

# Decoding Machine Safety

## Understanding Ranking Protocols

By Chris Soranno

**W**hen OSH personnel and controls engineers collaborate with suppliers to implement protective measures for industrial equipment, the discussion can quickly get off track, as various terminologies and jargon are used, often with little to no true understanding of what the terms actually mean. Often, the only way to decipher these code words has been to track down the appropriate standard for context. This article is a

primer for those looking for a single reference source to understand this seemingly confusing lexicon.

As is the case in many specific fields of study, one must first be familiar with the basic expressions that are often used to speak intelligently about a given topic, and industrial safety is no different. In the safety marketplace, safety standards are heavily relied on to present basic concepts and specific definitions to establish common ground. Many of the nomenclatures used in these standards rely on seemingly simple ranking systems; however, because many of the classifica-

tions utilize alphabetical or numerical designators (Figure 1), confusion is common.

### IN BRIEF

- Many of the nomenclatures used in industry standards for machines rely on seemingly simple ranking systems; however, because many of the classifications utilize alphabetical or numerical designators, confusion is common.
- As is the case in many specific fields of study, one must first be familiar with the basic expressions that are often used in order to speak intelligently about a given topic.
- This article is a primer for those looking for a single reference source to understand this seemingly confusing lexicon.

### Stratification of Safety Standards

Most safety standards aim to provide the audience (readers) with an overall framework and guidance for decisions during the entire life cycle of machinery to enable them to maintain machines that are safe for their intended use. Many standards-developing organizations use the following structure (Figure 2):

- Type-A standards (basic safety standards) contain basic concepts, principles for design and general aspects that can be applied to machinery.

- Type-B standards (generic safety standards) deal with one safety aspect or one type of safeguard that can be used across a wide range of machinery:

- a) Type-B1 standards cover particular safety aspects (e.g., safety distances, surface temperature, noise);

- b) Type-B2 standards cover a safeguarding device (e.g., two-hand controls, interlocking devices, pressure-sensitive devices, guards).

- Type-C standards (machine safety standards) contain detailed safety requirements for a particular machine or group of machines.

This stratification was first developed by ISO/IEC Guide 51 and was implemented in Europe during the development of European Norms (EN) standards; these documents were then elevated to international (ISO or IEC) standards, and the interrelationships as laid out were maintained. Many organizations follow ISO/IEC Guide 51, which was updated in April 2014. As a practical application of this structure in use in North America, the ANSI B11 (2010) series of standards for machine tools has implemented a similar organization (Figure 3, p. 30).

### Stop Functions

When designing and implementing circuits to initiate a stop, one must consider the three classifications of stop functions:

- Stop category 0: Stopping by immediate removal of power to the machine actuators (i.e., an uncontrolled stop).

- Stop category 1: A controlled stop with power available to the machine actuators to achieve the

**Chris Soranno** is a safety application specialist with SICK Inc. He has more than 15 years' experience in the industrial safeguarding field. During his career, his responsibilities have included delivering training, performing safeguarding assessments, designing machine safety system solutions, implementing risk reduction methodologies, and contributing to the development of domestic and international safety standards. Soranno is a member of ASSE's Northern Ohio Chapter and he holds a degree in engineering physics from Miami University. He is cochair of the ANSI B11.3 subcommittee addressing press brake safety. He is also a voting delegate for several accredited standards committees, including ANSI B11 (machine tools), RIA (robotics) and ASSE (control of hazardous energy).

**Figure 1**

## Ranking Protocols Used Within the Safety Industry

Performance Levels (PL) ISO 13849-1	a	b	c	d	e		
Standards (Type) ISO/IEC & ANSI B11	A	B	C				
Circuit Categories (Cat) EN 954-1		B	1	2	3	4	
Safety Integrity Levels (SIL) IEC 61508			1	2	3	4	
Safety Integrity Levels (SIL) IEC 62061			1	2	3		
Stops (Category) IEC 60204-1		0	1	2			
ESPE Devices (Type) IEC 61496				2	3	4	
Interlocking Devices (Type) ISO 14119			1	2	3	4	
Two-Hand Controls (Type) ISO 13851			I	II	IIIA	IIIB	IIIC

**Note.** This image is not intended to imply any equivalency across standards or rating systems.

Many industrial safety standards for machinery rely on seemingly simple ranking systems; however, because many of the classifications utilize alphabetical or numerical designators, confusion is common.

stop, then removal of power when the stop is achieved.

- Stop category 2: A controlled stop with power left available to the machine actuators.

These definitions are harmonized in both international (IEC 60204-1, 2005) and domestic (NFPA 79, 2015) standards, and they form the basis for functional requirements when discussing different types of stop circuits. Understanding this terminology helps describe how equipment motion is controlled in a concise manner (Table 1, p. 30).

As a general primer to the typical types of stop circuits, ANSI B11.19 (2010) provides a clear differentiation between the common purposes for stop circuits:

- Normal stop. Stopping of a machine, initiated by the control system, at the completion of a cycle.

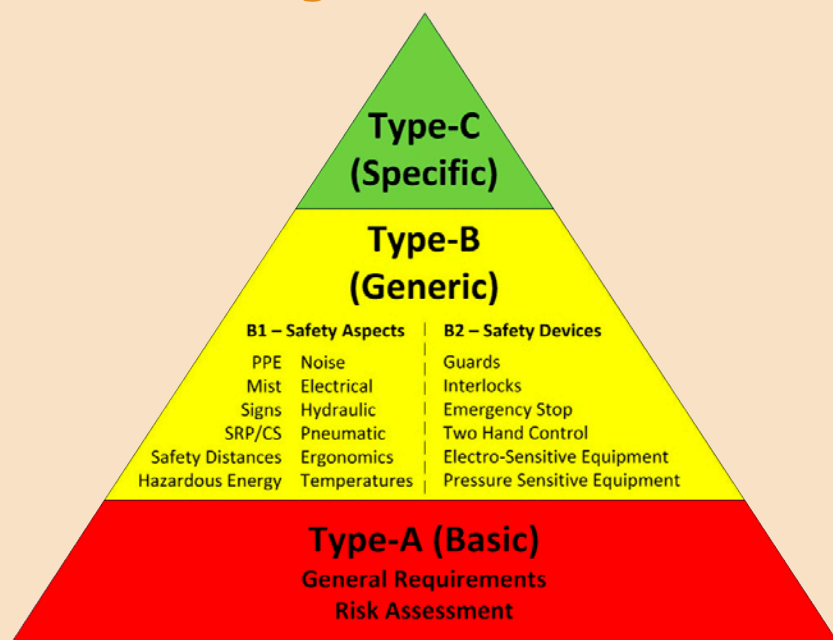
- Emergency stop. Stopping of a machine, manually initiated, for emergency purposes [requirements for emergency stop functions are clearly addressed in NFPA 79, ANSI B11.19, IEC 60204-1 and ISO 13850 (2006)].

- Protective stop. Stopping of a machine initiated by protective devices for safeguarding purposes (referred to in some earlier standards as safety stop).

safety-related parts of the control system (SRP/CS). These functional aspects can be separate or integrated parts of the control system, consist of both hardware and software, and are intended to provide the safety functions of control systems. Safety functions define how risks are reduced by engineering

**Figure 2**

## Structural Organization of Standards



### Circuit Performance & Reliability Requirements

Certain parts of machinery control systems are frequently assigned safety functions; these parts are referred to as the

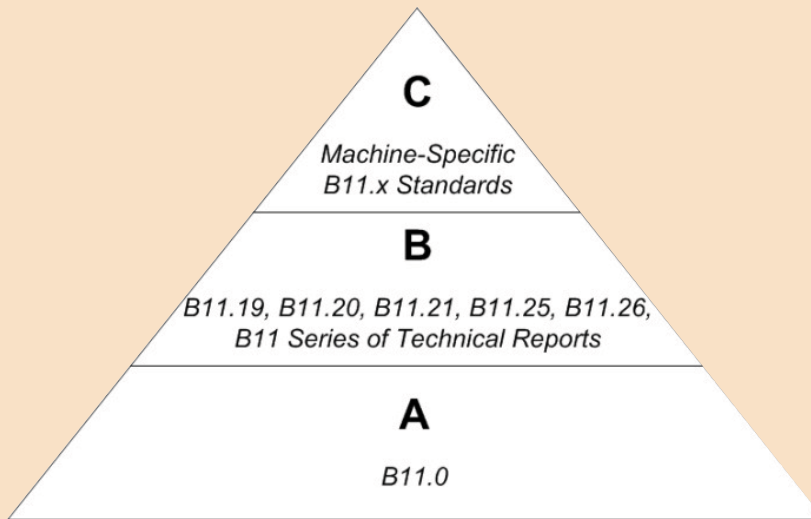
controls, and must be defined for each hazard that has not been eliminated through design measures. At its core, a safety function is any element of the protective system whose failure leads to an immediate increase of risk.

To accurately design, implement and validate safety functions to achieve the required level of risk reduction, it is necessary to provide a precise

description of each safety function. The type and number of components required for the function are derived from the definition of the safety function. Many different safety functions are possible, and some applications may require more than one function to adequately reduce risk. Likewise, it is possible for a single protective measure (safeguarding component) to play a part in more than one safety function simultaneously. [See more on this topic in Soranno (2014).]

**Figure 3**

## ANSI B11 Organization of Standards



### Circuit Architecture:

#### Categories B, 1, 2, 3 & 4

The first predominant standard developed and used in Europe to functionally describe circuit design requirements was EN 954-1 (1996). This document classified five categories (B, 1, 2, 3, 4) of design architecture for SRP/CS with respect to the occurrence of faults. The categories can be applied to:

- control systems of all kinds of machinery, from simple (e.g., small kitchen appliances) to complex manufacturing installations (e.g., packaging machinery, printing machines, presses);
- control systems of protective equipment (e.g., two-hand control devices, interlocking devices, electro-sensitive protective devices, pressure-sensitive protective devices).

According to EN 954-1, the design of SRP/CS and the selection of appropriate

**Table 1**

## Comparison of Stop, Emergency Stop & Protective Stop Requirements

	Stop	Emergency stop	Protective (safety) stop
<b>Location</b>	Personnel have quick, unobstructed access. Stop category 0 required on every machine (other categories may be used as determined by a risk assessment). Required on all operator stations.	Personnel have quick, unobstructed access. Required on all operator stations and other locations as determined by a risk assessment.	Located such that an individual cannot access the hazard. Determined by the safety distance formula.
<b>Initiation of stop signal</b>	Manual or automatic	Manual only	Manual or automatic
<b>Stop category (see above)</b>	0, 1 or 2	0 or 1 only	0, 1, or 2
<b>Circuit performance</b>	As determined by a documented risk assessment		
	Typically single channel (non-safety-rated)	Minimum single channel safety rated controls. Greater performance may be required when interfaced with a safeguarding device(s).	Typically control reliable
<b>Circuit reset</b>	Manual only	Manual only	Manual or automatic (hardware or software)
<b>Bypass and mute</b>	Allowed (e.g., for cycle completion)	Not allowed	Allowed (e.g., for muting, modes of operation, setup)
<b>Use frequency</b>	Variable; frequent (every cycle) to infrequent	Infrequently; only in emergency	Variable; frequent (every cycle) to infrequent
<b>Effect</b>	De-energize the relevant circuit and override related start functions	Remove all energy sources to hazards and override all other functions and operations in all modes	Remove or control energy sources to the safeguarded hazard and override all other functions and operations in all modes associated with the safeguarded hazard
<b>Final removal of power</b>	Electromechanical or solid-state components	Electromechanical components or solid state output devices (drives) designed for safety related functions	Electromechanical or solid-state components

categories was based on a methodology of evaluating risk factors (Figure 4). Table 2 presents a summary of the categories presented in EN 954-1. These definitions provided a clear basis on which the design and performance of any SRP/CS could be assessed. This document was subsequently elevated to the status of an international standard (ISO 13849-1, 1999) with essentially no changes to the requirements.

At this point, we are only beginning to scratch the surface of the confusion that can be introduced when a common word like *category* is misapplied or used out of context. When used in reference to a safety circuit, a statement such as “designed as a category 2 circuit” will have a different meaning if the context is not provided. The recipient may be thinking that the system has been designed with category 2 system architecture (per EN 954-1), while the intent was simply to say that the hazards are controlled without fully removing power to the machine actuators (per IEC 60204-1).

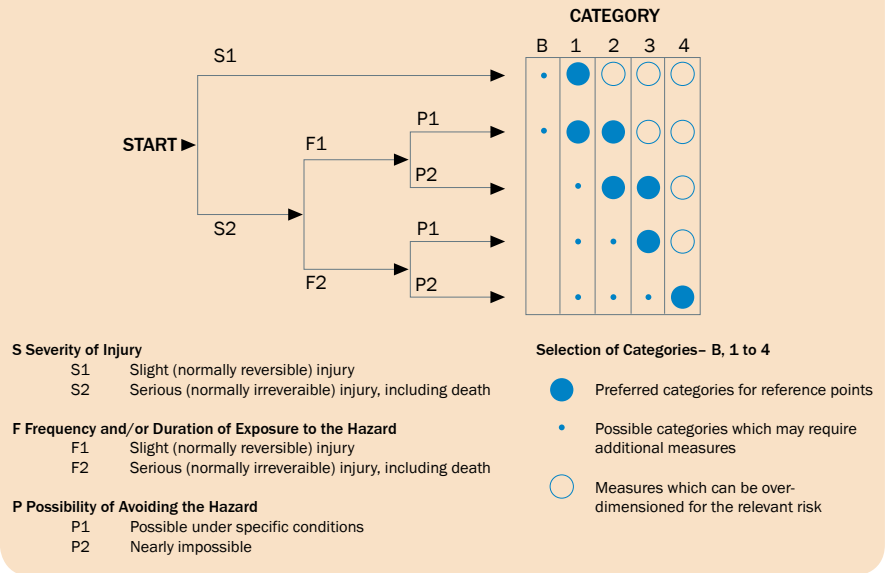
#### Performance Levels: PL a, b, c, d & e

Building on the guidance initially provided by EN 954-1 and ISO 13849-1 in 1999, the concept of safety

performance was explored on an even deeper level with the release of a revised ISO 13849-1 document in 2006. While the architecture of the circuit design has a direct effect on the overall performance of an SRP/CS, it was subsequently acknowledged that other factors play an equally important role. The updated (and still current) ISO 13849-1 was revised to

**Figure 4**

## EN 954-1 Selection of Categories for SRP/CS



**Table 2**

## Categories of Safety-Related Parts of Control Systems (SRP/CS)

Category	Brief summary of requirements	System behavior	Principles for achieving safety
B	The safety-related parts of control systems and/or their protective devices, as well as their components, must be designed, built, selected, assembled and combined in compliance with applicable standards so that they are able to tolerate anticipated influencing factors.	•The occurrence of a fault can result in the loss of the safety function.	Primarily characterized by component selection
1	The requirements of category B shall be met. Proven components and proven safety principles shall be used.	•The occurrence of a fault can result in the loss of the safety function, but the probability of occurrence is lower than in category B.	
2	The requirements of category B shall be met and proven safety principles used. The safety function must be checked by the machine controller at appropriate intervals (test rate 100 times higher than requirement rate).	•The occurrence of a fault can result in the loss of the safety function between checks. •The loss of the safety function is detected by the check.	Predominantly characterized by the structure
3	The requirements of category B shall be met and proven safety principles used. Safety-related parts shall be designed such that: •A single fault in any of these parts will not lead to the loss of the safety function. •Wherever it is reasonably possible, the single fault is detected.	•When the single fault occurs, the safety function is always retained. •Some, but not all faults are detected. •Accumulation of undetected faults may lead to loss of the safety function.	
4	The requirements of category B shall be met and proven safety principles used. Safety-related parts shall be designed such that: •A single fault in any of these parts will not lead to the loss of the safety function. •The single fault is detected on or before the next request for the safety function. If this is not possible, an accumulation of faults will not lead to the loss of the safety function.	•The safety function is always retained when faults occur. •The faults are detected in a timely manner to prevent the loss of the safety function.	

Figure 5

## Risk Graph for Determining Required Performance Level (PL<sub>r</sub>) for Safety Functions

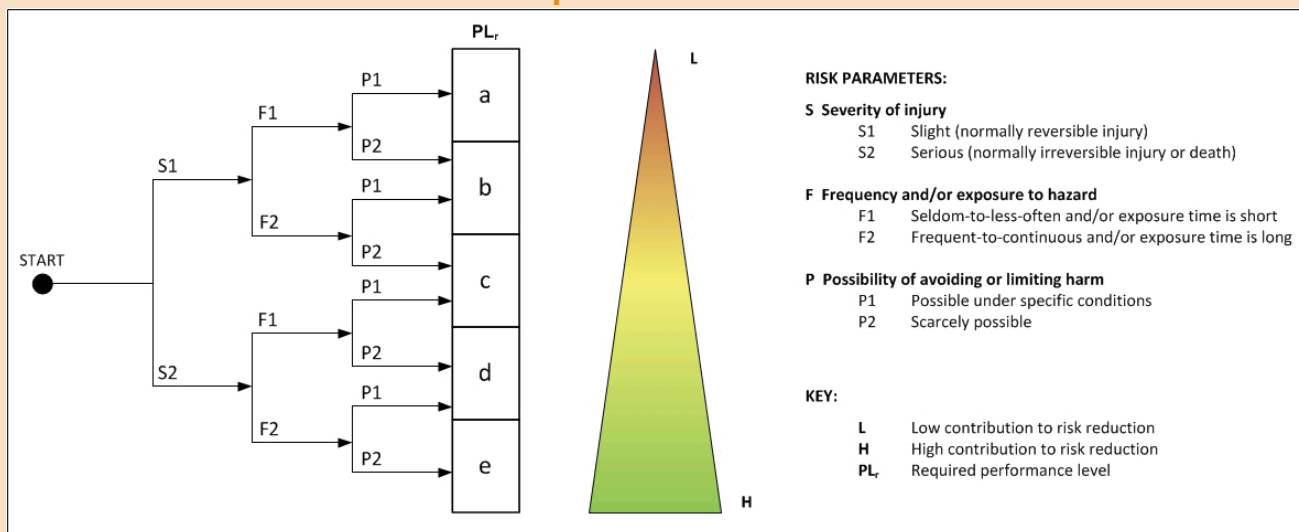
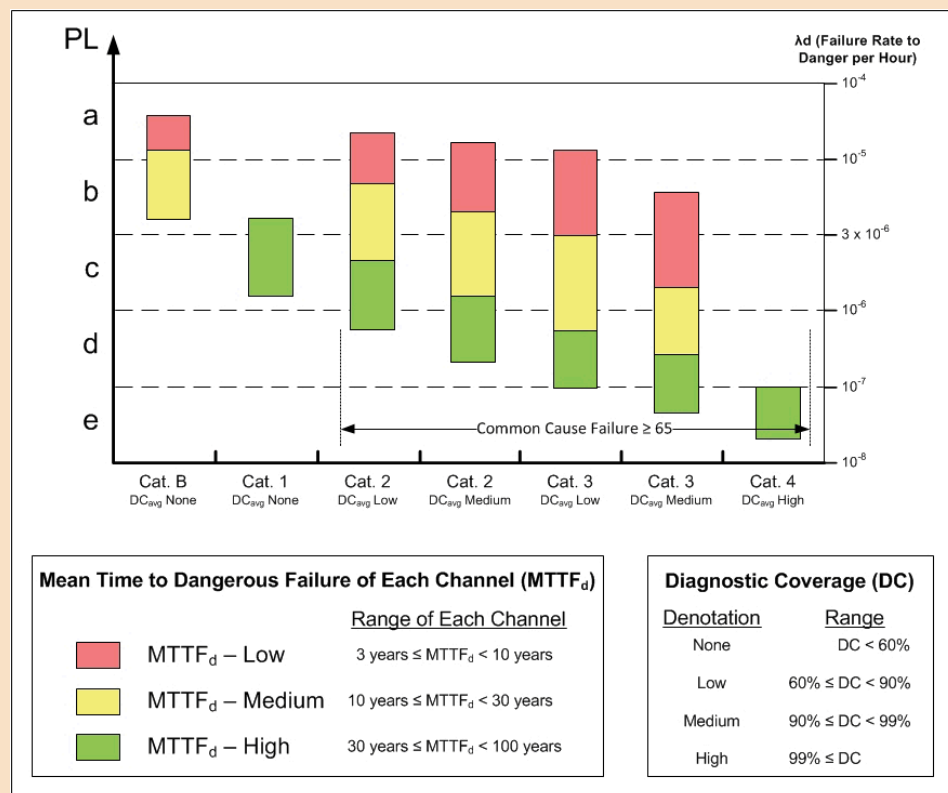


Figure 6

## Determination of the Performance Level (PL) of a Subsystem



focus on a higher order concept of control system performance and integrity, known as performance levels (PLs).

Contrary to what some believe, the defined categories first established in EN 954-1 did not get replaced or supplanted by PLs. Instead, the PL recognizes that additional factors must be accounted for to determine a circuit's overall performance. These factors are:

1) Structure and behavior of the safety function under fault conditions (category). This is the same circuit architecture concerns addressed previously in EN 954-1, utilizing the same category ratings (B, 1, 2, 3, 4).

2) Reliability of individual components defined by mean time to a dangerous failure (MTTF<sub>d</sub>) value. This value represents a theoretical parameter expressing the probability of a dangerous failure of a component (not the entire subsystem) within the service life of that component.

3) Diagnostic coverage (DC). The safety level can be increased if fault detection is implemented in the subsystem. DC is a measure of capability to detect dangerous faults.

4) Common cause failure (CCF). External influencing fac-



tors (e.g., voltage level, overtemperature) can render identical components unusable regardless of how rarely they fail or how well they are tested. These CCFs must always be prevented.

5) Process. The process for the correct implementation of safety-relevant topics is a management task and includes appropriate quality management, including thorough testing and counter checking, as well as version and change history documentation.

As was the case in EN 954-1, the required performance level ( $PL_r$ ) of the SRP/CS must be based on an evaluation of the inherent risk associated with the hazard (Figure 5). Based on the risk assessment, the  $PL_r$  determined can be achieved through combinations of circuit architecture (utilizing categories), DC and reliability of components (based on  $MTTF_d$ ), as long as CCF and the overall process are accounted for. Figure 6 presents this concept visually.

In North America, ANSI B11.26 (201x) is being developed to address this topic. This standard builds on the PL concepts and provides detailed explanation and examples of categories applied to real-world scenarios. It is intended to improve the understanding of electrical, pneumatic and hydraulic control circuits used in safety-related functions.

#### **Safety Integrity Levels: SIL 1, 2, 3 & 4**

A similar approach to determining system performance and reliability uses safety integrity levels (SILs). The SIL concept is similar to the PL approach in that it looks at many aspects of system design rather than simply concentrating on the architecture implemented to combine individual components. When safety systems are comprised of electrical, electronic and/or programmable electronic elements to perform safety functions, the applicable international standard is IEC 61508-1 (2010). This standard presents a rational and consistent technical development protocol for all electrically based safety-related systems. The essential objective is to ensure that control elements with safety-related functions will perform to a degree of reliability equivalent to the level of risk for the application. Table 3 identifies the average probability of a dangerous failure ( $PFD_{avg}$ ) that is required to achieve each specified SIL, depending on the level of demand placed on the elements.

Another standard that utilizes the SIL is IEC 62061 (2005). As a result of automation and the associated demand for increased production and reduced operator physical effort, this standard was developed to address safety-related electrical control systems of machines. Since these systems play an increasing role in the achievement of overall machine safety, they also increasingly employ

**Table 3**

### **IEC 61508 Safety Integrity Levels: Target Failure Measures for a Safety Function**

Safety integrity level (SIL)	Average probability of a dangerous failure on demand of the safety function ( $PFD_{avg}$ )	
	High demand or continuous operation	Low demand
4	$\geq 10^{-9}$ to $< 10^{-8}$	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-8}$ to $< 10^{-7}$	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-7}$ to $< 10^{-6}$	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-6}$ to $< 10^{-5}$	$\geq 10^{-2}$ to $< 10^{-1}$

**Table 4**

### **IEC 62061 Safety Integrity Levels: Target Failure Values for Safety-Related Control Functions**

Safety integrity level (SIL)	Probability of a dangerous failure per hour ( $PFH_D$ )
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

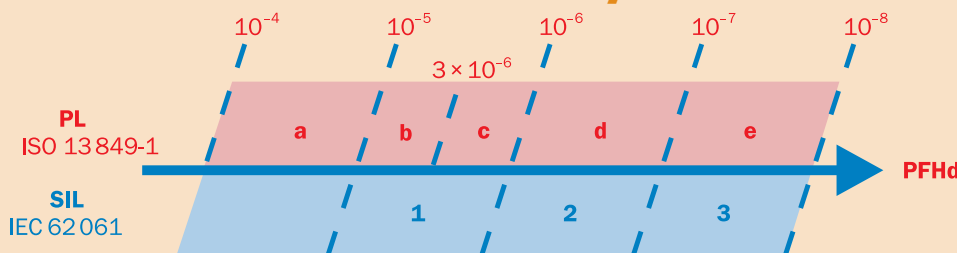
complex electronic technology. Prior to the development of such standards, many were reluctant to accept safety-related electrical control systems in safety-related functions for significant machine hazards because of uncertainty regarding the performance of such technology.

In conjunction with IEC 61508, IEC 62061 was developed specifically for the machine sector and is intended to facilitate the performance specifications of the safety-related electrical control systems in relation to the significant hazards of machines. IEC 62061 also relates the performance reliability of safety-related control functions to the probability of a dangerous failure per hour ( $PFH_D$ ). As shown in Table 4, the performance requirements of SILs 1-3 are identical to the IEC 61508 expectation for systems used in continuous operation or with high mode of demand. However, SIL 4 is not considered in IEC 62061 because it is not relevant to the risk reduction requirements normally associated with machinery, but rather those risks associated with

In general, design engineers apply the SIL process to applications with complicated electrical and electronic control systems, while the PL process is more common in the industrial machine market.

**Figure 7**

## Scale of Functional Safety Levels



It is important to note a key difference between most North American and international standards. Few application standards in North America require ESPEs to be certified by a third-party testing organization to any of the types defined earlier, whereas most EN and ISO Type-C standards set

the process industry (e.g., chemical, oil, gas).

In relation to industrial machine safety, the two primary methodologies to determine the likelihood of a dangerous failure are PLs in accordance with ISO 13849-1 and SILs as addressed in IEC 62061. In general, design engineers apply the SIL process to applications with complicated electrical and electronic control systems, such as in process industries, while the PL process is more common in the industrial machine market, which utilizes both electronic and electromechanical components. Figure 7 illustrates the similarities of these methodologies in terms of probability to a dangerous condition.

### Subsystem (Product) Ratings

Additional standards exist to create classifications or tiers of specific product types. These Type-B2 standards are known as “product family standards” and may be used as a normative reference in a dedicated Type-C standard for machinery safety. As noted in the following sections, the non-descript terminology *type* can also easily be misapplied, further hindering the comprehension of the typical layperson.

### Electrosensitive Protective Equipment: Types 2, 3 & 4

One of the most recognized, yet still misunderstood, product classification systems applies to electrosensitive protective equipment (ESPE) or electro-optical devices. The primary standard for this equipment is IEC 61496-1 (2012); it defines both common and specific requirements for the different component technologies that comprise ESPEs.

This IEC standard also defines the specific performance requirements necessary to achieve a type qualification. Interestingly, there is no Type 1 designation, only Types 2, 3 and 4. Additionally, subsequent parts to the standard provide specific requirements for each product technology. Table 5 identifies the various ESPE technologies that are considered, as well as the possible type achievable for each.

As Table 5 indicates, Type 2 and Type 4 ratings are reserved for through-beam technologies, which utilize distinct transmitting (sender) and receiving (receiver) elements to constantly monitor an optical signal. Table 6 represents a comparison of the primary differences between these ratings.

Since ESPEs contain logic components with self-checking and monitoring features performing safety functions, they are also considered subsystems. In turn, these subsystems can achieve specific PLs and SILs (Table 7, p. 36).

minimum type requirements when ESPEs are utilized as part of the risk reduction solution.

For example, when an ESPE is utilized for presence-sensing device initiation, not only must the minimum object sensitivity be 30 mm, but the device must also be a Type 4 component per IEC 61496. While the regulatory requirements and consensus standards in North America do not stipulate that ESPEs meet a specific rating system (such as the types defined by IEC 61496), many proactive organizations, both suppliers and users, have a higher degree of confidence in the overall reliability of their safeguarding systems when such devices are used.

That said, it is also interesting to report that UL, a leading third-party testing organization, has developed a series of test standards based strongly on the IEC standards—specifically a standard for general requirements (UL 61496-1, 2002) as well as another for active optoelectronic protective devices (UL 61496-2, 2002).

### Interlocking Devices: Types 1, 2, 3 & 4

Another example of a standard that identifies a product classification system using types with numeric rankings is ISO 14119 (2013) for interlocking devices. While completely unrelated to the type categories applicable to ESPEs, this standard describes the technology and typical characteristics of four types of interlocking devices. These four types are not presented in a hierarchical order, and other solutions may be adopted as long as they comply with the standard’s principles. Users must conduct a risk assessment of the specific machine application to determine the correct application of each type of interlocking device.

Since interlocking methods involve a broad spectrum of technological aspects, many different criteria are used to classify interlocking devices. This may include grouping according to the nature of the link between the guard and the output system, or by the type of technology (e.g., electromechanical, pneumatic, electronic) associated with the output system. Table 8 (p. 36) shows the actuation principles and actuators for the defined interlocking device types, as well as examples of products available on the market to fill many of the categories.

As a basic introduction to this technology, an interlocking device is used to monitor the position of a guard to sense whether it is closed or open. The device is then intended to produce a stop command when the guard is not in the closed position. Interlocking devices can be used to control other functions as well (e.g., application of a brake to stop hazardous machine functions before access is permitted).

Table 5

## Types of ESPE Addressed by IEC 61496

Technology	Abbreviation	Applicable standards	Possible type achievable	Examples
Active optoelectronic protective devices	AOPD	IEC 61496-1 IEC 61496-2	2 or 4	<ul style="list-style-type: none"> <li>•Light curtains</li> <li>•Single/multiple beam systems</li> <li>•Close proximity point of operation AOPDs (laser-actuated AOPDs in Europe)</li> </ul>
Active optoelectronic protective devices responsive to diffuse reflection	AOPDDR	IEC 61496-1 IEC 61496-3	3	<ul style="list-style-type: none"> <li>•Laser (area) scanners</li> </ul>
Vision-based protective devices	VBPD	IEC 61496-1 IEC 61496-4	3	<ul style="list-style-type: none"> <li>•Camera systems</li> </ul>

Furthermore, some interlocking devices also perform a guard-locking function to keep the guard locked while hazardous machine function is present or simply to prevent interruption of the machine process. The guard-locking device is often an integral part of an interlocking device, but it may also be a separate unit. Monitoring the status of the guard-locking device determines whether the device is engaged or released and produces an appropriate output signal accordingly. Table 8 presents the operating principles and associated terminology for these devices.

### Two-Hand Controls: Types I, II, IIIA, IIIB & IIIC

Two-hand control devices are another example where subcategories are defined using terminology with alphanumeric types. As used within the industrial safety market, a two-hand control device is a safety device that provides a measure of protection for the operator. The level of risk reduction is gained by

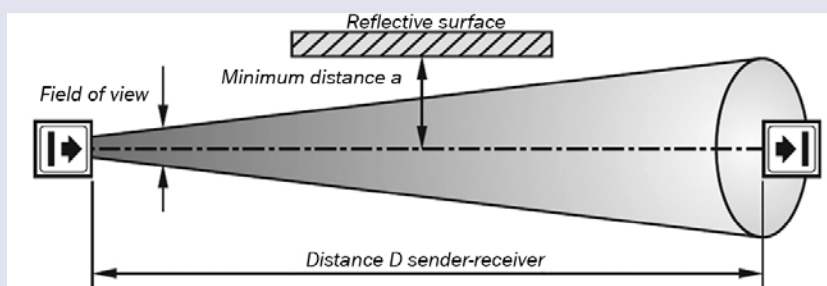
preventing the operator from reaching danger zones during hazardous situations by locating the control actuating devices at a specific position and distance.

ISO 13851 (2002) describes the main characteristics of these devices used in safety applications and sets out combinations of functional characteristics for three types. Table 9 (p. 37) provides a brief overview of the functional requirements for each device type as defined by the ISO standard. In some applications, enabling devices and hold-to-run devices may comply with the definition of a two-hand control device, but the ISO standard is not intended to apply to these devices.

In contrast to the ISO standard, the North American market does not segment the requirements for two-hand control devices into different classifications. Instead, OSHA 1910.217 (1971), ANSI B11.19 (2010) and Canadian Standards Association Z432 (2004) set forth a single group of requirements (as noted in the last three columns of Table 9).

Table 6

## Type 2 vs. Type 4 Active Optoelectronic Protective Devices According to IEC 61496



	Type 2	Type 4
Functional safety	The protective function may be lost if a fault occurs between test intervals	The protective function is maintained even if multiple faults occur
EMC (electromagnetic compatibility)	Basic requirements	Increased requirements
Maximum aperture angle of the lens	10°	5°
Minimum distance (a) to reflective surfaces at a distance (D) of < 3 m	262 mm	131 mm
Minimum distance (a) to reflective surfaces at a distance (D) of > 3 m	= distance x tan (10°/2)	= distance x tan (5°/2)
Several senders of the same type of construction in one system	No special requirements (beam coding is recommended)	No effect or OSSDs shut down if they are affected



Table 7

## Achievable Reliability of Safety Functions With Active Optoelectronic Protective Devices

		Performance level (PL) per ISO 13849-1					Device examples
		a	b	c	d	e	
ESPE type per IEC 61496-1	2						Safety light curtains, single-beam photoelectric safety switches, multiple light beam safety devices
	3						Safety laser scanners, safety camera systems
	4						Safety light curtains, single-beam photoelectric safety switches, multiple light beam safety devices
		1			2	3	
		Safety integrity level (SIL) per IEC 62061					

### Commonalities of Product Classifications

The international Type-B standards that categorize product segments do not specify which machines require specific classifications of devices. They also do not specify which types of device shall be used. Instead, the standards provide requirements and guidance addressing the design and selection (based on a risk assessment) while also establishing performance requirements for design and certification of devices used in safety functions. While the use of types is noted in each cited example, the requirements are completely unrelated. Thus, understanding the language and the different meanings that can be communicated is important to ensure that proper use is put into perspective based on the given application.

### Conclusion

It should now be apparent that the various ranking systems used within the industrial safety marketplace are each unique. Some ranking systems utilize common terminology (such as category or type) or similar classification levels (either with

alphabetical or numerical identification systems). However, the context of the terminology is the most important element to ensure that all parties understand the intended meaning.

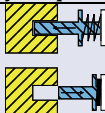
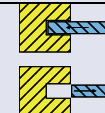
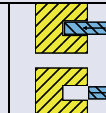
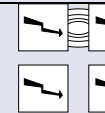
Based on this primer, OSH professionals should better understand control engineers when they hear the following during an exchange.

We've designed a functional safety system to exceed the requirements of the Type-C standard. This system is comprised of an emergency stop device used in a Category 0 stop circuit with Category 2 architecture, as well as a separate protective stop circuit with a Category 2 stop function achieving PL<sub>d</sub> with Category 3 architecture. The protective stop circuit has the following components compliant with the applicable Type-B standards: a Type 4 light curtain rated as PL<sub>d</sub> and SIL 3, a Type 2 power to unlock guard-locking interlock device and a Type IIIB two-hand control device.

While many OSH personnel may not be able to review the control schematics to confirm the component selection and circuit design, the language used

Table 8

## Principles of Operation & Terminology for Locking Interlock Devices

		By shape			By force
					
Principle of operation	Actuation (locking)	Spring	Power ON	Power ON	Power ON
	Release (unlocking)	Power ON	Spring	Power ON	Power OFF
Terminology		Mechanical locking device (preferred for safeguarding)	Electrical locking device (preferred for process protection)	Pneumatic/hydraulic locking device	Magnetic locking device

by control engineers should now have clearer meaning or at least it should be more understandable. As with any type of communication, misunderstanding is often the root of many disappointments. Conversely, proper use of industry-specific language can only aid in achieving intended goals. **PS**

## References

- ANSI. (2010). Performance criteria for safeguarding (ANSI B11.19). New York, NY: Author.
- ANSI. (2010). Safety of machinery: General requirements and risk assessment (ANSI B11.0). New York, NY: Author.
- ANSI. (201x). Functional safety for equipment (electrical/fluid power control systems): Application of ISO 13849—General principles for design (ANSI B11.26). New York, NY: Author.
- British Standards Institution. (1996). Safety of machinery: Safety-related parts of control systems—Part 1: General principles for design (superseded by BS EN ISO 13849-1:2006). London, U.K.: Author.
- CSA Group. (2014). Safeguarding of machinery [CSA Z432-2004(R14)]. Toronto, Ontario: Author.
- International Electrotechnical Commission (IEC). (2005a). Safety of machinery—Electrical equipment of machines—Part 1: General requirements (IEC 60204-1). Geneva, Switzerland: Author.
- IEC. (2006). Safety of machinery—Functional safety of safety-related electrical, electronic and programmable electronic control systems (IEC 62061). Geneva, Switzerland: Author.
- IEC. (2007). Safety of machinery—Electro-sensitive protective equipment—Part 4: Particular requirements for equipment using vision-based protective devices (IEC/TR 61496-4). Geneva, Switzerland: Author.
- IEC. (2008). Safety of machinery—Electro-sensitive protective equipment—Part 3: Particular requirements for active opto-electronic protective devices responsive to diffuse reflection (IEC 61496-3). Geneva, Switzerland: Author.
- IEC. (2010). Functional safety of electrical, electronic, programmable electronic safety-related systems—Part 1: General requirements (IEC 61508-1). Geneva, Switzerland: Author.
- IEC. (2012). Safety of machinery—Electro-sensitive protective equipment—Part 1: General requirements and tests (IEC 61496-1). Geneva, Switzerland: Author.
- IEC. (2013). Safety of machinery—Electro-sensitive protective equipment—Part 2: Particular requirements for equipment using active optoelectronic protective devices (IEC 61496-2). Geneva, Switzerland: Author.
- ISO. (1999, 2006). Safety of machinery—Safety-related parts of control systems—Part 1: General principles for design (ISO 13849-1). Geneva, Switzerland: Author.
- ISO. (2002). Safety of machinery—Two-hand control devices: Functional aspects and design principles (ISO 13851). Geneva, Switzerland: Author.
- ISO. (2006). Safety of machinery—Emergency stop—Principles for design (ISO 13850). Geneva, Switzerland: Author.
- ISO. (2013). Safety of machinery—Interlocking devices associated with guards: Principles for design and selection (ISO 14119). Geneva, Switzerland: Author.
- ISO. (2014). Safety aspects: Guidelines for their inclusion in standards (ISO/IEC Guide 51). Geneva, Switzerland: Author.
- NFPA. (2015). Electrical standard for industrial machinery (NFPA 79). Quincy, MA: Author.
- OSHA. (1971). Mechanical power presses (29 CFR 1910.217). Washington, DC: Author.
- Soranno, C. (2014). Functional safety for machine controls. Retrieved from <http://bit.ly/1HDqJly>
- Underwriters Laboratory (UL). (2002). Standard for electrosensitive protective equipment, Part 1: General requirements and tests (UL 61496-1). Northbrook, IL: Author.
- UL. (2002). Standard for electrosensitive protective equipment, Part 2: Particular requirements for equipment using active optoelectronic protective devices (UL 61496-2). Northbrook, IL: Author.

**Table 9**

## Minimum Safety Requirements for Two-Hand Control Devices & Type Classifications

	Type					North American requirements		
Requirement	Per ISO 13851					OSHA 29 CFR 1910.217	ANSI B11.19	CSA Z432
	I	II	III					
			A	B	C			
Use of both hands (simultaneous actuation)	X	X	X	X	X	X	X	X
Relationship between input and output signal	X	X	X	X	X	X	X	X
Cessation of the output signal	X	X	X	X	X	X	X	X
Prevention of accidental operation	X	X	X	X	X	X	X	X
Prevention of defeat	X	X	X	X	X	X	X	X
Re-initiation of the output signal	a	X	X	X	X	X	X	X
Synchronous actuation			X	X	X	X	X	X
Use of Category 1 circuit architecture	X		X				a	a
Use of Category 3 circuit architecture		X		X		b	a	a
Use of Category 4 circuit architecture					X		a	a

**Note.** a = dependent on a risk assessment; b = OSHA refers to circuit architecture in terms of “control reliable.”