CONTROL ENGINEERING

Sponsored by

ABB

Is your safety system compliant with today's safety standards?

The ABB Group

ABB is a global leader in power and automation technologies that enable utility and industry customers to improve their performance while lowering environmental impact.

ABB Safety Systems

Over the past 30 years, ABB has successfully delivered and installed safety systems in more than 55 countries worldwide. We work hard with end-users to maintain and evolve existing installations, thereby maximizing customer value and ensuring safe plant operation throughout the safety system lifecycle.

The Power of Integration

The potential and the power of integra- tion lies in what can be achieved when information is made available, in context, to all of the devices, systems and individuals responsible for controlling, maintaining and managing production.

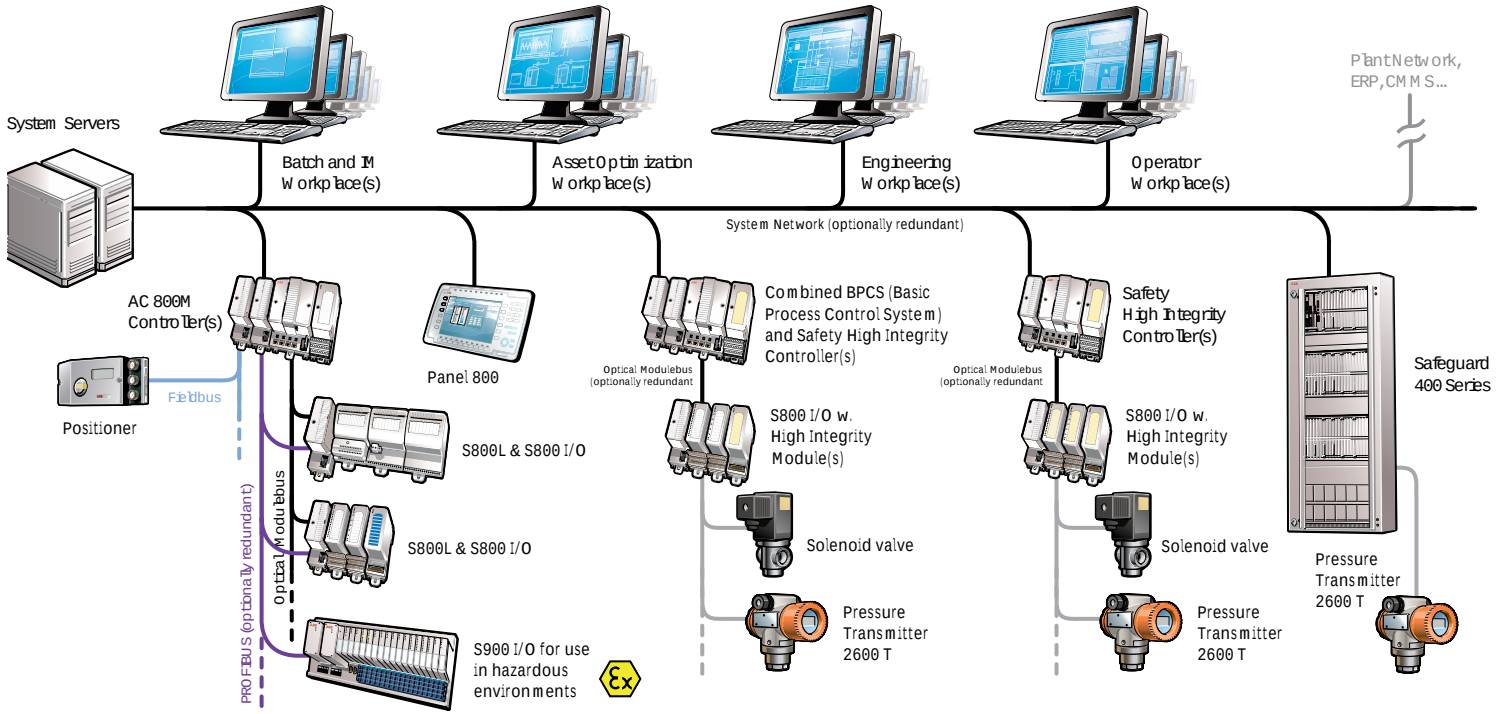
ABB's integrated approach to safety and control is yielding more cost effective safety system (SIS) implementations while delivering significant operational benefits. ABB's System 800xA architecture offers the flexibility of hosting both safety and process critical control applications in the same controller or on separate hardware if desired.

Either way, the user gains many of the same integration benefits, including common operator interface and engineering tools, plant-wide sequence-of-events (SOE) lists for consolidated root cause analysis, as well as centralized historian and data archiving.

Join the Discussion

Safety impacts many areas of plant operations including profitability, security, operator effectiveness and availability to name a few.

Visit ABB's Process Automation Insights blog to join the conversation at http://www.processautomationinsights.com/



Independent, But Connected

By Ron Johnson and Luis M. Duran

Operational aspects of safety systems are under increased scrutiny throughout the automation industry these days. Beyond the pure financial benefits, which focus on reducing operational cost throughout the system lifecycle, the real driver is safer operations.

Systems continue to get more complex, and with a larger number of systems in any given plant combined with a knowledge pool continuously depleting through retirement, the risk of safety critical mistakes understandably inch upward.

One counter-measure to negate this risk is a reduction in system complexity and the number of systems used.

Just take a look at Dow Chemical. For a long time the Midland, MI-based chemical giant used a combined basic process control system and safety instrumented system (BPCS/SIS) logic solver platform.

Dow's proprietary home grown computer system is TÜV certified for SIL-3 plus BPCS control (providing they follow the safety manual). The company successfully used it this way since the mid-1990's and they now have hundreds of installations utilizing this concept.

Today there are integrated SIS/BPCS logic solver platforms available all over the place. Since the early 2000's, Dow started using an ABB SIL certified platform in a similar manner as their own home grown computer system. At one facility in Michigan that uses toxic chemicals and a gas fired curing oven. This 1,500 I/O facility uses multiple dual certified safety controllers to perform all of the normal process control plus roughly 75 safety instrumented systems (SIL-1 & SIL-2).

In some cases Dow has gone one step further and utilized the common pool of field data to enhance the basic process control and the safety systems by sharing sensors. In one case, the same two temperature signals see use by the oven's fuel gas controller for temperature control and by the high temperature SIS trip that shuts the fuel block valves.

Conventional thinking would wire one sensor to the BPCS computer for temperature control and the other sensor to the SIL certified computer for the SIS. But by sharing these sensors, the temperature control becomes more robust and fault tolerant thereby decreasing the probability of control failure. At the same time, the SIS with two sensors is more robust and fault tolerant resulting in a lower failure probability. Dow recognizes the potential common cause issues associated with sharing sensors and consequently calculates proof test intervals with fault tree based tools.

In another case, a 1,300 I/O European Polyurethanes expansion with over 100 SIS loops utilized multiple dual certified safety controllers. The safety systems and the normal process control fully integrate within this single platform. Roughly 25% of the safety loops also share sensors with the basic process control. Although the front end design is more complex to ensure they do not compromise safety, the long term benefits are worth the effort.

The integration of safety and basic process control has proven itself with safer and less complex operating environments. Within the last five years, Dow has installed over 20,000 I/O on commercially available dual certified logic solver platforms. Dow's history with over 1,000,000 I/O on Dow's proprietary dual certified platform ensures this is the future for Dow. History shows when properly designed and implemented, safety and basic process control can integrate in a safe and cost effective manner.

Industry shift

Dow's move should not be a surprise because over the past decade the automation market has consolidated vendors and started to develop BPCS and SIS using similar hardware and software for sequential logic control and regulatory process control. Integration became more than sharing the process network.

As the advances in technology continued, the industry benefited from improvements in the reliability of hardware and software, including embedded software. The 1oo2 dual, 2oo3 triple, and quad systems available on the market today come from a design era that used redundancy and fault tolerance as a means of reducing the probability of a dangerous failure occurring. Today, a manufacturer can design out dangerous failure modes and they can provide more than 99% diagnostic coverage to protect integrity without resorting to duplication. The requirements of 'fail safe" for 'safety integrity" and 'fault tolerance" for 'availability" can now undergo independent consideration and used when and where they are applicable.

Other advances are in the form of the design process. Safety standards recommend product life cycle design processes which include product development or 'validation and verification" to ensure everyone takes proper care in the development of the product.

This new degree of integration challenges the common accepted practices of satisfying and demonstrating the SIS is not subject to common cause failures with the BPCS. Furthermore, even though they are integrated, both systems can provide independent protection layers and meet the safety standard's requirements.

The debate about the separation of the safety function from the BPCS will no doubt continue. However, the IEC 61508 and IEC 61511 standards recognize safety and non-safety functions can reside in the same system if 'it can be shown that the implementation of the safety and non safety functions is sufficiently independent (i.e. that the failure of a non safety related function does not cause a dangerous failure of the safety related functions)". Also, the standards also require the possibility of common mode dependent failures reduces down to an acceptable level.

Standards and integration

It is easy to quote safety standards to answer the question of if it is possible to comply with standards in an integration scenario. IEC 61511-1 clause 11.2.4 states 'the BPCS should be designed to be separate and independent to the extent that the functional integrity of the SIS is not compromised." ISA-84.00.01-2004 Part 2 Clause 11.4.2 adds 'physical separation between BPCS and SIS may not be necessary provided independence is maintained, and the equipment arrangements and the procedures applied ensure the SIS will not be dangerously affected by:

- **Failures of the BPCS;**
- **Work carried out on the BPCS for example: maintenance, operation or modification."**

The same reference suggests 'in order to safely use a single platform for BPSC and safety, you need to effectively separate the BPCS from the SIS. They need to be as independent as possible to ensure interference is eliminated. This is managed by a strong Operating Discipline (OD) program."

The traditional approach for reducing common cause was to use totally different systems for the BPCS and the SIS, using different hardware and software to reduce common cause failures. These systems would come from different providers so common cause failures could most likely go out the door because the user would assume the provider's logic solver manufacturing process used different development organizations, knowledge, manufacturing processes, as well as different installation, operation, and maintenance procedures.

Additionally, the SIS provider would need to have a third party certification of their products according to applicable safety standards. In one case, a certification provided by TÜV includes a complete assessment of the hardware and software of the product including failure modes, installation requirements, operating restrictions in case of a failure, design and verification process, and many others.

Dual system training

One obvious disadvantage emanating from today's work intensive and engineer depleted environment is the manufacturer needs to engineer, commission, operate and maintain two totally different systems throughout the lifetime of the plant. Engineers, operators and maintenance personnel would need training and continuously need to maintain knowledge about different systems.

An alternative approach is to build independence in the design process of the integrated system. Independence is possible using diverse design engineering and programming teams provided with different software architecture specifications and guided by an overall concept for diversity from the start of the detailed design specifications.

The use of different toolsets in the development process provides even further diversity and facilitates reduction of common cause faults. Development techniques utilizing formal methods, the V-model (as defined in the safety standards), strict coding guidelines, separate development teams, and diverse implementation ensure a structured approach to avoid common mode failures throughout the entire specification, design and development process. When supported by a structured approach to test and formal verification at different levels, performed by an independent team, it is possible to enhance system reliability even more.

More than one solution

It is possible to design out dangerous failure modes and to provide more than 99% diagnostic coverage to protect integrity without resorting to duplication. Technology has evolved to a point where there are multiple options to address a similar technical problem. By using two or more technologies, diversity will embed into the system design. Diversity can occur in the embedded software by using different operating systems and then using different teams to develop the software on multiple cooperating modules.

By combining two different technologies (such as Micro Processor (MPA) or Micro controllers and Field Programmable Gate Arrays (FPGA)) to perform the same functionality in parallel to each other the design achieves a truly redundant and diverse implementation with a minimum of possible common cause failures. To eliminate the potential sources for common cause failures originating from design, development and test, this approach requires different development and test tools, as well as different programming languages for implementing the functionality,. By using two different development teams for creating system overheads in these two technologies, common cause failures can be minimal.

Memory management unit

In addition to implementing access control, password protection and a firewall, logical separation can come in the form of memory management. A memory management unit (MMU) can provide independence between different partitions of memory areas. These memory partitions then connect to different executing processes of the CPU such as regulatory process control or safety instrumented function. This approach ensures only the memory area belonging to that process is accessible while the CPU is executing one of its processes.

However, in order to fully answer any question, each user should seek for their answers by applying standards to assess the independence of both systems.

The pros and cons of integrated safety systems are 'soft" and are often not easy to prove. Nevertheless, they constitute an important consideration when evaluating the overall performance of a safety system. The benefits are in the following areas:

- **There is only a single process automation computer platform in the facility. That means there is only a single operator interface for operations to learn and operate. In addition, there is only one computer language for programmers to learn and one platform for maintenance personnel to maintain.**
- **All field instruments are wired to the common system, meaning there is less field splitting (optical isolators) or less communication required between two separate systems. That means there is easier instrument design and field wiring because all the I/O for a given unit operation wire to the same logic solver, regardless of wheth er it is safety I/O or not.**
- **The complete pool of plant information is avail able for the BPCS and the safety system because all the facility's I/O wires to the same logic solver. This allows for easy and safe communication of information between the SIS and the BPCS by utilizing the platform's certified safe guards to maintain "non-interference" and "functional independence." That also means the SIS operating window can be flexible since it can intimately know what is going on with the BPCS. For each unit operation the boundaries of the operating window change as the plants start up and shut down. This is much more difficult to manage with independent BPCS/SIS systems because there is only one SIS trip setting which forces operations to sometimes bypass these restrictive trip set points (for example during start-up activities). This introduces the need to bypass, and consequently the chance of leaving these hardware and software by passes in place after startup. With an integrated system, you can automate manual SIS bypasses and enables by coordinating with process operations and thereby eliminate the issues associated with having to remember to re-enable the safety systems. In a more abstract way, signals are not simply used, but rather the data they represent is used. The data goes in the data pool and validated first. This allows the use of multiple information sources as well as more final elements to execute decisions.**

A commonly referred to publication by the UK Health and Safety Executive summarizes primary causes of failure of safety systems as follows:

- **Inadequate specification: 44%**
- **Changes after commissioning: 20%**
- **Design and Implementation: 15%**
- **Operation and Maintenance: 15%**
- **Installation and Commissioning: 6%**

Although these problems loom larger with Baby Boomers retiring, the publication points out close to three-fifths of all sources of failure already exist before operation of the system has started. Improvements during specification and design stages of projects will to reduce these types of failures.

Human error unquestionably plays a significant role in a majority of failures occurring during system installation, commissioning, operation, maintenance and subsequent upgrades or modifications, according to these numbers. ISA-84.00.01-2004 part 2 says in clause 11.4.2: 'Identical separation between the SIS and BPCS may have some advantages in design and maintenance because it reduces the likelihood of maintenance errors." Additionally, there may be a reduction in systematic trips.

The use of Integrated Safety Systems offer ways to enhance safety and, as an added benefit, reduce the cost of ownership. Engineering efficiencies, improved system understanding and support will have positive impact on safe plant operation and bottom line performance.

When safety standards and best engineering practices start with the initial design, it is possible to develop an automation system that integrates the BPCS and SIS function within the same operational, maintenance and engineering environments.

This approach changes the paradigm from building robustness and reliability around multiple redundant paths to the use of the technology options available today to creatively satisfy the core design principles of independence, diversity and separation. These can then enable independent protection layers that integrate the user work functions. These systems have TÜV certification without the need of certifying the complete automation infrastructure, and without the need of ensuring the non-interference nature of the process control system.

Users can enjoy the benefits of integration without compromising safety and be in compliance with safety standards. However, the most important factor is plant operators are able to detect and react promptly to process conditions before they develop into near misses or incidents. Additionally, operations have the ability to track, analyze and report within the environment used to perform those functions for all other plant operations.

Behind the byline

Ron Johnson is an engineering solutions safety instrumented systems subject matter expert at Dow Chemical. His e-mail is RKJohnson@dow.com.

Luis M. Duran is a safety systems business development manager at ABB. His e-mail is luis.m.duran@us.abb.com.

This story emanated from a paper written for **ISA EXPO 2009.**

Revised Functional Safety Starts Now

By Nicholas Sheble

'Sixty six percent of your safety systems are between 11- and 30-years-old. Indeed, many are from the days of the DCS (distributed control system) and relay-based control systems," said ABB's Luis Durán.

Durán, a certified functional safety engineer and is product-marketing manager — safety for BU Control Technologies for ABB, Inc., conducted a webinar Tuesday entitled 'Is Your Safety System Compliant? Find Out and Plan Your Next Steps."

RELATED STORIES

Functional Safety: A Growing Concern

Safety, Productivity in Real Time

Back to Basics with Functional Safety

'Safety is Good Business'

Durán also said a new edition of IEC 61508 takes effect this month. IEC 61508 is 'Functional Safety of Electrical/Electronic/Programmable Electronic (E/E/PE) Safety-related Systems."

The standard is applicable to all kinds of industries defining functional safety as 'part of the overall safety relating to the EUC (Equipment under Control) and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems, and external risk reduction facilities."

Functional safety relies on active systems. For instance:

- **The detection of smoke by sensors and the ensuing intelligent activation of a fire suppression system is an example of an active system and functional safety.**
- **As well, the activation of a level switch in a tank containing a flammable liquid, when a potentially dangerous level has been reached, which causes a valve to close to prevent further liquid entering the tank and thereby preventing the liquid in the tank from overflowing is another example.**

Safety achieved by measures that rely on passive systems is not functional safety.

Durán said safety automation infrastructure might very well have gone into service while today's safety standards including IEC 61508 and IEC 61511/ISA 84 were still in development.

'Some of these safety systems, particularly the ones installed between the late 1980's and early 2000, are either general-purpose PLCs, or are not designed as a safety system according to the IEC 61508 standard," Durán said. Other systems might not satisfy current requirements with IEC 61508 and overall they don't comply with IEC 61511, which is the standard that sets out practices in the engineering of systems that ensure the safety of an industrial process using instrumentation – Safety Instrumented Systems (SIS).

The standard is 'Functional safety – Safety instrumented systems for the process industry sector" and it is fully incorporated in ISA84 and applicable to manufacturing processes like refineries, petrochemical, chemical, pharmaceutical, pulp and paper, and power.

Durán didn't cover all the changes to 61508 but did note the new approach to the management of functional safety, which provides for more comprehensive normative requirements:

- **Appointment of one or more persons by an organization with responsibility for one or more phases necessary for the achievement of functional safety of an E/E/PE safety-related system;**
- **Identification of all persons undertaking defined activities relevant to the achievement of functional safety of an E/E/PE safety-related system;**
- **All those persons undertaking defined activities relevant to the achievement of functional safety of an E/E/PE safety-related system shall be competent for the duties they have to perform.**

To see all the changes in IEC 61508 click on this International Electrotechnical Commission link.

Nicholas Sheble
nsheble@isssource.com is an engineering writer and technical editor in Raleigh, NC.

An instrumentation device that is supposed to keep your process from erupting during an upset may sit there for years if there is no emergency. Will it work when the time comes? Safety sensors can help you sleep better.

William Goble, PhD

You won't have to look far to find examples of automation component failures in critical situations with catastrophic results. Several Toyota owners reported experiencing problems with their anti-lock braking system causing their cars to speed up when not expected. There were many contributing causes to the Deepwater Horizon spill, but a major one was the failure of the blowout preventer. Safety sensors can help maximize safety and reliability by minimizing critical failures and help ensure that safety is not compromised in the event of a failure.

What is a safety sensor?

Many understand the term as suggesting an instrumentation device used to measure process conditions that could be potentially dangerous. The device is typically a part of an equipment set for a safety instrumented function (SIF) which also includes a logic solver and final element. The SIF is part of a safety instrumented system (SIS), whose purpose is to drive a process to a safe state or to allow it to move forward when specific conditions are present. Examples of safety-sensor products include a pressure transmitter, temperature transmitter, gas detector, level transmitter, flow transmitter, flame detector, acoustic detector, or even proximity switch. These common items are recognizable but do not differentiate between an ordinary process sensor and a safety sensor. So what is the difference?

Safety Integrity Level	SIL Capability - Design Quality Rating	Probability of Dangerous Failure
4	4	0.00001 - <0.000001
3	3	0.001 - <0.0001
2	2	0.01 - <0.001
1	1	0.1 - <0.01

Figure 1: Safety integrity levels and the associated SIL capability.

The standard for design and development of safety sensors

IEC 61508 is a multi-industry international standard that covers functional safety of automatic systems. The term functional safety is not the same as electrical safety or hazardous area safety. This standard is not concerned with shock hazards, burn hazards, or explosive atmospheres; rather, it covers the correct operation of a device (reliability) and, perhaps most importantly, how a device fails. Two different types of failures are covered: random failures and systematic failures.

When an instrumentation sensor has been assessed and meets the requirements of IEC 61508, it is common to label it as a safety sensor or safety-certified instrument.

The two main goals of the standard are clear-cut. The first is correct operation—a device must be sufficiently reliable. Reliability requires protection against both random and systematic failures. A random failure is defined as 'a failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware." Systematic failures are defined in IEC 61508 as 'a failure, related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation, or other relevant factors." The standard protects against systematic failures by having hundreds of requirements for the design, test, and manufacturing processes. These requirements reflect the best engineering practices known to avoid design mistakes and manufacturing faults.

The second main goal is that the device must fail in a predictable manner. A quantitative failure-mode analysis is done for random failures with published numbers for each failure mode. These numbers provide a safety-system designer with the information needed to determine if a safety sensor is sufficiently reliable when used in combination with a logic solver and final control element to meet the required safety integrity level (SIL). This task called SIL verification.

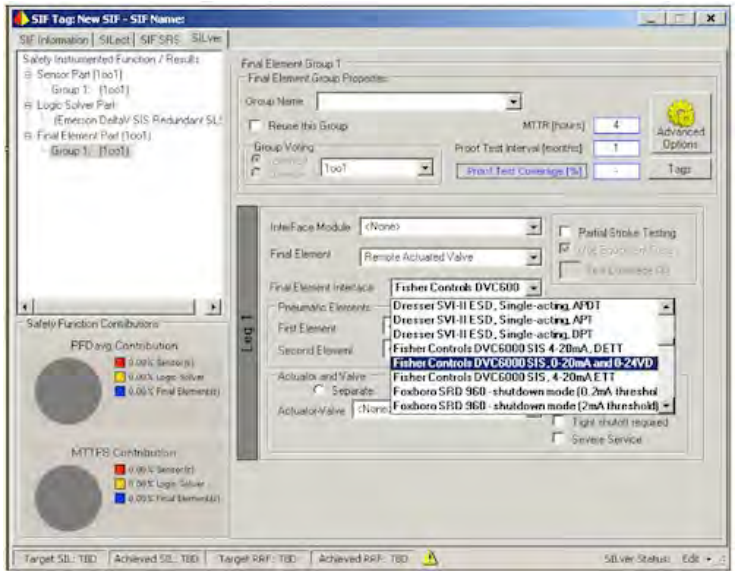


Figure 2. Tool for designing safety instrumented functions (including SIL verification) based on FMEDA data.

There are four different levels of safety integrity defined by IEC 61508 (Figure 1). The requirements for each safety integrity level are different. SIL 1 represents the lowest level. Each safety integrity level is intended to represent an order of magnitude improvement in safety and reliability and thus carries with it more stringent requirements. The requirements for a SIL 3 certification are much tougher than for SIL 2 certification, and those for SIL 2 certification are tougher than those for SIL 1.

When an instrumentation sensor has been assessed by a competent, third-party agency and meets the requirements of IEC 61508, it is common to label it as a safety sensor or safety-certified instrument. The 2010 version of IEC 61508 introduced the term systematic capability, which indicates the best-case safety performance that the device can provide when it is applied per its safety manual. Certified devices can have a systematic capability rating from one to four that matches the SIL level of a SIF in which it may be used.

Failure mode analysis

Minimizing the impact of random failures can best be evaluated with a quantitative failure rate and failure mode analysis, as required by IEC 61508. The best technique is called a failure modes, effects, and diagnostic analysis (FMEDA). An FMEDA requires each component in a device (resistor, transistor, capacitor, etc.) to be examined individually to evaluate its failure modes and their impact on the operation of the device. The ability of any selfdiagnostic to detect the failure is evaluated, and the cumulative impact of all component failures is calculated. This produces a set of numbers for a device—a failure rate for each failure mode. These numbers are then used by system designers to meet the targeted and required SIL levels for each SIF.

The FMEDA process is quite detailed and systematic, often identifying design problems that can be fixed to improve the design safety and reliability. As part of the certification, the number and type of product field failure data are analyzed as a function of the total accumulated operating hours. This observed failure rate can then be compared to the calculated failure rate in the FMEDA. If the values are comparable, this helps demonstrate the product development and quality process is effective.

Should you choose a safety sensor for your SIS?

The process industry-specific functional safety standard is IEC 61511 (ISA 84.00.01-2004). This standard requires that equipment used in a SIS be carefully selected and

Complex electronics in a field-device transmitter makes for a lengthy analysis process requiring lots of hand work.

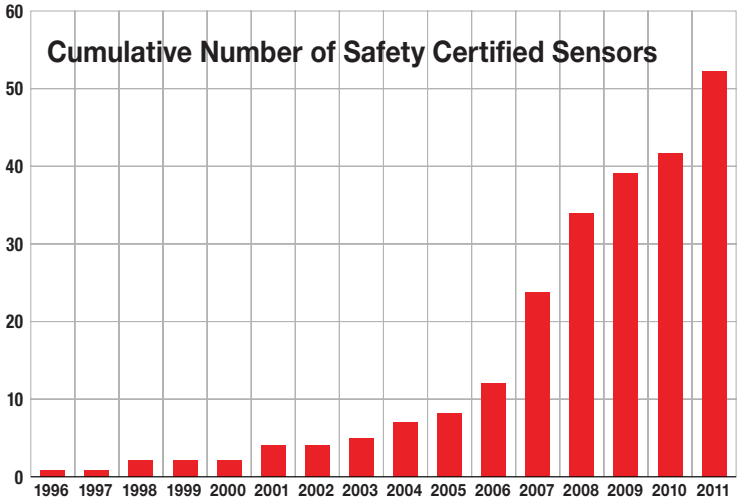


Figure 3: The offering of certified sensors continues to grow.

justified. While all sensor devices must be evaluated for any specific application, choosing equipment that 'meets the requirements of IEC 61508" is a common way to justify sufficient safety integrity performance. If not using safetycertified sensors, IEC 61511 allows an end user to perform his or her own proven-in-use justification. With a proven-in-use justification, the burden is placed on the end user to audit the vendor's design and quality assurance processes, to review manufacturer documentation of failure modes and failure rates, as well as to gather evidence of suitability by documenting the operating history in similar applications in other plants.

SIS designers choose safety certified sensors rather than doing a proven-in-use justification for a number of reasons, including:

- **Assuring that the product has high design reliability and safety**
- **Avoiding the burden of ven dor design and manufactur ing audits**
- **Reducing effort and cost for safety-system design (SIL verification)**
- **Reducing risk and potential liability from application of the product**
- **Regulatory agency prefer ences or demands IEC 61508 certified products, and**
- **Avoiding the recording of operating hours and analy sis of all repairs and failures.**

Without complete plant maintenance records, especially proof-test-as-found condition records, a designer would have difficulty providing documented trouble-free operating history from his or her plants. As a proven-in-use justification means taking responsibility for the reliability and safety of a sensor, high-quality data is important. Some will prefer to avoid the burden of vendor auditing and the documentation of those audits. Beyond just the safety integrity issue, other process operators specify safety sensors to get the assurance of high levels of design quality and reliability. There are regulations in some countries that indicate safety-certified products must be used in certain applications.

Certification of device manufacturers

When the functional safety standards were written in the late 1990s and early 2000s, the safety certification concept was in its developing stages. While several PLC products were IEC 61508 safety certified, there were fewer sensor devices at that time. The E+H Liquiphant Fail-Safe, a tuning-fork level switch, was safety certified per the German VDE0801 / A1 standard in 1996. The first safety-certified sensor per IEC 61508 was the 345 pressure transmitter from Moore Products in 1998. Over time, additional sensor devices passed the tough requirements with strong growth, which began in 2006. Today there are a number of safety-certified sensor devices for almost any process variable from every major instrumentation manufacturer. Figure 3 shows a cumulative count of the number of safety-sensor devices. A list of safety-certified devices, including sensors, is maintained on the Safety Automation Equipment List (www.sael-online.com). This list is updated regularly as new certifications are added from a variety of competent certification agencies, while obsolete products are removed.

Developing safer products

Developing products compliant with IEC 61508 is a rigorous and demanding process. Roughly 70% of the approximately 330 requirements for device-safety certification involve the design and test process. The clear objective of this level of attention is design quality. It is interesting to note that a majority of the requirements (about 200) relate to the software development process. Why is this? Remember that software was prohibited from safety applications by regulation in many countries

through the late 1990s. There is software paranoia in the nuclear industry that is still so strong that new custom designs implemented purely with hardware are continually being developed even when well-proven alternatives exist. The software engineering requirements of IEC 61508 are quite strong for SIL 3 capability, and most consider this appropriate as it seems so easy to write software without sufficient testing. Yet some question the need for all this attention of software engineering in a simple sensor device. This thing is called a 'smart" pressure transmitter, but could the software really be that complicated? Some ask, 'Could this pressure transmitter that fits in my hand possibly be as complex as the rack of equipment in the safety PLC cabinet?"

Roughly 70% of the approximately 330 requirements for device-safety certification involve the design and test process. The clear objective of this level of attention is design quality.

No one questioned the need for safety certification of PLC products in the late 1990s. The PLC software designs were somewhat complex and appropriately perceived as such. One design example had software with two primary execution tasks: logic solving and communications. A rough idea of design complexity is given by the size of the processor and memory. A 1990s safety PLC did logic solving with a 16-bit microprocessor with four megabytes of memory. In the 2010s many sensor designs are much more complicated than the old PLCs. Today's sensor designs use multitasking operating systems with 32-bit microprocessors and larger memories. The sensor devices take full advantage of this processing power to provide high-speed statistical analysis of the process variable, much better automatic self-diagnostics, and more features. Given that the complexity of the new 2010-era designs is greater than ever.

No safety without security

According to IEC 61508, if a security threat is seen as being reasonably foreseeable, then a security-threats analysis should be carried out. If security threats are identified, a vulnerability analysis should be undertaken in order to specify security requirements to be incorporated into the design. The ISA Security Compliance Institute (ISCI) has developed a program for security testing and certification of critical control system products with an Ethernet connection, such as PLCs, digital-protective relays, communication modules, and even sensor devices. The program, called ISA Secure, utilizes test specifications and protocols developed from publicly available sources such as the ISA-99 industry standard. With the occurrence of the Stuxnet virus, and the potential of Stuxnet-like attacks in the future, there has certainly been great attention drawn to the importance of control-system cyber security. Thus cyber security has become part of the safety certification process in some certification bodies.

Certifying the certifiers

The IEC 61508 functional-safety standard requires a level of independence in the assessment of functional safety that varies according to the SIL level. However, it does not require any specific accreditation, even for SIL 3 or SIL 4, as is required in the electrical safety standards. The IEC 61511 standard even uses the words 'meets the requirements of IEC 61508" rather than using the term 'certified." Therefore, we can conclude that anyone could perform a functional safety evaluation of a sensor device per IEC 61508. As a practical matter, IEC 61508 is a large, complex document. The technical depth required to understand the issues is quite high, and this is recognized by the market. Therefore, purchasing specifications of major end-user companies routinely contain language indicating the competency required or even which specific certification agencies are accepted.

While self-certification by a manufacturer is not prohibited by the standard, few have followed this path as they recognize the market demand for an accredited test laboratory/ certification body with the technical skills beyond traditional electrical safety.

Certification agency accreditation is done per IEC Guide 65 (EN45011), which has requirements for the operation of a product certification program, and ISO 17025, which has requirements for a test laboratory. Technical competency is evaluated for each area of certification (e.g., functional safety, cyber security, electrical safety, etc.). Accreditation is done by an organization in each country that is governmental or quasi-governmental. In the U.S., for example, accredita-

Failure analysis starts with single components but also looks at various combinations as well as diagnostic capabilities.

tion is done by the American National Standards Institute (ANSI).

Path forward

It is not hard to imagine functional safety certification becoming a standard part of sensor devices. Hazardous area approval was an option in the early days of electrical safety standards. Today it is difficult to buy any field device without a hazardous area rating. As more and more devices are achieving functional safety certification, more manufacturers are making functional safety a standard part of the product development process. Functional safety will likely be a standard attribute of sensor devices in the future. This is indicated by one advertising campaign for a pressure transmitter product recently that said, 'Safety is not an option." Every device produced has the rating. This should provide a good return on investment as design quality improves and fewer mysterious field failures occur.

William Goble, PhD, is principal engineer and director of the functional safety certification group at exida, an accredited certification body. His doctorate is in quantitative reliability and safety analysis of automation systems.

Online:

Find more information about safety sensors at:

www.exida.com/certification

See a list of safety-certified sensors, logic solvers, final control elements, and more at:

www.sael-online.com

Dr Peter Clarke explains how process plants can benefit through proper and careful adoption of the IEC 61511 safety standard.

Process industry safety standard IEC 61511 and its parent, functional safety standard IEC 61508, have been in existence for several years now, and have enjoyed widespread acceptance as an effective method for managing high levels of industrial risk. Despite this success, some may view these standards as another complex, onerous burden imposed by regulators, with little tangible benefit to the end user. However, as we will explore in this article, the reality is far different.

The standards, which have grown out of industry needs rather than being imposed from outside, bring considerable benefits if applied properly. These benefits take the form of improved safety, cost-effective design and maintenance processes, and reduced downtime — all of which impact positively on the bottom line. Compliance also helps to demonstrate to the authorities that all reasonable precautions are being taken to prevent major accidents, as required by safety legislation nowadays.

Functional safety concept

The underlying need for IEC 61511 arises from the fact that processes involve major hazards, with significant potential to cause losses and harm. The risk of these undesirable outcomes is a function of both their severity – for example, how many people injured or killed, and how much damage and lost production – and their frequency, that is, how often such an event can be expected to occur.

We seek to control these hazards by reducing the risk to a tolerable level. How we do that is up to us, but it usually involves a range of measures, some engineering, some procedural, and some down to process technology.

But even after applying as many of these measures as we can, it is likely that a number of risks will still be too high. Simply loading up our plants with more alarms, relief valves and operating procedures will not resolve the issue; a law of diminishing returns applies, for reasons beyond the scope of this article. In such cases, we have to go to our next line of defence: active, automated trip systems, known properly as safety instrumented systems (or SISs).

Because of the weight of riskreducing responsibility placed on SISs, we must employ them with great care. There is no such thing as an off-the-shelf SIS, or a one-size-fits-all trip that we can simply install and forget. Each risk has to be matched with a customdesigned safety function from the SIS. If we don't design, install and maintain these correctly, they are more likely to fail on demand, trip when not required, or provide insufficient protection against the harm we are seeking to avoid. For the process industry, our guiding hand through the complex and challenging world of SIS is the international standard IEC 61511. It explains that our SIS needs our attention from cradle to grave – and even before the SIS arrives in the cradle, when we are still wondering whether we need to install a SIS at all.

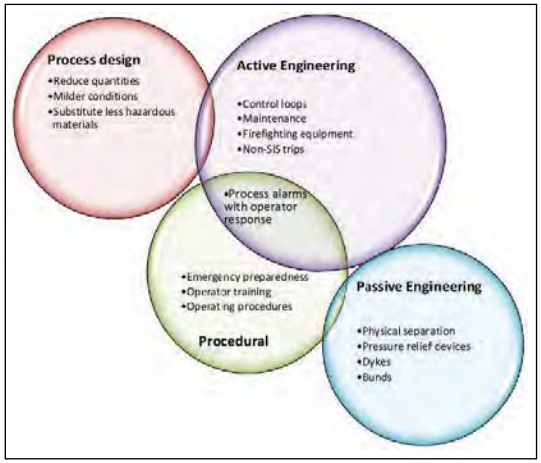
The standard addresses this lifetime care through the concept of a safety lifecycle. Broadly speaking, the lifecycle can be separated into three periods, in which we ask respectively:

- **Do I need a SIS, and if so, what type?**
- **How can I design a SIS to meet that need?**
- **When I'm up and running, how can I make sure the SIS keeps working?**

Examining the safety lifecycle

In the first lifecycle period, we analyse the risks involved in running the plant. First, we must decide how much safety risk we can tolerate; optionally, we can also consider other types of harm such as environmental damage, downtime, equipment damage and loss of reputation. Zero risk is not a meaningful

target, because it is unachievable – however much our top management team might like to believe otherwise. So, we have to set finite risk targets, as the basis for all our subsequent lifecycle activities.



Typical (non-SIS) measures to reduce hazards in process plants.

Next, we examine the process to identify all the causes of risk. For each event that can lead to unwanted outcomes, we have to determine the probable frequency of the event (for example, how many times per year) and the severity (for example, the cost of damage to the plant). We assign risk reduction measures – safety features like those depicted (left) – and decide how much additional protection is needed from an SIS.

For each intolerable risk, a safety function is defined, that is, an action to take when specified dangerous conditions are met. Based on this, we prepare a specification known as an SRS (we'll discuss this later). The SRS will document, among other aspects, how reliable each safety function must be, in terms of its probability of failure to act when required due to some random hardware fault. This safety integrity measure is defined in terms of a safety integrity level or SIL, which is a numerical value from 1 to 4.

In the second safety lifecycle period, we design an SIS to meet the specification. Hardware is selected; calculations are performed to ensure the hardware can achieve the specification; software and maintenance procedures are written; and extensive tests and checks are performed, both before and after the safety equipment is installed and commissioned. And then in the third lifecycle period, we operate the plant with the SIS in place. We document the performance of the SIS and the demands that are made on it by the plant (whether real events or spurious). We carry out the maintenance of the SIS as planned; and we carefully control every change to the SIS design through a management of change procedure (discussed in detail later in this article).

Control of design errors

So far, in our discussions of SIS reliability, we have implicitly considered only one type of failure: a random component failure, caused by natural degradation and/or unpredictable external stressors such as heat, cold and vibration.

In reality, another type of failure is just as important – in fact, even more so, in the case of tech-heavy equipment such as safety PLCs. This type is characterized by design errors, which may lie hidden like the proverbial snake in the grass until an unfortunate combination of circumstances conspires to bring it to full, ugly manifestation.

In instrumented safety parlance, these undesirable incidents are known as systematic failures, because they occur systematically whenever the right conditions exist. Some typical systematic failure types are listed in Table 1. A simple (non-SIS) example is a check valve (non-return valve) installed the wrong way round: on the day when a backpressure occurs, it's guaranteed to allow the reverse flow you don't want. In other words, its failure is deterministic: failure is determined only by circumstances, and is not dependent on random outside influences.

The approach to dealing with these two types of failure – random and systematic – is radically different. Random failures will always be with us, and can never be engineered away entirely. We see this in our own bodies: we get sick due to random outside influences, we have accidents, and our bodies eventually wear out and die. That's why we have health checks, preventative maintenance (do you brush and floss regularly?), and insurance. These have echoes in the maintenance strategies we apply in the operational third period of the safety lifecycle.

Systematic failures, on the other hand, can be eliminated by good engineering and management practices. Indeed, not only can they be eliminated, but they must be. Providing the methodology for dealing radically with the causes of systematic failure is one of the great strengths of IEC 61511.

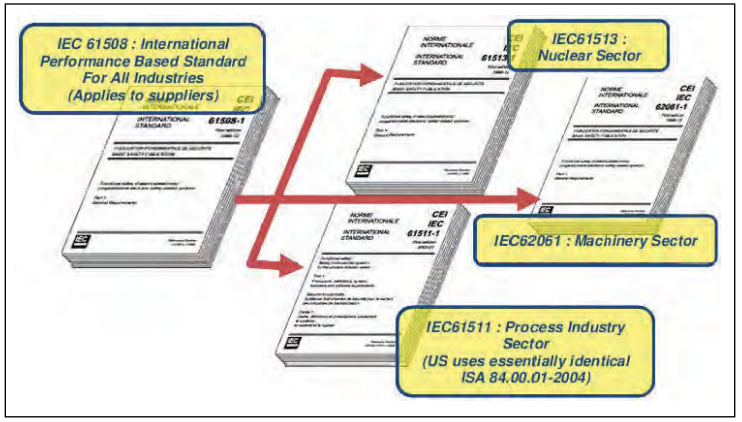
Multi-layered strategy

IEC 61511 develops a multi-layered strategy for tackling systematic failures. To understand this, we can divide our focus into three main concepts: components, SIS design, and project management.

At the component level

IEC 61511 requires us to take steps to eliminate design errors in the components of our SIS. This can be done in one of two ways: either we buy components whose design and construction methods are proven adequate (the SIL certification route), or we select components with a good track record (the prior use or proven-in-use route). Getting SIS components such as sensors, valves and safety PLCs SIL-certified is usually the responsibility of the equipment manufacturer. The requirements for SIL certification are detailed in IEC 61508, which is the 'mother standard" of IEC 61511 (and of other sector-specific standards dealing with safety instrumented systems, such as IEC 62061 for the machine industry).

More and more equipment vendors are recognising the value of SIL certification; it generates an easy pathway for end users to justify selection of their equipment, and also provides assurance of the quality of their manufacturing and design processes.



The requirements for SIL certification are detailed in IEC 61508, which is the "mother standard" of IEC 61511 and other sector-specific standards dealing with safety instrumented systems.

SOFTWARE-RELATED	HARDWARE-RELATED
Bugs in the application software	Unsuitable for process or physical environment
Errors in user programming	Wrong material of construction
Software bypasses left in place	Manufacturing flaws or errors
Out of date versions or version mismatches	Incorrect installation
Inadequate training or bad information provided to operators	Hardware bypasses or forces left in place
Inadequate training or bad information provided to maintenance personnel	Wrong specification in SRS (e.g. due to poor risk analysis)
Miscalibration	Design does not meet specification in SRS
Wrong set point or other parameter	Equipment not installed according to design
Confusion over engineering units	Equipment limitations (as listed in safety manual) not complied with
Uncontrolled changes	Uncontrolled changes

Table 1: Typical systematic failures.

SIL certification services are provided by a handful of independent auditors, including TÜV Rheinland, TÜV Nord and Exida. The latter also maintains a Safety Automation Equipment List, which is available for consultation online (www.sael-online.com), and is also built in to the risk analysis software exSILentia. When a product is SIL certified, the certificate will specify the maximum SIL that is achievable by any safety function using that component. All the data required to quantify the reliability of the safety function should also be provided, either in the certificate or in the associated assessment report, and many other sources of failure rate data are available.

Prior use, the alternative, and generally more arduous, approach is for individual users to show that the components perform as well as expected in real applications. The standard does not define exactly how much history is required, but typically the minimum requirement for SIL 1 will be for 100,000 operating hours and 10+ items in different applications over at least one year, with failure rates no worse than those predicted by theoretical calculations. The higher the intended SIL of the proposed application is, the more prior use evidence is needed.

Prior use data need not necessarily refer only to safety applications; non-safety applications, such as basic process control systems, can also be taken into consideration. Crucially, however, the standard does require that the historical data be demonstrably relevant to the intended application. In practice, this means the item must be essentially exactly the same as the ones used before – in particular, the revision number of any built-in software must match; and the components must have been used in 'similar operating profiles and physical environments", in the words of IEC 61511.

IEC 61511 demands proper management of every activity undertaken, from first concept to final disposal of the safety equipment.

Proving this is often a major stumbling block to the successful deployment of prior-use justification. Clearly, it also depends critically on the quality of reliability data collection – a topic we will return to later.

Because of these challenges, many users are inclined to default to the use of SIL certified components for all SIS applications. However, this is not always the best strategy. Sometimes it is better to stick with the equipment you already know well, if it has been performing incident-free in your application for many years. There are several reasons for this:

- **Your technical personnel are already familiar with it, and are therefore less likely to make mistakes during installation and maintenance.**
- **Fewer different models of equipment onsite means fewer spares and, again, reduced likelihood of errors.**
- **You already know, from direct experience, what its performance limitations are – for example, how long it lasts before wear out in your specific plant environment.**

Thus, users should not rule out the 'prior use" route, despite its difficulties. And software tools such as exSILentia are available to help with the process of developing prior use justification.

At the SIS design level

Compliance with IEC 61511 helps us to eliminate design errors in the SIS itself. Again, there are two aspects to this, both of which run like a mantra throughout the subtext of the standard: designing it right, and documenting it right.

First of all, let's look at designing it right. Because IEC 61511 places a heavy emphasis on upfront risk analysis, it compels us to make sure we really understand the demands we are making of our safety functions. Historically, improper specification is known to be one of the major factors that can lead safety functions to fail in their objective of preventing accidents. Getting to a correct specification requires us to go meticulously through a thorough risk analysis process, with all of its attendant benefits.

Up to this point, we know what our risk reduction target is. The next crucial step is to ensure our design can achieve it. IEC 61511 once again drives this process by requiring a calculation of the theoretical risk reduction achievable by our design, long before we ever go on site to install the hardware. The calculation is not trivial to perform, and can be delegated to outside consultants, but suitable software tools – even for highly complex safety functions – are also available.

As for documenting it right, today's large projects are becoming more and more subdivided and distributed among different contractors – a process which, whilst it has its advantages, can lead to communication breakdown and nebulous responsibility. The ultimate consequence can be disastrous, as numerous process plant disasters have shown.

To address these issues, IEC 61511 places a strong emphasis on effective documentation at every stage of the safety lifecycle. In particular, it requires the creation of a document known as the safety requirements specification (SRS), which we met briefly earlier.

The SRS is first generated when the requirement for a SIS has become clear, and the target performance specification of the SIS is known – for example, how much risk reduction it should provide, what hazards it is designed to address, and what it must do to prevent harmful outcomes when those hazards arise. Later in the design process, the SRS is revised to include specific details of the hardware that will be used to realise these objectives.

The SRS is a critical document in the safety lifecycle, for many reasons, but particularly because:

- **It provides a touchpoint for all parties involved in the safety**

lifecycle, whether they are designing, constructing, commissioning, maintaining, or modifying the SIS.

- **It defines a benchmark against which the performance of the safety lifecycle is measured. This applies to every aspect of the life cycle. For example, designers must check that their designs match the requirements of the SRS; maintenance personnel must ensure they carry out the maintenance as detailed in the SRS; and operational management must confirm that the real-world situation (magnitude of the risks and performance of the SIS) matches the assumptions made in draw ing up the SRS. All of these checks are explicitly demanded by the standard.**

Thus, the SRS serves as a hub for validation of all subsequent lifecycle activities. Compiling an effective SRS is an onerous task but, as with many other aspects of lifecycle activity, consultants and tools are available to help.

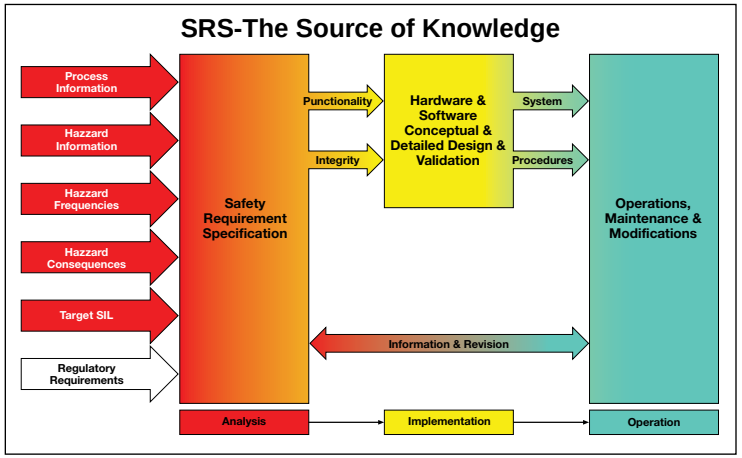
At the project management level

In parallel with all the phases of the safety lifecycle, IEC 61511 demands proper management of every activity undertaken, from first concept to final disposal of the safety equipment. There are many aspects to this – competency requirements, planning, and documentation control, to name a few – but, for our purposes, we will focus on two particular aspects here: confirmation that the lifecycle is doing its job in delivering safety, and management of change.

Confirming lifecycle performance is not a new concept to those familiar with ISO 9000. Not only must procedures be followed, but they must be shown to be followed. Not only must procedures be written, but they must be shown to achieve the objectives for which they were designed. Not only must quality be pursued, but it must also be achieved in real life. Not only must we say it, but we must also prove we do it (and know how to do it).

These four axioms of quality management are right there in IEC 61511, too. In the safety world, they are referred to respectively as Verification, Validation, Functional Safety Assessment, and Auditing. They may seem tough, but they allow us to reap rewards by getting it right the first time, and ensuring all the mistakes are found while they exist only in ink, and not in hardware – or in disasters.

Because the standard is performance-based, it does not impose many specific, prescriptive demands on our plant design, or on the process by which we achieve that design. Thus, we can develop a safety management strategy that suits our own corporate culture and framework. It is not necessary to develop a whole extra tier of paperwork to manage the safety lifecycle; integrating the lifecycle requirements into our existing procedures for planning, design, construction and maintenance is just as acceptable.



A critical document, the safety requirements specification (SRS) provides a touchpoint for all parties involved in the safety lifecycle.

For the second aspect, there is nothing extraordinary about requiring a management of change (MoC) procedure in an operating plant. What is noteworthy is the thoroughness of the MoC approach required for IEC 61511 compliance.

Indeed, it is at this stage that the cyclic nature of the lifecycle becomes most apparent: for the MoC strategy demands that we analyse all the possible effects of any changes to the plant, however trivial, and, if necessary, revert to an earlier stage of the lifecycle. Thus, we may need to revisit and revise our risk analysis steps, SRS, design, and/or maintenance procedures. Again, the value of excellent documentation is highlighted: if we took the trouble to write everything up properly the first time around, the impact of plant changes will be that much easier to evaluate later.

Demanding a thorough analysis of the impact of potential

changes is a good discipline that chokes off the cause of many accidents. For example, the terrible disaster at the Flixborough chemical plant in the UK in 1974, which cost 28 lives, could have been avoided by proper MoC. Another benefit of rigorous MoC procedures is that they shouldprevent the 'stealth" changes that gradually insinuate their way into a plant over time: set points changed, trips overridden, and hardware bypassed. They should spell the end of unforeseen impacts due to staffing reductions, loss of experienced staff, and temporary fixes left in place for months.

Because the standard is performance-based, it does not impose many specific, prescriptive demands on our plant design, or on the process by which we achieve that design.

Thorough attention to design integrity provides the only viable way to eliminate systematic failures, which can otherwise take out an entire safety system in one step. Detailed management of the design process ensures costly errors are eliminated before purchase orders are written for pricey safety hardware. Finally, the rigorous discipline of planned, appropriate maintenance procedures and scrupulous management of change are practically guaranteed to pay for themselves in reduced downtime and enhanced safety.

Bottom line benefits

So what is the benefit of adopting an IEC 61511 approach to functional safety? The short answer: it pays. Properrisk analysis avoids dangerous under-engineering that leaves a plant vulnerable to huge losses; it also cuts back on over-engineering, often paying for itself many times over in reduced upfront and maintenance costs, not to mention significant gains in operational uptime.

IEC 61511 helps you win all of these benefits through its integrated approach to instrumented safety, which you will be able to enjoy for the entire lifetime of your plant.

The author, **Dr Peter Clarke,** Senior Safety Consultant, Exida Asia Pacific, welcomes comments or questions in response to the article; please email peter.clarke@exida.com.

All respondents before 31 December will receive a free full color A2 sized poster of the safety lifecycle. And the first five respondents will receive a complimentary copy of the book *Safety Integrity Level Selection* by **Ed Marszal** and **Eric Scharpf.**

For process plant owners, through its integrated approach to instrumented safety, IEC 61511 can pay for itself many times over.

Is your current safety system compliant to today's safety standard?

By Luis M. Duran

It is estimated that about 66% of the Programmable Electronic Systems (PES) running in the process industry were installed before the publication of today's commonly used safety standards (IEC 61508 and IEC 61511/ISA 84)

Some of those safety systems, particularly the ones installed between the late 1980's and early 2000, are either

1. **General-purpose PLCs,**
2. **Not designed or certified according to the IEC 61508,**
3. **Might not satisfy current requirements on IEC 61508**

In some cases they were not implemented according to ISA84 or IEC 61511.

This whitepaper covers the changes in the safety standards affecting those systems, a follow up whitepaper will address the safety life cycle activities involved in modifying or decommissioning an existing system to install certified Safety Systems according to today's standards.

What is the issue?

The economic growth of heavy regulated industries such as Oil & Gas and Power, increased demand for energy from BRICs

economies, particularly China and India, and the increased acceptance of international functional safety standards, especially after major incidents are driving the growth of the Safety Automation Market in the Process Industries, growth estimated in 9% CAGR.

This trend is likely to continue for the process industries (which include non-nuclear power, chemical, petrochemical, refining and oil & gas production) as about 66% of the Programmable Electronic Systems used in safety applications were installed between 11 and 30 years ago; before ISA 84, IEC 61508 or IEC 61511 were issued and recognized as good engineering practices. The same source indicates that many users have extended the lifespan of their system beyond their supplier's obsolescence notice.

Additionally there are many relay-based safety systems that missed the initial wave of automation or were left alone as installing a digital electronic programmable system was not economically feasible for the plant in those applications at the time.

Prescriptive vs. Performance Base Functional Safety Standards

The international Functional Safety standard IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems is a general standard applicable to multiple industries. In addition to IEC 61508, there are industry specific standards. For the process industries, the applicable international safety standard is IEC 61511; ISA has adopted IEC 61511 in their latest revision of ISA84. Although there are similar changes affecting the machinery safety standards, this paper will only cover the process industries and IEC 61511.

IEC 61508 and IEC 61511/ISA 84 are known as performance based safety standards, contrasting with previous standards that prescribe the type of protective functions needed to reduce risk, performance base standards require an analysis of the hazards associated to the process, the risk reduction alternatives and the determination of the performance needed to reduce risk to an acceptable level.

Grandfather clause

The concept of the 'grandfather clause" in ISA-84.01-2004-1 originated with OSHA 1910.119. The grandfather clause's intent is to recognize prior good engineering practices (e.g., ANSI/ISA-84.01-1996) and to allow their continued use with regard to existing Safety Instrumented Systems.

According to ISA-TR84.00.04-2005 Part 1 Guidelines for the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511 Mod) 'For existing SIS designed and constructed in accordance with codes, standards, or practices prior to the issuance of this standard (e.g.,ANSI/ISA-84.01-1996), the owner/operator shall determine that the equipment is de-

signed, maintained, inspected, tested, and operating in a safe manner."

The Technical Report highlights two essential steps:

1) **Confirm that a hazard and risk analysis has been done to determine qualitatively or quantitatively the level of risk reduction needed for each SIF in the SIS.**
2) **Confirm that an assessment of the existing SIF has been performed to determine that it delivers the needed level of risk reduction.**

According to ISA-TR84.00.04-2005 Annex A.2. , if those activities have not been done, they should be scheduled for review at the 'next appropriate opportunity" which mean if any of the following conditions is met:

- **Modifications to the process unit that impact process risk managed by the SIS;**
- **Modifications to the control system that impact protection layers used to achieve safe operation;**
- **When an incident or near miss investigation has identified an SIS deficiency; or**
- **When the review of another process unit designed according to similar practice has identified an SIS deficiency.**

Where are the Safety Certificates?

In reviewing project specifications during the bidding phase of a project, it is common to find ISA 84 or IEC 61511 as a requirement of mandatory compliance. Compliance to IEC 61511 implies more than a certified system, particularly at the time of design and implementation. On the subject of PES, this standard requires that components and subsystems selected for use in SIL 1 through SIL 3 shall either be designed in accordance with IEC 61508-2 and IEC 61508-3 or comply with the 'Proven-in-Use" criteria. Additionally, the system programming tool should use Limited Variability Languages, defined in the standard as 'software programming language, whose notation is textual or graphical or has characteristics of both, for commercial and industrial programmable electronic controllers with a range of capabilities limited to their application" .

As the reader might anticipate, the majority of the Programmable Electronic Systems used before 1995 were not certified to the same criteria as those released to the market over the last ten years, legacy systems are likely to be general purpose systems (i.e. standard PLC) or an early version of Safety PLCs/Programmable Electronic Systems (First Generation Safety Systems).

Proven-in-Use

In order to keep using a system that is not certified according to IEC 61508, the user must demonstrate 'Proven in Use" and such demonstration shall include:

1. **The manufacturer's Quality Management system**
2. **Adequate identification and specification of the components and sub-systems**
3. **Demonstration of the performance of the components or sub-systems in similar operating profiles and physical environments**
4. **The volume of operating experience**

The documented evidence shall demonstrate that the likelihood of any failure of the subsystem is low enough so that the required safety integrity level(s) of the safety function(s) is achieved.

Certified to IEC61508

If the system has an IEC61508 certification, then it's important to understand the criteria used by the third party assessor for issuing such certification to a First Generation Safety System. The IEC 61508 standard recognizes the following four criteria in the assessment of a Safety PLCs/Programmable Electronic Systems:

- **Hardware Safety Integrity**
- **Behavior in presence of failure**
- **Safe Failure Fraction**
- **Systematic Capabilities**

Most First Generation Safety Systems were certified on the basis of the Hardware Safety Integrity which is related to redundancy and behavior in presence of failure, and these two concepts were sufficient

to describe their performance that at the time included few and maybe limited software diagnostics. Many of these systems used Relay Ladder Logic as a programming language which was a representation relay based logic and useful at the transition point between said technology and the emerging digital systems.

Safe Failure Fraction (SFF) and Systematic Safety Integrity are new terms for many users, particularly Systematic Capabilities is a new concept that many of the First Generation of certified systems today do not support and is a requirement gaining more visibility in the new edition of IEC 61508 published in 2010.

To release a certified system following the new revision of the standards, the vendor needs to start by establishing a Functional Safety Management System (FSMS) and having the development organization certified by an independent assessor. The FSMS requires the design process to document and track functional requirements, review functional specifications and test against requirements and validate performance and results during the development of the product. Every step needs to be properly documented; the competence of the personnel involved in each step is also documented.

It might be easier understand for the reader if the FSMS is compared to a Quality Assurance process, it will be difficult, if not impossible, to assure or even test performance if the performance criteria is not well defined and documented.

Over time it will be very challenging for a product vendor to certify a system to the latest revision of IEC61508 if their development organization was not previously certified and if their design practices lack the FSMS and the document trail explained in the previous paragraphs.

The reader is probably familiar with the discussions around the architecture of Programmable Electronic Systems used in safety applications as the majority of First Generation Safety Systems used redundancy (Hardware Safety Integrity) to satisfy the requirements of Low Demand Applications commonly found in the process industries.

Product Developers in the Safety Automation market might adopt different design methodologies, but current Functional Safety standards encourage the use of software diagnostics and diverse technologies.

Diverse Technology

As indicated by this author in previous publications , technology has evolved to a point in which there are multiple options to address a similar technical problem. For example, by selecting two or more of these technologies, diversity can be embedded in the system design.

Examples of diverse implementation include using different operating systems and then using different teams to develop the software on multiple cooperating modules, or combining two different technologies (such as Micro Processor (MPA) or Micro controllers and Field Programmable Gate Arrays (FPGA)) to perform the same functionality in parallel to each other. Unlike traditional redundancy, by applying diverse technologies, the design achieves a redundancy scheme with minimum or no common cause failures.

IEC 61508 Edition 2

There are other concepts added to IEC 61508 Edition 2 that might affect compliance and should be considered when choosing a PES. This paper will concentrate only on the following three areas, but the author encourages the reader to seek additional information on the topic.

1. **Systematic Capabilities**
2. **Competence**
3. **Security**

Systematic Capabilities

Today, it's well understood that a system can be designed following a very strict development process, using a rock-solid Functional Safety Management System and even certified by the best independent authority, yet the system can be programmed in a way that disables its safe action under some conditions. Systematic Capabilities should assist in the assessment of the programming tools to avoid this kind of situation.

Systematic Capabilities is a concept developed to replaces the term: 'effectiveness against systematic failure" and is a measure (on a scale of 1-4) that the systematic safety integrity of an element fulfills the given safety function, considering the instructions stated in the product safety manual.

Competence

Competence has been recommended in the previous edition of the standard, however it is now of mandatory compliance (normative). The following are the requirements:

1. **Organizations involved on safety system projects or activities shall appoint one or more persons with responsibility for one or more phases of the Safety Lifecycle (per IEC61511)**
2. **All persons, departments or organizations shall be identified, the responsibilities clearly defined and communicated**
3. **Activities related to management of functional safety shall be applied at the relevant phases**
4. **All persons undertaking specific activities shall have the appropriate competence**
5. **The competence shall be documented**

Competence is particularly critical in the Management of Functional Safety and in the case of a Functional Safety Assessment which in addition to competence may require independent individuals or departments depending on the consequence of the hazard.

As concerning as the competence requirements may sound, it's important to highlight that there are competent resources available worldwide, either as independent consultants or associated to product vendors and available to support throughout the implementation of the safety lifecycle.

Security

Infrastructure Security and Network Security have been the subject of several papers and blogs. The targeted attack of the Stuxtnet worm in 2010 , confirmed the industry concerns. The subject is recognized in the revision of the standard, not in the application specifics or to specify the requirements needed to meet a security policy that may be required, but consider potential security threats to be added to the safety requirements.

Section 7.4. (Hazard Analysis) of the IEC 61508 standard, requires that in the case the hazard analysis identifies that malevolent or unauthorized action, constituting a security threat, is reasonably foreseeable, then a security threats analysis should be carried out, followed by section 7.5. (Overall Safety Requirements) where it recommends that a vulnerability analysis should be undertaken in order to specify security requirements.

Summary

This whitepaper explains some of the changes in the Functional Safety standards IEC 61508 and IEC 61511/ ISA 84 and identifies the key elements to assess if a safety system installed the late 1980's and early 2000 meet the certification requirements for applications in the process industries.

An existing installation is only covered by the ISA84 'Grandfather Clause" if the owner/ operator can demonstrate that the equipment is designed, maintained, inspected,

tested, and operating in a safe manner.

Some of the systems running today might not be certified according to IEC61508, if that is the case and according to IEC 61511 those systems should comply with the 'Proven-in-Use" criteria, which requires the user to demonstrate using documented evidence that the likelihood of any failure of the system is low enough so that the required safety integrity level(s) of the safety function(s) is achieved.

For those systems certified to the first edition of IEC 61508 only on the basis of Hardware Fault Tolerance (i.e. redundancy and architecture), there are technical challenges that might limit the ability of those system to retain that certification when the industry moves to IEC61508 Edition 2, this will occur on the next product release cycle for those vendors.

In addition to criteria such as Hardware Safety Integrity, behavior in presence of failure, Safe Failure Fraction (SFF) and Systematic Capabilities; the latest revision of IEC 61508 (Edition 2) introduce additional criteria such as security and increased the importance of systematic capabilities and competence.

Competence was made normative in the latest revision of the standard, this requires organizations involved on safety system projects or activities to appoint one or more persons with responsibility for one or more phases of the Safety Lifecycle (per IEC61511) and the adoption of a Functional Safety Management System.

The follow up whitepaper will address how to start an assessment of your existing safety instrumented system and the safety life cycle activities involved in modifying or decommissioning an existing system to install certified Safety Systems according to today's standards.

Luis M. Duran
TUV FS Eng# 902/07
Product Marketing Manager
Safety Systems
ABB
Houston, TX
e-mail:
luis.m.duran@us.abb.com

Visit ABB's Process Automation Insights blog to join the conversation at http://www.processautomationinsights.com/