Session 3:

Proof Test Procedure Effectiveness on Safety Instrumented Systems

Mohamed Abdelrhafour, TUV FS
Senior Control System Specialist,
Autopro Automation Consultants Ltd., Calgary, Alberta
Naresh Bajaj, P.Eng., CFSP
Electrical and Control Engineer,
Autopro Automation Consultants Ltd., Calgary, Alberta
Stephane Boily, P.Eng., CFSE
Safety System Technology Account Manager
Autopro Automation Consultants Ltd., Calgary, Alberta

Abstract

Proof tests are done periodically based on Safety Instrumented Function (SIF) design criteria and past experiences, to maintain Safety Integrity Level (SIL) ratings. Failure to perform an effective proof test may result in equipment damage, create an environmental hazard, or put personnel at risk. Requirements of proof tests are specified in IEC 61511; however, requirements can be interpreted differently. This paper will:

- Identify methods to calculate % proof test coverage and its importance in average Probability of Failure on Demand (PFDavg) calculations; and
- Review guiding principles upon which proof tests of Safety Instrumented Systems (SIS) should be developed;
- Highlight examples of good and poor practices.

Introduction

Safety Instrumented System (SIS) periodic proof test and diagnostic test are integral elements of the overall design and are required to ensure that the system will provide the risk reduction required to safely operate the facility. Their primary objective is to reveal undetected failures and, in the case of diagnostics, to alarm operations for a possible degradation in the SIS.

Another more important objective is to maintain the required level of safety integrity for a specified SIF. During the risk assessment phase of the safety lifecycle, risk reduction performance targets are set for the Safety Instrumented Functions (SIF). The Safety Requirements Specification (SRS) is then developed to clearly identify the many performance requirements of the SIS including proof testing requirements.

The effectiveness of a proof test is measured by its coverage factor (C_{PT}). This paper shows the impact of the effectiveness of a proof test on the achieved average Probability of Failure on Demand (PFDavg) of a device. It will then explore various approaches to evaluating the C_{PT} and show how this is directly related to the proof test procedures developed to test the SIF. The paper concludes by looking at a process of developing proof test procedures and it highlights some good and not so good proof test practices.

Diagnostic Tests Vs. Proof Tests

IEC 61511-2003 defines Proof Test as follows: “test performed to reveal undetected faults in a safety instrumented system so that, if necessary, the system can be restored to its designed functionality” (IEC 61511-2003 part 1 clause 3.2.58).

Diagnostic tests are normally referred to as online tests or automated tests and are performed either continuously or very frequently. Diagnostic tests detect dangerous failures and can change them to “safe” failures by bringing the process to a safe state or alarm operations/maintenance personnel to take some action.

On the other hand proof tests verify that the device will respond as expected to an unsafe condition and has not experienced a dangerous undetected failure.

Diagnostic tests are usually performed online through diagnostic hardware and software features often built into components (e.g., memory test, CPU test, internal watch dog, and HART diagnostics). Some forms of diagnostics are external to the components such as automated partial stroke test for final elements.

Proof tests are usually performed at pre-defined test intervals per the Safety Requirement Specification (SRS). Ideally real operating process conditions should be present or simulated for the proof tests and can be divided into parts versus complete end to end testing depending upon safety conditions.

The advantage of diagnostic tests is that they can detect failures online. Whereas a proof test is performed at a predefined time interval, then there is chance that the process could be running with a failed safety function for a long time before it is revealed.

Proof Test Coverage (C_{PT}) and its effect on PFDavg

Proof testing has significant influence on the final PFDavg value and the effectiveness of proof testing is not negligible. The effectiveness of a proof test is measured by its C_{PT}. The proof test coverage factor (C_{PT}) gives the fraction of dangerous undetected failures which can be detected by proof testing. [5, 7]

Proof test coverage is calculated as:

$$C_{PT} = \frac{\lambda_{DU_{Identified\ by\ PT}}}{\lambda_{DU_{Total}}}$$

Where:

C_{PT}	is the proof test coverage;
$\lambda_{DU_{Identified\ by\ PT}}$	is the dangerous undetected failure rate identified by the proof test; and
$\lambda_{DU_{Total}}$	is the total dangerous undetected failure rate.

The following simplified equation can be used to show the impact of proof test coverage on the PFDavg for a 1oo1 configuration.

$$PFD_{AVG} = \frac{\lambda_{DU_{Total}} \times C_{PT} \times TI}{2} + \frac{\lambda_{DU_{Total}} \times (1 - C_{PT}) \times MT}{2}$$

Where:

TI	: Proof test interval
MT	: Mission Time

These parameters influence the final PFDavg calculation and the ultimate integrity of the SIF. [5]

The data used in the following table and graphs were calculated using commercially available software based on Markov modeling. It shows the impact of proof test coverage on the PFDavg for a generic Coriolis Flow Transmitter with failure rate of 900 FITs [4] , a 10-year mission time, common cause failure rate (β) of 10% for redundant architectures and a proof test interval of three (3) years.

Figure 1: Effect of C_{PT} on PFDavg for a generic flow transmitter in a 1oo1 architecture ($\lambda_{DU_{Total}}$=9.00*10^{-7}failures/hour, TI= 3 years and MT= 10 years)

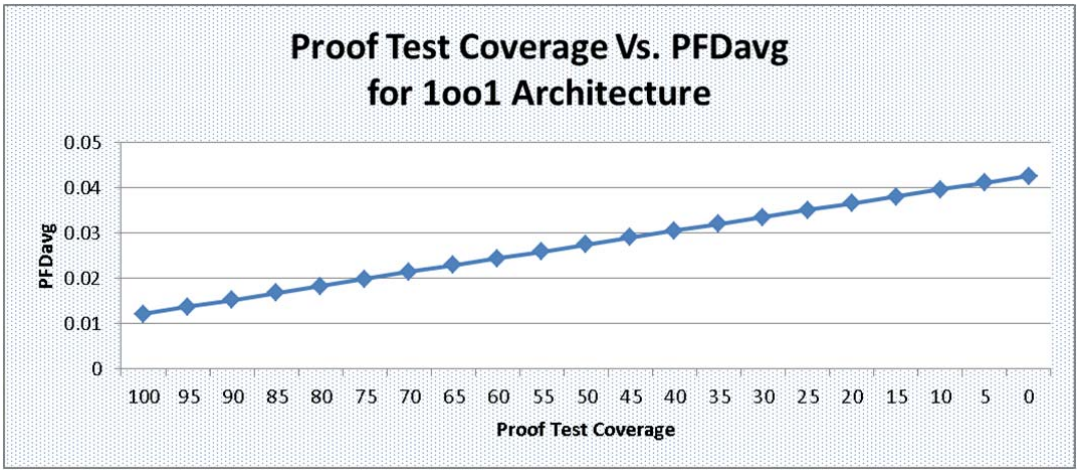


Figure 2: Effect of C_{PT} on PFDavg for a generic flow transmitter in a 2oo3 architecture ($\lambda_{DU_{Total}}$=9.00*10^{-7}failures/hour, TI= 3 years, MT= 10 years and β = 10%)

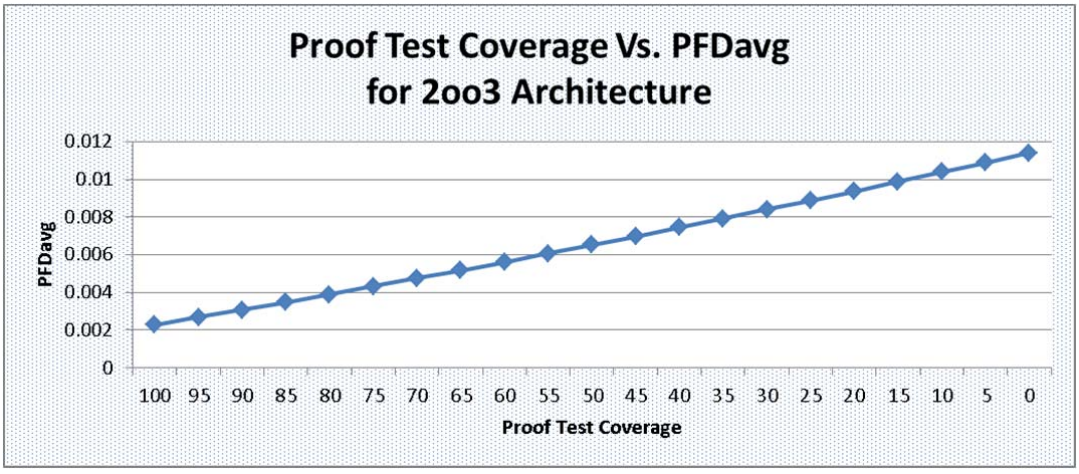


Table 1: Influence of C_{PT} on PFDavg for a generic flow transmitter in a redundant/voting architecture. ($\lambda_{DU_{Total}}$=9.00*10^{-7}failures/hour, TI= 3 years, MT= 10 years and β = 10%)

Proof Test Coverage	PFDavg 1oo1	Change (%)	PFDavg 1oo2	Change (%)	PFDavg 2oo2	Change (%)	PFDavg 2oo3	Change (%)
100	0.0121	0	0.001390	0	0.0227	0	0.00229	0
99	0.0125	3	0.001430	3	0.0233	3	0.00236	3
98	0.0128	6	0.001480	6	0.0238	5	0.00244	7
97	0.0131	8	0.001520	9	0.0244	7	0.00252	10
96	0.0134	11	0.001560	12	0.0249	10	0.00260	14
95	0.0137	13	0.001610	16	0.0255	12	0.00268	17
94	0.0140	16	0.001650	19	0.0260	15	0.00276	21
93	0.0143	18	0.001690	22	0.0266	17	0.00284	24
92	0.0146	21	0.001740	25	0.0272	20	0.00292	28
91	0.0149	23	0.001780	28	0.0277	22	0.00300	31
90	0.0152	26	0.001830	32	0.0283	25	0.00308	34
85	0.0168	39	0.002050	47	0.0310	37	0.00349	52
80	0.0183	51	0.002270	63	0.0338	49	0.00390	70
75	0.0198	64	0.002500	80	0.0365	61	0.00432	89
70	0.0214	77	0.002730	96	0.0393	73	0.00475	107
65	0.0229	89	0.002970	114	0.0420	85	0.00518	126
60	0.0244	102	0.003200	130	0.0447	97	0.00562	145
55	0.0259	114	0.003440	147	0.0474	109	0.00607	165
50	0.0275	127	0.003680	165	0.0501	121	0.00652	185
45	0.0290	140	0.003930	183	0.0528	133	0.00698	205
40	0.0305	152	0.004180	201	0.0555	144	0.00745	225
35	0.0320	164	0.004430	219	0.0582	156	0.00792	246
30	0.0335	177	0.004680	237	0.0608	168	0.00840	267
25	0.0350	189	0.004940	255	0.0635	180	0.00889	288
20	0.0365	202	0.005200	274	0.0661	191	0.00938	310
15	0.0380	214	0.005460	293	0.0687	203	0.00988	331
10	0.0396	227	0.005720	312	0.0714	215	0.01040	354
5	0.0411	240	0.005990	331	0.0740	226	0.01090	376
0	0.0426	252	0.006260	350	0.0766	237	0.01140	398

The result demonstrates that the proof test coverage cannot be neglected.

If it is necessary to claim 100% proof test coverage during a SIL verification in order to achieve the target risk reduction, then it will also be necessary to develop a proof test procedure that is able to reveal 100% of the dangerous failures that cannot be detected by diagnostics. In addition, the test should be performed without possibility of human errors. It is unlikely to be able to achieve 100% proof test coverage in the field but we nevertheless must strive to get as close to 100% as practical.

One Approach to Obtaining C_{PT} – Certified Devices

We have seen how critical the proof test coverage can be on a SIF; however, obtaining proof test coverage factors for various devices may be difficult. To calculate the proof test coverage, it is necessary to have the failure rates of the different failure modes of all the devices used in the SIF and evaluate how the proof test detects each failure mode.

Some manufacturers of equipment have their equipment assessed to comply with IEC 61508. Purchasing equipment that has been assessed and certified compliant with IEC 61508 gives the advantage of having failure rates available. In this case, the manufacturer usually provides the proof test procedure(s) and associated proof test coverage. It is sometimes the case that multiple test procedures are provided, each with different proof test coverage. As well, a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) report will normally be available for certified equipment. An FMEDA is a systematic detailed procedure used to determine, in a predictive manner, the failure modes and failure rates of an instrument. If the report includes the full FMEDA analysis, then details of the failure modes and their associated failure rates will be available. This makes it easier to design proof tests to cover the maximum number of dangerous undetected failures and, consequently, calculate the proof test coverage associated.

When preparing proof test procedures for an existing facility where the equipment in place is not certified to IEC 61508, it is much more difficult to estimate the proof test coverage achieved by the proof test and inspection. Unless the facility has a reliable data collection program in place, which has been running for a few years, where the failures and failure modes are recorded, failure data is generally not available making it difficult to evaluate the proof test coverage.

Another Approach to Obtaining C_{PT} – Example Credit System

An approach to estimating the proof test coverage that the authors of this paper have recently seen used in one existing facility uses a form of standardized “credit” system, where a fraction of the overall proof test coverage is given to different test and inspection activities based on the type of equipment. This older facility was designed prior to the publication of IEC 61511. Consequently the instrumented protective functions had not been designed and implemented per the requirements of the standard. However, management at the facility recognized the value of new safety standards, such as IEC 61511, and implemented new corporate standards and guidelines accordingly. These include new risk assessments and assigning risk reduction targets to the existing instrumented protective functions. During these reviews it was found that some of these instrumented protective functions required a risk reduction, which made them fall into the category of SIFs per IEC 61511. Following this, effort was made to assess the “As Is” state of the SIFs by documenting their performance in an “As Is” SRS, and calculating the risk reduction achieved by each SIF. This was done by performing reliability calculations on the hardware and looking at the existing test and inspection plans in order to compare with the risk reduction targets. Using the results of the “As Is” reliability calculations,

various recommendations were made in order that the target risk reduction may be achieved.

To estimate the proof test coverage achieved by the existing test and inspection plans, generic tables were developed for sensors, logic solvers, valves, and motors. We will limit the scope of this discussion to the tables that were developed for sensors and valves.

Note: It is important to note that at this facility these tables were intended to be used as guidelines only. The reliability engineer must still use experience and judgment and can use different values for the proof test coverage if more data is available.

The calibration of the tables shown below tends to generate conservative values of proof test coverage.

Table 2 describes the test and inspection activities proposed for a generic analog sensor.

Table 2 – Sensor Proof Test Coverage Per Activity

Sensor _____	
Test/Inspection Action	**Suggested Proof Test Coverage (%)**
Visual field inspection of field sensor: • Installation, • Sensing lines, • Utilities and cabling, • etc. (Ref.: ISA TR84.00.03).	0 - 20
Compare sensor signal with local gauges, or Compare sensor signal with other measurements using history trends.	0 - 35
Single-point calibration checks (e.g. zero check).	5
Three-point calibration check (do not take also credit for single-point check).	20
Simulate field signal and verify in DCS or, using Smart communicator or HART AMS, perform high and low output diagnostic checks and verify in DCS. Also verify state of safety critical software parameters (i.e., tx fail action, eng range, damping) and diagnostic flags using Smart communicator or HART AMS.	20
Proof Test Coverage Total	

Table 3 below describes the test and inspection activities proposed for a typical shut-off valve.

Table 3 – Valve Proof Test Coverage Per Activity

Valve _____ ANSI Leakage Class Requirement _____			
Test/Inspection Action		**Suggested Proof Test Coverage (%)**	
Visual Inspection of final element, accessories and utilities, etc. (Ref.: ISA TR84.00.03).		0-20	
Partial stroke test of valve (Manual).		10	
Stroke test of valve confirmed by visual inspection.		5	
Stroke test from logic solver.		5	
Stroke test under worst case process and ambient conditions (e.g., P&T).		10	
Full stroke test of valve (do not also take credit for partial stroke).		20	
Analyze valve stroke signature using smart valve positioner.		5	
Time stroking speed of valves and compare with history and SRS response time requirements.		5	
Seat loading test measured and compared to design specification.		5	
Choose only one of the following:			
ANSI Leakage Class Requirement.	I	II/III/IV	V/VI
Chose only one of these three tests:			
1. Visual inspection of valve sealing surfaces (e.g., seat/plug/gate/trim/seal ring, etc.).	20	15	5
2. Shop pressure leak-by test with results compared to ANSI Leakage Class requirement per SRS.	20	20	15
3. In-line pressure leak-by test with results compared to ANSI Leakage Class requirement per SRS.	20	20	20
Proof Test Coverage Total			

Example Credit System Applied to a Sensor

Based on the different tests and inspections performed by the existing test plans, proof test coverage can be estimated. For example: an existing SIF has a single pressure transmitter. The test plan for the transmitter states that it is to be tested every five years at turnaround. The plan includes:

- A visual field inspection must be performed (20%);
- A three-point calibration check is made (20%);
- A field signal test is performed up to the DCS and the transmitter parameters are verified (20%); and
- The results are documented and maintained.

Depending on the number of items that can be inspected for this device per the checklist, a number between 1% and 20% can be credited for the visual inspection. ISA TR84.03 section 7.4 and annex O can be used as an example of items to verify and a way to document issues during a visual inspection. In this case the proof test coverage could be 60% based on the values in Table 2.

Note: It is important to note that the results of the three-point calibration check must be recorded along with the pass/fail results (i.e., per the criteria provided in the procedure) prior to re-calibrating the sensor. As well, the functional trip test of the SIF must be done prior to the calibration check. (At the above-mentioned facility, this was included in the logic solver test).

Example Credit System Applied to a Valve

In this case let's assume it is a shut-off valve requiring tight shut-off to ANSI class VI. The test plan states that the valve is tested every year. The plan includes:

- A visual inspection (20%);
- Time the stroking speed of valves and compare with history and SRS response time requirements (5%);
- A full stroke test of the valve (20%); and
- In-line pressure leak-by test compared to ANSI class VI leakage requirements (20%).

In this case, the proof test coverage estimated would be 65% for the valve assembly (i.e., valve and actuator) based on the values from Table 3.

A Third Approach to Obtaining C_{PT} – Failure Rate Databases

One possible way to complement the credit system approach is to develop tables of the most frequent failure modes and associated failure rates for different devices. Obtaining failure data for the different ways a device can fail can be a real challenge; in the absence of plant data, there are some databases that can be consulted. Some are based on predictive methods, such as FMEDA (e.g. ., exida SERH) and others are based on field failure collection programs (e.g., OREDA and PERD). Both types of databases are useful however in order to calculate a proof test coverage, the better sources will be those that provide more detailed descriptions of failure modes and their associated failure rates. In any case, the best source of data for any facility would be collected from field failures for the same equipment used in the same

facility or similar application under similar environmental and plant maintenance conditions.

For example some of the most frequent failure modes identified for a safety shut-off valve are shown in the following table:

Table 4 – Common failure modes for Safety shut-off valve

Failure Mode	Category(1)	Failure Rate(2) (FITs)
Valve fails to close	DU	250
Valve slow to close	DU	200
Valve leaks internally	DU	100
Valve leaks externally	SU	150
Other hidden failures(3)	DU	25

(1) The distribution of the failure modes in Dangerous Detected (DD) and Dangerous Undetected (DU) for the valve depends on the application.

(2) The values used here are for illustrative purposes only and do not represent neither actual nor generic failure rates.

(3) Hidden failures are those dangerous failures that would not be detected by proof test. Human factors could be one source of such failures.

Using the tests from table 4:

1) the full stroke test would detect the failure to close,
2) the time stroking speed test would detect that the valve is slow to close,
3) the leak test would detect the internal leak,
4) The visual inspection would detect the external leak.

Using the failure rates the proof test coverage associated to each test could be calculated with more precision as follows:

1) Full stroke test Proof Test Coverage = 250/(250+200+100+25) = 43%
2) Time stroking test Proof Test Coverage = 200/(250+200+100+25) = 35%
3) Leak test Proof Test Coverage = 100/(250+200+100+25) = 17%

The same approach can be used for the other devices used in a Safety Instrumented Function.

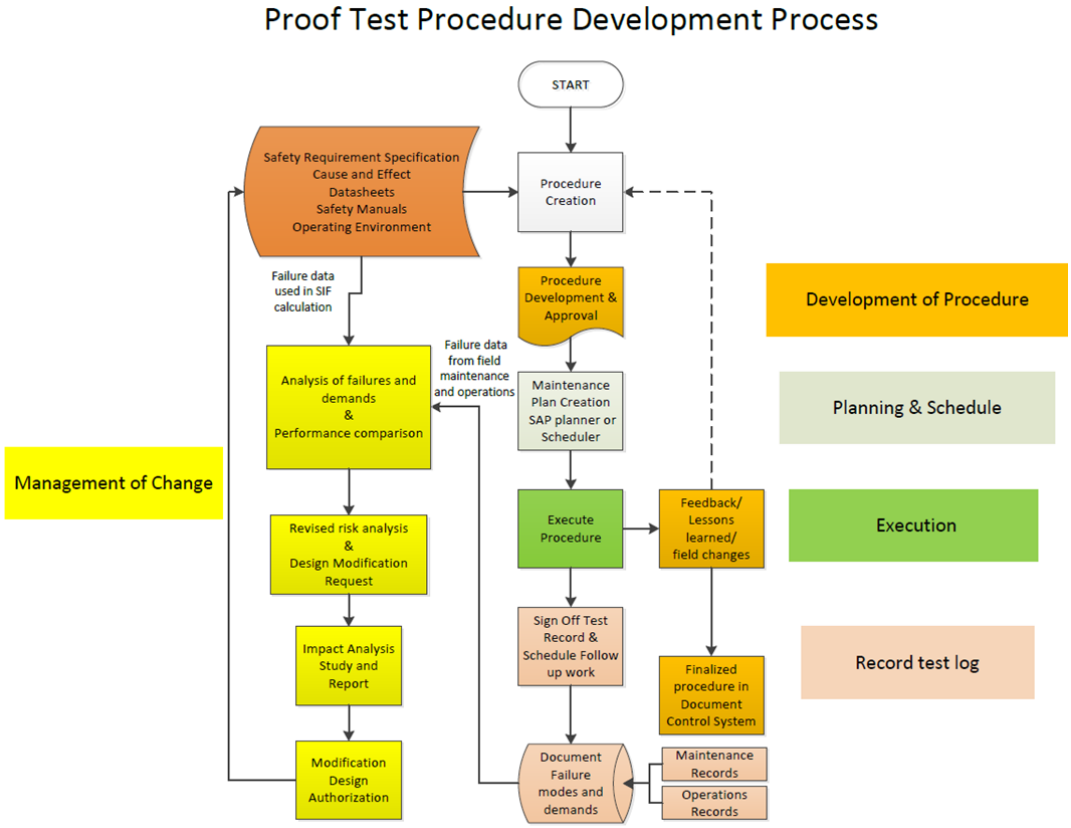
Proof Test Procedure Development Process

The proof test procedures must be controlled documents and could be managed using a process similar to the one shown below. The objectives of this process are to ensure:

1. that the procedures are fully tested while in a development stage,
2. that revisions are reviewed by a person responsible for the integrity of the SIS,
3. consistency among various business units and maintain a standard presentation for technicians to work with,

4. that failure data is collected from the field under operating conditions and used to adjust the necessary parameters of the proof tests (e.g. test frequency),
5. that a Management of Change is used to modify the design changes.

The following figure shows a proof test procedure development process at a high level.



Below are some of the recommendations and guiding principles to perform an effective proof test:

- The procedure should be written such that the full SIF trip test is performed first. It is possible to perform inspection prior to the trip test but in this case it is critical to not perform any repairs or cleaning prior to the trip test. This is to ensure that the conditions for the proof test are as close as possible as they would be if a demand were to occur.
- When testing sensors, it is imperative that proof tests should take into consideration different characteristics of the sensors. Evaluating the SIL requires consideration of the following characteristics during the proof test: accuracy, linearity, consistency and repeatability, immunity to EMI, hysteresis, and vibration.
- When testing valves, it is imperative that the proof test is able to detect different type of failures, such as: valve packing is seized or tight,

actuator airline is crimped or blocked, valve stem sticks, seat contains debris, seat plugged, etc.

- The test equipment used for conducting the proof testing should be subject to periodical calibration.
- Proof testing should conform as closely as possible to the exact operating conditions. Tests in the lab may not demonstrate that the SIS will function properly under operating conditions.
- The SRS should document the dangerous failure modes in order to assist with the development of the proof test procedures.
- The written proof test procedure should consider recognized human factors in order to reduce the potential for errors and violations.
- The proof test should be performed from end-to-end, including process connections, as simulations built into the system cannot demonstrate that the test is effective.
- The proof testing should also take in consideration the auxiliary equipment, such as power, instrument air, and heat tracing.
- Proof testing procedures should be reviewed and understood by the technician prior to the test. Personnel performing the test should be competent and able to interpret the result. Their responsibilities should be clearly identified and communicated.
- The scope of proof test procedures should be clear, and initial conditions prior to conducting the test should be in place.
- Planning and scheduling should be an integral part of the safety management system.
- The procedure should be clear, systematic, precise, and easy to understand and follow and have pass/fail criteria for each test and inspection.
- All successful and unsuccessful test records will be documented and maintained as records. Test records can be useful to perform future analysis and to build plant failure database.
- If the proof test is performed online, a plan must be in place where applicable to address a real demand in the event that one occurs during the proof test.
- Bypasses with alarms shall be provided as required by the proof test procedures. Testing of legacy systems that rely on the uses of forces shall have additional steps and checks in the procedures to verify that any forces put in places were removed at the completion of the tests.

On the flip side of the practices stated above, some bad practices to avoid include:

- Developing and/or using proof test procedures that are vague and general with statements like:
    a. “perform visual inspection” without providing a specific checklist of items to check.

    b. Non specific references such as: “User manual”
- Developing proof test procedures in a cocoon without the participation of the maintenance technicians who will be responsible for executing them.
- Not getting operation’s input into proof test procedures and proof test frequency.
- Calibrating the sensors prior to performing the trip test.
- Cleaning or performing preventive maintenance prior to performing the trip test.
- Claiming 100% proof test coverage.

Conclusion

The proof testing of SIS is defined in the safety standards (IEC 61508 and 61511) but the interpretation of it is ambiguous. The paper showed that choosing accurate C_{PT} has its own limitations due to different practical considerations and various factors influence the outcome.

The paper also demonstrated that there is a need to focus on the dangerous undetected failure modes. It also proposed a process which can help develop effective proof test procedures. Various methods to quantify the C_{PT} were explored which can be used in real world situations. It was confirmed that the impact of the C_{PT} is real. There’s no such thing as a perfect proof test although it is desirable to strive to get as close to it as possible. This is why the C_{PT} has to be addressed in Safety Life Cycle Management. .

References

[1] Feng Tao, Users need detailed reliability analysis not just numbers, IDC Safety Control Systems Conference 2010

[2] W.M. Goble and H.Cheddie, Safety Instrumented Systems Verification, Practical Probabilistic Calculations

[3] O’Brien, C. and Bredemeyer, L., Final Elements & the IEC 61508 and IEC 61511 Functional Safety Standards,

[4] Safety Equipment Reliability Handbook, exida

[5] D. Fournier, How critical is Proof Test Coverage?, You asked: Functional Safety Clarified, Canadian Process Equipment & Control News Aug 2009

[6] Principles for proof testing of safety instrumented systems in the chemical industry, Health & Safety Executive, contract research report 428/2002.

[7] György Baradits, János Madár, János Abonyi, Novel Model of Proof Test Coverage Factor, 10th International Symposium of Hungarian Researchers on Computational Intelligence and Informatics, Nov 2009