SIF testing – it's more complicated than you think

Andy Brazier, AB Risk Limited, UK; Nick Wise, SSE Hornsea Limited, UK; Harvey Dearden, Time Domain Solutions Limited, UK

Summary

Safety Instrumented Systems (SIS) have rarely been identified as a cause of major accidents but IChemE's recently published *Learning from major incidents*[1] linked them to 13 of its 52 case studies. Installing SIS is often identified as a recommendation after an incident and is consistent with the hierarchy of risk controls that suggests that engineered controls can be relied on. On this basis it seems likely that they will feature in more accidents in the future, especially if people over-rely on them, which would be consistent with natural human behaviour. If this trend is going to be beneficial in terms of risk reduction it will be necessary to ensure that all Safety Instrumented Functions (SIF) are reliable when required.

Keywords: Safety instrumented functions

The development of SIF used in industry

Safety Instrumented Functions have been used in industry for many years. Previously known as an Emergency Shutdown (ESD) or 'trip,' publication of *IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems* standardised the term SIF and has been followed by sector specific standards including IEC 61511 for process plant[2,3].

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[4]. 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 dangerous, unrevealed faults with a SIF; confirming that all components and the system as a whole will operate with the required reliability so that risks posed by a hazardous system are As Low as Reasonably Practicable (ALARP).

Potential issues with proof testing methods that can create human error traps are discussed below and 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. These types of failure are described as 'revealed.' Other 'unrevealed' failures are not so obvious because the components may not provide any evidence of degradation during normal operations, and these 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 the same state. Analogue sensors will usually create fewer unrevealed failures because they are measuring a condition continuously. However, if the parameter is static (e.g. a flare knock-out drum that usually has no level) this is not the case because there will be no routine process changes that can confirm the sensor is working.

A valve used only as a final element for a SIF (i.e. not operated routinely) can have unrevealed failures because most of the time it is inactive (either open or closed). This is less likely to be the case for valves that have a dual role (SIF and routine operation). However, they may have two triggering solenoid valves (SOV) (one for the SIF and one for routine operation) so that operation 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 and mean people carrying out the test become less alert to the more obscure but critical failure modes.

What does a test tell us?

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 it will close with a high flow (and pressure drop) or that it will stop the flow successfully.

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

0260-9576/23/$17.63 + 0.00

and usually conveniently carried out at the same time as a proof test. The challenge with inspection is that it is highly subjective. How does someone decide that the condition is good enough?

Other possible issues that can be very easily overlooked during a proof test include instrument tubing that may be blocked by ice or hydrates. In these cases, insulation or trace heating can be critical for the instrument and hence SIF reliability, but are easily overlooked because they are not part of the SIF loop. Trace heating is likely to be temperature controlled so very difficult to confirm it is working if tested on a warm day.

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?

Technicians who carry out proof testing are likely to spend a lot of their time fixing problems reported by operators. For non-SIF items prompt repairs minimise disruption to operations and are encouraged. For SIF it is critical that all faults are reported so that a performance history can be acquired, and possible wider implications identified. The best way to achieve this is to raise a specific corrective maintenance for each fault. From testing we must distinguish between 'passed first time' and 'failed but now fixed'. 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.

How can we prevent human error during proof testing?

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.

Competence is critical but even the most competent people need to be working with SIF test procedures that are perfectly explicit regarding the test method with pass/fail criteria specified[5]. This is not downgrading the role of competence but a 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, the test procedure cannot be left to the tester's discretion.

We should aim 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). Test coverage is not a question of what proportion of the SIF elements are exercised but rather the proportion of possible unrevealed failures that will be identified. 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 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 are 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?

A more complete analysis can be downloaded at https://www.abrisk.co.uk/sifprooftesting

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)

Performance Influencing Factors are aspects of the job, person and organisation[6] that affect the likelihood of human error. An onsite assessment or walk-through talk-through is required to determine how they apply to specific SIF.

Job factor PIFs most relevant to SIF proof testing are illustrated in the table opposite.

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 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. This allows 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.

PIF – Job Factors	Applicability to SIF proof testing
Labelling	Poor labelling may mean that SIF components are not inspected or the wrong ones (from another system) are inspected meaning that degradation that can affect SIF reliability is not detected.
Human Machine Interfaces	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.
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	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	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	Time pressure can encourage short cuts and may lead to obscure or infrequent failures being overlooked.
Tools	Correct test equipment with suitable accuracy and reliability. In date calibration.
Communication	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	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.
Visibility	Items may be hidden from view by insulation (lagging), structures or pipework. Issues may only be recognised when out on plant and may not be considered when reviewing a procedure from the office.

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[7]. 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

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.

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 coverage and practicality. Having applied task and human error analysis to a range of SIF tests it has been possible to generate an overarching approach.

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

1. *IChemE 2022. Learning lessons from major incidents - Improving process safety by sharing experience https://www.icheme.org/media/18415/learning-lessons-from-major-incidents-v10.pdf*
2. *IEC 61508:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems – Parts 1– 7.*
3. *IEC 61511:2017, Functional Safety: Safety Instrumented Systems for the process industry sector – Parts 1 – 3.*
4. *Foord, Gulland and Howard, 2011. Ten Years of IEC 61508; Has it Made Any Difference. Hazard XXII. IChemE*
5. *Dearden, 2022. Functional Safety in Practice. 4th Edition. A SISSuite Publication.*
6. *Health and Safety Executive, 2009. Performance Influencing Factors (PIFs). Accessed August 2022 at https://www.hse.gov.uk/humanfactors/topics/pifs.pdf*
7. *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*

0260-9576/23/$17.63 + 0.00