Back to basics – getting a grip on functional safety

Imagine a facility where there are safety systems provided because without them, the risk of an accident is intolerable. They'd be the best managed and maintained systems on the facility, right? Unfortunately, that's not the reality we often see on process plants. Here's a brief article to support getting back to basics and getting your grip back on functional safety. Getting some help from a qualified functional safety engineer is a good idea!

Firstly, let's consider why these systems are installed. The guidance in the Health & Safety Executive's publication R2P2, Reducing Risks, Protecting People requires risks to people reduced to as low as reasonably practicable (ALARP). Risk should be controlled such that, under most circumstances, the risk of a fatality from any single event is no greater than 1 in 1000, and only considered broadly acceptable when less than 1 in 1 million.

For intolerable risks, risk reduction measures must be implemented, or the design changed. A quantum of risk reduction is determined which must be achieved or bettered. One method is to install an electrical, electronic or programmable electronic (E/E/PE) system which can detect, decide and act upon a rogue process variable. For example, a pressure trip which closes a valve upon sensing a high pressure.

The international standards IEC 61508 (for equipment designers) and IEC 61511 (for operators of chemical plants) represent industry good practice. Safety trips are referred to as Safety Instrumented Functions (SIFs); one or more SIFs may make up a Safety Instrumented System (SIS). The risk reduction factor (RRF) determines the Safety Integrity Level (SIL) to be achieved. There are four safety integrity levels:

Safety Integrity Level (SIL)	Risk Reduction Factor (RRF)
1	10-100
2	>100-1,000
3	>1,000-10,000
4	>10,000-100,000

Table 1: The relationship of SIL to RRF

Getting started:
The standards dictate what is required; the most important part is a functional safety management system (FSMS). The FSMS ties together who does what, with what, and when. We suggest a single document that references other documents and includes:

- Functional Safety Policy & Planning
- SIS Safety Lifecycle: Design Phase, Operations & Maintenance Phase, Decommissioning
- Management of Change
- Facility Security and Cybersecurity Management
- Functional Safety Assessments & Verification
- SIS Performance Criteria
- Post-incident and Post-accident analysis
- Supplier Management
- Functional Safety Audits

The FSMS should be communicated to those responsible for functional safety. A key part is the policy; this demonstrates management commitment to meeting the requirements of the standard, stopping functional safety from being another item in an already overpacked schedule and budget; it is the barrier in place to prevent a major accident and needs due care and attention.

The next steps:
Establish the extent of the problem. We suggest you undertake a Stage 4 Functional Safety Assessment (FSA 4). There are five stages of FSA in IEC 61511:

FSA 1: After production of a Safety Requirements Specification

FSA 2: After SIS design and engineering

FSA 3: After installation, commissioning and validation of the SIS, and any other risk reduction measures

FSA 4: periodically throughout the operation and maintenance phase

FSA 5: before modifications and decommissioning

The FSA 4 determines whether SIFs are functioning as expected and that any design assumptions remain valid. For example, how often a SIF is required to protect your workforce from a major accident. It will also review the findings from any previous FSA. It may identify that there was none. If this is the case, you will need to undertake an FSA 3.

The FSA 3 is the last check before a SIF provides protection against a major accident hazard. It is thorough and determines if the functional safety lifecycle has been followed. It also reviews FSA 1 and 2; if you can't prove these were done, you have a significant problem. Speak to a qualified functional safety engineer.

Next, address the problem. We suggest surveying your plant and producing a safety requirements specification (SRS); used to convey the design requirements and constraints.

Then, perform a SIL verification calculation; a pass or fail exercise. Failure means you have an urgent problem to solve: your safety system isn't good enough.

At this point, you are regaining your grip on functional safety, but there is lots still to do!

6 Engineering are specialists in functional safety. We're here to help and happy to support you https://6engineering.co.uk/ - Good luck!