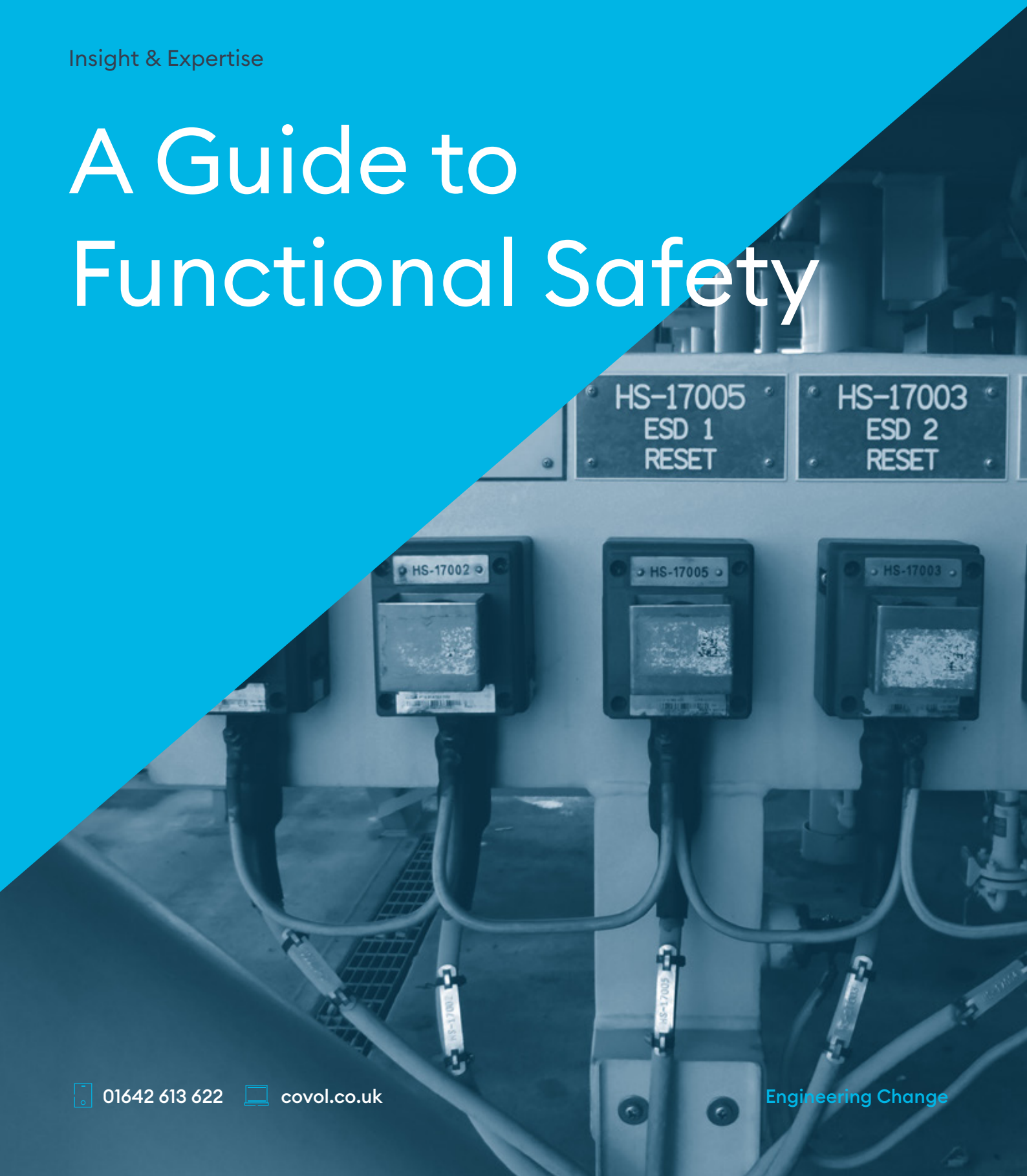
covol

Insight & Expertise

A Guide to Functional Safety



01642 613 622 covol.co.uk

Engineering Change

Contents

What is Functional Safety?

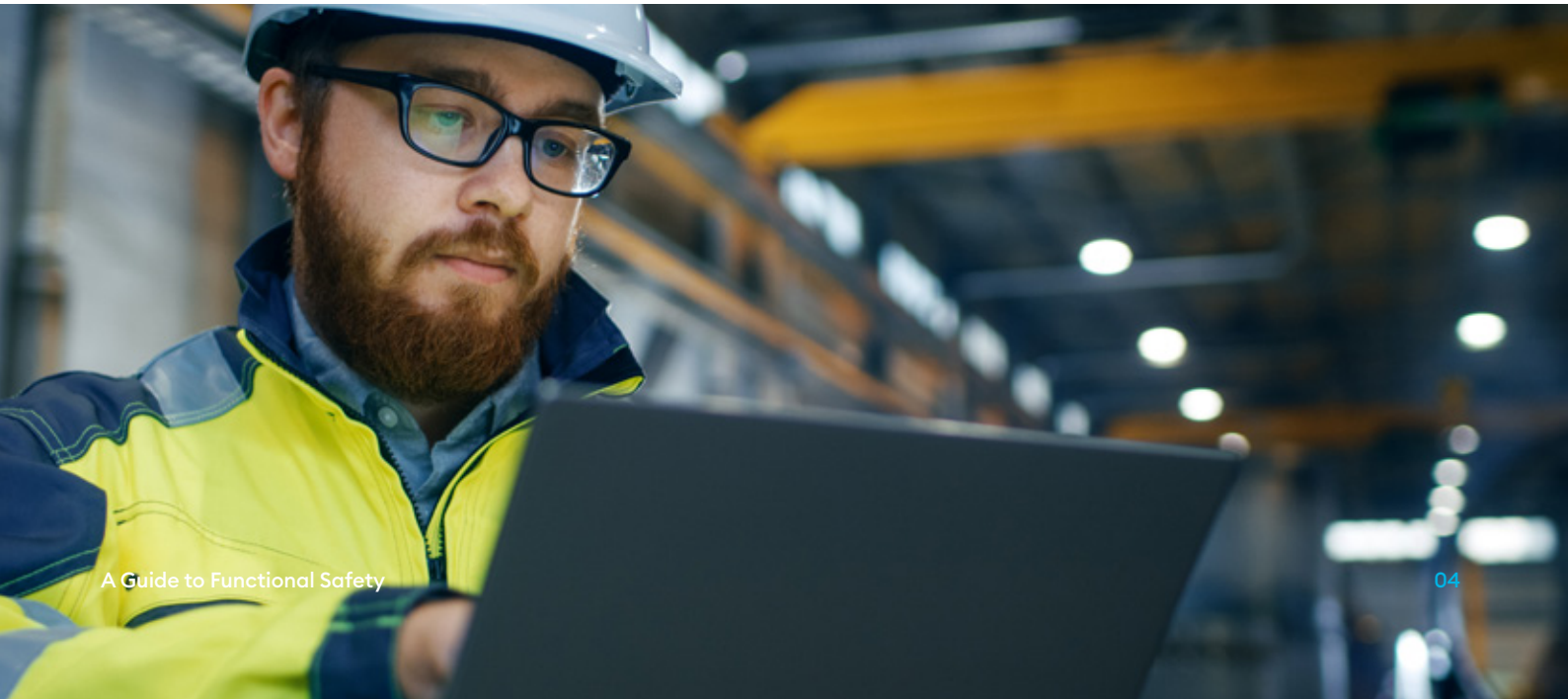
In an Industrial Process environment, Functional Safety is concerned with the appropriate responses of instrumented process systems to hazardous or dangerous conditions that are likely to lead to injury and/or equipment damage or indeed injury and damage beyond the boundaries of the plant.

Functional safety provides a proactive means of detecting the potential onset of a hazard or dangerous condition and subsequently preventing it from arising in the first place rather than simply offering primary, passive protection after the event.

How does it apply to me?

Inspections by the Competent Authority for Functional Safety are concerned with the management, design, installation, operation and maintenance of instrumented process safety systems that reduce the risk of a major accident. The benchmark standard for these activities is given in BS EN 61511 Functional safety - Safety instrumented systems for the process industry sector.

It's common for companies to focus on identifying the required Safety Integrity Levels (SIL) and designing systems with appropriate Safety Instrumented Function (SIF) to achieve the required level of risk reduction however the SIF is only one of several layers of protection. Other systems also play a key role in achieving the overall risk reduction requirements. The process control system (BPCS), when it is working optimally, will respond and maintain a safe and efficient operating envelope for the process plant or unit. A failure of this system will lead to a demand on the next layer such as a process alarm.



What should I be doing?

IEC 61508 and 61511 describe the overall functional safety lifecycle from concept, through hazard analysis, requirements, realisation and operation to end of life decommissioning and is explained further below.

Hazard Identification

The identification of hazards considers a number of categories including hazard to personnel leading to injury, damage to the environment, financial and societal hazards. There are a number of recognised approaches to hazard identification. These need to be formally and fully documented to a corporate procedure. Often such methods include review by teams, applying judgement and experience when looking at the risks. These judgements need to be fully and clearly documented, both for evidence of application of an appropriate process and to assist in future reviews. The consequences of identified hazards should be according to documented corporate standards. The ultimate aim of the process should be the identification of the required level of risk reduction that the SIF is expected to fulfil. Companies can use various approaches to determine the required level of risk reduction for a given hazard. These can broadly be divided into qualitative or quantitative categories. An example of a qualitative approach would be a risk graph or matrix where the output is given as an order of scale. While relatively simple to apply, this approach is conservative and may lead to over-specification in design. The most frequently used quantitative approach is Layers of Protection Analysis (LOPA). LOPA studies produce a target risk reduction expressed as the required probability of failure on demand (PFD) of the safety instrumented function. While the output of the LOPA approach is definitive, it is still subjective and relies on the experience and knowledge of the team applying the method.

What should I be doing? cont...

Safety Requirement Specification

The starting point of functional safety is often the Safety Requirement Specification (SRS). Although this comes after hazard analysis in the standard lifecycle model, companies should begin the development of the SRS at the concept stage and build its detail as their scope and hazard assessments progress. Good practice is to create a single document containing all the core information with appropriate mapping to other managed documents. For example, the SRS will contain details of all current SIFs, including a demonstration of the risk reduction achieved. The SIL demonstration calculations may be kept in a separate system provided it is easy to follow a full audit trail. It can also be useful to provide a link back to the main process hazard tables to identify the hazard basis for each SIF used in the plant.

What should I be doing? cont...

Engineering Design

Evidence that sufficient effort has been put into the SIF engineering and design process will be required. It is important that a company has not only completed work to the right standard, but that it can provide documentary evidence that it has done so. This documentation should include;

- How the design achieves the Safety Requirement Specification
- Which components will be used within the safety circuits
- How the circuits will be designed, built and commissioned
- The design basis and programming conventions for the software used to program the logic solver or safety PLC
- The competence of contributors to the design

This phase of the lifecycle needs to demonstrate that the design meets the SRS, including the required level of risk reduction and calculation of the SIL required to deliver the appropriate PFD is only part of the requirements of IEC61511. The design also has to demonstrate the required level of Hardware Fault Tolerance (HFT) for the desired SIL.

What should I be doing? cont...

Commissioning

A company must be able to demonstrate comprehensive testing prior to introducing the hazard relating to the SIF.

Factory acceptance testing should include a definitive hold point date and must be designed to include extensive negative testing (testing that shouldn't happen). There should be a definitive test script against an approved cause and effect logic along with approved testing documents in place, to evidence hardware and software compliance meets the design intent.

Site acceptance testing should include integrated function tests that include full system architecture performance testing including validation of a system's ability to allocate extra resource or to move operations to back-up systems in the event of a primary failure. It should include the testing of any services such as electrical power and/or air supplies plus failover testing and UPS autonomy.
Final proof testing should cover full end-to-end loop testing including settings, parameters and trip points. Any failed tests should be rectified and fully proof tested again. There's more detail on proof testing in our Proof Testing guide.

Can I do this myself?

The standards relating to Functional Safety, IEC 61511 and IEC 61508 cover the Functional Safety lifecycle from concept, through hazard analysis, implementation and operation to end-of-life decommissioning. IEC 61511 is targeted specifically at the design, operation and maintenance of process plant Safety Instrumented Systems used in the Process Industry. IEC 61508 covers a broader range of safety-related systems, including emergency shutdown, fire and gas, machine safety devices and networks and much more.

The whole safety lifecycle relies on the application of people with the right skills to the relevant tasks. The Competent Authority look for evidence that an organisation has appropriate competence management systems in place to ensure this is the case. The benchmark document used in the HSE Competent Authority guide is HSE Human Factors Guides –. Managing competence for safety-related systems.

Where Covol can help

Following a structured process is key to compliance, we can assist you in ensuring the safety of your people, plant, and environment. We provide businesses with a systematic review and assessment in line with the appropriate standards to indicate where any shortfalls in Functional Safety are apparent. This comprehensive analysis for areas of improvement provides tangible recommendations and practical solutions to rectify any shortfalls.

We have an excellent track record in providing this service to clients in numerous high hazard environments including major oil and gas and chemical site operators as well as smaller manufacturing facilities. Using Exida qualified competent Functional Safety engineers, we have delivered highly technical safety solutions to clients across a range of sector groups.

If our help in supporting you with Functional Safety is something that you would like to know a bit more about then please get in contact with us.

Ready to engineer change and progress in your business?

Get in touch to speak to our experts

01642 613 622 info@covol.co.uk

covol.co.uk

Company No. 11184319 / Registered in England & Wales