Architectural Constraints and Tracking Performance of Field Devices

Nagappan Muthiah, Aracely Acevedo – Wood Group Mustang

Abstract: In order to make process plants compliant with IEC 61511, upgrade or grass roots projects sometimes oversupply redundant hardware or don't have enough redundancy in their design and hence, fail to meet Hardware Fault Tolerance (HFT) requirements. This paper emphasizes a holistic approach to satisfy IEC-61511 HFT requirements. It is important to understand that architectural constraints should be considered along with PFDavg calculations when verifying Safety Integrity Level (SIL). Tracking performance of field devices can help optimize how much redundancy is needed.

1. INTRODUCTION

The Functional Safety standard, IEC 61511-1 provides the framework, definitions, system, hardware and software requirements for Safety Instrumented Systems (SIS) for the process industry sector. Whether good engineering practice or required by regulation, SIS designers, integrators and end users should follow IEC 61511 while designing and using a SIS for the process industry. Process industries include chemicals, oil refining, oil and gas production, pulp and paper, non-nuclear power generation.

1.1. IEC 61511 SAFETY LIFECYCLE

IEC 61511-1 defines the Safety Lifecycle as: "*necessary activities involved in the implementation of safety instrumented function(s) occurring during a period of time that starts at the concept phase of a project and finishes when all of the safety instrumented functions are no longer available for use*" [1]

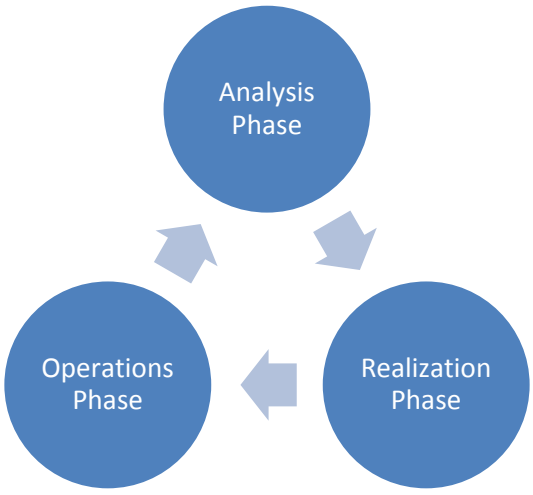

Figure 1. Safety Lifecycle Phases

The Safety lifecycle encompasses all the steps needed for ensuring that a reliable and effective SIS is defined, implemented and maintained, starting at the conceptual design, through operations and maintenance, to decommissioning. It can be broadly divided into 3 phases as shown in Figure 1, Analysis, Realization and Operations.

In the Analysis phase, hazards are identified, risks are evaluated and the necessary safeguards and safety functions that reduce the risk to a level that is acceptable by the end user are identified. It is during this phase that the Safety Integrity Level (SIL) of the Safety Instrumented Functions (SIF) is also defined.

In the Realization phase, the conceptual design of the safeguards and SIFs is converted to detailed design. After the completion of detailed design, verification and testing is performed to ensure that the current design meets the reliability and availability requirements specified in the Analysis phase. The SIS is then implemented in the field.

Finally in the Operations phase, the SIS is operated, tested and maintained through the rest of its useful life. Once the SIS gets close to the end of its useful life, it is decommissioned and the Safety Lifecycle cycles back to Analysis phase.

This paper is focused on the Realization phase, particularly on the SIL Verification process and the role of Architectural Constraints in complying with IEC 61511-1 requirements.

2. SIL VERIFICATION

Each Safety Instrumented Function has two key performance parameters that have to be considered:

a) Is the Safety Function effective to protect against the hazard?
   It is necessary to make sure that the right type of sensors are used to measure the appropriate process variable and that the right action is taken to bring the process to a safe state.

b) Will the Safety Instrumented Function perform every time it is needed? Does it meet the SIL requirements?
   Compliance with SIL requirements is addressed by evaluating the following items
   1. SIL Based on Probability of Failure on Demand average (PFDavg)
   2. SIL Based on Architectural Constraints

It is a common mistake to consider only the failure rates of the devices and PFDavg calculations of the SIFs. During SIL Verification, it is important to realize that Architectural Constraints are also a factor per the standard for compliance with SIL requirements.

3. ARCHITECTURAL CONSTRAINTS

Architectural constraints refer to the Hardware Fault Tolerance (HFT) requirements defined by IEC 61511 to achieve each SIL. The intention of these requirements is to prevent designs that are based on extremely low failure rate data for devices, that don't necessarily reflect the actual behavior of the elements under specific process and environmental conditions and could result in systems being under-designed or "less safe" than required. Additionally, it prevents designs that rely on very high (and usually not practically achievable) test frequencies.

With this in mind, IEC 61511 has defined two sets of HFT requirements that prescribe the level of redundancy needed: one for Programmable Electronic (PE) Logic solvers, that use microprocessors, and another for field devices and non-PE logic solvers. The figure below explains the different approaches allowed by IEC 61511.

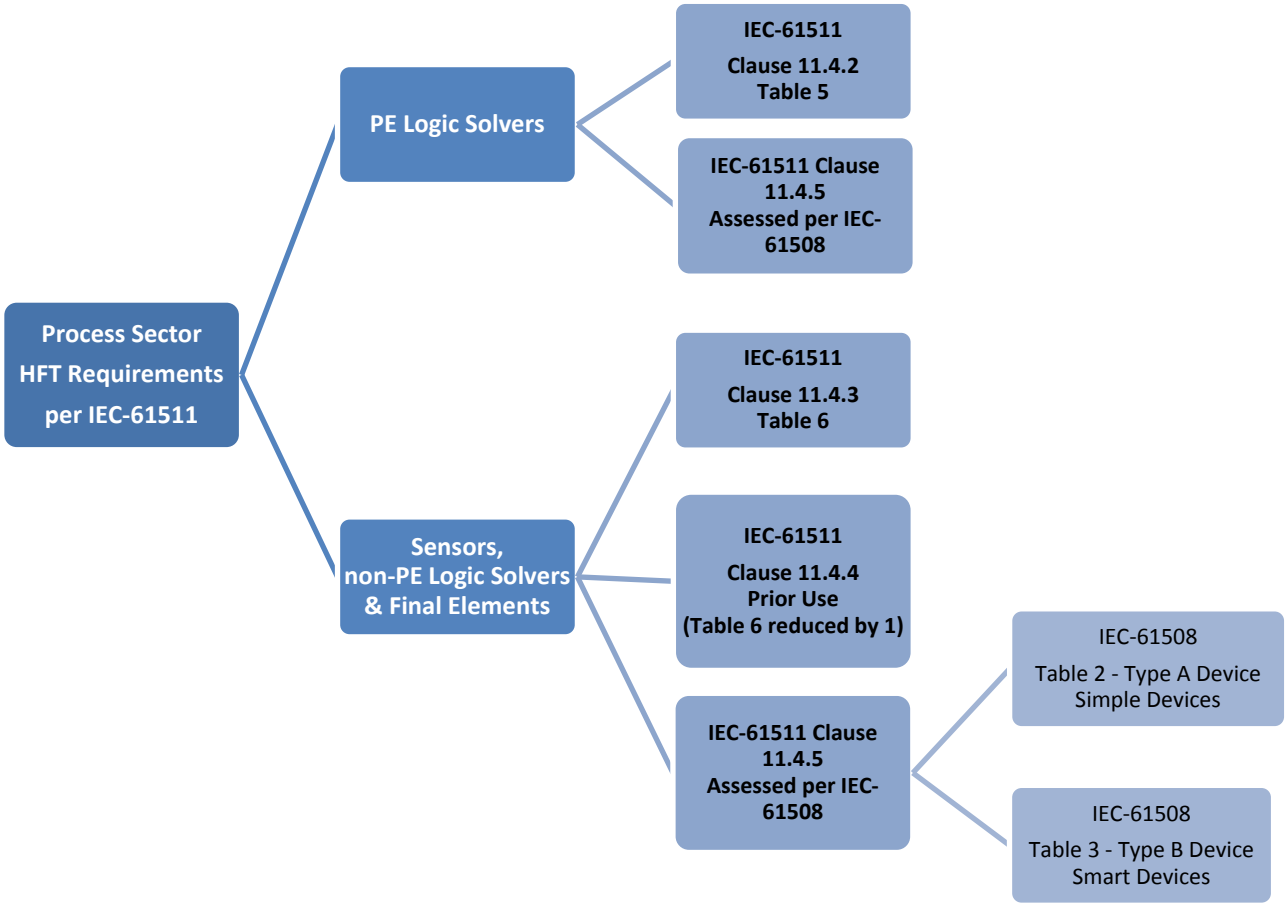

Figure 2. IEC 61511 Hardware Fault Tolerance Requirements

3.1. PE Logic Solvers

Minimum HFT for PE Logic Solvers is defined in IEC 61511 depending on the Safe Failure Fraction (SFF) of the device. According to Clause 11.4.2 Table 5, Minimum HFT for PE Logic Solvers shall be as depicted in Figure 3.

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

Figure 3. Minimum HFT of PE logic solvers per IEC 61511 - Table 5

Industry generally accepts the use of general purpose PLCs for SIL 1 applications without redundancy by making an implicit assumption that SFF is between 60% and 90%. If Logic Solvers are assessed per IEC-61508, then the HFT tables from 61508 can be used.

3.2. Sensors, non-PE Logic Solvers and Final Elements

IEC 61511 defines HFT requirements for *"all subsystems (for example, sensors, final elements and non-PE logic solvers) except PE logic solvers"* [1] in Clause 11.4.4 Table 6 as show in Figure 4.

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

Figure 4. Minimum HFT of sensors & final elements & non-PE logic solvers per IEC 61511-Table 6

The above table is applicable provided that the dominant failure mode is to the safe state or dangerous failures are detected, otherwise the fault tolerance shall be increased by one. This requirement will apply for energize to trip configurations [1].

The HFT requirements in Figure 4 are a conservative approach when compared with requirements in IEC 61508-2 as it is assumed that if it is a simple device, the SFF is always less than 60% and if it is a smart device, the SFF is always between 60% to 90% [2]. In some cases, this can result in over-redundancy which in turn can result in high initial capital and lifecycle costs for the implementation of SIFs.

Taking this into consideration, IEC 61511 provides alternatives to reduce HFT requirements defined in Figure 4 , as long as other required conditions are properly fulfilled and when there is a complete understanding of the failure modes of the elements under evaluation in the application specific process conditions.

3.2.1. Selection Based on Prior Use

IEC 61511 Clause 11.4.4 allows for the reduction of HFT requirements for Sensors, non-PE logic solvers and final elements in Figure 4 as long as the devices comply with the following conditions:

- *"the hardware of the device is selected on the basis of prior use (see 11.5.3);*
- *the device allows adjustment of process-related parameters only, for example, measuring range, upscale or downscale failure direction;*
- *the adjustment of the process-related parameters of the device is protected, for example, jumper, password;*
- *the function has a SIL requirement of less than 4."* [1]

Compliance with the last three requirements of Clause 11.4.4 is considered relatively "easy" to achieve; it is the compliance with prior use claim (i.e. proven in use) requirements that demands more attention. For devices selected based on prior use, the resulting HFT table in Figure 5 is used.

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

Figure 5. HFT requirements based on Prior Use per IEC 61511-Table 6

The standard requires "*appropriate evidence*" of the suitability of components and subsystems for its use in a specific Safety Instrumented System and asks for the evidence to include:

- *"Consideration of the manufacturer quality, management and configuration management systems;*
- *Adequate identification and specification of the components or subsystems*
- *Demonstration of the performance of the components or subsystems in similar operating profiles and physical environments*
- *The volume of operating experience*" [1]

Claiming prior use compliance can be seen as a tempting "way-out" of restrictive or overly conservative HFT requirements of IEC 61511 Table 6; however, it must be kept in mind that *appropriate evidence* needs to be available. The rest of this paper will cover how to acquire that appropriate evidence using information from tools and tasks that are very likely to be already in place in a typical process industry facility.

3.2.2. Selection Based on IEC 61508

For devices that have better SFF than the assumptions made in IEC 61511, clause 11.4.5 allows the use of HFT requirements, referenced in IEC 61508-2, provided that the devices are assessed per IEC 61508 requirements by third party companies like TÜV or exida (i.e. SIL certified devices). Refer to [3] for more details.

4. TRACKING PERFORMANCE OF FIELD DEVICES

Prior use compliance allows the end user to take advantage of the operating experience of field devices either in safety or non-safety applications, giving the user the opportunity to select devices that have been used in actual field conditions and that are well understood by operations and maintenance personnel. Hence, it is essential that operating companies closely track the performance of the field devices that can allow them to take credit for "Selection based on prior use" and possibly reduce the amount of redundancy needed based on HFT requirements of IEC 61511.

4.1. What data is needed?

Appropriate evidence of a device being proven-in-use requires the construction of an operating profile that should compile some relevant information about the device and its operating conditions. Figure 6 shows some of the important points to be considered when constructing an appropriate operating profile [4].

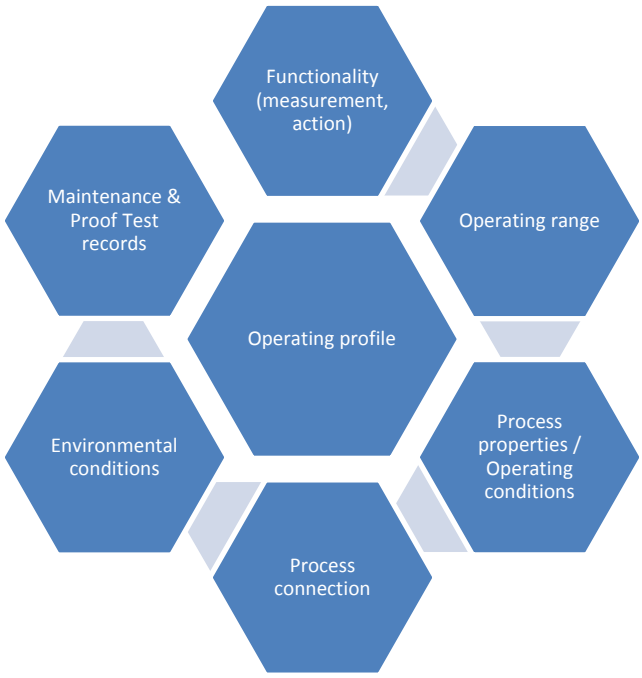

Figure 6. Device Operating Profile Construction

Construction of the operating profile of a device should answer the two questions stated in Section 2 of this paper:

Is the Safety Function (in this case the particular field device) effective to protect against the hazard? It should be ensured that the appropriate technology is being used for a particular application in terms of the selection of: measuring method, wetted materials, housing (weather and/or hazardous area protection method), connections to process, electrical connections and protection.

Will the Safety Function perform every time it is needed? The collection of maintenance and proof test records can be used to provide an answer to this question, as a failure model of the field devices can be constructed after proper data analysis is performed.

4.2. Where to find this data?

Using the already existing maintenance management systems and tools, the performance of field devices can be tracked and a body of knowledge can be constructed that can be used as the required evidence for proven-in-use compliance. It is also a tool for validation of the actual failure rates of a SIF vs. the failure rates used in the SIL verification – PFDavg calculations and an evaluation of the real performance of the SIF under actual application conditions.

End users should also include documentation of proof test results and device diagnostic information with special attention on actual automatic diagnostics and proof test coverage.

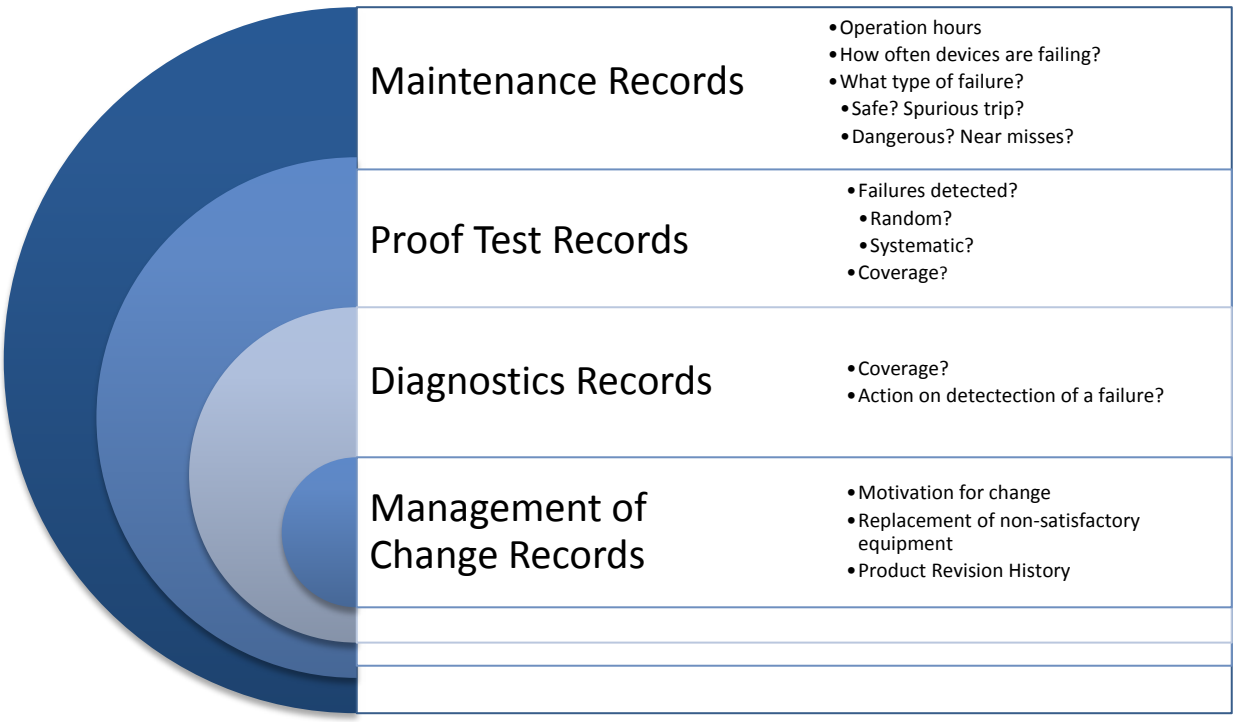

Figure 7. Device performance tracking tools

Figure 7 shows the various methods and tools that can be used for tracking the performance of field devices and some of the important types of information to be collected.

4.2.1. Maintenance Records

Tracking of the maintenance records of field devices should be done in the form of a centralized database. There are several maintenance management systems that are currently used by various process safety facility maintenance teams to plan and execute preventive and corrective maintenance tasks. Existing records in these systems can be used to find out how often the field devices are failing.

4.2.2. Proof Test Records

The Safety Requirements Specification provides the proof test requirements for each safety instrumented function; however, it is important to read the safety manual of each field device or company standards to understand the proof test coverage of different types of testing. For instance, testing of a transmitter may not include testing the impulse lines and therefore not all possible failures will be detected.

As an example, the Rosemount 3051S Safety certified transmitter manual [5] specifies 2 methods of proof testing and their corresponding test coverage. A simplified version is shown below.

Proof Test 1 (Analog output loop test)	Proof Test 2 (Sensing element testing)
1. Required tools: HART host/communicator and mA meter.	1. Required tools: HART host/communicator, mA meter and pressure calibration equipment.
2. Use the HART host/communicator to enter the mA value representing a high/low pressure alarm.	2. Perform the analog output loop test according to Proof Test 1.
3. Use the mA meter to read the current output of the device and check that it corresponds with the set value.	3. Perform a two point calibration check according to the range of the transmitter.
4. Document the results	4. Use the mA meter to read the current output of the device and check that it corresponds to the pressure input value
	5. Document the results.
Proof Test Coverage: <60%	**Proof Test Coverage: >90%**

Figure 8. Example Proof Test Coverage for pressure transmitters

For this particular example, Proof Test 1 does not include testing of the actual pressure sensing element, but only the analog output circuit resulting in a lower Proof Test Coverage than Proof Test 2. Proof Test 2 includes testing of the sensing element by actually applying pressure to the sensing element and providing a Proof Test Coverage greater than 90% for the pressure transmitter. However, if the calibration pressure is applied close to the sensing element, impulse line testing may not be included in this procedure and failures like plugging or freezing may not be detected. Proof test procedures should consider failures associated with the device installation, not just the safety manual requirements.

Anytime a failure is detected during proof testing, that data should be captured in the maintenance records. Sometimes the technicians may fix something in the field to make the proof test pass. It is important to document such type of "as found as left" information back to the maintenance records central database.

4.2.3. Diagnostics Records

Diagnostics can be used to detect failures in field devices. As operating companies start upgrading to Smart field instrumentation, the diagnostics coverage continues to improve as these Smart devices have many inbuilt features that allow self-detection of faults and failures. Some of the typical diagnostics are listed below:

- Plug impulse line detection
- Partial stroke testing of valves
- Deviation alarms of transmitters in similar service
- Valve Positioner self-diagnostics (pressure vs. stroke, air supply pressure, load pressure, drive signal)

These types of failures detected based on diagnostics should also be tied back to the maintenance records central database.

4.2.4. Management of Change Records

The management of change work process should provide information to the maintenance records central database. Anytime a certain field device is replaced or upgraded to a newer hardware or firmware revision, that information should be recorded properly. Such type of changes can affect the operational hours of the field instruments under consideration.

Motivation for changes should also be documented as they can be triggered by non-satisfactory performance of devices.

4.3. How to analyze this data?

After the above mentioned records are gathered, data needs to be analyzed so that information relevant to performance of the devices is presented in an appropriate way for SIS design purposes.

IEC 61511 Clause 5.2.5.3 specifies the implementation of procedures to evaluate the performance of the SIS during the Operational phase against the design requirements and assumptions made in the Analysis phase. The clause requires procedures for:

- *"identification and prevention of systematic failures which could jeopardize safety;*
- *assessing whether dangerous failure rates of the safety instrumented system are in accordance with those assumed during the design;*

- *assessing the demand rate on the safety instrumented functions during actual operation to verify the assumptions made during risk assessment when the integrity level requirements were determined"*[1]

A root-cause analysis should be performed on maintenance, proof-test and diagnostic records to identify the possible causes of device failures and then categorize the type of failures:

- Was this a random failure?
- Were there evidences of systematic failures in repair order cases? For example, inadequate installation of devices or inappropriate selection of a device for a given application.
- Was the failure safe or dangerous? (i.e. Did it cause a spurious trip or was it only detected at Proof Test?) Frequency of spurious trips should also be considered as it can be an indication of design deficiencies (systematic failure).
- Do we have common cause resulting in multiple failures? For example, failure of power or instrument air supply systems.
- Did the failure have no effect on the SIF performance? For example, if a transmitter's calibration is slightly off, this should not be logged as a dangerous failure if the SIF is looking for something not affected by accuracy such as a no-flow condition.

The maintenance records should allow analysis of data to recognize failure patterns. Additionally the repair time for each work order should also be documented. For example, there should be a way to provide statistical analysis of failure data by equipment model number or equipment type that can provide the following information:

- Safe Failure Rate
- Dangerous Failure Rate
- Operational hours
- Mean Time to Repair

Gathering such information allows for truly gauging the performance of the field devices used in the SIS design. Accumulation of this information over several years and several similar locations can help provide the "evidence" needed for proven-in-use compliance per IEC 61511 Clause 11.4.4. Combining all this data together will also allow verification and validation of the failure rate data that was used in the PDFavg SIL calculations.

4.4. What is the bottom-line?

An operating company's selection of field devices based on prior use can be paraphrased as follows:

- Having a specific manufacturer in the facility or company approved vendor list based on the good experience to date with specific manufacturer's products.

- The devices are selected according to specific datasheets. The devices are completely identified and versions of firmware are known.
- The device is used in control or safety applications. It has a history of good performance and periodic maintenance and testing of the device gives satisfactory results. No failures have been detected in a long time.
- The device is used in this facility and also in other similar facilities of the same company with a good performance history.

In order to comply with IEC 61511, attention should be directed to having *"appropriate evidence"* for each of the statements above, to make the selection based on prior use claim justifiable. A performance tracking management system should be implemented to provide such evidence. This system can utilize the information from the maintenance, diagnostics and testing tools currently in place in any process facility.

5. CONCLUSION

Tracking performance of field devices is essential to gather relevant information for both of the following a) Proven-in-use justifications aiming to optimize the minimum HFT requirements. b) Provide feedback of an operating SIS to validate assumptions made during the SIS design stage for key parameters such as device failure rate, common cause failure, actual proof test intervals and SIF demand rate.

6. ACRONYMS

SIS	Safety Instrumented Systems
SIL	Safety Integrity Level
SFF	Safe Failure Fraction
HFT	Hardware Fault Tolerance
PE Logic Solvers	Programmable Electronic Logic Solvers
PFD	Probability of Failure on Demand
PFDavg	Probability of Failure on Demand - average

7. REFERENCES

1. IEC 61511-1, International Electrotechnical Commission. Functional Safety - Safety instrumented systems for the process industry sector - Part 1: IEC, 2003

2. What does proven in use imply? Amkereutz, Rachel and van Beurden, Iwan.: Hydrocarbon Processing, 2004.

3. IEC 61508-2, International Electrotechnical Commission. Functional Safety of electrical/electronic/ programmable electronic safety-related systems - Part 2: IEC, 2010.

4. IEC 61511-2, International Electrotechnical Commission. Functional Safety - Safety instrumented systems for the process industry sector - Part 2: IEC, 2003

5. Rosemount 3051S Safety-Certified. Manual Supplement. Rosemount Inc.: Rosemount Inc, 2007. 00809-0700-4801, Rev BA.

6. Gruhn, Paul and Cheddie, Harry L. Safety Instrumented Systems: Design, Analysis and Justification: ISA, 2006.