



Safety systems – why fitting SIL Systems is only the start of it

In this article, Matthew Morton, Technology Director and Functional Safety Engineer (TÜV Rheinland) at Inspec Solutions, looks at the importance of carrying out SIF (Safety Instrumented Function) proof testing of SIL (Safety Integrity Level) rated systems, to meet proof test schedules and ensure continued plant safety, particularly in hazardous environments.

Safety Instrumented Systems and the importance of proof testing

Much of UK industry, especially plants with hazardous environments, have an installed base of SIL (Safety Integrity Level) rated systems. There is a good network of consultancies and safety system providers covering the life cycle up to installation and commissioning. However, there is a common misconception amongst end users that once a SIL rated SIS (Safety Instrumented System) is installed then they automatically have a functional, certified safety system going forwards. The reality is that from when you have a completed Stage 3 FSA

The reality is that from when you have a completed Stage 3 FSA you only hold a compliant SIS until the date of the first cycle of proof testing

(Functional Safety Assessment) you only hold a compliant SIS until the date of the first cycle of proof testing.

Following the Stage 3 FSA, the plant operators must follow a defined proof test schedule, performing tests as directed in the schedule and at the requisite frequency, or the SIS will no longer be compliant. More importantly, the real possibility exists that plant is actually unsafe; as you can no longer expect that the SIS will operate correctly on demand.

Proof testing regimes must continue until decommissioning is completed, or

the system is no longer needed for risk reduction.

Periodic proof testing is not revalidating the SIS as a whole; it is checking that dangerous undetected failures (identified in the earlier stages of the life cycle) have not occurred, and if necessary, perform rectification measures.

Types of dangerous faults found during proof testing might include for example a level switch in a tank which must detect a low level (a dangerous state) sticking above this level. The level sensor spuriously indicating a low level state is not dangerous as this is the trip state, but the switch sticking in the level detected state is dangerous as a genuine low level in the tank would not be signalled. Although oversimplified, this identifies the need for (and importance of) proof testing to identify a fault that may have occurred and be silently awaiting a demand it cannot action.

Taking the above example further, the tank may be located in a hazardous area and the sensor connected to the SIS via an IS (Intrinsic Safety) barrier. Another potentially



SIF loop testing

dangerous undetected failure here is the IS barrier indicating a healthy output signal to the SIS despite the connected instrument driving a trip signal.

Proof tests are designed to check these faults have not occurred, consequently undermining the system's efficacy to operate safely when a demand arises. Proof tests must be undertaken as per a defined procedure developed in line with the Safety Requirements Specification (SRS).

A good proof test procedure will clearly describe each test to be carried out, alongside clear pass/fail criteria, with space for recording results and signing off the system as returned to normal operation.

Defining the frequency at which the testing needs to take place and the expected rate of detection of faults provided by the proof test is part of the SIS design. The onus is then on the plant owners/operators to ensure that testing occurs to this schedule (and as per procedure). Proof testing schedules need to be considered with regards to the plant operations. Plant operators need to consider whether they have the resource in-house to carry out the work effectively and, if not, outsourcing is often the most viable option.

Proof testing schedule

Proof tests are often carried out during plant shutdown and the lack of process product could reduce the failure detection. It is important to ask the question, does your procedure actually meet the proof test coverage claim?

Increasingly, plant owners/operators are falling foul of HSE inspections by failing to address the aforementioned question. The

HSE are now paying particular attention and have specialists with an in-depth understanding of the intricacies of Safety Instrumented Systems and the requisite legislation.

With operational demands, de-manning strategies and skill base in-house, such notices from the HSE are prompting operators to outsource SIF proof testing to specialists to ensure the ongoing integrity of their Safety Instrumented Systems.

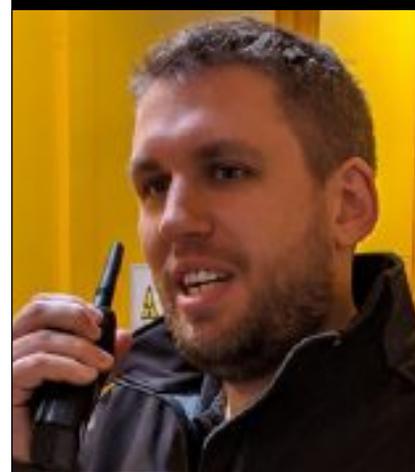
The benefit to outsourcing these specialist services is more than simply carrying out the tests. The first element of a service is a thorough independent review of the actual proof testing procedures. Benefits of this include a practical review of the tests from a specialist company which understands both control systems and Functional Safety, ensuring proof testing procedures are realistic and can actually achieve the intended outcome.

Previously we have identified proof test procedures which are overly complex and ultimately unnecessary to fulfil the need of the safety life cycle. Over testing impacts on operations by the cost of time to carry out the tests, as well as increasing the likelihood of tests not being carried out properly (or worse, not at all!). In this scenario we have saved operational expenditure over time while still ensuring the validity of the installed system.

Conversely, where we have identified proof test procedures that are missing potentially dangerous faults, the basis of design may need revisiting since there may be a real possibility that the plant/process is not actually safe.

By outsourcing proof testing, plant operators can be confident that fully qualified personnel are reviewing their procedures and performing this essential service, ensuring they are compliant with all relevant legislation. Ultimately this provides peace of mind and reduces risks. ■

About the author



Matthew Morton is Technology Director at Inspec Solutions. A master's level graduate with his BSc (Hons) Computer Science from Nottingham Trent University and MSc Applied Instrumentation and Control from Glasgow Caledonian University, Matthew has over a decade of experience in Safety Systems and industrial Control / SCADA / Telemetry across various industries. He is also certified as a Functional Safety Engineer (TÜV Rheinland). Matthew's role at Inspec Solutions involves guiding the selection and implementation of complex technology on projects across many industries and providing Process Safety Consultancy both to internal projects and directly to clients. He is a member of the IET and also a registered STEM Ambassador.