Functional Safety Assessment and Certification to IEC 61511

White Paper

KENEXIS

>> INTRODUCTION

Selecting an organization from which to receive a functional safety assessment or certification is an important step in the safety lifecycle because some organizations are more qualified than others.

Certification by independent third parties is a valuable tool that has been utilized by industrial companies to ensure that the products (and more recently services) that they receive are performed in compliance with some national or international standards of relevance. Standards and certifications that are related to functional safety of safety instrumented systems and the equipment that is employed in safety instrumented system service have a high level of importance due to the very significant consequences that could occur if these equipment or these services were performed in a non-compliant manner. Furthermore, selecting an organization from which to receive a functional safety assessment or certification is an important step in the safety lifecycle because some organizations are more qualified than others in various parts of the safety lifecycle that is defined in the international standards on functional safety.

In the context of functional safety of safety instrumented systems in the process industries, certification indicates compliance with the appropriate standard defining the equipment and/or activities for which the end user would like certification. The standard, or standards, or sections of standards that form the *requirements* that must be certified need to be determined by the end user and then a certificate that demonstrates compliance to that particular standard should be obtained.

>> BACKGROUND OF CERTIFICATION

In the field of functional safety of safety instrumented systems, certifications have a long and successful history, but their application has primarily been limited to the design and manufacture of components. For instance, when an operating company desires to employ a field device such as a pressure transmitter, they may wish to have the device be *certified* for use in a safety critical application. If so, they would seek out a device manufacturer whose process for the design and manufacture of the pressure transmitter device is compliant with the IEC 61508 standard, which is the standard that defines the requirements for the design and manufacture of SIS equipment (often referred to as the “manufacturer’s standard”). At this point in time, almost every reputable manufacturer who desires to have their equipment employed in safety critical applications has gone through the process of obtaining a certification of their device against the requirements listed in the IEC 61508 standard.

The primary certification agencies that have provided *equipment* certificates against IEC 61508 are Technischer Überwachungsverien (TUV), Factory Mutual (FM), and Exida.com. Two of these agencies TUV and FM have a history as testing laboratories which made extending their capabilities into the field of certification of devices to IEC 61508 natural because they were already testing devices (specifically, electronic devices) to a wide variety of other standards such as one that define level of intrinsic safety, resistance to electromagnetic interference, and myriad other electronic specifications. Currently, Exida.com and TUV perform the

bulk of all certifications of equipment items against the IEC 61508 standard.

There is no independent third party that certifies or bestows on any organization a *license* to practice equipment certification to ISA/IEC standards. The ability of a company to provide a certificate and have that certificate considered legitimate stems from the reputation of the firm providing that certification. Standards bodies such as IEC or ISA have to-date not issued approvals or licenses.

In some cases, government regulations require that a certain test be performed by a "National Recognized Testing Laboratory" (NRTL), especially when the there are physical tests where measurements must be made and procedures must be followed. Since there are no physical tests required for compliance with the IEC 61508 standard, there are no NRTL requirements placed on certification providers for any of the functional safety standards (i.e., IEC 61508 / IEC 61511). This is obvious, because at least one of organization currently performing IEC 61508 certifications is itself not a registered NRTL.

>> DEVICE VERSUS APPLICATION CERTIFICATION

All of the foregoing discussion is related to devices that are utilized in safety instrumented system applications. This category of certification would include transmitters, programmable logic controllers, and valves. While the certification of devices is very important, the compilation of a group of certified devices into a system does not in any way guarantee that the entire system is compliant with its relevant functional safety standard – which is most likely not the same standard that the devices were determined to be compliant with. In fact, device certification reports typically are explicit that this is the responsibility of the designer.

In the process industries, the functional safety standard that should form the basis for safety instrumented system design is IEC 61511 – *Functional Safety: Safety Instrumented Systems for the Process Industries Sector*. This sector specific standard was developed under the *umbrella* of IEC 61508, but is specifically designed to meet the requirements of the process industries. It is generally not acceptable to design an application to the umbrella standard, as the sector specific application standards have a lot more information that is specific to the industry in question, and may have stricter requirements and more relevant rules that are based on the applications that are seen in that specific industry.

While certifications for specific equipment items or devices that are designed and manufactured in accordance with the IEC 61508 standard are quite common, certifications for applications in accordance with IEC 61511 are less common. There are several reasons that applications are not often certified. First, there is very little demand from the end user community for certification of applications. Unlike SIS devices, whose manufacture is not readily evident or understood by their purchasers,

applications of SIS are often a core competency of the purchasers. Much of the work that is performed in the development of an application is either performed directly by the operating company or an engineering contractor. Historically, there is only rarely a desire by an operating company to certify its own work was done in conformance to the functional safety standards. Furthermore, there is no certification organization that is promoting the use of third party certifications of applications.

>> INCREASED DEMAND FOR APPLICATION CERTIFICATIONS

While the use of third party certifications for applications in accordance with IEC 61511 is not as prevalent as certifications for component equipment, their popularity is increasing for a number of reasons. Primarily:

1) the use of "packaged" equipment with pre-approved designs, and,

2) the reliance on engineering companies and systems integrators to provide turn-key solutions.

3) Desire by corporate-level SIS authorities to ensure conformance in local or subsidiary companies

More and more, operating companies are turning to "packaged" equipment to meet the requirements of their operating facilities. When packaged equipment is utilized, the operating company cannot be involved in the detailed design of every SIF loop that is used. Instead, meeting the requirements of the IEC 61511 standard falls back to the equipment vendor. Since the operating company is not directly involved in the design, the use of the certificate process can meet the operating company requirements of managing functional safety when their staff is not directly involved in executing the project tasks.

In addition to the use of "packaged" equipment, operating companies are also relying heavily on engineering companies, equipment vendors and systems integrators to supply turn-key SIS systems instead of building them with their own resources. Since the operating company still needs to ensure the management of functional safety – even though external contractors are performing safety lifecycle tasks – some means of assuring the project tasks are executed in accordance with the requirements of the functional safety requirements is necessary. The use of independent third-party experts to certify the work of engineering companies, equipment vendors, and systems integrators who are supplying SIS equipment (or simply performing SIS lifecycle tasks) will ensure that projects are executed in conformance with the standards.

>> QUALIFICATIONS FOR APPLICATION ASSESSMENT AND CERTIFICATION

While the concept of independent third party certification against IEC 61511 for "packaged" equipment and operating company applications (provided by engineering companies, equipment vendors, and systems integrators) is a desirable goal, the selection of a suitable qualified certification agency is not a trivial task. First off, for the same reasons that were described for the IEC 61508 standard, there is no agency or authority who determines whether or not any specific company or agency is "qualified" to perform an assessment or certification against IEC 61511. Similarly to IEC 61508 certification agencies, companies who undertake projects whose goals is functional safety assessment and certification in accordance with IEC 61511 will need be selected based only on the credibility of their organization based on the experience level of the company and the specific assessors who are employed by the company who perform the assessments. Furthermore, the process of selecting an IEC 61511 certification agency is not simply a matter of selecting agencies who have established practices in providing IEC 61508 certificates. In fact, agencies that provide IEC 61508 certificates may not be effective assessors of the requirements of IEC 61511. The basic reason is that "device" design is an "equipment" issue that is the domain of electronics (usually micro-electronics) engineers and industrial engineers/designers. Application design (which is the purview of the IEC 61511 standard) is a completely different discipline that is mainly chemical (process) engineering, with controls systems engineering and mechanical engineering requirements. These are highly different skill sets. As such, traditional "device" certifiers are may not be well suited to analyze a process plant to determine IEC 61511 conformance.

No other organization is more suitably qualified to perform functional safety assessments of chemical process facilities against the IEC 61511 standard than Kenexis. Since Safety Instrumented System Design Basis Development and Validation of process industry applications is, and has always been, the core business function of the Kenexis organization, our initial projects related to conformity assessment were done at the special request of super-major oil and gas companies who trusted our experience in SIS design and standards development as opposed to a desire to undertake the certification line of business. Our super-major oil and gas company clients were concerned about the quality of workmanship and engineering being provided to them in safety critical "packaged" units – such as subsea HIPPS systems, compressor packages, fired heater packages, and other specialty process applications – and wanted a highly qualified independent third party that they knew that they could trust based on prior project experience to provide a highly skilled and detailed assessment.

>> DETERMINING COMPETENCY OF ASSESSORS

In order to determine the competency of an organization to perform functional safety assessment against IEC 61511, it makes sense actually refer to the IEC 61511 standard in order to identify the criteria that should be considered when determining competency.

The IEC 61511 standard states in clause 5.2.2.2:

> 5.2.2.2 Persons, departments or organizations involved in safety life-cycle activities shall be competent to carry out the activities for which they are accountable.
>
> NOTE: As a minimum, the following items should be addressed when considering the competence of persons, departments, organizations or other units involved in safety lifecycle activities:
>
> a) engineering knowledge, training and experience appropriate to the process application;
>
> b) engineering knowledge, training and experience appropriate to the technology used (for example, electrical, electronic or programmable electronic);
>
> c) engineering knowledge, training, experience appropriate to the sensors and final elements;
>
> d) safety engineering knowledge (for example, process safety analysis);
>
> e) knowledge of the legal and safety requirements;
>
> f) adequate management and leadership skills appropriate to their role in safety life-cycle activities;
>
> g) understanding of the potential consequence of an event; h) the safety integrity level of the safety instrumented functions; i) the novelty and complexity of the application and the technology.

In addition, in the functional safety assessment section of the standard, the following requirements for the membership of an assessment team are listed:

> 5.2.6.1.2 The membership of the assessment team shall include at least one senior competent person not involved in the project design team.
>
> NOTE 1 When the assessment team is large, consideration should be given to having more than one senior competent individual on the team who is independent from the project team.
>
> NOTE 2 The following should be considered when planning a functional safety assessment:
>
> - The scope of the functional safety assessment; - Who is to participate in the functional safety assessment;

- The skills, responsibilities, and authorities of the functional safety assessment team;

- The information that will be generated as a result of the functional safety assessment activity;

- The identity of any other safety bodies involved in the assessment;

- The resources required to complete the functional safety assessment activity;

- The level of independence of the assessment team;

- The means by which the functional safety assessment will be revalidated after modifications.

Considering the requirements, Kenexis is uniquely qualified to perform functional safety assessment and certification of SIS at a chemical process facilities.

>> UNPARALLELED COMPETENCY OF KENEXIS

Kenexis is uniquely qualified to perform functional safety assessments of *applications* against the requirements of IEC 61511 each of the requirements because:

1. (competence in) engineering knowledge, training and experience appropriate to the process application

Knowledge, training, and experience appropriate to the process application is where Kenexis is most dramatically differentiated from all other firms who provide IEC 61511 functional safety assessment and certification. Kenexis are engineers by trade, not assessors. The background of the Kenexis team is in process engineering.

First off, all of our Principal Assessors are degreed chemical engineers, as are the preponderance of the Kenexis Staff. While SIS design for chemical process facilities requires knowledge of a variety of engineering disciplines, ultimately, the process under control is a chemical one, and thus a detailed understanding of the process is of the highest criticality and complexity, thus our strong preference for chemical engineering degrees as the foundation for professional skill. Furthermore, all of the Principal Assessors at Kenexis have many years of experience in the design of chemical process plants and control systems for chemical process plants prior to embarking in a specialization in safety instrumented systems.

In the opinion of Kenexis, our process is absolutely unparalleled in the industry. Kenexis understands the chemistry and process engineering involved in the design of all facilities for which it performs SIS engineering

work. This level of expertise is not readily available in firms who have few if any chemical engineers on staff, and even fewer (if any) staff that understand refining processes and oil and gas production processes at the level of a process engineer.

2. (competence in) engineering knowledge, training and experience appropriate to the technology used (for example, electrical, electronic or programmable electronic);

The “engineering knowledge, training, and experience appropriate to the technology used” at Kenexis is again, absolutely unparalleled. The Kenexis Principal Assessors have performed numerous projects where they were singularly responsible for selecting components, component layout, component wiring design, physical installation and wiring of components, PLC programming, installation of finished systems, field interconnect wiring design, and commissioning and testing of complete SIS systems. These systems include hardwired relay based systems through virtually all models of PLC and safety PLC.

The experience of Kenexis Principal Assessors in not only engineering but physically wiring, installing, and testing physical implementations of SIS systems makes Kenexis more qualified than other firms in an area that is very subtle, but critical to process safety.

3. (competence in) engineering knowledge, training, experience appropriate to the sensors and final elements;

This is another area that shows the relative Kenexis strength among the potential options. Many problems in SIS design stem from a lack of experience with field instrumentation as applied in very specific process applications. It is unfortunately quite common for instrument engineers with insufficient experience to install sensor and final element types in situations where they are not suitable due to the process service environment in which the equipment is installed. This kind of knowledge can only be gained from many years of instrument specification and start-up and ongoing monitoring of actual process operations.

Kenexis has strong experience in design and specification of instrumentation in general, and in safety applications specifically. This goes well beyond other firms whose experience is largely derived from their detailed knowledge of micro- electronics.

4. (competence in) safety engineering knowledge (for example, process safety analysis);

Process safety engineering is an area where Kenexis excels and possesses experience, knowledge, and tools that are far superior to any other organization. Kenexis has experience in all facets of safety engineering – from preliminary process hazards analysis all the way through standards compliant design of safety critical equipment. The Kenexis Principal Assessors have all performed a large variety of projects where hazard and risk analysis in many forms was employed to determine if overall plant risk levels were tolerable and then to use the results of those risk analysis to design (or re-design) the plant to reduce risk levels to a tolerable level.

At Kenexis, process safety analysis is a core competency that is part of all engineer's day-to-day tasks. Furthermore, Kenexis has a core competency in executing SIS safety lifecycle tasks. In the past five years that Kenexis has been an independent company, Kenexis has analyzed over 15,000 safety instrumented functions – analyzing, documenting, and specifying systems through ALL of the phases of the lifecycle.

5. (competence in) knowledge of the legal and safety requirements;

Kenexis has unparalleled knowledge of the legal and safety requirements of safety instrumented system. Kenexis is well versed, and has participated in all standards, recommended practices, and technical reports that define safety instrumented system design. Furthermore, Kenexis has detailed knowledge of the legal and regulatory requirements related to SIS design in all jurisdictions in which it performs services.

All of the Principal Assessors at Kenexis are active members of the ISA 84 committee – which is the US contributor to the IEC 61508 and IEC 61511 standards. The work of Kenexis went into the release of the ISA 84 standard (1996 version) which is the precursor to the IEC 61508 standard (1998) and the IEC 61508 standard (2002). All Principal Assessors participate in every committee meeting and provide detailed review including comments on every standard and technical report that is released by the subcommittee. In addition to standards work, Kenexis performs a great deal of the technical report development for ISA. It should be known that much of the detailed engineering that goes on during the SIS safety lifecycle is based on technical reports and reference literates as opposed to information in the documents themselves. For instance, SIL verification calculations are typically performed in accordance with the equations shown in the ISA TR84.00.01 technical report, as the equations are not provided in the IEC 61511 standard. All of the Kenexis Principal Assessors provide a great deal of service and input to all technical report committees. In fact, two of the recent technical reports (TR 84.00.07 on fire and gas detection and suppression systems and TR 84.00.06 on SIS in fired heaters) were predominantly (more than 50%) written be Kenexis staff.

In addition to work in the field of standards development, Kenexis also has experience with the legal and regulatory requirements related to SIS and other safety related equipment.

6. adequate management and leadership skills appropriate to their role in safety life-cycle activities;

All Kenexis Principal Assessors have the appropriate management and leadership skills. Two of the assessors are owners of the corporation, which has over 25 employees in three offices in three countries. Other Principal Assessor have had management responsibility in various companies for over 25 years.

7. understanding of the potential consequence of an event;

Kenexis, more so than any other competing certification agency, understands the potential consequences of an event in the process industries. This deep understanding comes from a background in chemical engineering along with extensive experience in performing quantitative

analysis of the consequences that can occur as the result of loss of containment of chemical hazards.

8. the safety integrity level of the safety instrumented functions; and novelty and complexity of the application and the technology.

These last two items on the list of considerations for competency are not requirements such much as that they are reminders that as the SIL level increases and the novelty and complexity of the process under consideration increases, the skill level and experience of any personnel performing safety lifecycle tasks (including functional safety auditing) will also need to increase commensurately.

Based on the foregoing assessment of the factors that determine competency to perform SIS safety lifecycle tasks, it is clear that Kenexis is abundantly and uniquely qualified to provide functional safety assessments of SIS implementations on process industry applications in conformance with the IEC 61511 standard.

>> CONCLUSION

No other organization is more suitably qualified to perform functional safety assessments of chemical process facilities against the IEC 61511 standard than Kenexis.

Certification by independent third parties is a valuable tool that has been utilized by industrial companies to ensure that the products and services that they receive are performed in compliance with some national or international standards of relevance. In the field of functional safety of safety instrumented systems, certifications have a long and successful history, but their application has primarily been limited to the design and manufacture of components. While the use of third party certifications for applications in accordance with IEC 61511 is not as prevalent as certifications for devices, their popularity is increasing for a number of reasons. Primarily:

1) the use of "packaged" equipment with pre-approved designs, and,

2) the reliance on engineering companies and systems integrators to provide turn-key solutions.

3) Desire by corporate-level SIS authorities to ensure conformance in local or subsidiary companies

While the concept of independent third party certification against IEC 61511 for "packaged" equipment and operating company applications (provided by engineering companies, equipment vendors, and systems integrators) is a desirable goal, the selection of a suitable qualified certification agency is not a trivial task.

No other organization is more suitably qualified to perform functional safety assessments of chemical process facilities against the IEC 61511 standard than Kenexis.

>> REFERENCES

Kevin Mitchell, et al., *Safety Instrumented Systems Engineering Handbook*, Kenexis, Columbus, OH, USA, 2010.

Marszal, Edward and Scharpf, Eric, *Safety Integrity Level Selection with Layer of Protection Analysis*, Instrumentation Systems and Automation Society, Research Triangle Park, NC, 2002.