SIF Testing – it's more complicated than you think

Andy Brazier, AB Risk Limited, www.abrisk.co.uk

Nick Wise, Business Support Manager, Gas Storage, SSE Hornsea Limited

Harvey Dearden, Time Domain Solutions Limited, https://www.tdsl.org.uk

Accidents like Buncefield, Deepwater Horizon and Boeing 737 Max highlight how active engineered systems failing to operate correctly when we need them can allow events to escalate, resulting in major consequences. In these cases the systems were high level alarms, blowout preventer (BOP) and Manoeuvring Characteristics Augmentation System (MCAS).

Safety Instrumented Functions (SIF) are an example of an active engineered barrier intended to reduce the risk of major accident hazards. They use technology to take over when a process strays from its intended safe operational envelope. Although the concept is simple the requirements to achieve target risk reductions of sufficient reliability result in complex systems made up of multiple components. We need to be able to prove that the systems are reliable over their whole life. Testing SIFs is essential to achieve this and is a critical human activity with potential for error. If it is not properly planned and executed the testing may not actually prove that the system will respond as required when there is a demand. Also, the testing can be a cause of faults. Given that SIFs are usually one of our last lines of defence, a fault may be catastrophic.

The components that typically make up a SIF are all fairly standard in the process industry. Any Instrument Technician will encounter them on a daily basis as part of their routine maintenance, inspection and testing responsibilities. They can certainly test a SIF using their generic competence to confirm that it functions, but that may not be sufficient. The testing needs to demonstrate that there are no unrevealed failures that may degrade the protection, particularly in redundant channels, and that there is no significant degradation in performance. Despite what our procedures may say and what people think, this is actually almost impossible to achieve completely.

Task and human error analysis provides an effective way of determining how a SIF proof test is and should be carried out; and identifying potential human errors and consequences. It shows that there are multiple opportunities for error to contribute to potential major accident hazards.

Some aspects of SIF testing are generic, which allows us to standardise our approach and helps people to understand what needs to be done and what is critical. Other aspects depend on the type of SIF and components used (e.g. pressure or temperature? Transmitter or switch?). Some aspects are localised and specific to individual SIFs as installed.

Causes of complexity to be aware of include:

- Most tests will rely on a form of simulation, which may not replicate reality exactly;
- Redundancy in the system creates additional failure modes that need to be tested;
- Common cause faults with other systems (e.g. control system);
- Potential for physical degradation means a successful test today does not mean the system will work tomorrow;
- Components may not be visible to the technician;
- Using the wrong test medium can introduce faults;
- Some final element valves have physical bypasses (rider lines);
- Testing causes wear and tear.

And arguably the most prevalent human error is failure to reinstate the SIF properly after testing.

Compiling knowledge gained from published guidance, practical experience and human error analysis allows the potential pitfalls to be identified so that the risks can be mitigated. Fully detailed explicit test procedures implemented by technicians with specific competence in SIF testing will be a significant part of, but not the whole solution. Whilst there are generic aspects of testing, a generic human error analysis is unable to address the specific differences between systems, which can be critical. Also, local Performance Influencing Factors (PIFs) can have a significant effect on the likelihood of human error. On the other hand, for sites with a large number of SIFs on a site, completing human error analyses for each will be onerous and quickly suffer from diminishing returns from the effort.

The solution that will be presented in this paper is an overarching assessment that covers the generic aspects of SIF proof testing and specific actions performed for testing a representative set of SIF types. This is followed up with a review of all SIFs vs the overarching assessment to identify any differences. The most useful outputs from this approach include a standardised way of representing SIF testing procedures to enhance understanding of the overall goals and clear identification of differences between SIFs to ensure they are not overlooked by technicians when carrying out the test. A follow-up Walk-Through Talk-Through is used to identify Performance Influencing Factors that need to be optimised to minimise the likelihood of the critical human errors.

Key words: Safety Instrumented Functions, SIF, Proof Testing, Functional Safety, Human Factors

Short summary: Safety Instrumented Functions (SIF) are included in our systems as critical safety barriers. We need them to be reliable and proof testing is important in making sure this is achieved. However, testing is more complicated than you think and potentially prone to human error.

Introduction

Safety Instrumented Functions (SIF) are intended to reduce risk. They are typically actioned by a 'loop' where an 'initiator' is triggered by process conditions and a 'final element' is activated to place the plant or equipment in a safe state. The initiator may include one or more sensors, logic solvers, amplifiers and relays. Final elements may include relays, valves (including actuators) and electrical contactors or breakers.

How are SIF used in industry?

Safety Instrumented Functions have been used in industry for many years. Often known as an Emergency Shutdown (ESD) or 'trip' the benefits of an automated response to a deviation from the normal or safe parameters were recognised for safety and asset protection.

The application of SIF was standardised in 1998 with the publication of the first three of seven parts of IEC 61508 "Functional safety of electrical/electronic/programmable electronic safety-related systems." The remaining four parts were published in 2000 (IEC 61508, 1998 & 2000) and subsequently revised in 2010. This formalised the means by which Safety Integrity Levels (SIL) were determined based on the level of risk reduction required. Several sectors specific standards have been subsequently published including IEC 61511 for process plant (IEC 61511, 2003 and 2017).

Practical improvements arising from applying IEC 61508 have included avoidance of single point failures for subsea isolation valves, reduced use of relief valves and reduced reliance on alarms and operators' response (Foord et al 2011). On the flip side it may have reduced the application of inherent safety and increased complexity; creating a false perception that technology increases safety because it eliminates the risks of human error.

Proof testing SIF

Periodic proof testing is carried out to confirm there are no hazardous, unrevealed faults with a SIF. The testing is intended to confirm all components and the system as a whole will operate with the required reliability if there is a demand. This testing is required to confirm that the actual reliability of the SIF is consistent with the assumptions made when deciding whether the overall risks posed by a hazardous system are As Low as Reasonably Practicable (ALARP).

Whilst there are many similarities between SIF loops, each is required to perform a specific action for a specific scenario. This means the proof testing has to be specific to the SIF. The high-level activities are generally similar but the devil is in the detail. This creates human error traps that can mean that system faults remain unrevealed and may even result in faults being introduced during testing.

Potential issues with proof testing methods include:

- Covering the 'obvious' failures and not considering the less common and potentially more obscure and potentially hidden failures;
- Assuming successful operation during a test proves the system is reliable enough;
- Fixing faults found without looking for systematic weaknesses;
- Assuming it is a simple task that can be performed by a competent person without using a procedure.

What failures should we be looking for?

SIF can fail in lots of different ways. Some of these are likely to be noticed during normal operation because the initiator gives out some bad data that is easy to detect or because the final element is routinely operated. In many cases a component failure will cause the SIF to activate and take the system to its safe state. These types of failure are described as 'revealed.'

Other failures are not so obvious because the initiator and/or final element may not provide any data during normal operations. These types of failure are described as 'unrevealed' and they are the ones our proof testing should focus on.

Switch-type sensors (e.g. level, flow, pressure, temperature) can suffer unrevealed failures because most of the time they are in same state. Analogue sensors will usually create fewer unrevealed failures because they are measuring a condition continuously. However, if the parameter is static this is not the case. For example, a flare knockout drum will usually operate with no liquid level. An analogue sensor included as part of high-level SIF will usually be reading zero and so there is no reliable indication that it would measure a high liquid level if one arose.

A valve used only as a final element for a SIF (i.e. not operated routinely) can have unrevealed failures because most of the it is inactive (either open or closed). This is less likely to be the case for valves that have a dual role as part of the SIF and routine operations. However, in some cases the valves will have two triggering solenoid valves (SOV) (one for the SIF and one for routine operation). The fact that the valve is operating under normal conditions does not mean the SIF SOV will work when required.

There is no technical reason why revealed failures cannot be included in proof testing. However, doing this can make the procedure unnecessarily long. This may lead the people carrying out the testing to be satisfied when most of the tests have passed satisfactorily and so become less alert to the more obscure failure modes. It certainly highlights why a specific and detailed procedure is required for every SIF proof test.

What does a test tell us?

The question our proof testing should be answering is whether the SIF has any unrevealed failures that need to be rectified so that it is likely to operate correctly when required.

One issue is that testing can never cover every set of conditions under which the SIF may be required to operate. In many cases it is simply not possible or sensible to test the SIF with plant operational. A valve closing during a proof test with no flow in the pipe (with the plant shutdown) proves the valve has not seized open but does not prove that is will close with a high flow (and pressure drop) or that it will stop the flow successfully.

Potential deterioration of components is another issue to consider. A SIF might pass a proof test and yet be showing signs of a developing failure. Inspection of the installation for signs of such deterioration are an important aspect of SIF management. Inspection is usually conveniently carried out at the same time as a proof test but may be independently scheduled. The challenge with inspection is that it is highly subjective. Insisting all components are ‘as new’ may be unnecessarily demanding, but what is good enough? Even routinely changing components according to a time schedule is likely to be expensive and may only work for ‘average’ conditions, which may not address local arrangements.

There are other possible issues that can be very easily overlooked during a proof test. One is the potential for instrument tubing to be blocked by ice or hydrates due to cold ambient and/or process conditions. In these cases insulation or trace heating can be critical for the instrument and hence SIF reliability. The importance of these items is easily overlooked because they are not part of the SIF loop. Trace heating is particularly difficult to check because it likely to be temperature controlled. If the proof test is carried out on a warm day there is almost no way of proving that it will be effective at preventing ice or hydrates formations.

Faults can be introduced during or after testing. Potentially critical examples include failing to reconnect cables or pipework properly that had to be disturbed to allow testing to take place.

What does a failure under test tell us?

The immediate conclusion from a failure under test is that part of the SIF did not satisfy requirements. But we need to understand why the failure occurred. Simply fixing the faults founds is not good enough unless the fault is truly a ‘random failure’ that carries no wider implication for the SIF design. Identifying causes and looking for evidence of systematic failures is important if we are going to ensure that the SIF will be as reliable as required and potential issues with similar installations are addressed.

One of the challenges is that the technicians who carry out proof testing are likely to spend a lot of their time fixing problems reported by operators. For non-SIF items the strategy is usually to operate components to failure and to fix them as quickly as possible to minimise disruption to operations. We need to make sure that this same approach is not applied to faults found when testing SIF. A technician may not be very popular with the operations department if they do not repair a fault immediately but they will be even less popular if a SIF fails to operate when there is a genuine demand.

It may be possible and appropriate to carry out an immediate repair or correction to a SIF when a fault is found but it is critically important that the fault is reported so that a performance history (e.g., population failure rate) can be acquired and possible wider implications identified. We must distinguish between ‘passed first time’ and ‘failed but now fixed’.

How can we prevent human error during proof testing?

The simple answer is that it is impossible to completely prevent human error during proof testing, but that applies to all human activities. However, there is plenty that we can do to reduce or manage the risks.

One of the key measures we can take is to make sure that proof testing is carried out by competent people. That means they need to be skilled in the techniques used when testing but they must also have a thorough understanding of SIFs and the role of proof testing in the overall management of risk.

Even when the people carrying out the proof testing are highly competent they need to be provided with a detailed procedure that they follow rigorously. These need to be perfectly explicit regarding the test method with pass/fail criteria specified (Dearden, 2022). This can be perceived by some as downgrading the role of competence. This is not the case. The procedures are provided to support competent people in recognition of the complexity and criticality of the task. It is not making the task ‘idiot proof’, it is making sure that the test is executed to provide the intended coverage. There will likely be easier, faster ways to perform a test but these may inadvertently compromise the coverage achieved, which is why the test procedure must be explicit and not left to the tester’s discretion.

Something we should aim to do is to make testing as simple as possible. Whilst the ideal may be to complete a full “end to end” test with 100% coverage under real operating conditions this is rarely, if ever possible. Fixating on this ultimately impossible aim can add complexity with little benefit. Taking the risks introduced by testing itself into account highlights that a pragmatic approach with the aim of reducing risk to ALARP is required.

It is often more practical to test a SIF in separate sections rather than as a whole (e.g. individual channels with associated logic for the sensor subsystem, separately from the final element subsystem). If the SIF has redundant channels this approach will be necessary to check that all of them are healthy. For example, if there are two shut off valves that operate as '1 out of 2' (1oo2) you need to confirm that both are healthy. A single function test of the system as a whole might 'prove' that the SIF works but it might not reveal a failed channel. This is critical because the very point of redundancy is that the SIF should still be able to function in the presence of a fault or faults. This explains the fundamental distinction between a function test and a proof test.

Exercising all of the SIF does not itself guarantee full coverage. Test coverage is not a question of what proportion of the SIF elements are exercised but rather the proportion of possible unrevealed failures will be identified. For example, we can exercise a shut off valve during a plant shutdown and confirm it has closed. This test can reveal a solenoid valve failure or a stuck open valve but not degradation in its stroking speed. It would not reveal the condition of its seat and its ability to stop the flow (if tight shut off is required). It would not reveal a failure that only occurs when the plant is operating and the valve is at normal pressure and temperature and pipework stresses on the valve body change and there is a pressure drop across the closure member. Careful thought is required to enhance the test coverage as far as is practicable whilst minimising the disturbance to the installation.

Testing that requires disturbance of the physical installation or process connections, modifications to set points or use of overrides raises the potential of introducing dangerous errors.

The achieved test coverage should be factored into the evaluation of the probability of failure on demand of the SIF, and approaches are available for this (Dearden, 2022). The proportion of unrevealed failures that would not be covered by the test are usually addressed by overhaul or replacement of equipment so that it is thereby returned to the 'as new' condition at an appropriate extended interval, designated the 'mission time'.

The most effective measure for reducing the risk of human error is to consider proof testing during design of the plant and SIF. This is not much help to you when developing procedures for existing SIF but does emphasise why it is important to involve people with practical experience in design teams.

An overarching method of proof testing

Having carried out task and human error analysis for proof testing of a number of SIFs it has been possible to develop an overarching approach that allows some standardisation and structure to developing test methods, technician competence and supporting procedures.

Preconditions for the task will normally include:

- Inhibits and overrides have been approved (if required);
- Operations have made the plant available;
- Access is in place (e.g. scaffold if required);
- Permit to work has been issued;
- Correct test equipment is available and calibration is in date;
- Minimum two personnel will carry out the test if coordinated activity is required (e.g. one in field and one in control room);
- Radio communication has been confirmed between field and control room.

The test itself can be broken down into seven subtasks, summarised in the table below.

Sub-task	**Comments**
1. Identify system components	Ensures the correct SIF is tested and all components are inspected.
2. Visually inspect the SIF components	Labelling, supports, cabling, process connections, electrical (Ex). Also, other items relevant to SIF reliability (e.g. insulation, trace heating). There is a high degree of subjectivity at this stage, which should be captured through competence management.
3. Prepare to activate the SIF/SIF section	The method for this subtask depends on the type of SIF (e.g. initiation by electronic simulation, pressure source, level bridle, exposing the sensor to a controlled condition).
4. Activate the SIF/SIF section	Adjust a simulated condition to activate the SIF or expose the sensor to a controlled condition that will activate the SIF. Monitor final elements to confirm operation. Record findings.

5. If test is successful, return SIF to operating status	The method for this subtask depends on the type of SIF (as above). An independent inspection of installation should be included after reinstatement wherever the physical arrangement was disturbed.
6. If test is unsuccessful, develop an appropriate plan	Deciding the operational strategy whilst waiting for repair. An Operational Risk Assessment (ORA) or similar may allow operations to continue but must be carried out by people with a thorough understanding of what the risks and how the SIF (when operational) contributes.
7. Update and review SIF data file	Collecting data for future analysis and demonstration. Who looks at this data and how do they identify systemic issues?

Of course the devil is always in the detail, which is captured in the steps performed under each of the sub-tasks above[1]. It is important to have a traceable record of the testing and that the testers understand that they are accountable for the work they undertake as competent, responsible individuals. The purpose of including overarching sub-tasks above is to illustrate the importance of actions that are not directly associated with the hands-on testing of the SIF loop. From the full analysis the following potential errors have been identified as being of particular concern:

- Activating the SIF too early when people are not in place to confirm correct operation of the final element (e.g. valve closure time) can be critical for some SIF. This is the case where the final element is not operated routinely and so delayed activation (e.g. sticking valve) is a concern;
- Failing to consider how SIF components may degrade before the next test or inspection;
- Not recognising the importance of items beyond the immediate loop to SIF reliability (e.g. connection between instrument and process, insulation, trace heating);
- Not confirming the final element was in its healthy state before the test and failing to observe it changing from healthy to tripped to confirm it did activate as required (if needed to achieve claimed test coverage);
- Using the wrong test fluid or failing to remove it from the sensor after the test (e.g. water remaining in a level instrument that can freeze);
- Collecting insufficient data to confirm the SIF is operating within its performance criteria;
- Failing to remove inhibits or overrides, or leaving sensors isolated after completing the test;
- Reconnecting cables to the wrong terminals;
- Failing to restore the in-service configuration of intelligent devices;
- Failing to cross check outputs from the SIF initiator with other process data to confirm it has been returned to service correctly.

The last error highlights issues raised above with using switch-type sensors as SIF initiators because they do not provide any output that can be used to confirm operation. If the sensor is disturbed for testing (e.g. high-level switch removed from a vessel and placed in a container of liquid) an independent check of physical status is probably the only risk control available and should certainly be included in the procedure.

Performance Influencing Factors (PIF)

It is not possible to eliminate the potential for human error but there are many factors that can affect its likelihood. These are commonly known as Performance Influencing Factors. Although a task and human error analysis can identify potential issues, an onsite assessment or Walk-Through Talk-Through through is required to determine whether the error identified are likely to occur. The aim should be to optimise PIFs

The UK Health and Safety Executive (HSE) has published a list of PIFs, categorised as Job, Person and Organisation (Health and Safety Executive, 2009). The list of Job factors is particularly relevant to SIF proof testing, as illustrated below.

PIF – Job Factors	**Applicability to SIF proof testing**
Clarity of signs, signals, instructions and other information	Poor labelling may mean that SIF components are not inspected and so degradation that can affect SIF reliability is not detected.
System/equipment interface (labelling, alarms)	Poor interfaces can affect the ability to confirm the SIF is operating within its performance criteria. Data may be obtained from computer screen graphics, digital display, local gauges and test equipment.

[1] Download a more complete analysis at https://www.abrisk.co.uk/sifprooftesting

PIF – Job Factors	Applicability to SIF proof testing
Routine or unusual	Whilst the general approach to all testing is similar and uses a lot of routinely used skills, individual SIFs are likely to be tested relatively infrequently and so specific requirements may not be remembered.
Procedures inadequate or inappropriate	High quality, detailed procedures are required to ensure tests are comprehensive and correct judgements are made about system reliability. Additional procedures may also apply (e.g. permit to work. inhibit/override management, operation of critical locked open/closed valves).
Preparation for task (e.g. permits, risk assessments, checking)	Failing to prepare can lead to work-arounds to get the job done or time pressures. Items that require planning include plant status, authorisation from operations, availability of test equipment and test fluid.
Time available/required - Divided attention	Time pressure can encourage short cuts and may lead to obscure or infrequent failures being overlooked (i.e. satisfied that the SIF has activated).
Tools appropriate for task	Correct test equipment with suitable fidelity. In date calibration.
Communication, with colleagues, supervision, contractor, other	Many tests require people at different locations to confirm correct operation. This is particularly relevant for time-critical actions (e.g. valve closure).
Working environment (noise, heat, space, lighting, ventilation)	Lighting inevitably affects the ability to identify the correct components, check and monitor operation of components. Noise and heat can cause distraction and increase the likelihood of error.

Having emphasised the importance of visual inspections as part of proof testing it is important to note that visibility is not always available because items are hidden from view by insulation (lagging), structures or pipework. This can be particularly significant when electronic simulation is used for proof testing because the sensor is not tested directly and so it is critical to check that the sensor is positioned and secured correctly. These types of factors are unlikely to be recognised when reviewing a procedure from the office or during task analysis performed as a workshop whether online or face to face; and highlight the importance of the onsite Walk-Through Talk-Through.

Avoiding analysis paralysis

Whilst having a suite of detailed and explicit proof test procedures is an expectation there is also a requirement to demonstrate that overall risks are tolerable or ALARP (depending on applicable regulations). Task and human error analysis is recognised as an effective method of supporting that demonstration but requires significant resource. Unless you have a very small number of SIFs, it will not be practical to complete a task and human error analysis for every proof test.

The development of the overarching assessment provides us with an opportunity to optimise the analytical effort and has some additional benefits. By using it as a generic benchmark each SIF can be evaluated to determine whether its proof test follows the generic method; and to identify and differences due to the specific SIF arrangement. This is potentially very useful because it allows these differences to be highlighted in procedures and training, reducing the likelihood that they are lost in the detail and overlooked when proof testing is being carried out.

The perfect (or optimal) proof test on paper is of no value if it cannot be performed in practice. A follow-up Walk-Through Talk-Through for each SIF should be carried out to evaluate the job, person and organisational arrangements to confirm PIFs are optimised and the likelihood of human error is minimised. This would be a requirement even if a task and human error analysis was carried out for every proof test, but using the approach suggested above means resources can be used more effectively to the greatest benefit.

By way of a sense check for anyone evaluating their SIF proof testing, the HSE has published a list of ‘Common Failings,’ highlighting failure modes that are commonly found to be missing from proof test procedures (HSE, OG-00054 Appendix 4). Examples include some general issues (e.g. failure to test redundant channels) and some item specific issues (e.g. level sensors with test buttons). It includes some very good reminders to be aware of ‘strong but wrong’ indications, such as valve linkage failures that can mean the valve position indicator does not match the actual valve status.

Conclusion

As active engineered barriers intended to reduce the risk of major accident hazards, SIFs often act as a last line of defence to prevent major accidents. Testing is essential and is a critical human activity with potential for error.

Whilst the methods used to test SIFs are fairly standard, the reality can be quite different. Testing must be carried out by competent technicians but they must also work to specific and detailed procedures. These need to present test methods that strike the right balance between 100% coverage, which is very rarely possible, and practicality. Having applied task and

human error analysis to a range of SIF tests it has been possible to generate an overarching approach. This highlights that a high proportion of the actions go beyond physical interactions with the SIF components and visual inspections

Our overall aim has to be continual management of SIF reliability and not simply relying on proof testing. Proof testing is more complicated than you think and this needs to be taken into account when deciding if a SIF is an appropriate risk control measure. More thought about proof testing during early design could help to simplify it as much as possible, and may lead to other strategies being adopted, including inherent safety and passive engineered solutions.

An example of an overarching task and human error analysis for SIF proof testing can be downloaded from https://www.abrisk.co.uk/sifprooftesting

References

Dearden, 2022. Functional Safety in Practice. 4th Edition. A SIS-Suite Publication.

Foord, Gulland and Howard, 2011. Ten Years of IEC 61508; Has it Made Any Difference. Hazard XXII. IChemE

Health and Safety Executive, 2009. Performance Influencing Factors (PIFs). Accessed August 2022 at https://www.hse.gov.uk/humanfactors/topics/pifs.pdf

Health and Safety Executive, 2014. Operational Guide 0054. Proof Testing of Safety Instrumented Systems in the Onshore Chemical / Specialist Industry. Appendix 4 Common Failings. Access August 2022 at https://www.hse.gov.uk/foi/internalops/og/og-00054-appendix4.pdf

IEC 61508:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems – Parts 1– 7.

IEC 61511:2017, Functional Safety: Safety Instrumented Systems for the process industry sector – Parts 1 – 3.