What does Proven In Use imply?

White Paper
exida
80 N. Main St.
Sellersville, PA
www.exida.com

exida White Paper Library
http://www.exida.com/Resources/Whitepapers

Copyright exida.com L.L.C. 2018-2020

Keywords

Safety Integrity Level (SIL), Safety Instrumented Function (SIF), IEC 61508, IEC 61511, PFDavg, Proven In Use, Prior Use, Architectural Constraints

Abstract

The functional safety standards, IEC 61508 [1], IEC 61511 [2], and ANSI/ISA 84.01 [3] each specify the Safety Integrity Level performance parameter for Safety Instrumented Functions. For a Safety Instrumented Function to meet a specific Safety Integrity Level the sum of the PFDavg of all components part of that Safety Instrumented Function needs to fall in the PFDavg bandwidth related to that Safety Integrity Level.

Besides the PFDavg requirement for a specific Safety Integrity Level, the IEC 61508 standard defines the concept of architectural constraints. This concept puts additional requirements on equipment items that are part of the Safety Instrumented Function. The architectural constraints are expressed in the required level of Hardware Fault Tolerance. The required level of Hardware Fault Tolerance is a function of the equipment item's Safe Failure Fraction (SFF), the type of equipment item, and the desired Safety Integrity Level.

IEC 61511, the process industry sector specific functional safety standard, also specifies minimum levels of Hardware Fault Tolerance. However, this standard allows a reduction in the required level of Hardware Fault Tolerance for field equipment when the equipment item under consideration can be deemed Proven In Use. Specific Proven In Use requirements are listed in the standard that need to be followed before an equipment item can be called Proven In Use, however interpretation of these requirements is arguable. This paper will provide an overview of the Proven In Use requirements as listed by the IEC 61511 standard and where appropriate the IEC 61508 standard. Furthermore a practical interpretation of the Proven In Use requirements used by exida will be discussed.

Conclusion

The architectural constraints concept as defined in IEC 61508 prevents the use of ridiculously low proof test intervals to achieve a certain SIL level. It goes without saying that no continuous process will be shutdown every week to perform a proof test if that is the test interval used in the SIL verification. The architectural constraints concept as defined in IEC 61511 follows the IEC 61508 concept and is generally restrictive, or more conservative, than IEC 61508. The reduction of the Minimum Hardware Fault Tolerance by one through the argument of Proven In Use opens up a wide door that may seem rather inviting if the Hardware Fault Tolerance achieved in the conceptual design is not sufficient. Both the IEC 61508 and IEC 61511 proven in use requirements lack easy practical implementation. The exida Proven In Use Criteria have been derived from both IEC 61508 and IEC 61511 and give practical and quantitative guidelines on how to assess if an equipment item is Proven In Use. The exida Proven In Use Criteria have been used successfully in several IEC 61508 product certification and have also been used by end-users as guidelines to assess if Prior Use according to IEC 61511 applies.

Introduction

The functional safety standards, IEC 61508 [1], IEC 61511 [2], and ANSI/ISA 84.01 [3] each specify the Safety Integrity Level performance parameter for Safety Instrumented Functions. For a Safety Instrumented Function to meet a specific Safety Integrity Level the average Probability of Failure on Demand (PFDavg) sum of all components, part of that Safety Instrumented Function, needs to fall in the PFDavg bandwidth related to that Safety Integrity Level.

Besides the average Probability of Failure on Demand requirement for a specific Safety Integrity Level, the IEC 61508 and IEC 61511 standard define the concept of architectural constraints. This concept puts additional requirements on equipment items that are part of the Safety Instrumented Function. The architectural constraints are expressed in the required minimum level of Hardware Fault Tolerance. The achieved level of Hardware Fault Tolerance is a function of the equipment item's Safe Failure Fraction (SFF), the type of equipment item, and the desired Safety Integrity Level.

For compliance with the IEC 61508 or IEC 61511 functional safety standards, the achieved Safety Integrity Level of a Safety Instrumented Function is determined by the lower of two calculated SILs, i.e. the SIL based on the average Probability of Failure on Demand and the SIL based on the Architectural Constraints. This is also illustrated in FIGURE 1. The SIL based on the average Probability of Failure on Demand is often represented by SILpfd. The SIL based on the Architectural Constraints is often represented by SILac [4].

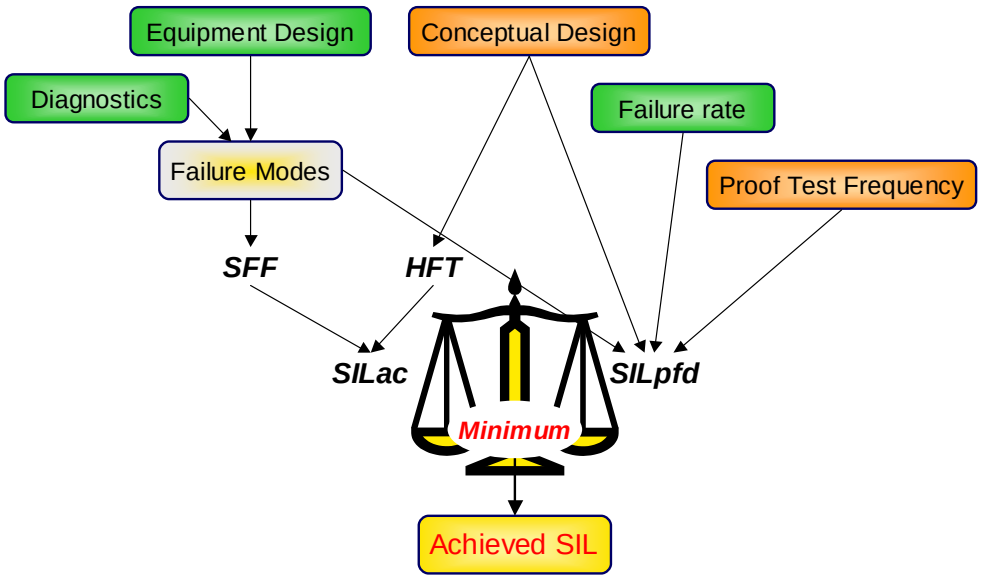

FIGURE 1 SIF ACHIEVED SIL

The architectural constraints requirements are an additional threshold when trying to create a Conceptual Design to achieve a certain Safety Integrity Level. One of the reasons for this was that it is relatively simple to manipulate the resulting average Probability of Failure on Demand result by changing the Safety Instrumented Function's Proof Test frequency or using optimistic failure rate data from "field failure reports". The Safe Failure Fraction and Hardware Fault Tolerance of a Safety Instrumented Function on the other hand can only be changed by revising the Conceptual Design. This mostly means adding

redundancy or selecting more superior products in the Safety Instrumented Function. Both solutions usually imply a higher procurement cost for the specific Safety Instrumented Function.

As a refresher the following section will discuss the Safe Failure Fraction. In the subsequent sections the architectural constraints per IEC 61508 and IEC 61511 will be described. Next the difference between the two standards when it comes to the architectural constraints will be discussed. Finally the concept of Proven In Use is addressed. The exida interpretation to the Proven In Use concept will also be explained.

Safe Failure Fraction

The Safe Failure Fraction (SFF) of a device is defined as the "fraction of the overall random hardware failure rate of a device that results in either a safe failure or a detected dangerous failure" [IEC 61511-1 3.2.65.1]. The Safe Failure Fraction is usually calculated through one of the two following equations.

$$SFF = \frac{\lambda^{SD} + \lambda^{SU} + \lambda^{DD}}{\lambda^{SD} + \lambda^{SU} + \lambda^{DD} + \lambda^{DU}}$$ **EQUATION 1**

$$SFF = 1 - \frac{\lambda^{DU}}{\lambda^{SD} + \lambda^{SU} + \lambda^{DD} + \lambda^{DU}}$$ **EQUATION 2**

Elaborating on EQUATION 1 it is relatively straightforward to demonstrate that the Safe Failure Fraction is independent of the actual total failure rate of a device. The total failure rate of a device is the sum of the Safe Detected, Safe Undetected, Dangerous Detected, and Dangerous Undetected failure rates.

$$\lambda = \lambda^{SD} + \lambda^{SU} + \lambda^{DD} + \lambda^{DU}$$ **EQUATION 3**

The Safe failure rate of a device is equal to the total failure rate of that device multiplied by the percentage of Safe Failures (%Safe).

$$\lambda^{S} = \lambda^{SD} + \lambda^{SU} = \lambda \cdot \%Safe$$ **EQUATION 4**

The Dangerous Detected failure rate of a device is calculated by multiplying the total failure rate of that device times the percentage of Dangerous Failures (one minus the percentage of Safe Failures) times the Dangerous Coverage factor (C^D).

$$\lambda^{DD} = \lambda \cdot (1 - \%Safe) \cdot C^{D}$$ **EQUATION 5**

Substituting equation 3, 4, and 5 into equation 1 yields:

$$\begin{aligned} SFF &= \frac{\lambda \cdot \%Safe + \lambda \cdot (1 - \%Safe) \cdot C^{D}}{\lambda} \\ &= \frac{\lambda \cdot \left(\%Safe + (1 - \%Safe) \cdot C^{D}\right)}{\lambda} \\ &= \%Safe + C^{D} - \left(\%Safe \cdot C^{D}\right) \end{aligned}$$ **EQUATION 6**

So the Safe Failure Fraction of a device is equal to the percentage of Safe Failures plus the Dangerous Coverage Factor minus the product of percentage Safe Failures and Dangerous Coverage Factor.

In order to calculate the Safe Failure Fraction of a device one needs the detailed failure rate / failure mode distribution information that can be obtained from a Failure Mode, Effects, and Diagnostic Analysis (FMEDA). A source with detailed failure rate information including the Safe Failure Fraction for a variety of equipment items is the Safety Equipment Reliability Handbook [5].

Architectural Constraints Per IEC 61508

For the "Requirements for hardware safety integrity" [IEC 61508-2 7.4.3] two architecture types are defined for equipment items in IEC 61508. These two architecture types are Type A and Type B.

An equipment item is considered of architecture Type A when for the components required to achieve the safety function:

1. The failure modes of all constituent components are well defined; and
2. The behavior of the subsystem under fault conditions can be completely determined; and
3. There is sufficient dependable failure data from field experience to show that the claimed rates of failure for detected and undetected dangerous failures are met.

An equipment item is considered of architecture Type B when for the components required to achieve the safety function:

1. The failure mode of at least one constituent component is not well defined; or
2. The behavior of the subsystem under fault conditions cannot be completely determined; or
3. There is insufficient dependable failure data from field experience to support claims for rates of failure for detected and undetected dangerous failures.

In other words if an equipment item consists of a microprocessor or complex ASIC it is of architecture Type B, simply because the first two requirements of a Type A equipment item are not met. Valves, relays, switches, etc. are usually Type A devices. Transmitters, PLCs, etc. are usually Type B devices.

The Architectural Constraints concept as defined in IEC 61508 [1] can be summarized as is done in FIGURE 2 and FIGURE 3 for equipment items of architecture Type A and Type B respectively.

Safe Failure Fraction	Hardware Fault Tolerance		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % - < 90 %	SIL 2	SIL 3	SIL 4
90 % - < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4
NOTE A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function			

FIGURE 2 IEC 61508 ARCHITECTURAL CONSTRAINTS ON TYPE A SUBSYSTEMS

Safe Failure Fraction	Hardware Fault Tolerance		
	0	1	2
< 60 %	Not allowed	SIL 1	SIL 2
60 % - < 90 %	SIL 1	SIL 2	SIL 3
90 % - < 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4
NOTE A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function			

FIGURE 3 IEC 61508 ARCHITECTURAL CONSTRAINTS ON TYPE B SUBSYSTEMS

As an example on how to read these tables; assume a Generic Smart Pressure Transmitter. Architecture Type is Type B, as the transmitter consists of a microprocessor that is part of the safety critical path. The Safe Failure Fraction for this transmitter is 60% [5]. Referring to FIGURE 3, a Safe Failure Fraction of 60% allows use of this device up to SIL 1 with Hardware Fault Tolerance of 0, e.g. a 1oo1 or 2oo2 voting arrangement.

Architectural Constraints Per IEC 61511

In contrast to IEC 61508, IEC 61511 does not define two different architecture types for equipment items. IEC 61511 defines a set of Minimum Hardware Fault Tolerance requirements for Programmable Electronic Logic Solvers. These Minimum Hardware Fault Tolerance requirements are displayed in FIGURE 4.

SIL	Minimum Hardware Fault Tolerance		
	SFF < 60%	SFF 60% to 90%	SFF > 60%
1	1	0	0
2	2	1	0
3	3	2	1
4	Special requirements apply (see IEC 61508)		

FIGURE 4 IEC 61511 MINIMUM HFT PE LOGIC SOLVERS

In addition to the Minimum Hardware Fault Tolerance for Programmable Electronic Logic Solvers, IEC 61511 also defines a table for the Minimum Hardware Fault Tolerance of all other equipment items. This table applies to Sensors, Final Elements, and non-Programmable Electronic Logic Solvers. The table is depicted in FIGURE 5.

SIL	Minimum Hardware Fault Tolerance
1	0
2	1
3	2
4	Special requirements apply (see IEC 61508)

FIGURE 5 IEC 61511 MINIMUM HARDWARE FAULT TOLERANCE

As an example on how to read these tables; assume a Generic Smart Pressure Transmitter. Referring to FIGURE 5 and considering that the transmitter has a Hardware Fault Tolerance of 0 in single use, this device can be used up to SIL 1.

Furthermore IEC 61511 states that for the Minimum Hardware Fault Tolerance table for Sensors, Final Elements, and non-Programmable Electronic Logic Solvers to be valid, the dominant failure mode is to the safe state or dangerous failures are detected. If this is not the case the Minimum Hardware Fault Tolerance must be increased by one.

Additionally IEC 61511 states that the Minimum Hardware Fault Tolerance for Sensors, Final Elements, and non-Programmable Electronic Logic Solvers may be reduced by one if the equipment items used in the Safety Instrumented Function comply with all of the following:

1. The hardware of the device is selected on the basis of prior use;
2. The device allows adjustment of process-related parameters only, for example, measuring range, upscale or downscale failure direction;
3. The adjustment of the process-related parameters of the device is protected, for example, jumper, password;
4. The function has an SIL requirement of less than 4.

Finally IEC 61511 allows the user to consider alternative fault tolerance requirements providing an assessment is made in accordance to the requirements of IEC 61508-2, Tables 2 and 3.

Comparing Architectural Constraints Concepts

Though the Architectural Constraints concepts may look quite different at first glance, the IEC 61511 concept is clearly derived from the concept described in IEC 61508. Arguably IEC 61511 is in some cases more restrictive, i.e. requires a higher level of Hardware Fault Tolerance, than IEC 61508.

When analyzing FIGURE 4, which shows the IEC 61511 Minimum Hardware Fault Tolerance requirements for Programmable Electronic Logic Solvers in detail, one can conclude that this table represents the IEC 61508 Architectural Constraints on Type B subsystems table that was shown in FIGURE 3. There are only two noticeable differences between FIGURE 4 and FIGURE 3. The first one is that the IEC 61511 table does not specify any SIL 4 requirements. This is because IEC 61511 only defines SIL1, 2, and 3 and argues that SIL 4 processes do “not occur” in the process industry, i.e. if one comes across a SIL 4 requirement it usually indicates bad engineering practices. The second noticeable difference is that for an equipment item with a Safe Failure Fraction of less than 60% a Minimum Hardware Fault Tolerance requirement of 3 is specified for SIL 3 applications in the IEC 61511 table whereas the IEC 61508 table does not specify achievable SIL levels for a Hardware Fault Tolerance of 3. Of course, the Minimum Hardware Fault Tolerance requirement of 3 is a logical extrapolation of the IEC 61508 table, on the other hand one might argue that in such a case it would be really better to use different equipment.

When analyzing FIGURE 5, which shows the IEC 61511 Minimum Hardware Fault Tolerance of Sensors, Final Elements, and non-Programmable Electronic Logic Solvers, it can be concluded that the Safe Failure Fraction is not part of this table anymore. One of the reasons for this is that it was argued that the Safe Failure Fraction of field equipment is usually within the 60% to 90% bandwidth (IEC 61511 assumes that

the dominant failure mode is to the safe state or dangerous failure are detected). Using this as a basis and comparing FIGURE 5 with FIGURE 2 and FIGURE 3 that showed the IEC 61508 Architectural Constraints Type A and Type B restriction respectively, it can be concluded that the IEC 61511 table follows the IEC 61508 Architectural Constraints on Type B subsystems table. The comparison also reveals that IEC 61511 requires an additional level of Hardware Fault Tolerance for Type A equipment items with a Safe Failure Fraction within the 60% to 90% bandwidth and is consequently more restrictive than IEC 61508 for these type of devices. In addition, if a Type B equipment item effectively uses the diagnostic capabilities that a microprocessor provides, yielding a Safe Failure Fraction within the 90% to 99% bandwidth IEC 61511 would restrict that equipment item to SIL1 whereas IEC 61508 allows use up to SIL2. Of course, for all these situations where the Architectural Constraints concept as defined in IEC 61511 is more restrictive than the concept defined in IEC 61508, IEC 61511 allows the user to follow the Architectural Constraints requirements per IEC 61508.

The main “loophole” in IEC 61511 is however the statement that the Minimum Hardware Fault Tolerance for Sensors, Final Elements, and non-Programmable Electronic Logic Solvers may be reduced by one if the equipment items used in the Safety Instrumented Function comply with all of the following:

1. The hardware of the device is selected on the basis of prior use;
2. The device allows adjustment of process-related parameters only, for example, measuring range, upscale or downscale failure direction;
3. The adjustment of the process-related parameters of the device is protected, for example, jumper, password;
4. The function has an SIL requirement of less than 4.

For field devices and non-Programmable Logic Solvers in process industry applications it will be relatively easy to argue compliance with requirements 2, 3, and 4. The key requirement is “The hardware of the device is selected on the basis of prior use”. Evidence to argue compliance with this requirement is purely based on Proven In Use. The next section of this paper will describe the requirements of IEC 61508 and IEC 61511 on Proven In Use arguments. The subsequent section describes the Proven In Use arguments that where derived from these by exida.

Proven In Use

Both IEC 61508 and IEC 61511 have clauses describing Proven In Use requirements. The requirements are however rather descriptive and no quantitative guidelines are proved. The next two subsections show the IEC 61508 Proven In Use requirements and the IEC 61511 Proven In Use requirements respectively.

Proven In Use Requirements IEC 61508

IEC 61508 states that a previously developed subsystem shall only be regarded as proven in use when it has a clearly restricted functionality and when there is adequate documentary evidence which is based on the previous use of a specific configuration of the subsystem (during which time all failures have been formally recorded), and which takes into account any additional analysis or testing, as required. The documentary evidence shall demonstrate that the likelihood of any failure of the subsystem (due to random hardware and systematic faults) in the E/E/PE safety-related system is low enough so that the

required safety integrity level(s) of the safety function(s) which use the subsystem is achieved [IEC 61508-2 7.4.7.6]. The documentary evidence required, shall demonstrate that the previous conditions of use of the specific subsystem are the same as, or sufficiently close to, those which will be experienced by the subsystem in the E/E/PE safety-related system, in order to determine that the likelihood of any unrevealed systematic faults is low enough so that the required safety integrity level(s) of the safety function(s) which use the subsystem is achieved [IEC 61508-2 7.4.7.7].

Additionally IEC 61508 states that when there is any difference between the previous conditions of use and those which will be experienced in the E/E/PE safety-related system, then any such difference(s) shall be identified and there shall be an explicit demonstration, using a combination of appropriate analytical methods and testing, in order to determine that the likelihood of any unrevealed systematic faults is low enough so that the required safety integrity level(s) of the safety function(s) which use the subsystem is achieved [IEC 61508-2 7.4.7.8].

Furthermore, the documentary evidence required by 7.4.7.6 shall establish that the extent of previous use of the specific configuration of the subsystem (in terms of operational hours), is sufficient to support the claimed rates of failure on a statistical basis. As a minimum, sufficient operational time is required to establish the claimed failure rate data to a single-sided lower confidence limit of at least 70 % (see IEC 61508-7, annex D and IEEE 352). An operational time of any individual subsystem of less than one year shall not be considered as part of the total operational time in the statistical analysis [IEC 61508-2 7.4.7.9].

And the final Proven In Use requirement in IEC 61508 states that only previous operation where all failures of the subsystem have been effectively detected and reported (for example, when failure data has been collected in accordance with the recommendations of IEC 60300-3-2) shall be taken into account when determining whether the above requirements (7.4.7.6 to 7.4.7.9) have been met [IEC 61508-2 7.4.7.10].

In summary IEC 61508 requires that in order to consider an equipment item proven in use the functionality of the equipment item is limited. In addition, the previous operating environment should be identical or near identical to the newly considered operating environment. Finally, all failures should be documented and reported and a 70% confidence limit of the failure rate should be calculated based on sufficient operational time. Note that the single-sided lower confidence limit of at least 70 % mentioned in the failure rate calculation requirement should in fact be a single-sided upper confidence limit of at least 70 % as this is more conservative and more appropriate for functional safety considerations [6].

Additional details and guidelines to the IEC 61508 Proven In Use requirements are provided in IEC 61508-7, B.5.4.

Prior Use Requirements IEC 61511

IEC 61511 states two main requirements for the selection of components and subsystems based on prior use. First of all the appropriate evidence shall be available that the components and subsystems are suitable for use in the safety instrumented system [IEC 61511-1 11.5.3.1]. Where in the case of field elements, there may be extensive operating experience either in safety or non-safety applications used as a basis for the evidence. The level of details of the evidence should be in accordance with the complexity of the considered component or subsystem and with the probability of failure necessary to achieve the required safety integrity level of the safety instrumented function(s).

The second main requirement concerns the evidence of suitability of the equipment item to be considered Proven in Use. The evidence of suitability shall include the following:

1. Consideration of the manufacturer's quality, management and configuration management systems;
2. Adequate identification and specification of the components or subsystems;
3. Demonstration of the performance of the components or subsystems in similar operating profiles and physical environments;
4. The volume of the operating experience [IEC 61511-1 11.5.3.2]

Where in the case of field devices (for example, sensors and final elements) fulfilling a given function, this function is usually identical in safety and non-safety applications, which means that the device will be performing in a similar way in both type of applications. Therefore, consideration of the performance of such devices in non-safety applications should also be deemed to satisfy this requirement. For field devices, information relating to operating experience is mainly recorded in the user's list of equipment approved for use in their facilities, based on an extensive history of successful performance in safety and non-safety applications, and on the elimination of equipment not performing in a satisfactory manner. The list of field devices may be used to support claims of experience in operation, provided that

- The list is updated and monitored regularly;
- Field devices are only added when sufficient operating experience has been obtained;
- Field devices are removed when they show a history of not performing in a satisfactory manner;
- The process application is included in the list where relevant.

In summary IEC 61511 requires that in order to consider an equipment item proven in use the previous operating environment should be similar to the newly considered operating environment. In addition equipment items must be clearly specified and the equipment item manufacturer should have appropriate quality management and configuration management procedures in place. Finally an adequate number of operating experience needs to be demonstrated.

Additional details and guidelines to the IEC 61511 Prior Use requirements are provided in IEC 61511-2, 11.5.3.

exida Proven In Use

exida maintains an internal Proven In Use Evaluation Criteria document [7] with guidelines on how to assess and justify the Proven In Use applicability of an equipment item. In order for an equipment item to be considered acceptable for Safety Instrumented System applications the equipment item must meet all criteria listed below.

Time In Use

In order for field experience to apply IEC 61508 requires that the equipment item has been in service for at least one year with unchanged specification [IEC 61508-7 B.5.4]. IEC 61511 has no Time In Use requirements. exida concluded that before an equipment item can be considered proven in use it must meet either of the following Time In Use requirements

1. The equipment item must be shipping for one year without any revisions or changes; or
2. The equipment item must be shipping for two years without any significant revisions or changes.

Hours In Use (Adequate Operating Experience)

For field experience to apply IEC 61508 requires that the equipment item has an operating experience of 100,000 hours with equipment items in 10 different applications [IEC 61508-7 B.5.4]. IEC 61511 has no adequate operating experience requirements.

In addition IEC 61508 lists techniques and measures to avoid systematic failures and their effectiveness [IEC 61508-2 Table B.6]. Field experience can be used as a measure to avoid systematic failures. In order to claim low effectiveness 10,000 hours of operation time are required for at least one year of experience with at least 10 devices in different applications (this is equivalent to the 100,000 hours requirement). The statistical accuracy claimed should be 95 % while no safety critical failures may have occurred. In order to claim high effectiveness 10,000,000 hours of operation time are required for at least two years of experience with at least 10 devices in different applications. The statistical accuracy claimed should be 99.9 % and detailed documentation of all changes (including minor) during past operation should be available.

The exida adequate operating experience requirement is that the equipment item needs to meet a minimum number of Hours In Use of 30,000,000 hours. These 30,000,000 hours of estimated usage should be obtained from a minimum of 10 different applications with stress conditions equal to or above average conditions of the application.

When estimating the number of hours in use the equipment item actual installation dates shall be considered, not the shipment dates of the equipment items. In case the actual installation dates are not available for the hours in use estimation it shall be assumed that the installation occurs six months after the equipment item shipment.

In addition if the equipment item has a wear out mechanism, it shall be assumed that all units operate no longer than the useful life period. Furthermore it shall be assumed that no wear out failures are reported to the manufacturer (this is a worst case assumption as wear out failure will be considered as random hardware failures).

Operating Conditions

IEC 61508 requires similar conditions of use, i.e. functionality and environment, for an equipment item to be considered Proven In Use. IEC 61511 requires that the operating profile of equipment items be considered in the Prior Use assessment. Several points contribute to the operating profile [IEC 61511-2 11.5.3]. For field devices the points to consider are functionality (for example, measurement, action), operating range, process properties (for example, properties of chemicals, temperature, pressure), process connection, EMC, and environmental conditions. For logic solvers points to consider are version and architecture of hardware, version and configuration of system software, application software, I/O configuration, response time, process demand rate, EMC, and environmental conditions.

It should be pointed out that IEC 61511 allows for field devices (for example, sensors and final elements) that the non-safety function experience is considered in the safety function proven in use argument. This

is based on the assumption that the function is usually identical in safety and non-safety [IEC 61511-1 11.5.3.2]. Though this may be the case for sensing devices like transmitters, it is definitely not the case for valves. A control valve is usually a dynamic valve; it is continuously moving to adjust process parameters. A safety valve on the other hand is usually a static valve; it is continuously open and will only move, i.e. close, when there is a demand from the process. Partial valve stroke testing is considered a good diagnostic for detecting stuck failures, however it does not make the valve dynamic.

When it comes to the operating conditions exida requires that the stress conditions of the considered prior use applications are equal to or above average conditions of the application. This includes an assessment of the functionality and the application environmental limits.

Failure Rate Calculation

Based on the Hours In Use determined for the equipment item and the reported field failures a failure rate calculation shall be performed. This calculated field failure rate should be lower than the failure rate predicted for the equipment item using a Failure Modes, Effects, and Diagnostic Analysis (FMEDA). If the calculated field failure rate for the equipment item is higher than the FMEDA predicted failure rate it is an indication of systematic problems with the equipment item and the equipment item cannot be considered Proven In Use.

Failure rates calculated on the basis of field returns shall only consider hours recorded during the warranty period of the manufacturer. It is to be assumed that all failures after the warranty period are not reported to the manufacturer. In addition, without evidence to the contrary, it shall be assumed that only 50 % of the failed units are returned during the warranty period and that 0 % are returned after warranty. When calculating the field failure rate a single-sided upper confidence limit of at least 70 % shall be considered. The confidence limit is based on clause 7.4.7.9 of IEC 61508-2, taking into consideration the more conservative, and for safety applications more appropriate, approach of calculating the upper limit instead of the lower limit.

Failure Data Comparison

In addition to the failure rate calculation a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) must be performed for the equipment item. Part of the Proven In Use assessment is the review of the actual FMEDA. As indicated above the failure rate calculated from the field data must be less than the failure rate predicted by the FMEDA. If the field failure rate is larger than the predicted failure rate this is an indication of serious systematic design issues and equipment item cannot be considered Proven In Use.

The FMEDA also allows for a detailed evaluation of the Safe Failure Fraction. An additional requirement for a product to be considered Proven In Use is that the FMEDA results must show a Safe Failure Fraction greater than 80 %, considering the safe failure definition as presented in IEC 61508-4. In case of for example temperature transmitters the Safe Failure Fraction threshold of 80 % shall be considered without including a thermocouples or RTD. Furthermore the Failure Modes, Effects, and Diagnostic Analysis must be verified through fault insertion testing.

Safety Manual

For and equipment item to be considered Proven In Use the manufacturer must produce a safety manual meeting the requirements of IEC 61508. The safety manual will describe how end-users shall install the equipment item for the Proven In Use considerations to be valid.

Quality System

IEC 61511 requires consideration of the manufacturer's quality, management, and configuration management systems. Consequently the exida proven in use criteria have, in addition to specific equipment item requirements, also requirements to the quality system that the manufacturer has in place. The manufacturer must have an ISO 9000 (or better) certified quality system that covers all manufacturing operations and field failure returns. Especially the field failure return process is important to determine an as accurate as possible field failure rate for the equipment item. Therefore the field failure return procedures must require that statistics be maintained on all field returns. When a trend is indicated by the statistics, the trend must be analyzed for root cause failure. The root cause failure reports must be communicated to those responsible for product improvement and a corrective action system must be in place to assure that a corrective action is taken.

In addition the manufacturer must have a detailed version control system that identifies all changes and revisions. The equipment item must be marked with sufficient information to allow the user to identify each revision. The modification procedures must meet the requirements of IEC 61508.

Finally the quality system should meet specific development process requirements. In order to establish the maturity of the development process a development process gap analysis must be performed per IEC 61508. For equipment items that were first installed within the last two years, the process must meet at least SIL1 requirements. For products that were first installed more than two years ago, the modification process must meet all requirements for IEC 61508 SIL2.

Process Parameter Adjustment Only

The final exida Proven In Use requirement follows the Architectural Constraints Concept per IEC 61511. In order to reduce the required Minimum Hardware Fault Tolerance IEC 61511 requires that, apart from the Proven In Use argument and that the target SIL should be less than SIL4, the equipment item allows adjustment of process-related parameters only and that the adjustment of the process-related parameters of the device is protected.

This means that the equipment item should be assessed as being not programmable. Generally this excludes all products that are capable of running function blocks or configurable calculations (most Fieldbus products). In addition the equipment item must have means to protect parameter changes, i.e. the equipment item should including a jumper and/or a password protection.

References

1. IEC 61508, Functional safety of electrical / electronic / programmable electronic safety-related systems, 2000, International Electrotechnical Commission, Geneva, Switzerland
2. IEC 61511, Functional safety: Safety Instrumented Systems for the process industry sector, 2003, International Electrotechnical Commission, Geneva, Switzerland
3. ANSI/ISA 84.01, Application of Safety Instrumented Systems for the Process Industries, 1996, Instrument Society of America, Research Triangle Park, NC, USA
4. exida.com Safety Integrity Level verification tool, SILver, Version 2.0, exida.com LLC, Sellersville, PA, USA
5. Safety Equipment Reliability Handbook, 2003, exida.com L.L.C., Sellersville, PA, USA, ISBN 0-9727234-0-4
6. Amkreutz R., Selection of Failure Rate Data for SIL Verification, Technology update ISA volume 424, ISA 2002, Chicago, Illinois, USA
7. exida.com, Proven In Use Evaluation Criteria, revision R0.3, July 2003, Internal document, exida.com LLC, Sellersville, PA, USA

Abbreviations and Definitions

%Safe	Percentage of Safe Failures
C^D	Diagnostic Coverage Factor for Dangerous failures
FMEDA	Failure Modes, Effects, and Diagnostic Analysis
HFT	Hardware Fault Tolerance
IEC	International Electrotechnical Commission
PE	Programmable Electronic
PFDavg	Average Probability of Failure on Demand
SFF	Safe Failure Fraction
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SILac	Achieved Safety Integrity Level based on Architectural Constraints
SILpfd	Achieved Safety Integrity Level based on the Safety Instrumented Function's PFDavg
SIS	Safety Instrumented System

Revision History

Authors: Iwan van Beurden, Rachel van Beurden-Amkreutz

exida – Who we are.

exida is one of the world's leading accredited certification and knowledge companies specializing in automation system cybersecurity, safety, and availability. Founded in 2000 by several of the world's top reliability and safety experts, exida is a global company with offices around the world. exida offers training, coaching, project-oriented consulting services, standalone and internet-based safety and cybersecurity engineering tools, detailed product assurance and certification analysis, and a collection of online safety, reliability, and cybersecurity resources. exida maintains a comprehensive failure rate and failure mode database on electrical and mechanical components, as well as automation equipment based on hundreds of field failure data sets representing over 350 billion unit operating hours.

exida Certification is an ANSI (American National Standards Institute) accredited independent certification organization that performs functional safety (IEC 61508 family of standards) and cybersecurity (IEC 62443 family of standards) certification assessments.

exida Engineering provides the users of automation systems with the knowledge to cost-effectively implement automation system cybersecurity, safety, and high availability solutions. The exida team will solve complex issues in the fields of functional safety, cybersecurity, and alarm management, like unique voting arrangement analysis, quantitative consequence analysis, or rare event likelihood analysis, and stands ready to assist when needed.

Training

exida believes that safety, high availability, and cybersecurity are achieved when more people understand the topics. Therefore, exida has developed a successful training suite of online, on-demand, and web-based instructor-led courses and on-site training provided either as part of a project or by standard courses. The course content and subjects range from introductory to advanced. The exida website lists the continuous range of courses offered around the world.

Knowledge Products

exida Innovation has made the process of designing, installing, and maintaining a safety and high availability automation system easier, as well as providing a practical methodology for managing cybersecurity across the entire lifecycle. Years of experience in the industry have allowed a crystallization of the combined knowledge that is converted into useful tools and documents, called knowledge products. Knowledge products include procedures for implementing cybersecurity, the Safety Lifecycle tasks, software tools, and templates for all phases of design.

Tools and Products for End User Support

- exSILentia® – Integrated Safety Lifecycle Tool

- PHAx™ (Process Hazard Analysis)
- LOPAx™ (Layer of Protection Analysis)
- SILAlarm™ (Alarm Management and Rationalization)
- SILect™ (SIL Selection and Layer of Protection Analysis)
- Process SRS (PHA based Safety Requirements Specification definition)
- SILver™ (SIL verification)
- Design SRS (Conceptual Design based Safety Requirements Specification definition)
- Cost (Lifecycle Cost Estimator and Cost Benefit Analysis)
- PTG (Proof Test Generator)
- SILstat™ (Life Event Recording and Monitoring)

- exSILentia® Cyber- Integrated Cybersecurity Lifecycle Tool
  - CyberPHAx™ (Cybersecurity Vulnerability and Risk Assessment)
  - CyberSL™ (Cyber Security Level Verification)

Tools and Products for Manufacturer Support

- FMEDAx (FMEDA tool including the exida EMCRH database)
- ARCHx (System Analysis tool; Hardware and Software Failure, Dependent Failure, and Cyber Threat Analysis)

For any questions and/or remarks regarding this White Paper or any of the services mentioned, please contact exida:

exida.com LLC

80 N. Main Street

Sellersville, PA, 18960

USA

+1 215 453 1720

+1 215 257 1657 FAX

info@exida.com