Fire and gas safety systems:
Conquering the complexities of functional safety products and systems certifications

Owners and operators of hazardous processes need their fire and gas safety systems to function at the highest safety levels. In this article, Jon D. Miller and Mark A. Gaalswyk of Det-Tronics Inc. look at ways to ensure this performance is assured.

In an industry governed by standards and certifications, it doesn't seem that caveat emptor should apply – but in fact, buyers do need to beware when it comes to selecting products for fire and gas systems used in hazardous locations.

It's not easy for a process owner or manager to identify and evaluate the compliance levels of fire and gas safety components or systems, even those that claim to be "certified" for functional safety systems applications. Components such as flame and gas detectors may have very different levels of compliance or certification, granted by different certifiers, each of which may or may not be accredited by an approved agency.

In addition, the standard or standards that a component must comply with may evolve over time. If the device in question has not been assessed against the latest version of the applicable standard, functional safety certification may not be granted. Even more complicated are situations where a product originally obtained a "proven in use" certification, because any changes to that product or system will require following the rigours of complete process certification to maintain certification.

This means hazardous process owners and operators must investigate and verify the compliance and certification claims for each component in their fire and gas safety systems, as well as the accreditation level of the certifying organisations involved. But what methodology should they use to make this assessment? Which certifier should a process or facility owner select? What matters in product certification? How can systems owners be confident they are purchasing and installing fully certified products – or selecting fully qualified companies to conduct proper and complete product certifications?

A good place to start is by defining some key terms.

Standard. An agreed upon description of what satisfies proper function and the associated requirements to be met. Standards use technical, verifiable language so local and international groups can establish best practice for an industry. IEC 61508 and IEC 60079-29-1 are examples of standards. Standards establish the minimum criteria of acceptability, and individual safety goals may set a higher standard.

Compliance. Establishes that a specific component complies with a given standard. In particular, under IEC 61508, by definition products are never "certified" as achieving a Safety Integrity Level (SIL) but rather are determined to be "compliant with" a SIL.

Certification. Establishes that a specific solution (product, service or system) meets the standard. Through an assessment, certification offers confidence that the solution is safe, functional, and will perform as expected. A functional safety certificate is issued to confirm the assessment was determined compliant. For valid certification, the product certifier must achieve accreditation to the standards used as indicated by the accreditation body logo on the certificate.

Product certifier. A group that has been accredited as able to assess and audit products, services and systems for public safety—meeting the standard—and therefore are able to properly provide certification. For example, exida is an accredited functional safety product certifier.

Accreditation body. A group that identifies and accredits companies that possess the necessary knowledge and rigour to certify function for solutions. They may also be the organisation that endorses the standard. The American National Standards Institute (ANSI) is an example of an accreditation body.

Standards are where everything starts

There are thousands of local, regional and national standards that apply to fire detection devices, ranging from basic electrical standards under Underwriters Laboratories (UL) and Canadian Standards Association (CSA), fire- and explosion-specific standards established by organisations such as Factory Mutual (FM), and functional safety-specific standards set by the International Electrotechnical Commission (IEC).

IEC 61508 defines the requirements for ensuring that systems are designed, implemented, operated and maintained to provide the required SIL. Four SILs are defined according to the risks involved in the system application, with SIL4 being used to protect against the highest risks. The standard also calls for a process that can be followed by all links in the supply chain so that information about the system can be communicated using common terminology and system parameters.

The specific safety integrity level (SIL 1, 2, 3 or 4) characterises the development requirements that must be met in order to achieve an overall risk reduction target. A risk assessment effort yields a target SIL, which thus becomes a requirement for the final system. The requirement informs how to set up the development process - using appropriate quality control, management processes, validation and verification techniques, and failure analysis - so that one can reasonably justify that the final system attains the required SIL.

As an international safety standards authority, IEC strives to anticipate safety hazards and develop requirements, processes and procedures that mitigate them. As voids and weaknesses in the code are identified or new issues and technologies emerge, requirements evolve to bridge the gaps, address the issues and improve the standard.

For example, IEC 61508 and 61511 standards present general requirements when it comes to certification. This has led to a variety of interpretations, and has opened the door to many forms of self-certification.

The global importance of Safety Integrity Levels has grown substantially in the oil and gas, petrochemical and other process industries over the last 10 years

Designing and implementing a fire and gas detection system for hazardous applications requires a custom solution tailored to the site's unique layout and certification needs.
Legend: 1. Addressable smoke and heat (ASH) module 2. Acoustic gas detector 3. Point gas detector 4. Safety system controller 5. Explosion-proof smoke detector 6. EDIO Module (process area) 7. Line-of-sight gas detector 8. Flame detector

SIL has evolved through various editions

Major modifications were introduced to SIL as it evolved from early editions in 1998 and 2000 to its most current edition, IEC 61508 Series (2010). Specifically, IEC 61508 Series (2010) changed or added several requirements, including:

Traceability. Specification must now provide details of a component's supply chain and document how a component relates to other components in a sub-assembly or integrated system.

Element identification and synthesis. IEC 61508 (2010) introduces the concept of "element" and defines it as the lowest level item from which a safety-related system is composed. This naming convention supports analysis of the consequences of combining or synthesizing elements, for example when two detectors work together to form a level of redundancy.

Redundancy of SIL 2 products and services no longer achieves SIL 3. It is no longer the case that functional system level certification can be achieved by applying redundancy to SIL 2 components and processes. The only way to achieve SIL 3 functional system certification is by using SIL 3 compliant components in conjunction with SIL 3 certified processes (with or without redundancy) or using redundant SIL 2 compliant components in conjunction with SIL 3 certified processes.

Treatment of no-effect failures. The FMEDA calculations used now require the exclusion of non-safety, "no-effect failures." A no-effect failure is the failure of a component that is part of the safety-related circuit, but which has no effect on the functional/system level when it fails. Under edition 2000, no-effect failures were considered safe and could be tallied as such for purposes of calculating the overall safety score. Under edition 2010, no-effect failures cannot be added to the safe side of the ledger for purposes of balancing out unsafe findings.

Electromagnetic compatibility (EMC) requirements. Electromagnetic immunity is of critical importance to functional safety, and is now mandatory rather than optional.

Component Compliance or Certification?

It is not uncommon to see safety components and devices such as fire detectors referred to as being SIL "certified." Technically, this is not only incorrect but impossible. SIL certification applies to functional safety processes at the system level and not to components contained in that system. When a device manufacturer refers to its product as certified under SIL, what they are really communicating is that the product has been evaluated against the appropriate set of requirements, has passed them, and is therefore "compliant" with IEC 61508. In effect, the product is "SIL capable," helping to contribute to the SIL certification of the system, in which the product is used.

Safety system component manufacturers are tasked with getting their products approved against the required standards for their products. They too must seek out certifiers, coordinate testing schedules and achieve appropriate compliance and certification endorsements.

Companies offering to certify products are numerous and include organisations such as exida, FM, SIRA, UL and TÜV Rheinland. They provide a variety of services when it comes to certification, and each one is unique when compared to others. This means that as the owner or operator of a functional safety system, it is up to you to investigate and select a product certifier or certifiers (more than likely, more than one certifier will be needed) that best addresses the specific needs and objectives of a facility or process.

What to consider in functional safety system certification

Functional safety certification addresses how the entire fire and gas detection system meets the requirements and standards set by the regulatory agencies. This is a process that involves conducting an initial safety assessment, determining what actions need to be taken to enhance or upgrade the safety platform, and having the appropriate certifying companies and agencies evaluate the systems. The process also requires determining that components and sub-assemblies meet required standards.

Given that standards are always evolving, certifications can be confusing and expertise among certifiers is variable, owners and operators of hazardous processes need to be well informed and highly diligent in selecting products and services related to fire and gas safety systems. Here are some possible pitfalls to beware of:

1. Self-certification is risky

Selecting properly certified flame and gas detection products and installing these products to approved safety codes and standards are both vital for safety purposes. There are considerations to weigh each step of the way, including operational efficiency, maximum productivity and overall safety. Ultimately, certified products, correct installation and proper day-to-day operation are all factors in achieving the highest safety standard.

But even the best developed products, properly installed and operated, may not provide expected safety features without a legitimate product certification. Product certification is crucial to safety because it establishes a systematic means to evaluate safety at the extremes and for special use conditions. Without valid third-party product certification, the risk is greater for a catastrophic event due to the lack of diligence. Achieving full and reliable functional safety certification requires careful attention.

2. Not all product certifiers are equally qualified

Product certifiers are evaluated by accreditation bodies. Such organisations look for conformance with competency standards to ensure that products are evaluated and certified by the product certifier to meet expected performance levels. The responsibilities of accreditation bodies go beyond simple audits and include approving key policy documents, reviewing the evaluation process and monitoring the product certifier's audit programs. The accreditation body seeks to ensure products are properly certified, which generally means:

A. The product is labelled with the registered certification mark;

B. The product certifier issues certification to a well-recognised test standard that is within the certifier's scope of accreditation; and

C. The product certifier issues certification from one of its recognized facility locations.

Points A and C above are often well understood and applied. However, not all product certifiers issue functional safety certifications as per IEC 61508 within their scope of accreditation (see item B above). Such certificates will not include the certification body logo on the certificate. Without this crucial step there is no formal evidence of competency, and safety may be compromised.

The IEC 61508 standard requires "evidence of competence" for all who perform assessments. While it does not require a formal authorised or accredited status, most customers who purchase IEC 61508-certified products demand a product certifier that demonstrates a high level of technical competence. (See Figure 1 below for a matrix that depicts the different accreditation levels of product certifiers; it is significant to note that as of August 2016, no single group had achieved accreditation in all three areas, SIL, performance and hazardous location.)

The product certifier that meets this high level of accreditation must demonstrate strong competency in the key areas of functional safety. This is demonstrated during an audit by a well-established accreditation body. For example, to certify that a product meets IEC 61508, the product certifier must have full competency in functional safety areas including:

- Mechanical design (stress conditions, useful life and systematic design procedures)
- Software design (software failure mechanisms and systematic design procedures)
- Electronic hardware (electronic hardware failure mechanisms and systematic design procedures)
- Hardware failure modes, effects and diagnostic analysis (FMEDA)
- Hardware probabilistic failure analysis (stress conditions and useful life)
- Software and hardware testing procedures and methods
- Quality procedures, document control and functional safety management

3. What you can (and can't) learn from documentation

When evaluating products for a functional safety system, much can be learned through a careful review of the product certificate. Each certificate includes the standards met and particularly significant, the year of release of standard used to issue certification.

For instance, if a product has been evaluated to the older IEC 61508:2000 (Edition 1) Series released version, the potential buyer needs to be aware that this standard version is less specific and therefore allows for more optimistic Safe Failure Fraction values (and is therefore less safe) than the most current 2010 (Edition 2) released version. The significant difference is that FMEDA calculations now require the exclusion of non-safety related components, resulting in the requirement of a more stringent assessment. "The older version leads to a more favourable Safe Failure Fraction value because 'no-effect' failures were declared safe—a misleading factor when considering overall safety," says David Sullivan-Nightengale, Senior Compliance Engineer at Det-Tronics.

Accreditation Levels of Product Certifiers

Groups offering product certification	SIL IEC 61508	Performance IEC 60079-29 series ISO 7240 series	Hazardous Location IEC 60079
Group **A**	ACCREDITED	NO	NO
Group **B**	NO	ACCREDITED	NO
Group **C**	NO	NO	ACCREDITED
Group **D**	NO	ACCREDITED	ACCREDITED
Group **E**	ACCREDITED	ACCREDITED	NO
NONE	ACCREDITED	ACCREDITED	ACCREDITED
Group **F**	NO	NO	NO

Figure 1: The matrix above shows that each product certifying organization is unique in its accredited ability to certify products to different standards. As of August 2016, no product certifier was accredited for all three IEC certifications: SIL, performance and hazardous locations.

Additional information on manufacturer's claimed capabilities can be obtained by reviewing the product safety manual. This is necessary to determine the robustness of the product and process safety certifications. The product's proof test, which is contained within the safety manual, defines necessary maintenance required during product use to assure ongoing proper functionality. There are cases when a product claims a high SIL capability but it requires expensive field maintenance. This and other claimed capabilities noted in the safety manual should be reviewed in detail when comparing products.

4. Confusion surrounding SIL

It is important to understand that a SIL-capable certification does not mean that the product is performance approved. A SIL-capable product certificate may list a variety of codes and standards. Such a list must not be mistaken for compliance to each, as mentioned at the start of this paper. It may only reference that during evaluation such codes and standards were considered. Codes are not accreditable by any agency—the only way for a product to be properly certified is if a product certifier tests and evaluates it to the related standard, and the product certifier is recognised as competent for the standard by an accreditation body. Some groups that offer product certifications may not be able to issue accreditation certifications to the standards required for a specific application.

Another misperception relating to SIL is that a SIL 2 manufacturer can claim a SIL 3 product by simply requiring redundancy (HFT + 1). This is no longer acceptable. The product manufacturer must first prove it has a SIL 3 compliant development process (because process capability is fundamentally necessary as a systematic measure in assuring product design robustness). Product certifiers with competency in Functional Safety Certification will ensure product and process compliance to manufacturer-claimed capability. (See Figure 2 below for the product, redundancy and process certifications required for SIL 2 or SIL 3 functional safety systems.)

In summary

Products designed to reduce risks in hazardous industrial applications must be certified to particular standards, and those who offer product certification are responsible for examining these products to ensure that they meet functional safety requirements. However, not all product certifiers are in a position to certify what a specific application may require.

Confirming that a product certifier is accredited for the assessment of conformity to IEC 61508 is a critical step for wary buyers of functional safety products. The accredited product certifier will have proven competency to ensure not only product and process compliance, but also to ensure that all relevant information is reflected in the manufacturer's safety manual. Further, the safety manual and supporting manufacturer's documentation must be followed completely to ensure safe use of product and proper functionality of the 'Safety Function.' Only then can full and proper compliance ensure the highest possible level of product reliability and performance for safety purposes. ■

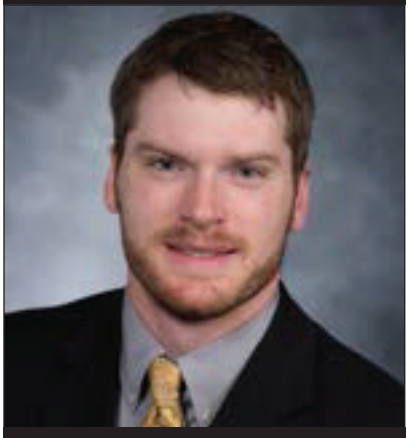
Requirements for SIL2/SIL 3 System Certification

Products		Redundancy		Process		RESULT
SIL 2	+	NO	+	SIL 2	=	SIL 2
SIL 2	+	YES	+	SIL 2	=	SIL 2
SIL 2	+	YES	+	SIL 3	=	SIL 3
SIL 3	+	NO	+	SIL 3	=	SIL 3

Figure 2 : Both product and process SIL certifications are required for SIL system certification. As highlighted, a system with SIL 2 products and SIL 2 process cannot attain SIL3 certification.

About the authors

Jon D. Miller has 30 years' experience in the field of hazardous locations and functional safety with a focus on fire and gas detection and systems with Det-Tronics since 1996. He is Chairman for the US Gas Detection Standards Development Committees for UL STP60079 TG79-29 (Combustible) and UL STP9200 (Toxic), and he is Convener for the International Gas Detection Standards Development Committees for IEC TC31 MT60079-29 (Combustible) and IEC TC31 JWG45 (Toxic). Miller is also a member of IEEE and a member of several ISA, UL, and IEC committees responsible for hazardous location and functional safety electrical equipment.



Mark A. Gaalswyk joined UTC in 2007. Since then, Mark has held roles at multiple UTC companies (Det-Tronics, Kidde R&C, Forney) in Engineering, Compliance, and Product Management, most recently serving as Group Leader for Det-Tronic's system solutions development group. Gaalswyk's compliance work is focused on Functional Safety and he is a certified FMEDA assessor.

Corporate Office
6901 West 110th Street
Minneapolis, MN 55438 USA
www.det-tronics.com

Phone: 952.946.6491
Toll-free: 800.765.3473
Fax: 952.829.8750
det-tronics@det-tronics.com