Functional Safety in High-Volatile Applications

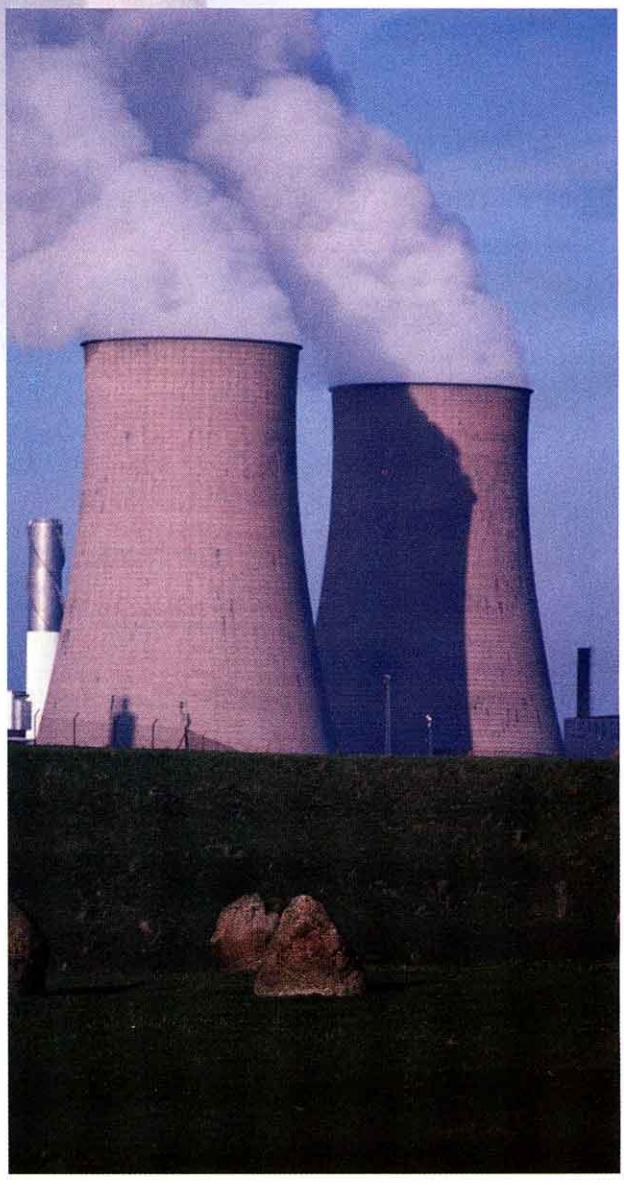
KRISTINA L. BALOBECK

With IEC 61508, manufacturers can ensure the functional safety of all aspects of a product's life cycle.

I use my computer for everything, from generating a white paper to conversing with our office in the UK. Sometimes, however, I make the mistake of having too many windows open, not saving properly, or committing some other fatal error. To recover, I hit the Control, Alt, and Delete keys simultaneously, and after a few moments, I can navigate back to the task. When this fails, I simply reboot the computer and start over. I accept such inconvenient errors as a regular part of using a computer.

Such a "reset mentality" might be used on the copy machine, the coffeemaker, or even a state-of-the-art laser printer. But what about the software and instrumentation on an airplane or in a nuclear power plant? In these applications, there simply is no reset button as an option when the safety reliability of hardware and software is so critical.

An electrical and electronic device must undergo a rigorous battery of tests to ensure that the product has been properly manufactured and can withstand the application's demands. However, such testing is focused solely on the end-product test data, not on other phases of the life cycle such as design or the manufacturing or even the individuals responsible for designing, manufacturing, and installing the product. Although manufacturers' specifications provide pertinent information, the assumption is that each manufacturer consistently produces exact duplicates of the tested product. Many facilities that maintain unstable applications implement standards and methods to prevent a hazardous event or to minimize the effects should one occur. A recently released safety standard extends this evaluation process. The new standard encompasses all aspects of the product's conceptualization, development, manufacturing, and testing of components. This broader scope ensures that each product is fully compliant—not just a specific unit sent to a testing facility.



Safety Systems

As technology has evolved, so have the capabilities of safety systems. However, the sophistication of instrumentation hardware and software has evolved much more rapidly than measures to ensure safety and reliability. The electronics

industry faces the difficult challenges of proving that software is correct when used in safety applications and that it explicitly matches the specifications provided by the manufacturer.

In response to these challenges, the International Electrotechnical Commission (IEC) initiated two studies on the functional safety of electronic systems. One study focused on system hardware, the other on software. IEC combined these two studies with the goal of developing a standard to guide the design and development processes of software and hardware in electronic systems. In 1995, a draft standard, IEC 1508, emerged that provided a risk-based approach to identifying safety requirements in a system. Further feedback was accepted on that draft and by 2000, IEC announced the release of international standard IEC 61508.

Formally titled "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems," IEC 61508 is a seven-part standard that directs the life cycle and all components of a safety instrumented system (SIS). IEC 61508 is an umbrella standard. It can be applied directly to any industrial process that uses electrical, electronic, or programmable electronic products and systems for safety. Industry-specific standards may be further developed, provided they follow a safety life cycle model similar to the one defined by IEC 61508. Currently, IEC 61511 is being developed for designers, integrators, and users in the process sector.

European nations, especially the UK, have already heartily embraced IEC 61508 and are realizing the benefits. The perspective of most plant managers is that IEC 61508–certified instruments greatly decrease or eliminate the likelihood that a hazardous event will occur. So, in addition to protecting personnel, the plant, and the environment, IEC 61508 can actually increase efficiency and improve a plant's bottom line.

Even one minor plant shutdown can result in exorbitant repair and replacement costs to the plant and equipment. A shutdown causes a major loss in production time and creates additional expenses for mitigating the situation and getting the plant running again. By implementing IEC 61508, the need for system verification is minimized, and plants can actually reduce procurement costs by avoiding reassessment on a product-by-product basis. Ultimately, plant managers that rely on equipment certified to IEC 61508 are confident that the safety of personnel and the facility are not compromised.

The Road to Certification

A manufacturer seeking IEC 61508 certification is assessed by a third-party certification company. This certifying body applies a framework to certify the manufacturer to IEC 61508.

IEC 61508 certification is a substantial undertaking, but quite a significant one. Unlike a product certification that involves a specific portion of a company for a brief period, committing to IEC 61508 affects the corporate structure to a much broader extent with a change that is permanent. A new functional safety management system must be established within the company that encompasses quality assurance, configuration management, project management, and functional safety assessment. Many organizations lack the staff and monetary resources to successfully obtain certification. A company that is contemplating IEC 61508 certification should be fully aware of the necessary investment. It is important to assess the organization to determine whether IEC 61508 certification would be feasible and beneficial.

Moore Industries (North Hills, CA) was the first U.S. company awarded IEC 61508 safety certification to design and manufacture process instrumentation hardware for safety-related applications. Although eager to enhance its commitment to safety, the company took steps to determine whether

European nations have already heartily embraced IEC 61508 and are realizing the benefits.

it was feasible to seek certification to IEC 61508. Questions included:

- Will this standard benefit our business?
- Are our customers ready to embrace this standard?
- Do we have all of the resources available to take on the arduous requirements of certification?

These questions had to be addressed before moving forward. Significant research was conducted within the company and within the marketplace. Formal discussions were held at the company's major locations worldwide, and extensive interviews were conducted with customers in industries most likely to apply IEC 61508–certified products. Based on the metrics and customer feedback received, certification was determined to be a viable option.

The company established a relationship with ABB Eutech (Warrington, Cheshire, UK) to manage on-site informational and training seminars about the certification requirements. In addition, Moore Industries set up a dedicated safety team. The team included a lead engineer, hired for his expertise in this field, and company personnel already very familiar with the company's processes and procedures. In addition, Moore Industries had already established ISO 9001 processes. With steps taken to ensure quality of documentation, competency of personnel, and so forth, ISO 9001 provided a solid foundation. This foundation eased the transition from a quality management system to a functional safety system with IEC 61508.

An Introduction to CASS

Currently, one of the most popular schemes is the conformity assessment of safety-related systems (CASS). This CASS guide provides specific criteria for a company to meet in order to obtain certification.

The CASS guide offers identifiable deliverables called targets of evaluation (TOEs). These TOEs are associated with the applicable causes for the specific assessment within IEC 61508. It was necessary to meet the criteria listed in four tables in the guide. The tables describe these TOEs. Eutech oversaw Moore Industries' step-by-step progress and advised the company on any modifications necessary to achieve the TOE objectives. For example, the very first TOE of the first table is called *functional safety management system.* The details of this TOE reference Part 1/6.2.1 and Part 1/6.2.2 of the standard. Its pur-

pose is to specify all of the management and technical activities that are necessary to ensure that the electrical/electronic/programmable electronic safety-related systems achieve and maintain the required functional safety.[1]

The first table in the CASS guide uses 18 TOEs to guide an assessor in the evaluation of a functional safety capability assessment (FSCA). The FSCA relates to the safety management system. It determines whether the company has the necessary safety management system (quality system such as ISO 9001) to support the safety life cycle. The FSCA must be successful before the remaining assessments can be performed.

The second table in the CASS guide uses 21 TOEs to guide the evaluation of IEC 61508, "Part One, General Requirements." This assessment pertains to systems integrators that are responsible for the overall safety function. Systems integrators may acquire components from suppliers to develop the overall safety function as an SIS.

The third table in the CASS guide uses 30 TOEs to help in the evaluation of IEC 61508, "Part Two, Requirements for Electrical/Electronic/Programmable Electronic Systems." This part pertains to component manufacturers of safety instrumented systems. A component is a safety-related product that performs part of a safety function.

The fourth table in the CASS guide uses 45 TOEs to direct the assessment of IEC 61508, "Part Three, Software Requirements." This assessment pertains to component manufacturers of SIS with software residing in the electrical, electronic, or programmable electronic systems, or software as a separate component in an SIS. It is important to note that software cannot be assigned a reliability number because software faults (miscalculates) and does not randomly fail. Software faults are systematic failures resulting from the software development processes. The company used IEC 61508 and the CASS guide as a basis for its safety procedures manual.

Making the Grade

Sira, a UK conformity assessment company, conducted a three-day evaluation of the company's new safety processes based on the standard and the CASS guide. The company's development process, manufacturing, quality assurance, personnel competency, management, and technologies were also closely examined. It was determined that the CASS requirements were met successfully and, therefore, the company was awarded IEC 61508 certification.

Conclusion

It is important to understand that when a manufacturer obtains IEC 61508 certification, the company's existing products are not IEC 61508 compliant. Not all phases of the existing products' life cycles were developed according to the standard. However, a manufacturer can either initiate reappraisals and redevelopment programs of specific products, or simply introduce completely new products designed and manufactured according to the safety standard.

IEC 61508 makes it possible to verify that safety considerations were made at every phase of a product's life cycle. The standard instills confidence that a plant can run more efficiently and profitably without decreasing the levels of safety required to protect personnel, the facilities, and the surrounding community. With more manufacturers seeking certification, and an increase in the awareness of compliance benefits, IEC 61508 will become common on quotes for sensors, transmitters, valves, and other safety-related apparatus.

Safety Life Cycle

Most certifications primarily address the end product. IEC 61508, however, is process based and, therefore, encompasses all activities involved in the implementation of safety-related systems. Such activities begin with the concept phase of a project and finish when all of the electric, electronic, programmable electronic safety–related systems, other technology safety-related systems, and external risk-reduction facilities are no longer available for use.

Safety-Integrity Level. IEC defines four safety-integrity levels (SILs) to statistically represent the integrity of the safety instrumented system (SIS). An SIL takes into account device integrity, architecture, voting, diagnostics, systematic and common-cause failures, testing, operation, and maintenance. An SIL establishes an order of magnitude target for risk reduction. This target failure measure is the intended probability of dangerous mode failures to be achieved with respect to the safety-integrity requirements. The failure is specified in terms of either the average probability of failure to perform the design function on demand (for a low demand of operation) or the probability of a dangerous failure per hour (for a high-demand or continuous mode of operation). The higher the SIL, the greater the impact of a failure and, therefore, the lower the failure rate that is acceptable.

SIL	Continuous/High-Demand Mode of Operation	Low-Demand Mode of Operation
	Probability of dangerous failure per hour	Average probability of failure on demand
4	$\geq 10^{-9}$ to $<10^{-8}$	$\geq 10^{-5}$ to $<10^{-4}$
3	$\geq 10^{-8}$ to $<10^{-7}$	$\geq 10^{-4}$ to $<10^{-3}$
2	$\geq 10^{-7}$ to $<10^{-6}$	$\geq 10^{-3}$ to $<10^{-2}$
1	$\geq 10^{-6}$ to $<10^{-5}$	$\geq 10^{-2}$ to $<10^{-1}$

Table I. The higher the safety-integrity level (SIL), the greater the impact of a failure. SIL 4 = catastrophic community impact; SIL 3 = employee and community protection; SIL 2 = major property and production protection (possible employee injury); SIL 1 = minor property and production protection.

Reference

1. Conformity Assessment of Safety-Related Systems (CASS) Guide, The CASS Scheme Ltd., Chislehurst, Kent, UK, 2000.

Kristina L. Balobeck is the communications specialist for Moore Industries-International (North Hills, CA). She can be reached at 818-830-5543 or kbalobeck@miinet.com. ■