Meeting Safety Requirements: 'Certified SIL Capable'

David Riddle, Detector Electronics Corporation (Det-Tronics), Phone: +1-800-765-FIRE Fax: +1-952-829-8750 Email: david.riddle@detronics.co.uk
Simon Pate, Director of Projects and Systems, Detector Electronics Corporation (Det-Tronics), Email: simon.pate@detronics.com

Life-saving safety equipment is becoming increasingly important in a wider cross-section of companies. So, at the same time, there is a growing trend to adopt best practices for the management of safety systems. Now industrial clients are looking for new design or upgrades to a plant to be in line with the Safety Instrumented System (SIS) standards of IEC61508 in addition to fire and gas system performance approvals. It is important that safety engineers and owners consider the fundamental elements of Safety Instrumented Systems and how they will implement these elements. The safety requirements specification of any SIS to IEC61508 includes the target Safety Integrity Level (SIL) for defined Safety Instrumented Functions (SIF). In a fire and gas safety system, a SIF could be a gas or flame detector combined with the outputs to annunciate or to initiate mitigation systems.*

Safety-system manufacturers today use the term SIL in different ways. How does an engineer determine the meaning of the words 'Certified SIL Capable'? Further, does that term differ significantly from the phrase SIL Suitable, indicating the practice of a manufacturer to perform self declaration?

Certified SIL Capable – An IEC61508 Assessment

When a device is given a certain SIL capability level, it means the device may be used in a design at that capability level or below. For instance, a Certified SIL2 device may be used in a SIF with a SIL2 or SIL1 risk reduction. To attain a Certified SIL Capability rating, an IEC61508 assessment must be done.

Properly assessing SIL Capability is an extensive process. It includes analysing the complete component design process: specification methods, design methods, design tools, testing methods, review techniques, and documentation. When this assessment is performed by a third-party on behalf of a safety manufacturer, the IEC61508 Certified SIL Capability rating provides simple and solid safety integrity justification. A statement of SIL conformance that is not validated by a third party does not reflect a complete SIL design and verification process.

The result of that assessment should be a Safety Case, which describes how an instrument manufacturer meets each requirement of IEC 61508. All safety and design engineers should be able to review the Safety Case of any device they are interested in.

Makers of equipment destined for safety-related applications have a duty of care on them to provide equipment that is fit for purpose. When purchasing an assessed device, the buyer should receive audited documentation on how to use the component in a safety application. In addition, they will receive information on failure rates, failure modes, useful life limits, suggested proof test procedures and application limitations.

Considerations in the Safety Assessment

The assessment considers many facets of the safety manufacturer's device and process, including hardware and software, manufacturer's management of change, the manufacturer's design and development process, and fault injection.

Manufacturer-Designed Software

With the latest advances in technology, detection devices and logic solvers rely on the manufacturers own designed algorithms, software, and firmware. The vast majority of gas and flame detection devices now rely on highly specified microprocessors at their core to provide levels of functionality never previously available. These microprocessors are more powerful with each passing generation, and modern devices far exceed the performance of processors used in personal computers only a few years ago.

Now that the capabilities are so extensive, the manufacturers take advantage of this by using more detailed and complex software code. It is, therefore, imperative that the software in a safety device be fully evaluated in accordance with IEC61508 for the targeted SIL. Otherwise, can users and engineers be sure that the selected hardware will be able to perform at the target SIL level?

While mechanical hardware data is crucial to the calculations for SIL systems and product capabilities, the importance of software functionality and potential failure must not be overlooked and specific proof of compliance should be sought for the firmware/software elements of any product.

When a component passes an IEC61508 assessment process, it meets the integrity requirements from both a random hardware failure perspective and a systematic design and software failure perspective.

Fault Injection Testing

The IEC61508 hardware assessment analyses the component failures and groups them into safe or dangerous, and detected or undetected. This process is called a Failure Modes, Effects and Diagnostics Analysis

(FMEDA). This analysis provides the failure rates used in the SIL capability. However, this is only a fraction of the complete requirements.

In most devices, and especially flame and gas detectors, there are thousands of lines of programming that enables them to detect the hazard. Product with untested software is analogous to a personal computer being checked for reliability based on component characteristics without having data on any element of the operating system or application vital to the correct function of it. The creation of this software can introduce failure modes and therefore IEC61508 has recommendations for coding practices for each target SIL.

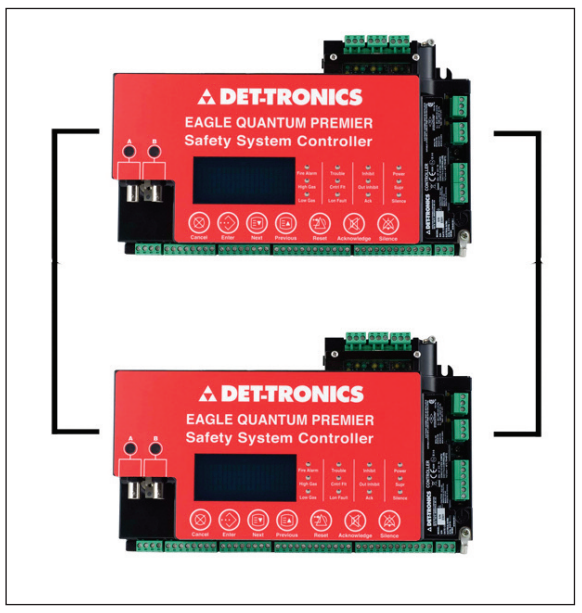
To verify that the design performs as predicted, the final device is then subjected to fault injection testing. Once a device has been created and released its ongoing updating and the management of change process is also evaluated as part of an overall device certification.

Management of Change (MOC)

Management of change is a critical part of the evaluation by a third-party for testing and achieving 'Certified SIL Capability.' The instrument manufacturer's change process is a potential for the introduction of faults as changes are made to the original device. While important for all products (including simple mechanical devices), MOC is especially so for any product that contains complex integrated circuits and software. Design mistakes can introduce dangerous failures. Therefore, any product change must go through a rigorous safety impact analysis to determine the scope of the change.

Development Process

When considering longer term operation, product updates should also be taken into account. Any product with a SIL certificate must go through a Safety Impact Analysis before any update is performed. This ensures that devices are kept within the original design parameters and that safety capabilities are



maintained. Use of SFF (Safe Failure Fraction) and FMEDA data at the system design stage will only be good for those devices at that time and that version. Any updates to the product, without a certified SIL capability, may result in a complete recalculation of the PFD (Probability of Failure on Demand.) Again, without third-party testing, many items could be overlooked by safety manufacturers.

Interval Test Requirements

Although the installation, usage, and operation parameters are important, the requirements for maintenance (the proof test interval stated in the report) will affect the long-term safety and availability, cost, and operation of the system. Each element of the system has a proof test interval associated with it. This proof-test interval is required to keep the system within the SIL safety parameters originally specified.

Selecting a product requiring many proof tests per year will result in higher maintenance costs, reduced productivity, increased downtime, and generally higher operational expenditure for the site. Conversely, a site decision to lengthen the maintenance period beyond the SIL calculated proof test interval will reduce the SIL of those Safety Instrumented Functions. To increase availability, an appropriate spares holding will ensure that the assumptions made for the mean time to restoration (MTTR) period are maintained.

The Engineer's Decision Process

Third-party certification compared to self tests and hardware reports provide engineers different data as they select the proper equipment to fit their safety, cost, and time requirements.

Users of fire and gas detectors and systems need to be sure that the devices and systems being selected are truly SIL capable. Mechanical and hardware failure data is not the full story. While FMEDA will provide the necessary raw data to start calculations, this may be the start of a long road of validation when it is far simpler, faster, and more cost effective for engineers to select equipment with completed 3rd-party certificates from reputable test houses.

The system designer always has to consider practical limits. Proof-test intervals are important to the downtime of the plant and the long-term operation expenditure, while attaining higher levels of SIL may not be economic with certain devices.

Engineers have pressure on them to select the best safety devices, with the best availability at the best balance of immediate and on-going costs and quality. When consideration of the extra cost in man-hours to engineer unverified raw data into an extra Safety Instrumented Function, an off-the-shelf solution is economically viable and provides peace of mind to user and safety engineer alike.

Conclusion

There is a duty of care on manufacturers to supply equipment that is fit for purpose. When safety engineers are presented with varying manufacturers' SIL claims, they should confirm that the IEC61508 standards have been correctly interpreted and that the tests for full capability as required in the standards have been completed and passed.

The overall benefit of an IEC61508 certification is that the buyer knows a component has a high enough level of design quality to match the SIL Capability rating.

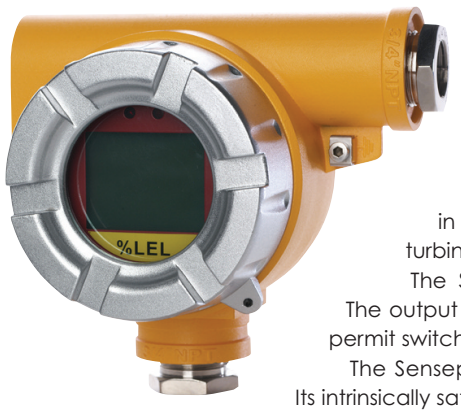
In choosing safety devices, consider the balance of immediate and on-going costs and quality. Extra cost in engineering time might be required by including self-certified 'SIL Suitable' hardware in a SIF. However, an off-the-shelf 'Certified SIL Capable' device is economically viable through reduced engineering to validate the design to target SIL solution. If any element of the product changes, the certification is updated, so as the product evolves, the certification evolves with it, enabling a secure maintenance programme. It also provides peace of mind to the user and safety engineer.

Some manufacturers are prepared to provide data from their engineering calculations and have those calculation validated by 3rd-parties. There are few who have submitted product for testing at 3rd-party laboratories and provide certified SIL capable products with the complete report for hardware and software/firmware ready to go for implementation.

There is a big difference between 'Certified SIL Capable' and manufacturers claims of SIL conformance.

* The IEC61508 organisation states that IEC 61508 is the international standard for electrical, electronic, and programmable electronic safety related systems. It sets out the requirements for ensuring that systems are designed, implemented, operated and maintained to provide the required safety integrity level (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 specifies 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.



New Gas Detection Transmitter for Monitoring Flammable Gases

Honeywell (UK) recently announced the launch of the Sensepoint RFD (Remote Flammable Detector). The Sensepoint range of gas transmitters can be used for the detection of flammable gases and is certified for use in potentially explosive atmospheres to International standards. Sensepoint RFD allows flammable gas sensors to be mounted either directly to or remotely from the transmitter with an integral gas concentration display, up to 45m/147 feet away. This versatility is essential for applications where the sensor is mounted in locations where the transmitter would not be visible to plant personnel. Typical applications would include the exhaust ventilation from gas turbine acoustic enclosures and the dryers of solvent-based drying machines.

The Sensepoint RFD transmitter can be configured to monitor flammable gases with a detection range of 0-20% or 0-100% LEL/LFL. The output from the transmitter is compatible with Honeywell Analytics or third party controllers via a 3 wire linear 4-20mA output. On-board relays permit switching of local alarm functions.

The Sensepoint RFD is ATEX and UL certified for use with the Sensepoint or 705 standard or high temperature range of flammable gas sensors. Its intrinsically safe infrared controller permits configuration and calibration without the need to open the controller or obtain a hot work permit.

Intelligent TS4000 Toxic Gas Detector Receives SIL 2 Suitable Rating

Providing advanced protection against a wide range of hazardous industrial gases and oxygen deficiency, the TS4000 Intelligent Toxic Gas Detector from **General Monitors** (USA) is now rated SIL 2 suitable.

The TS4000 Toxic Gas Detector has been third-party certified for SIL 2 applications and is approved by CSA, ATEX, CE Marking and GOST. Its sophisticated design offers many advanced features, including long distance remote mounting up to 2,000 feet, dual redundant MODBUS communications, 8 amp relays, three-digit display, 4-20 mA output, and an indication of remaining sensor life. All electronics are contained within an explosion-proof housing so that sensor information can be processed at the sensor site. The detector provides complete status and control capability in the control room. Additionally, the interface module's galvanically-isolated, intrinsically-safe design supports sensor field replacement without special tools or hot work permits.

Easy to install, the TS4000 features one-person calibration and can virtually self-calibrate by activating a magnetic switch and applying gas. Process engineers who need to protect people and equipment will find the TS4000 Toxic Gas Detector ideal for chemical, oil and gas, water and wastewater treatment, pulp and paper, and other hazardous environments. Additional applications include public utilities, refineries, pharmaceuticals, and food and beverage.

The TS4000 monitors a variety of toxic gases in the parts per million (ppm) range, including ammonia, carbon monoxide, chlorine, chlorine dioxide, hydrogen chloride, hydrogen sulfide, nitric oxide, nitrogen dioxide, oxygen, ozone, and sulphur dioxide. The system displays gas concentrations up to 500 ppm, fault codes for troubleshooting, prompts when calibration is needed, and provides complete status to the user. Additionally, the TS4000 simplifies operation and maintenance and reduces downtime by indicating remaining sensor life.

The TS4000 is comprised of a base unit, sensor housing with interface module and electrochemical sensor. The interface module processes information at the sensor site and communicates detected gas values to the base unit for data control and display. By combining explosion-proof certification with intrinsically safe inputs, the TS4000 provides high performance in hazardous locations.