vague in all the necessary places can be a lot better than one that deceives and bemuses the reader with unjustified precision and certitude. If you really don't know how big 'big' is, you are doing no one any favours by pretending that you do.

Notes

1. As such, a vague expression is not to be confused with an ambiguous one. An ambiguous expression is one that has two or more interpretations, and for which a context is required to achieve disambiguation. Such ambiguity can be particularly problematic when it is still not obvious from the context which of the equally valid definitions is meant to apply. It is also important to understand that a loosely qualifying expression is not necessarily vague. For example, 'less than ten', is not vague, since its applicability is straightforward. However, 'nearly ten' is vague, because the applicability of the term 'nearly' is not clear-cut.

2. This is actually an urban myth. Cruel scientists have determined that real frogs aren't that inattentive.

3. These include ideas such as Supervaluationism, Subvaluationism, Contextualism, Epistemicism, Fuzzy Plurivaluationism and Many-valued Logic. If long and horribly contrived words are your thing, see *Further Reading*.

Further Reading

K. van Deemter, *Not Exactly - In Praise of Vagueness*, Oxford University Press, 2012.

R. Keefe, *Theories of Vagueness*, Cambridge University Press, 2006.

'Vagueness', *Stanford Encyclopaedia of Philosophy*, http://Plato.stanford.edu

R. van Rooij, 'Vagueness and Linguistics', *Researchgate.net*

T. W. Grinsell, 'Avoiding Predicate Whiplash: Social Choice Theory and Linguistic Vagueness', *Proceedings of the 22nd Semantics and Linguistics Conference (SALT 22), University of Chicogo 18-20 May 2012*, pp. 424-440.

How Big is Big? by an author unknown, and long out-of-print.

John Ridgway is a retired analyst who spent most of his career working for Serco Transportation Systems. Having failed to change the World, he now lives in quiet retirement with his wife and two dogs. He can be contacted at j.ridgway4@ntlworld.com.

Conforming to IEC 61511: Operation and Maintenance Requirements

by Steve Gandy

It is hard to believe that the IEC 61511 standard has been in existence since 2003 and most companies operating in the process, chemical and refining industries (or any other process manufacturing) have adopted its practices. It is also significant that any plants with a Safety Instrumented System (SIS) will now be halfway through their useful life. It therefore seems opportune to ask how well companies have been recording the performance of their SISs, in terms of failures, spurious trips, time to repair/restore and proof testing results. Furthermore, the new 2016 edition of IEC 61511 emphasises the need for assessment of SISs more strongly, soeaking in terms of preventing systematic issues through procedures and competency. This paper highlights how testing and documenting the performance of the SIS is an essential part of ensuring that it is able to fulfill designated functional safety requirements. This is especially true as the SIS approaches the end of useful life.

Introduction

Over the past decade or so, automation has been one of the dominant factors

in enabling end users in the process, chemical and petro-chemical industries to be able to streamline their costs and improve efficiency; often at the expense of personnel. Most modern plants today have less manpower than plants of 1980 and even the 1990s. This means that the burden of running and maintaining a modern plant has fallen on fewer and fewer plant personnel. Coupled with the shortage of skilled employees, this places a significant burden on plant personnel to maintain and improve their skill set in order to maintain the technologically more complex instrumentation and automation systems. Aside from the Basic Process Control System (BPCS), there's the Plant Safety System (referred to as the Safety Instrumented System (SIS).

The advent of the IEC 61511 standard [1] for the process industries has provided a path to improve safety by introducing the concept of a Safety Lifecycle (SLC) and moving away from a strictly prescriptive methodology to a more performance based methodology, with the emphasis being placed on reducing risk and mitigating the potential for hazards that could lead to the loss of life, destruction of property and plant assets. The purpose of this paper is not to define the application of the standard but to examine one important aspect of the SLC: the Operations and Maintenance requirements for the plant SIS.

IEC 61511-1 Clause 16: SIS Operations and Maintenance

The term 'SIS' has been used rather than the term 'safety system' as there are many safety systems, not all of which are intended to comply with IEC 61511. Only safety instrumented functions that are part of a Safety Instrumented Function (SIF) are required to comply. Figure 1 has been excerpted from ANSI/ISA 84.91.01-2012 [2] to provide an illustration.

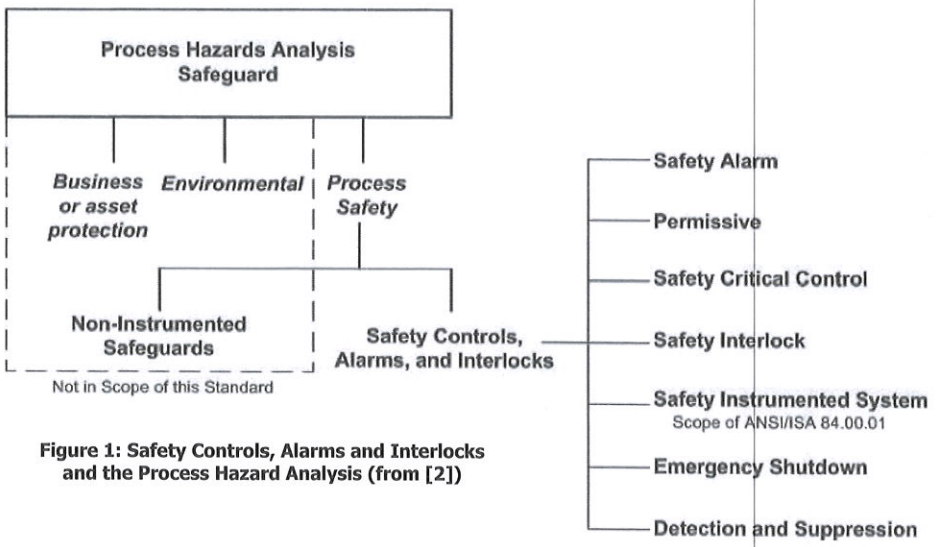

Figure 1: Safety Controls, Alarms and Interlocks and the Process Hazard Analysis (from [2])

The term 'SIS', as defined in IEC 61511-1 Clause 3.2.72, refers to a Safety Instrumented System, i.e. an instrumented system to implement one or more Safety Instrumented Functions (SIFs), which is composed of any combination of sensor(s), logic solver(s) and final element(s), as illustrated

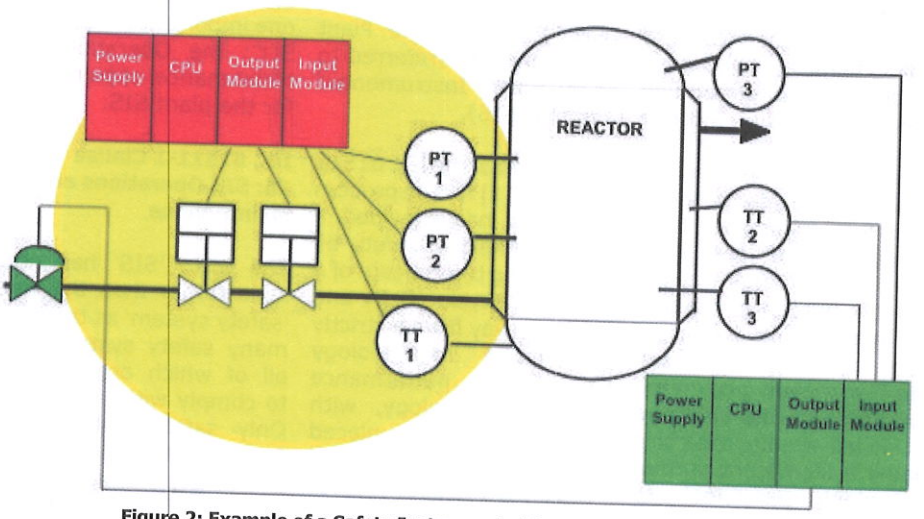

Figure 2: Example of a Safety Instrumented System Block Diagram

in Figure 2. A SIS can include safety instrumented control functions or safety instrumented protection functions, or both. A SIS may or may not include software (i.e. could be solid state or hardwired with electro-mechanical relays).

As mentioned in the introduction, the IEC 61511 standard is based around a Safety Lifecycle (SLC). Figure 3 illustrates a simplified version of the SLC and highlights the Operations and Maintenance Section of the lifecycle.

In order to fulfil the requirements of IEC 61511-1 Clause 16, the end user is required to have a properly and well defined Operation and Maintenance Plan to ensure that the required Safety Integrity Level (SIL) is maintained during operation and maintneance tasks to ensure that the SIS maintains its functional

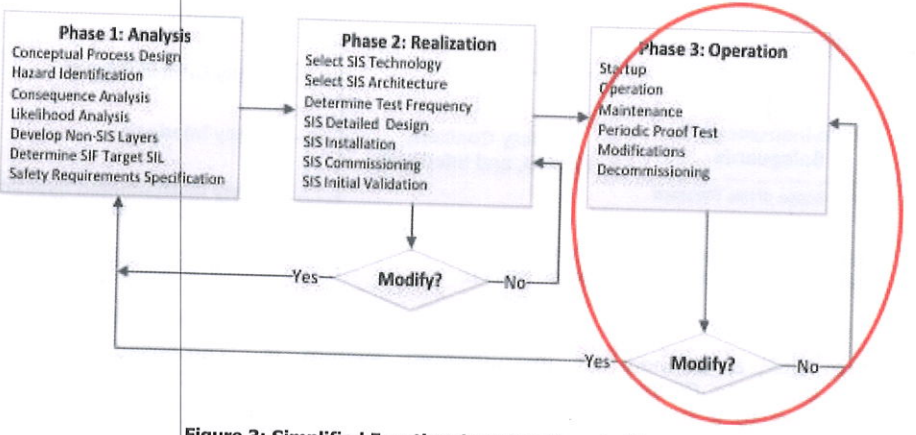

Figure 3: Simplified Functional Safety Lifecycle Diagram (Operations and Maintenance Phase Highlighted)

safety integrity throughout its entire lifetime.

The SIF and associated SIL are determined at the front end of the Lifecycle during the Analysis Phase and are beyond the scope of this paper.

The Importance of Leading and Lagging Indicators

IEC61511 is a "performance-based" standard that requires the owner/operators to undertake "periodic" assessments. This means that recording "lagging" data is essential. Lagging data would include such things as:

- Near misses;
- Trips, real and spurious;
- Faults, both random and systematic;
- Process upsets.

The purpose of lagging data is to be able to help in preventing future problems or events and/or developing training programs, procedure improvements, etc.

The purpose of "leading" indicators is to help predict future events. Examples of leading indicators would be:

- Inspections that were overdue;
- Maintenance that was not carried out in a timely manner (e.g. repair times exceeding the limits defined in the SRS).

By understanding both the leading and lagging indicators, operators can improve overall process safety, thus preventing potential spills, fires and explosions.

Operation and Maintenance Plan

The operation and maintenance plan is a working document that is designed to ensure the SIS is maintained to meet its designed functional safety and will need to cover:

- Routine and abnormal operation activities;
- Proof testing, preventative and breakdown maintenance;
- Procedures, measures and techniques to be used for operation and maintenance;
- Verification of adherence to operations and maintenance procedures;
- When these activities shall take place;
- The persons, departments and organisations responsible for these activities.

Procedures covering each of these aspects need to be developed and maintained, especially following any updates and/or modifications to the SIS. This could be viewed as developing a "safety checklist" that will help eliminate human (systematic) errors from creeping in during maintenance activities.

Operation and Maintenance Procedures

IEC 61511-1 Clause 16.2.2 states that the operation and maintenance procedures shall be developed in accordance with the relevant safety planning and shall provide the following:

- Routine actions which need to be carried out to maintain the "as designed" functional safety of the SIS, for example, adhering to proof test intervals defined by the SIL determination;
- Actions and constraints that are necessary to prevent an unsafe state and/or reduce the consequences of a hazardous event during maintenance or operation (for example, when a system needs bypassing for testing or maintenance, what additional mitigation steps need to be implemented);
- The information which needs to be maintained on system failure and demand rates on the SIS;
- The information which needs to be maintained showing results of audits and tests on the SIS;
- The maintenance procedures to be followed when faults or failures occur in the SIS, including: Procedures for fault diagnostics and repair, procedures for revalidation, maintenance reporting requirements

and procedures for tracking performance;
• Assurance that test equipment used during normal maintenance activities is properly calibrated and maintained.

These requirements place a heavy burden on the Operations and Maintenance (O&M) personnel, who need to have the requisite skill set in order to be able to maintain the SIS. IEC 61511-1 Clause 16.2.4 lists the skills criteria that have to be addressed:

• Understanding how the SIS functions (in terms of trip points and the resulting action taken by the SIS);
• Understanding the hazard the SIS is protecting against;
• Operation of all bypass switches, and under what circumstances these bypasses are to be used;
• The operation of any manual shutdown switches and manual start-up activity and when these manual switches are to be activated (may include system reset and system restart);
• Expectation on activation of any diagnostic alarms (for example, what action shall be taken when any SIS alarm is activated indicating there is a problem with the SIS).

The standard states that maintenance personnel should be trained as required to sustain full functional performance of the SIS (hardware and software) to its targeted integrity.

In addition, the O&M personnel will be required to follow a written proof test procedure as defined in IEC 61511-1 Clause 16.2.8, whereby a proof test procedure has to be developed for every SIF to reveal dangerous failures that are not detected by the SIS diagnostics. These written test procedures will need to describe the following steps:

• The correct operation of each sensor and final element;
• Correct logic action;
• Correct alarm and indications.

The proof tests will need to cover the entire SIS including the sensor(s), the logic solver and the final element(s) (e.g. shutdown valves and motors). In addition, the proof tests will need to be carried out at intervals that were specified and used to calculate the PFDavg for the SIF.

This implies that O&M personnel will be required to undergo regular training, competency audits and competency assessments, especially when new and/or updated components of the SIS are being incorporated and/or old or worn out components are being replaced. Personnel training is a key element in ensuring that the SIS can be maintained and operated correctly.

What Happens in Practice?

In order to be able to maintain and follow the requirements set forth in IEC 61511-1 Clause 16, the end users have to ensure that they have adequate procedures, as well as an adequate documentation and tracking system. Recording spurious trips, Process demands, failure data, audit results, test results, etc., requires a well-organized and maintained documentation system. It also requires the O&M personnel to be diligent in recording this information.

Of course it remains to be seen how diligent the personnel are at recording this data, since it is highly dependent upon the safety culture of the plant. Sadly, the recent Tesoro incident in 2010, which resulted in the deaths of 7 workers, as reported in the draft US Chemical Safety Board (CSB) findings [3], points to:

"..a deficient refinery safety culture, weak industry standards for safeguarding equipment, and a regulatory system that too often emphasized activities rather than outcomes. The conclusion of which suggests the need for refinery safety reforms."

The *Tesoro Report* by the CSB also states that in 2012 alone, the CSB tracked 125 significant incidents at U.S petroleum refineries. The draft report examines the effectiveness of refinery and chemical facility regulatory oversight, noting that Washington State's Department of Labor and Industries (L&I) does not have sufficient personnel resources to verify that process safety management requirements are being implemented adequately.

The inference is that end users need to be more vigilant in how they are maintaining and operating their plants. If end users follow the requirements of IEC 61511-1 Clause 16.3.1 and 16.3.2, regarding proof testing and inspection of the SIS (which would include visual inspection of piping) to ensure no observable deterioration and/or any unauthorized modifications have occurred, then incidents such as happened at the Tesoro plant, might have been preventable.

Although IEC 61511-1 Clause 16.2.5 dictates that maintenance personnel need to be trained, it doesn't define how frequently this training should be carried out and how competency is measured.

How Data is Recorded

The problem faced by many O&M personnel is how to record and archive the data. Most BPCS systems will have an historian for archiving plant data, which includes trips, alarms, diagnostic faults, etc. Normally, this type of data associated with the SIF is also recorded by the same and/or a separate historian. Proof testing and inspection are critical tasks that have to be performed as per IEC 61511-1 Clause 16.3. The purpose of proof testing is to reveal undetected faults and the proof tests shall be conducted in accordance with a written procedure. The sole purpose of this is to detect defects and/or faulty equipment prior to a demand being placed on the SIS. Proof test coverage is another important aspect as it's nearly impossible to achieve 100% proof test coverage, therefore, the frequency and thoroughness of manual proof testing is essential to maintaining the SIS.

IEC 61511-1 Clause 16.3.3 defines what needs to be maintained for record purposes. The clause defines that the user shall maintain records that certify that proof tests and inspections were completed as required. These records shall include the following information as a minimum:

- Description of the tests and inspections performed;
- Dates of the tests and inspections;
- Name of the person(s) who performed the tests and inspections;
- Serial number or other unique identifier of the system tested (for example, loop number, tag number, equipment number, and SIF number);
- Results of the tests and inspection (for example, "as-found" and "as-left" conditions).

The standard does not specify how and by what means these results are recorded and most end users will have a plant enterprise system or asset management system, which may require O&M personnel to upload this information. In most cases the O&M personnel will be using paper-based systems for recording, in which case it will require additional effort to scan these documents into a format that can be transferred to the plant's main system.

This would clearly place a further burden upon the O&M personnel, which could lead to short cuts being made and/or missing data because the O&M personnel didn't have time to do this. Statistically, most plant incidents occur during start-up and/or plant shut-downs, when the possibility of spurious trips, alarms and/or faults would be the highest, especially if a start-up was being implemented as a result of maintenance work and/or plant modifications. If there is a spurious trip then the O&M personnel will be

under pressure to get the plant and/or process line back up and running as quickly as possible. Does this mean they'll have the time to properly record all the data required (as listed above)? This is a very valid and pertinent question.

Technology Can Help

Advances in technology can now provide the means for O&M personnel to record data via handheld tablets in electronic format. However, having a dedicated tool that has been specifically designed for this purpose is the issue. Most O&M personnel will be recording their data in an excel spreadsheet or some form of database, if not using a paper-based system. There are some tools on the market that address part of the requirements but having one that addresses all the requirements is rare.

The O&M personnel would need a tool that can record functional safety related statistics/performance metrics, as well as record life events such as:

- Demands – both real and spurious.
- Inspection and Proof tests results.
- Maintenance activities (e.g. calibration).
- Failure reporting

Recording demands, such that the user is able to determine which layer of protection failed is another important aspect because the information provided would enable the user to determine the demand frequency of the hazard scenario (i.e. a specific hazard with all applicable protection layers - in sequence of operation). This would enable any discrepancies between the expected behavior and actual behavior of the SIS to be analyzed and any necessary modifications to be implemented to restore the SIS to its designed safety level. This is required per IEC 61511-1 Clause 16.2.6.

Having a tool that enables the O&M personnel to be able to record demands, such that they could identify which protection layer was successful protecting against a demand for a given hazard would be highly desirable. Figures 4, 5 & 6 below illustrate example templates for

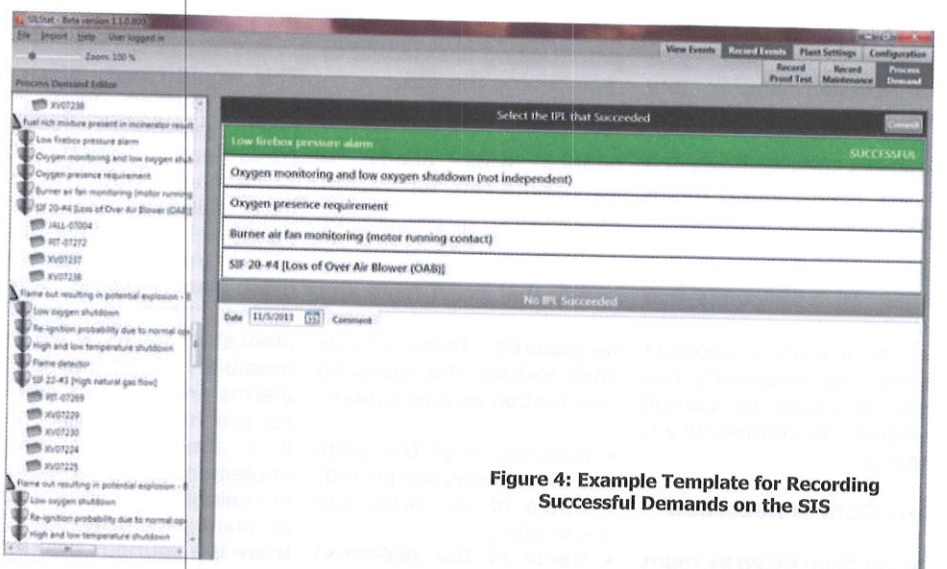

Figure 4: Example Template for Recording Successful Demands on the SIS

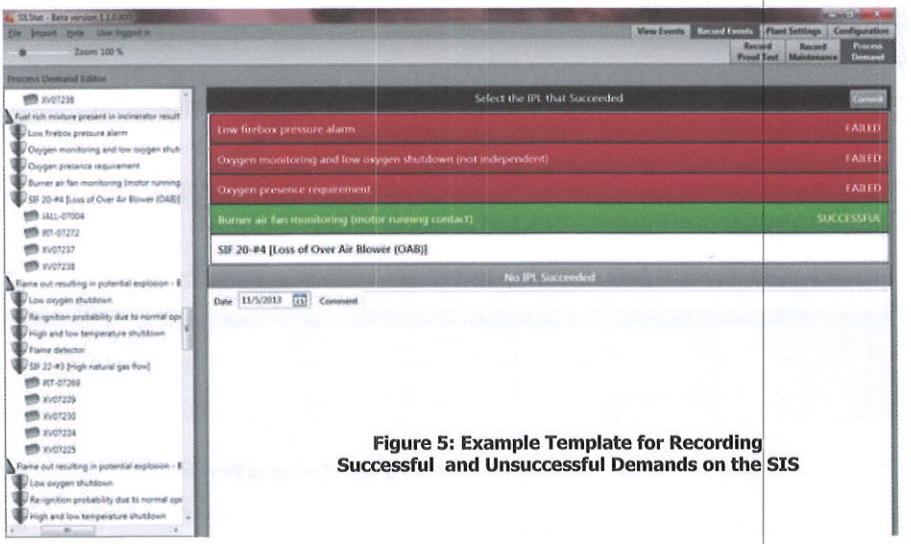

Figure 5: Example Template for Recording Successful and Unsuccessful Demands on the SIS

recording such events. The information could also be used to determine the demand frequency of the hazardous event. Having a tool that enables the physical devices of the SIS to be stored in a database and identified by their associated tags and/or descriptions will enable O&M personnel to be able to carry out effective maintenance and/or replacement procedures. Figure 7 illustrates an example template for recording and entering device information.

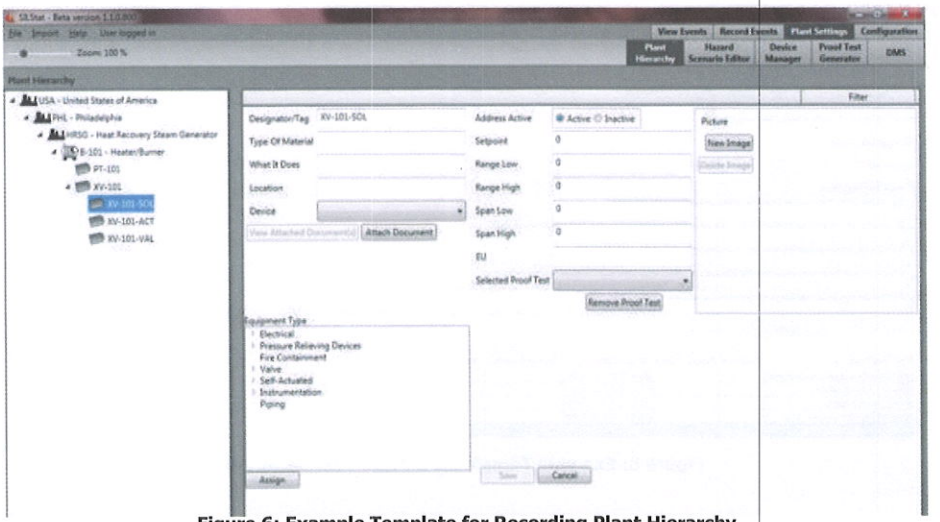

Figure 6: Example Template for Recording Plant Hierarchy

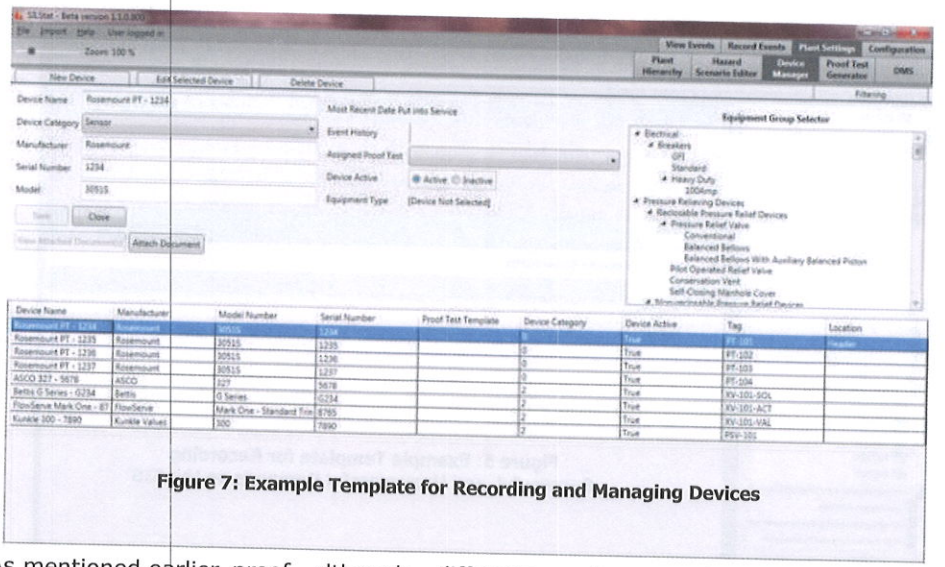

Figure 7: Example Template for Recording and Managing Devices

As mentioned earlier, proof testing is a very important step that has to be carried out in accordance with the PFDavg calculation that is included for each SIF within the Safety Requirements Specification (SRS), although different parts of the SIS may require different test intervals (e.g. the logic solver may require a different test interval than the sensors and/or final elements). Enabling the O&M personnel to have an automatic proof test generator that allows them to specify individual proof test steps, with pass/fail criteria, would be a significant benefit. This would allow the O&M personnel to record only

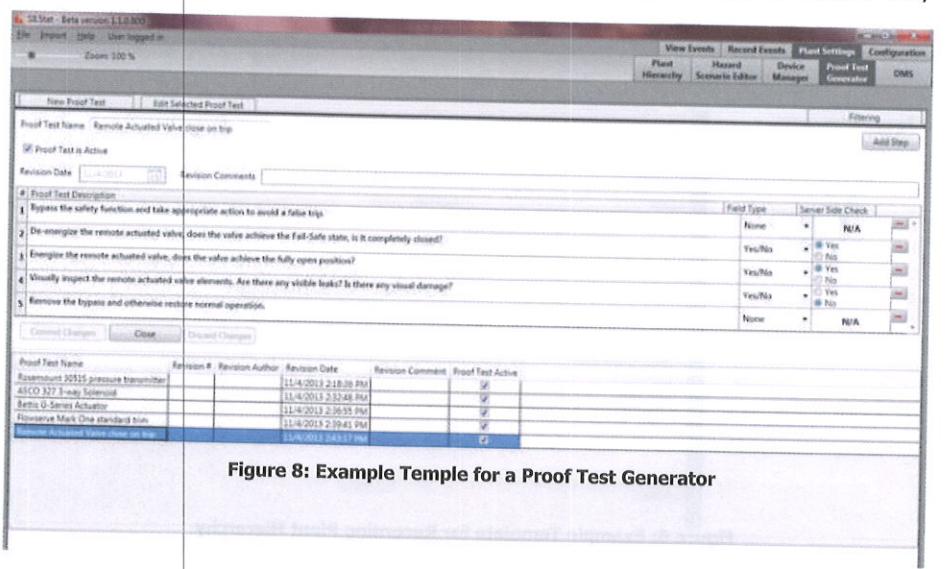

Figure 8: Example Temple for a Proof Test Generator

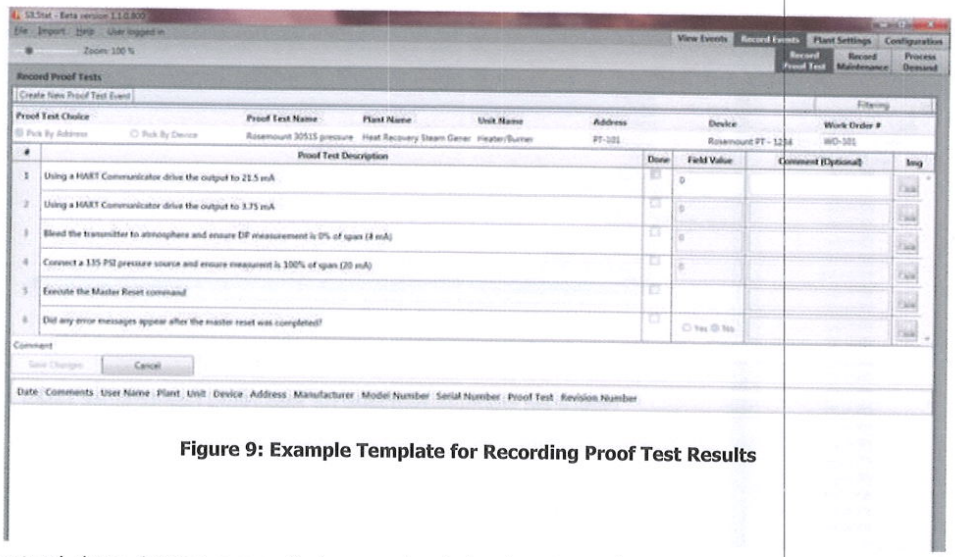

Figure 9: Example Template for Recording Proof Test Results

factual data during a proof test. Figure 8 illustrates an example template for a proof test generator.

Any problems found during proof testing will need to be repaired in a safe and timely manner, as defined in IEC 61511-1 Clause 16.3.1.4. Although the standard doesn't specify any particular time period, the Mean Time To Restore (MTTR), as used during the SIL determination of the SIF(s) and for the PFDavg calculation, must be adhered to in order to return the SIS to its safe state as soon as possible. Having the ability to identify and rectify any deficiencies quickly and effectively is the key.

Therefore, having a tool that enables the O&M personnel to identify the tag address of a device that is required to be tested, based upon steps defined for the proof test, which automatically determines a pass/fail condition for the test will save time and improve accuracy. Figure 9 illustrates an example template for recording proof tests.

Furthermore, being able to record these maintenance activities via a hand-held and/or mobile device would simplify the O&M personnel's job and enable a quick upload of all maintenance data to a central server where it can be reviewed and analyzed by the plant's safety or reliability team.

Essentially, being able to select and locate a device from the plant's hierarchy tree, for maintenance and/or replacement, via the tool, will save time especially if the O&M personnel can record the cause and any comments (the "as found" and "as left" conditions). Figures 10 & 11 illustrate example templates for recording maintenance tasks.

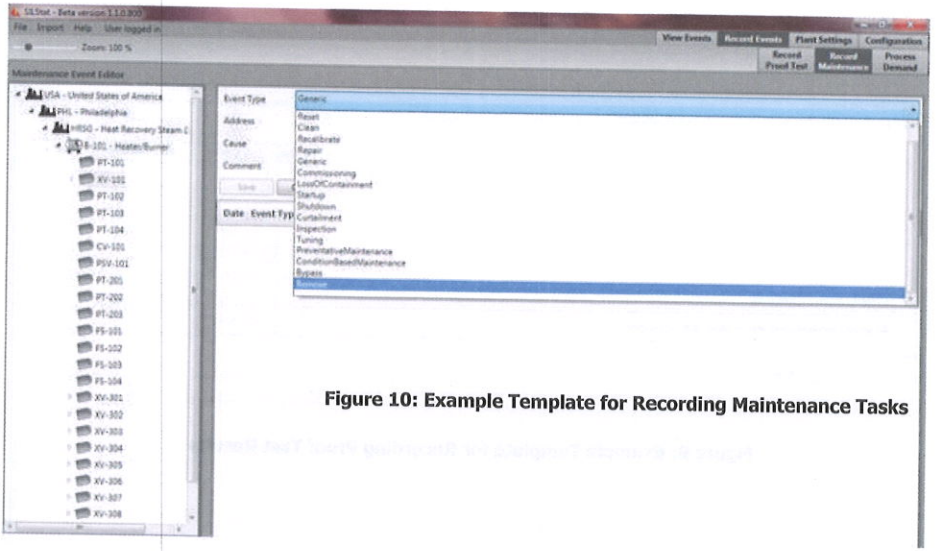

Figure 10: Example Template for Recording Maintenance Tasks

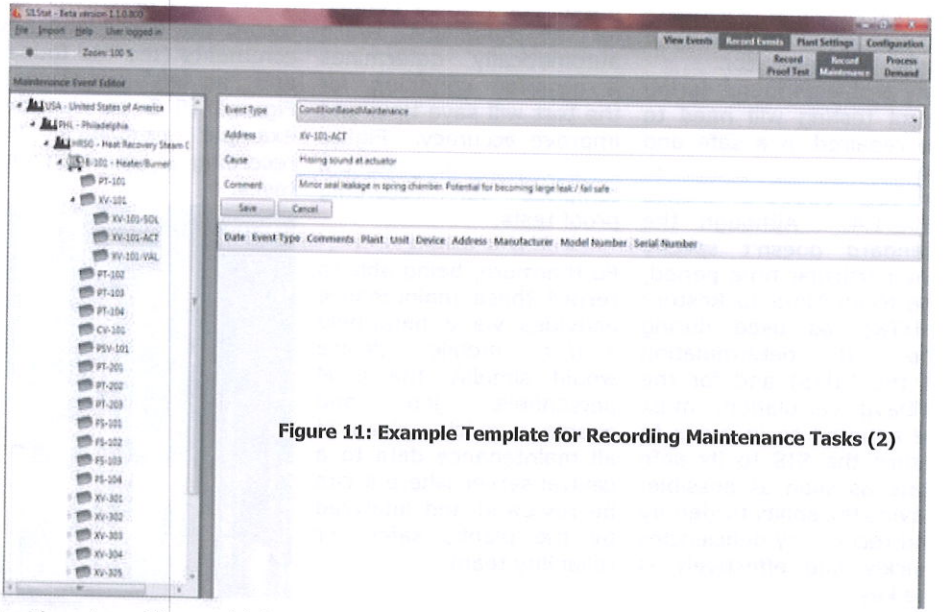

Figure 11: Example Template for Recording Maintenance Tasks (2)

Another benefit would be for the O&M personnel and the plant's safety manager or team to be able to view the events that had taken place, including the time and outcomes. Figure 12 illustrates an example template for displaying events that had occurred.

The benefits to be gained from having a well-structured, defined and automated recording system can be characterised

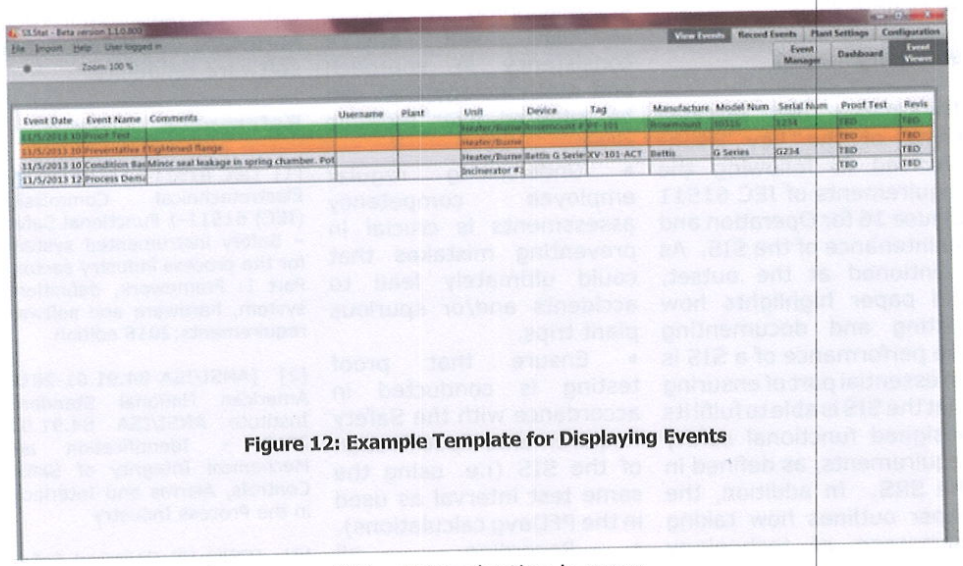

Figure 12: Example Template for Displaying Events

as the provision of:

- Detailed analysis of failures that can identify problems related to:
  - Specific addresses,
  - Specific devices,
  - Specific device types;
- The frequent benefit of reducing false trips of the plant;
- The ability to compare actual performance with assumed performance;
- The ability to ensure that the risk reduction is adequate;
  - Continue data collection;
- The ability to identify if the risk reduction is inadequate, i.e. if hazard risk is higher than expected and there is a need to return to Analysis phase of the SLC for redesign and implementation;
- The ability to identify if the risk reduction is more than adequate, i.e. if the system is overdesigned to prevent the hazard - this allows modification of design practices for future applications and potential for cost savings;
- Data for future Safety Lifecycle tasks, such as:
  - Risk Assessment
  - Layer of Protection Analysis
  - SIL Target Selection
  - SIL Verification.

The information gathered will enable the plant safety personnel to re-evaluate the frequency of proof testing, based upon the historical test data gathered, plant experience, hardware degradation and software reliability. The period for reviewing this will need to be determined by the plant safety manager.

In addition, a software tool can help solve any communication problems within the Plant that exist between the various "Managers" and their different departments. The following organizations are involved in O&M and most likely have different operational objectives:

- Operations;
- Maintenance;
- Process Safety (EHS);
- Reliability;
- Engineering.

Although these different groups will require their own particular data from this system, having all the information in a database that is easy to access and contains relevant, accurate data will ensure

consistency.

Summary

The paper has outlined some of the key issues involved in following the requirements of IEC 61511 Clause 16 for Operation and Maintenance of the SIS. As mentioned at the outset, the paper highlights how testing and documenting the performance of a SIS is an essential part of ensuring that the SIS is able to fulfil its designed functional safety requirements, as defined in the SRS. In addition, the paper outlines how taking advantage of technology and/or software tools to help with documenting and automating maintenance activities can help improve efficiency and reduce errors.

In summary, the key points are as follows:

- There is a need to manage risk - not ignore it.
- There is a need to adopt an appropriate safety-first culture to ensure O&M personnel are trained and competent to maintain the plant SIS.
- Recording lagging and leading indicators is an important part of maintaining and improving process safety.
- Having the proper Operation and Maintenance Procedures in place is vital to ensuring a safe and well-maintained SIS.
- Developing a "safety checklist" will ensure consistency in approach and methodology that can be adopted over multiple sites.
- Undertaking regular employee competency assessments is crucial in preventing mistakes that could ultimately lead to accidents and/or spurious plant trips.
- Ensure that proof testing is conducted in accordance with the Safety Requirements Specification of the SIS (i.e. using the same test interval as used in the PFDavg calculations).
- Recording all maintenance activities accurately and faithfully in accordance with IEC 61511 Clause 16.3.
- Use of software tools/technology to assist in recording and auditing maintenance activities, spurious trips, SIS demands, calibration and faults will save time and improve effectiveness.
- Use of software tools/ technology to help analyse failures, false trips and actual performance of the SIS compared to assumed performance will help in meeting IEC 61511 Clause 16.2.6. Any discrepancies will need to be assessed.
- Well recorded and accurate SIS performance data will enable plant safety personnel to be able to re-evaluate the frequency of proof testing, based upon the historical data gathered, plant experience, hardware degradation and software reliability.

References

[1] [IEC 61511-1] International Electrotechnical Commission (IEC) 61511-1 Functional Safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements:2016 edition

[2] [ANSI/ISA 84.91.01-2012] American National Standards Institute ANSI/ISA 84.91.01-2012 – Identification and Mechanical Integrity of Safety Controls, Alarms and Interlocks in the Process Industry

[3] [CSB] US Chemical Safety Board draft report 2010-08-I-WA JANUARY 2014 on April 2010 fatal explosion and fire at the Tesoro Anecortes Refinery Washington.

Steve Gandy is Vice President for Global Business Development and Director of the End User Service Business for Functional Safety and Cyber Security at exida Consulting LLC. He has nearly 40 years' industrial experience in training, senior, corporate and R&D management, having started his career as a hardware and software developer for fire protection systems. Steve is a former Board member of the IET, and a Certified Functional Safety Professional, and is in high demand as a speaker on safety and operational issues.