Functional Safety for Machine Controls

Part 4 of 5 in a series addressing the primary milestones to a safe machine

Introduction

When implementing technical protective measures (also referred to as “safeguards”) from the hierarchy of controls, as discussed in Part 3 of this series (*The Risk Reduction Process Utilizing a Hierarchy of Controls*), each risk reduction measure will be associated with a safety function or combination of safety functions. In order for these safety functions to be designed and installed to a degree of reliability commensurate with the risk level of the associated hazard(s), the concepts of functional safety must be applied.

What is Functional Safety?

Functional safety is a part of the process used to design, test, and prove that the safety-relevant components and circuits of a machine’s control system meet the intended reliability and risk reduction capability as determined by a risk assessment. As part of the overall risk reduction strategy for industrial machinery, it is typical to apply safeguards employing one or more safety functions (as described below) to achieve some measure of risk reduction. Parts of machinery control systems that are assigned to provide safety functions are called “safety-related parts of control systems” (SRP/CS). These can consist of hardware and/or software and can either be separate from the machine control system or an integral part of it. In addition to providing safety functions, SRP/CS can also provide operational functions, such as initiation of machine motion under safe conditions.

“Functional Safety” is the term used to refer to the portions of the safety of the machine and the machine control system, which depend on the correct functioning of the SRP/CS. To best implement functional safety, safety functions must first be defined. Once identified, the required safety level must also be determined and then implemented with the correct components necessary to achieve acceptable risk reduction. To confirm that the minimum requirements have been met (if not exceeded), subsequent verification must be performed and documented.

To look at it from another aspect, functional safety is an engineering approach to quantify the performance level of the SRP/CS to a level commensurate with the associated risk for a given technical protective measure. This includes the verification and validation aspects of the safety functions that have direct interaction with the machine control system, as represented in Figure 1.

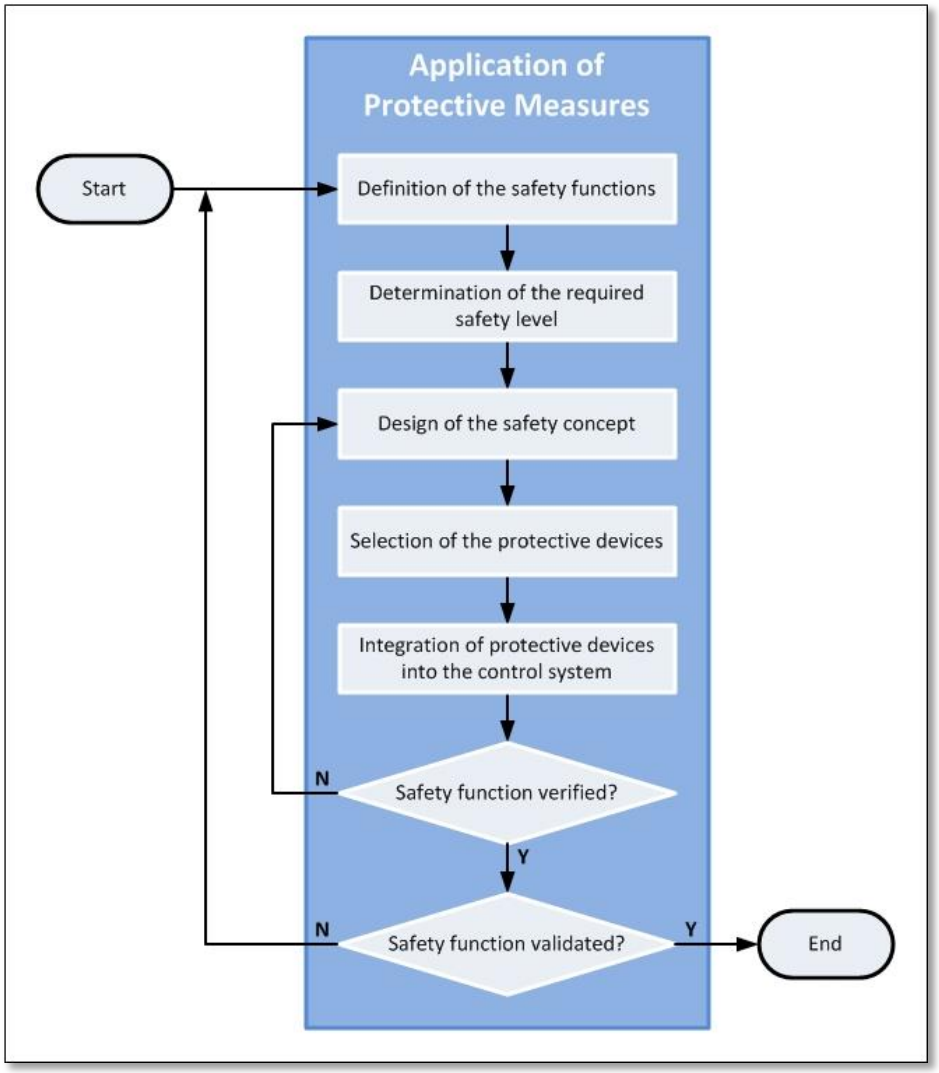

Figure 1: Application of Protective Measures

Safety Functions

Safety functions define how risks are reduced by engineering 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. As discussed in Part 2 of this series (*The Risk Assessment Process*), the risk assessment process will establish the minimum requirements for the reliability of safety functions, including mechanical, electrical, hydraulic, and pneumatic control system integrity. This level of reliability and integrity of the control portion of a safety function is referred to as 'functional safety.'

In order 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 in order to adequately reduce risk. Likewise, it is also possible for a single protective measure (safeguarding component) to play a part in more than one safety function simultaneously. Examples of common safety functions are listed in Table 1.

Safety Function	Example(s)	Functional Safety Aspects
Permanently Preventing Access	• Prevention of direct access to hazardous points using covers • Distancing protective devices (e.g., tunnels) to prevent access to the hazardous points and allow the passage of materials or goods • Prevention of access to hazard zones by using guards	☐
Retaining Parts, Substances, or Radiation	• Safety cover with special observation window on a milling machine for protection from flying chips and parts of workpieces • Fence that can retain a robot arm	☐
Avoiding Unexpected Start-Up	• Resetting the emergency stop device • Resetting an optoelectronic protective device • Restarting the machine once all the necessary protective devices are effective	☑
Allowing Material Passage	• Selecting suitable sensors and placing them in appropriate positions allows the material to be detected and the safety function is suspended for a limited time while the material passes through (muting) • Horizontal light curtains with integrated algorithm for person/material differentiation • Protective field switching on a safety laser scanner	☑
Disabling Safety Functions Manually and for Limited Time	• Movement only at reduced speed with enabling button engaged and +/- buttons actuated	☑
Temporarily Preventing Access	• On request, a machine stop is initiated. When the machine reaches the safe state, the blocking of access by the safety locking device is released.	☑
Monitoring Machine Parameters	• Monitoring of speed, temperature, or pressure • Position monitoring	☑
Combining or Changing Safety Functions	• After a change of operating mode between setup and normal operation, the machine is stopped. A new manual start command is necessary. • Adapting the monitored area of a laser scanner to the speed of the vehicle	☑
Initiating a Stop	• Opening a protective door with an interlock that has no locking function • Interrupting the light beams on a multiple light beam safety device providing access protection	☑
Initiating Stop and Preventing Start	• A two-hand control on single-person workplaces • Use of a light curtain so that standing behind or reaching around is not possible (hazardous point protection) • Use of a safety laser scanner for area protection	☑
Preventing Start	• Trapped key systems • Detection in the active protective field of a horizontal safety light curtain	☑
Shared Loading/Unloading Area between Man and Machine	• This workplace can either be used by the worker or by the machine (e.g., robot). In consequence, the simultaneous presence of both in the protected area triggers the safety function.	☑
Presence Sensing Device Initiation (PSDI)	• Use of a presence sensing device (e.g., light curtain) to initiate the machine cycle after a specified number of interruptions by the operator within a limited period of time	☑
Emergency Stop	• Shutting down in an emergency	☑
Safety-Relevant Indications and Alarms	• Interlocking indications • AGV speed and start-up warning devices • Muting lamps	☑

Table 1: Examples of Safety Functions

It is worth noting that not all safety functions have functional safety requirements, as is the case for the use of fixed barriers to permanently prevent access or to retain hazards, as shown in Table 1. Permanent separation of individuals from hazards is clearly a safety function, as is evident by the number of machines on the market with permanently fixed guards (such as fences, covers, or enclosures) or shields (such as viewing windows, weld flash curtains, or noise absorbing material) in place. While these components of the overall safety system have specific requirement pertaining to proper design and use, these elements do not have functional safety considerations because there is no interface to the SRP/CS. The level of risk reduction provided by these measures can be reliably maintained through proper installation, inspection and maintenance protocols.

A simpler way to distinguish between 'safety functions' and 'functional safety' is to view the idea visually, as shown in Figure 2. In essence, all functional safety concerns are related to a safety function, but not all safety functions require functional safety.

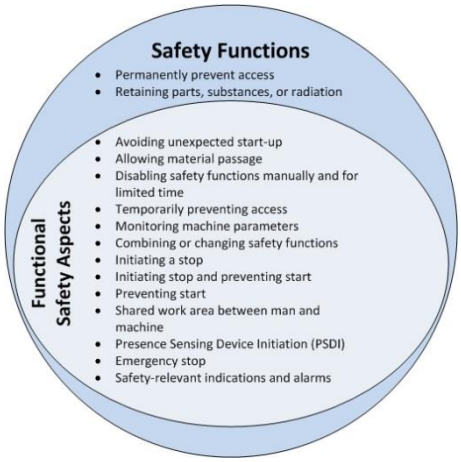

Figure 2: Visual Representation

Why Apply Functional Safety?

Safety technology continues to advance beyond simple electrical and electromechanical components (such as interlocking devices and relays) toward more complex electrical systems using transistors, integrated circuits and software-based components (such as microprocessors). With more basic elements, their behavior in the event of a component failure can be determined to a high degree of certainty because each component can be completely defined. The failure modes of more complex systems, on the other hand, are more difficult to define and in some cases can only be estimated.

Many industrial controls engineers were just beginning to grasp the idea of circuit architecture, whether it was referred to as "Control Reliable," according to OSHA and older ANSI standards, or "Categories," under the EN 954-1 standard from Europe. The introduction of functional safety does not diminish the importance of the circuit design, but rather builds on the concept to account for the greater number of possible failure modes inherent with more complex control systems. Essentially, the benefit of functional safety is to provide a means to "give credit" for other design aspects (aside from simply the circuit architecture), which the older standards didn't address, such as oversizing contactors, selecting more robust and reliable components for use in the circuit, providing higher levels of diagnostics, or addressing common cause failures through the process or implementation.

Essentially, the same reliability concerns exist when designing and evaluating SRP/CS – whether the control system is associated with simpler components or more complex elements. In order to consistently determine the overall reliability of these systems, various safety standards have been developed to outline the key elements. These elements must be considered to determine the overall reliability of the safety-critical control functions. Standards that address these elements include:

- ISO 13849-1 – Safety of machinery – Safety-related parts of control systems
- IEC 62061 – Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems
- IEC 61508 – Functional safety of electrical/electronic/programmable electronic safety-related systems
- IEC 61511 – Functional safety – Safety instrumented systems for the process industry sector
- ANSI B11.26 – Functional Safety for Equipment (Electrical/Fluid Power Control Systems) – Application of ISO 13849 – General Principles for Design

The primary principle behind these standards is that the overall reliability of a safety function can be qualitatively estimated. In terms of safety, the most important concern is to determine the probability that the system will fail to a dangerous condition. In terms of the standards, the reliability of the SRP/CS is estimated as the probability of a dangerous failure per hour (PFHd).

There are currently two primary methodologies to determine the likelihood of a dangerous failure; "Performance Level" (PL) as outlined in ISO 13849-1 and "Safety Integrity Level" (SIL) as addressed in IEC 62061. Figure 3 illustrates these methodologies in terms of probability to a dangerous condition.

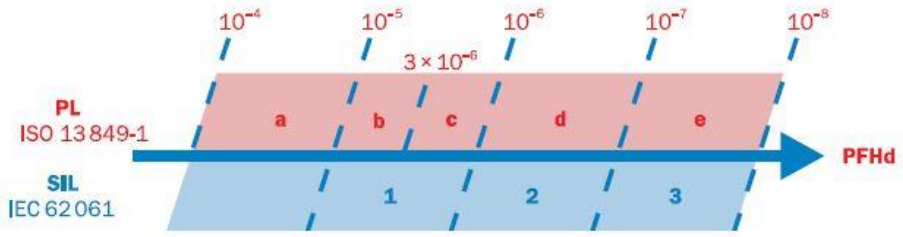

Figure 3: Scale of Functional Safety Levels

What are the Elements of Functional Safety?

As discussed in Part 3 of this series, the SRP/CS is the part of a control system that responds to safety-related input signals and generates safety-related output signals. These are parts of machinery control systems that are assigned to provide safety functions. The combined elements start at the point where the safety-related input signals are initiated (for example, obstruction of an optical beam of the safety light curtain) and end at the output of the power control elements (for example, the main contacts of a contactor), as shown in Figure 4. In some cases, the final element (such as the motor) is not included. It is also important to note that individual components of the safety system may play a role in multiple safety functions, with each safety function possibly requiring different levels of functional safety – again emphasizing the importance to precisely describe each safety function.

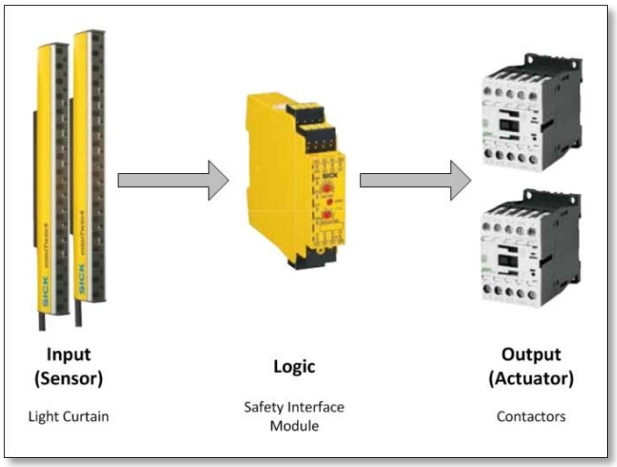

Figure 4: Basic Elements of SRP/CS

Primary Considerations of Functional Safety

The central pillars supporting the functional safety concept are exhaustively outlined in a number of sources, including the standards listed previously. As an overview, the primary considerations for determining the Performance Level for a sub-system are shown in Figure 5 and outlined below.

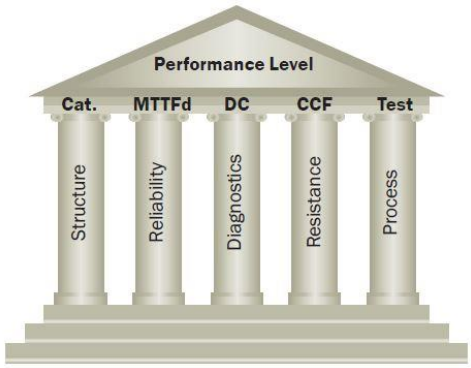

Figure 5: Performance Level (PL) Considerations

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 and 4).

2. **Reliability of individual components defined by mean time to a dangerous failure (MTTFd) values**
    - 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 level of safety can be increased if fault detection is implemented in the subsystem. The diagnostic coverage (DC) is a measure of capability to detect dangerous faults.

4. **Common cause failure (CCF)**
    - External influencing factors (e.g., voltage level, overtemperature) can render identical components unusable regardless of how rarely they fail or how well they are tested. These common cause failures 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.

Achieving Functional Safety

Through the combination of the considerations above, the PL achieved can be probabilistically determined to be a specific level. Figure 6 represents how the combination of component selection (MTTFd), diagnostic coverage (DC), and circuit architecture (Category) combine together to achieve various PL outcomes, with consideration for common cause failures (CCF).

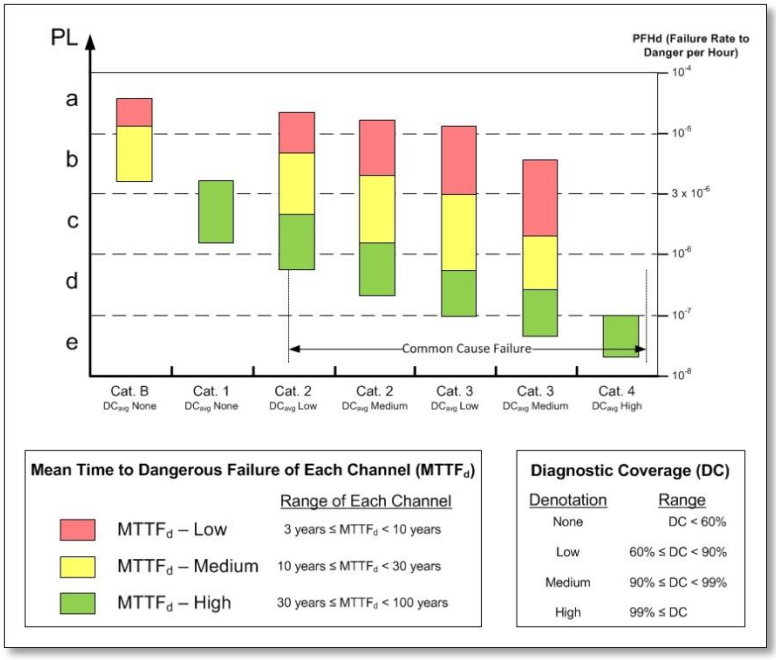

Figure 6: Determination of the Performance Level of a Subsystem (from ISO 13849-1:2006)

Validation of Functional Safety

As with any risk reduction measure, it is essential to verify that the PL achieved is at least as high as the PL required (PLr). This can be easily represented as **PL ≥ PLr**.

The confirmation that adequate PL has been achieved is covered in the overall process applied to the design of SRP/CS. The primary features include:

- Organization and competence
- Rules governing design (e.g., specification templates, coding guidelines)
- Test concept and test criteria
- Documentation and configuration management

All lifecycle activities of safety-related embedded or application software must primarily consider the avoidance of faults introduced during the software lifecycle. The main objective is to have readable, understandable, testable and maintainable software. The ISO 13849-1 standard outlines a V-model as shown in Figure 7, which has proven particularly effective in practice for software design.

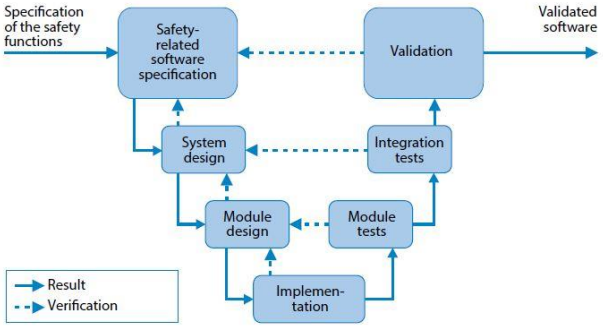

Figure 7: V-Model for Software Validation

In common language (outside of safety standards), there is little difference between the terms 'verification' and 'validation.' In essence, the goal is to test and check that the overall reliability of each subsystem of the SRP/CS is adequate for the associated risk, and that accurate documentation is collected for future revalidation throughout the entire lifecycle of the machine.

Confirmation of Functional Safety

Over the past ten to fifteen years, industry has been progressively adopting the concepts of evaluating risks based on a systematic methodology (*The Risk Assessment Process* as discussed in Part 2 of this series) and reducing identified risks through the application of multiple layers of protective measures from an orderly list of options based on their effectiveness (*The Risk Reduction Process Utilizing a Hierarchy of Controls*, addressed in Part 3 of this series). The next step to further advance safety is the concept of confirming that the established goals have been achieved. As such, after risk reduction measures have been implemented, their effectiveness must be confirmed.

When dealing with simple SRP/CS comprised solely of electrical and electromechanical components, the confirmation is based on review of the circuit design. However, when the SRP/CS utilizes more complex subsystems using software-based components, the confirmation must account for the other four pillars of functional safety as discussed above.

The process developed in Europe for conducting the necessary confirmation takes a mathematical approach to determine the reliability of the SRP/CS in terms of probability of a dangerous failure per hour (PFHd). The Institute for Occupational Safety and Health (IFA) in Germany has developed a tool to perform the mathematical calculations to apply the concepts of ISO 13849-1. This tool, called *Safety Integrity Software Tool for the Evaluation of Machine Applications* (SISTEMA), is available for free online.

SISTEM accounts for the fact that safety-related parts of a control system are engineered from subsystems, blocks and elements using components for industrial use which can generally be purchased commercially. When calculating the PLr of a system, the system designer must enter various values and information. Component manufacturers typically provide this data in data sheets or in catalogs, but many also make the information available to SISTEMA users in the form of libraries. This collaboration within the safety market allows designers to copy the necessary data from a library directly into a SISTEMA project quickly and accurately.

Acceptance of Functional Safety

While the notion of confirming that minimum reliability and performance levels are attained has been widely acknowledged on a global scale, the implementation of this theory has not received the same level of acceptance. This can be attributed – at least in part – to the legal approach to safety and where the responsibilities lie, as discussed in Part 1 of this series (*Selecting Safety Standards for Machine Safeguarding Requirements*).

A core element of the Machinery Directive 2006/42/EC is that machinery manufacturers (either the original OEM or the entity performing modifications to existing equipment) hold the responsibility to prove conformity to the essential requirements for machine safety. Conversely, the legal systems in North America place the liability directly on the user (employer). In the United States, the Occupation Safety and Health (OSH) Act of 1970 includes the General Duty Clause, which states, in Section 5(a)(1):

> Each employer shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees.

When the global market is considered in terms of number of users versus the number of manufacturers, it is easy to see that the number of end users in the marketplace far outweigh the number of OEMs. (For this discussion, we are not including organizations that build and use their own equipment – essentially undertaking the responsibilities of both OEMs and users.) For discussion purposes, let's suppose that the ratio of users to suppliers is 99:1 (by some accounts, this may be considered a conservative estimation of the global market).

In the model where liability is placed on the supplier (such as in Europe), this implies that 1% of the entities in the market assume the responsibility for implementing and verifying that the protective systems meet the essential requirements. Furthermore, this same 1% of the organizations also happens to be the entities that are most familiar with the design and function of the equipment since they are the exact same groups who designed the equipment. In this model, implementing the approach of functional safety is relatively easy – or at least much more palatable, because the designers are the most familiar with the design specification. Additionally, these organizations have a moderately small number of machine types with which they are involved, in turn allowing them to become experts regarding the application of functional safety on those limited types of equipment.

On the other hand, where the model places the requirements on the end user (such as in North America), the other 99% of the market now becomes responsible for verifying that an adequate level of risk reduction has been achieved. In this model, 99% of the organizations are not experts in machine design, but rather in utilizing machines built by others to produce their end products. Moreover, this portion of the industrial community typically uses many diverse machine types, making the task of achieving 'expert' level very difficult. Essentially, the North American legal system is not compatible with the functional safety concepts presented in standards like ISO 13849 – which is no surprise when we consider that most functional safety standards are developed outside of North America.
If we put the regional differences of market expectations and regulatory requirements aside, it is self-

evident that machinery suppliers are in the best position to apply the concepts of functional safety, regardless of the geographic size of their market. Those entities responsible for the design and implementation of safety functions which interface with the SRP/CS possess the essential information pertaining to this concept; expected mission time (life span) of the equipment, specification of the individual safety-related components, design parameters for circuit architecture and diagnostic coverage of the circuits, and the steps and processes in place to reduce common cause failures and general human errors.

Conclusion

As discussed in Part 3 of this series, achieving an acceptable or tolerable level of residual risk is possible through application of the hazard control hierarchy. However, to confirm that the desired degree of risk reduction is achieved, one must test and check that all safety functions are performing to the desired level of reliability. When the safety functions are directly interacting with the machine control systems, these portions of the control become SRP/CS, and in turn must be validated. Functional safety is an approach based on probabilistic evaluation of component data to validate the overall reliability of those safety functions as a necessary step to determine that minimum performance requirements have been achieved.

If the ideas of functional safety appear complex and intimidating, rest assured that you do not stand alone. As is the case with most new philosophies, change is often difficult to implement and even harder to accept. Do not hesitate to request assistance from outside resources to provide support as necessary.

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 functional safety, contact SICK Safety Application Specialist Chris Soranno at chris.soranno@sick.com, or visit our web site at www.sickusa.com.