GENERAL MONITORS

SIL 105: How Can IEC 61508 Approval Aid Users in the Selection and Application of SIL Suitable Fire and Gas Detectors?

Certification plays a valuable role in industrial fire and gas detection. Normative standards establish minimum requirements for the design, fabrication, and performance of these safety devices as necessary to maintain protection of personnel and property. As described earlier in this series, one particular set of standards that has gained wider acceptance among plant safety professionals is ISA 84.01, enacted to drive the classification of Safety Instrumented Systems (SIS) for the process industry within the United States, as well as norms introduced by the International Electrotechnical Commission (IEC), IEC 61508 and IEC 61511. Together, these standards have introduced several specifications that address safety and reliability based on optimizing processes for risk.

General Monitors has now received certification to IEC 61508 Parts 1, 2, and 3 from FM Approvals for twenty-one of its fire and gas detectors (see Table 1). Recognized by a global certification agency, these instruments are suitable for use in applications to safety integrity levels (SIL) ranging from 1 to 3. The company certified these instruments in response to increased demand for IEC 61508-compliant products and growing interest for third-party approvals. The result is one of the most extensive product lines of SIL suitable devices offered in the industry.

Flame Detectors	Gas Detectors	Ultrasonic Gas Leak Detectors
FL3100 (1, 2, or 3)	IR400 (1, 2, or 3)	Observer (1 or 2)
FL3101 (1, 2, or 3)	IR2100 (1 or 2)	Surveyor (1)
FL3102 (1 or 2)	IR4000M (1 or 2)	
FL3110 (1 or 2)	IR4000S (1 or 2)	
FL3111 (1 or 2)	IR5000 (1, 2, or 3)	
FL3112 (1 or 2)	S4000C (1, 2, or 3)	
FL4000 (1, 2, or 3)	S4000CH (1, 2, or 3)	
	S4000T (1, 2, or 3)	
	S4000TH (1, 2, or 3)	
	S4100C (1, 2, or 3)	
	S4100T (1, 2, or 3)	
	TS4000 (1 or 2)	

Table 1. General Monitors Products Certified by FM Approvals to IEC 61508. SIL Suitability in Parentheses.

The IEC 61508 standard is a risk-based approach for determining the SIL of safety instrumented functions. It is frequently applied in the hydrocarbon processing and oil and gas industries to seek instrumentation solutions that improve the inherent safety of industry processes, while imparting greater reliability and run time. Unlike other international standards, IEC 61508 takes a

holistic approach when quantifying the safety performance of electrical control systems: The design concept, the management of the design process, operations, and maintenance of the system throughout its lifecycle are within scope.

In order to determine an instrument's capacity for a certain SIL environment, developers and enforcement authorities must perform a variety of tasks. (At this stage, it is understood that a holistic process hazard analysis (PHA) has been conducted to identify SIS requirements and determine the need for fire and gas instrumentation to achieve the desired risk reduction levels.) A first step is to gather all background information about the device and its uses that are relevant to functional safety. Then they must generate a comprehensive set of product specifications (Safety Requirements Specifications) that include all relevant environmental conditions (ex. EMI, EMC, and thermal humidity), electrical requirements (ex. input voltage, current, throughput response time), software requirements, system requirements, and safety instrumented functional definitions. Next, a design and development plan with various verification and validation plans must be developed in accordance with the defined safety lifecycle.

Then they must execute a failure mode effect and diagnostics analysis (FMEDA), where component failures lead to detector failure modes classified as either safe detected (SD), safe undetected (SU), dangerous detected (DD), or dangerous undetected (UD). This analysis is combined with the component failure rates, an appropriate measure for the rate at which failures lead to accidents (dangerous failures), and validated by fault insertion testing of the instrument with regard to the defined Safety Instrumented Function. Armed with the FMEDA and accident rates, one can describe, categorize, and classify those credible accidents that result in significant risk. After rationalizing and tabulating the accident frequency, one can determine the risk reduction that can be achieved by the deployment of the detector in a particular safety instrumented system.

Detectors that are vetted and certified to comply with IEC 61508 offer several benefits. Certification provides greater assurance about a supplier's claim of SIL suitability. The voice of a globally recognized authority on normative standards for fire and gas detection equipment and an impartial organization like FM Approvals can lend added credibility to a supplier's assessment. Additionally, reliability calculations for end devices are already performed and available to the user, reducing the lead times for implementing SIL rated processes. All FM IEC 61508 certificates, for instance, supply the instrument's safe failure fraction (SFF), the average probability to fail on demand (PFD_{avg}), and the failure rates for safe detected (λ_S), dangerous detected (λ_{DD}), and dangerous undetected (λ_{DU}) modes. Last, certification helps potential customers in product selection, enabling them to compare alternative designs of safety instrumented functions (SIFs) before purchasing any of the elements in the SIF chain. The result is often simpler and less costly SIS architectures.

An important document associated with the IEC 61508 certificate is the product safety manual. This manual describes the operation necessary to ensure that the field device provides the claimed risk reduction. It contains information ranging from specifications to assumptions on repair time (RT) and requirements for proof test intervals (TI) and resulting SIL parameters. Moreover, ongoing test requirement and suggested test intervals are outlined. A copy of the safety manual for the products listed in Table 1 is available from the General Monitors website.

Despite the many benefits, IEC 61508 certification cannot be used to claim an individual product carries a SIL rating. One common mistake is to consider sensors in isolation. Sensors are but one out of three elements in the SIF chain and have a SIL budget of 30 – 35%[1]. Without taking into account the failure rate of the logic solver and the final elements, any SIL assessment would be incomplete.

Another common mistake is to ignore systematic safety integrity. Systematic safety integrity refers to the software process requirements outlined in IEC 61508-1 Annex B and IEC 61508-3, established to prevent systematic errors. It involves firmware, field programmable software used to configure devices, and software diagnostics, which provide coverage for dangerous and safe failures. A sensor, however SIL capable or certified as such, cannot ensure a reliable SIS architecture without full consideration of the software that makes these instruments smarter.

Product certification is simply not enough. IEC 61508 compliance encompasses a thorough examination of product design, manufacture, and quality control procedures. Nevertheless, it is the activities undertaken by the ultimate stakeholders of the SIF that will lead to fewer errors, and as a result, lower risk to people, facilities, and the environment. By certifying to IEC 61508, General Monitors has taken another step in implementing functional safety concepts in fire and gas detection. Certificates offer valuable information for the selection of SIL suitable detectors and for the design of a complete SIF. Taken together, the certificates of a large number of its products attest to General Monitors' commitment to help end users improve safety.

[1] Hoekstra, B., "Safety Integrity – Not Only a Matter of Reliable Hardware," *Business Briefing: Exploration and Production: The Oil and Gas Review,* 2005, 114 – 117.