



Selecting Instrumentation Equipment for Safety Applications

by exida

The end user must carefully choose all instrumentation equipment used in Safety Instrumented Systems (SIS) applications. All such equipment must be carefully justified. The justification must include sufficient information such that the end user is totally confident that the instrumentation will properly perform in the intended application. The instrumentation must be fully capable of performing the functional requirement. The materials used in the instrument must be compatible with process materials if the instrumentation sees wetted service. Process environmental conditions must not exceed the instrumentation ratings. The functional safety of the instrument must be assessed. All justification decisions must be documented as part of project records.

Functional Safety Assessment

IEC 61511, Functional Safety for the Process Industries, requires that equipment used in safety instrumented systems be chosen based on either IEC 61508 certification to the appropriate SIL level or justification based on "prior use" criteria (IEC 61511, Part 1, Section 11.5.3). Unfortunately the IEC 61511 standard does not give specific details as to what the criteria for "prior use" really means. Most agree however that if a user company has many years of documented successful experience (no dangerous failures) with a particular version of a particular instrument this can provide justification for using that instrument even if it is not safety certified. Most agree that prior use requires that a comprehensive system be in place to record all field failures and failure modes at each end user site. Version records of the instrument hardware and software must be kept as significant design changes may void prior use experience. Operating conditions must be recorded and must be similar to the proposed safety application. Of course the problem with the prior use approach is that many process sites do not have that level of record keeping in place.

Many users have asked manufacturers to help with their justification. Different levels of assessment have been done by third party assessors for instrumentation manufacturers. This work can help reduce the burden of documentation when an end user attempts to justify an instrument for use on safety applications. In the marketplace four levels of assessment have been done on instrumentation products:

1. FMEDA of the hardware according to IEC 61508

A hardware analysis called a failure modes effects and diagnostics analysis (FMEDA) is done to determine the failure rates and failure modes of an instrument (Gob01). A FMEDA is a systematic detailed procedure that is an extension of the classic FMEA procedure developed and proven decades ago. The technique was first developed for electronic devices and recently extended to mechanical and electro-mechanical devices (Gob02).

These device failure rates are then used to calculate the Safe Failure Fraction (SFF), the Diagnostic Coverage (DC) and the average Probability of Failure on Demand (PFDavg). This assessment for hardware devices provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. Some assessors also do a useful life analysis to provide the safety instrumentation engineer with any wearout mechanisms and the time periods until wearout. Some FMEDA analysis is also extended to evaluate the effectiveness of given Proof Test methods. This provides the safety instrument engineer with proof test coverage factors used for more realistic PFDavg calculations.

Many end users consider this level to be an essential minimum level of third party assessment. This level of assessment when combined with detailed end user evaluation and prior use experience is sufficient for some companies to allow the use of instrumentation in safety instrumented system applications.

2. Prior use consideration according to IEC 61511

Some manufacturers are working to help the end users in their prior use evaluation by providing additional information. Some manufacturers have had a third party assessment of the field failure records that exist for a

device. Failures attributable to both hardware and software should be considered. An assessment should also be made of the field return data gathering process and the product modification process.

A prior use report from a third party assessor does provide information that may help an instrument designer justify the use of a particular instrument according to IEC 61511 prior use criteria. However similar claims from different equipment vendors should be carefully reviewed to ensure their validity for a particular application. The prior use data must show environmental limitations and application limitations. Since the manufacturer does not actually “use” the equipment, prior use methods must depend on data gathered from the end users. The methods for collecting, reporting and analyzing this data should be critically reviewed. When field failure records are used to calculate failure rates, the methods must be more carefully reviewed, as field failures are notoriously under-reported.

Most agree that the information from a prior use report must be combined with detailed end user evaluation and specific plant experience before such equipment is approved for safety instrumented system applications.

3. Combination FMEDA and proven in use assessment per stringent defined criteria – exida Proven In Use

exida has defined specific extended criteria for a “Proven in Use” assessment that goes considerably beyond simple field failure analysis and modification process review. This method (Option 3) combines hardware FMEDA analysis, with a detailed study of collective field performance per stringent written criteria (exi03). When hardware failure rate and failure mode analysis is combined with an assessment of field failure performance, a greater level of confidence is gained. Also included is an assessment of the manufacturer’s field return process, engineering change and modification process and the manufacturer’s safety documentation. This method is intended to provide useful information to an end user that can contribute to the justification process when combined with several years of experience in a particular user application.

4. Full assessment according to IEC 61508

Option 4 is a full assessment according to the requirements of IEC 61508. The full assessment includes all the above assessment areas and adds an assessment of all fault avoidance and fault control measures during hardware and software development as well as detail study of the testing, modification, user documentation and manufacturing processes.

A full assessment according to IEC 61508 is the most comprehensive assessment available. Unfortunately it is becoming more necessary as more and more software gets into our instrumentation. Field failures due to design faults (systematic errors) are increasing. These are mostly software faults. This type of failure is very unlikely to be reported to the manufacturer, as “repair” is often a “software reset” or power cycle. Hence “prior use” or field failure evaluation techniques based on returns to the manufacturer are not sufficiently effective.

Many of the requirements of IEC 61508 focus on the elimination of systematic faults by use of the world’s best product design methods. In order to demonstrate compliance with all requirements of IEC 61508, a product creation process must show extensive use of many fault control and fault avoidance procedures. The software must be specifically designed to tolerate software faults. The members of the IEC 61508 committee have defined a set of practices that represent good software engineering. They must be applied with different levels of rigor as a function of SIL rating of the instrumentation product.

This option is suitable for newly developed products or for carefully developed existing products. When a product has demonstrated full compliance with the requirements of IEC 61508, the end-user has a higher level of confidence that the product will provide a level of safety according to the SIL level rating of the product.

Full compliance with the requirements of IEC 61508 is seen when a product does not have any significant “restrictions” on usage as documented in the product “Safety Manual.” A large safety manual with a long

detailed list of instructions on how to make the product “safe” is a sure sign the manufacturer does not meet requirements unless these restrictions are implemented by the end user.

The primary differences in the assessment techniques are summarized in Table 1.

Assessment Criteria	FMEDA only	FMEDA / exida	Prior Use / IEC 61511	exida Proven In Use Criteria	IEC 61508 Certification
Detail analysis of hardware failure modes	X	X		X	X*
Detail Analysis of hardware diagnostic capability	X	X		X	X*
Analysis of hardware useful life		X		X	X*
Analysis of proof test effectiveness		X		X	X*
Assessment of operational hours based on manufactured units			X	X	X
Assessment of Configuration Management system per requirements of IEC 61508			X	X	X
Assessment of Field Failure Return System - field failures corrected				X	X
Assessment of Field Failure Return System - notification to users of safety issues				X	X
Assessment of design revision history - few revisions based on design faults				X	X
Assessment of hardware design process					X
Assessment of hardware testing techniques					X
Assessment of software requirements					X
Assessment of software criticality					X
Assessment of software design techniques					X
Verification of Safety Manual per IEC 61508					X
Assessment of software testing techniques					X
Assessment of product testing techniques including environmental testing					X
Assessment of manufacturing process					X

* Depends on assessment agency - not all agencies perform detailed analysis

Table 1: Assessment Differences

Assessments are normally done by third party experts such as exida, TUV or FM. Often, two or more companies will team together to do the assessment as requested by the instrument manufacturer.

Most users demand full certification per IEC 61508 for safety PLC products. This is an easy request to make as most manufacturers have equipment that has been fully certified.

Full IEC 61508 certification for field equipment has been less available. However with the new product announcements recently it is clear that fully certified transmitters and even valves would soon be available.

It should be noted that all of these assessment techniques including full IEC 61508 certification do not evaluate the suitability of an instrument for a particular process or the failure probability of the process connection. The end user must evaluate these issues. Usage in a safety critical application must be carefully justified.

As safety instrumented systems are designed and implemented it is clear that both manufacturers and end users must work together to achieve functional safety. The manufacturer must specify the environmental and application limitations. The end user must design the product into an application that will not exceed the limitations of the instrument design. Field reliability and safety performance must be communicated to the manufacturer so that any unanticipated design issues are understood and communicated to all end users.

About exida:

Established in 2000 by the world's top safety, security, and reliability experts from TÜV, manufacturers and end users, exida is the leading global supplier engineering tools, services and certification for Functional Safety, Cyber Security and Reliability.

exida has worldwide successfully supported over 2000 Equipment Manufacturers, Engineering Companies and End Users in the Process Industry, Factory Automation, (Nuclear) Power Industry and Automotive Industry to meet IEC 61508/ IEC 6151/IEC 62061/ ISO26262 requirements.

For more information – contact AsiaPacific@exida.com