward.marszal@kenexis.com
2929 Kenny Road, Suite 225
Columbus, OH 43221
+1 (614) 451-7031

Mr. Marszal has over ten years of experience in safety instrumented systems design and risk analysis. Mr. Marszal is President of Kenexis and responsible for engineering consulting activities related to the implementation of engineered safeguards for process industry plants, such as safety instrumented systems, alarm systems, fire and gas systems, burner management systems, and relief and vent systems. In his current position, he has experience in the analysis and implementation of SIS and other engineered safeguard projects for a variety of process plants in diverse world-wide locations and industries. Mr. Marszal received a B.S.Ch.E. from The Ohio State University in 1992 with emphasis on control systems and expert systems. Mr. Marszal is the Director of the ISA Safety Division and the author of the award winning "Safety Integrity Level Selection" textbook from ISA. Mr. Marszal has developed and teaches many courses on process safety management and safety instrumented system design and analysis. Hel peer reviews papers for ISA Technical Conferences and ISA Transactions. Mr. Marszal is active in ISA at the local and national levels, as a senior member, and is an active participant in the ISA 84, 91, and 18 committees, all dedicated to utilizing instrumentation to safeguard process plants. He is also a senior member of AIChE and a member of NFPA. He is a registered professional engineer in Ohio and Illinois and also a TÜV certified functional safety expert.