SIS-TECH
12621 FEATHERWOOD, STE 120
HOUSTON, TX 77034
713-909-2100

Functional Safety Assessments of Safety Controls, Alarms, and Interlocks

How efficient are your functional safety projects?

Eloise Roche, Senior SCAI Consultant
Monica Hochleitner, Senior SCAI Consultant

For many oil, gas, and chemical companies, functional safety is achieved through implementation of process control and safety systems after inherently safer design practices are applied to the process design. Functional safety projects implement a variety of safeguards, including safety controls, alarms, and interlocks (SCAI). However, if these projects are not executed correctly, or if the systems are not operated and maintained per the design assumptions, the SCAI will not provide the desired amount of risk reduction. Functional safety assessments (FSA) are essential to sustaining the risk management plan and preserving the intended return on investment of the project.

FSA are performed throughout the safety lifecycle, during the project execution and long after the handover to operations, to verify that each SCAI system is in conformance with the applicable standards and its safety requirements specification. The assessor inspects many specific details within the SCAI to determine the correctness of the system and whether it meets the needs of the operating facility. Instrumentation, application programs, procedures, design documents and system performance are all subject to assessment.

Table 1 provides the purpose for each FSA stage as recommended in industry standards. A robust FSA program following this guidance should limit propagation of errors from one project phase to the next. The timing requirements for stages 3-5 are mandated, but deferring recommended stages 1 and 2 can result in increasingly costly rework. Deficiencies in timeliness or quality of SCAI deliverables have a higher cost impact the longer correction is delayed.

Table 1 – Scope and Timing of FSA per IEC61511-1:2016

Stage	Project Task	Timing	Purpose
1	Hazard and Risk Analysis (H&RA) Independence and Risk Reduction Limit Review	Immediately after initial H&RA has been performed and SCAI functional specification documented	Ensure risk reduction gaps are addressed and save money during project
2	Detailed Design Review	Immediately after detailed design is complete and before purchasing, programming, and installation begin	Ensure design achieves required risk reduction and save money during project
3	Functional Safety portion of pre-startup safety review (PSSR)	After installation, pre-commissioning and validation are complete and all procedures developed but BEFORE hazard is present	Ensure safety prior to startup
4	Operation and Maintenance Review	Periodically	Confirm performance of installed system
5	Proposed Change Review	Prior to implementing a proposed modification	Determine which assessments apply to the proposed change

While FSA stages have different scopes, all are alike in certain aspects. Each needs proactive planning for effective execution, including access to the detailed information covered by the scope. Each FSA involves at least one competent assessor who is independent of the work being assessed. Written procedures on how to carry out the assessment are required. In practice, FSA are usually performed with detailed checklists that ensure there will be clearly documented justification for each finding, whether positive or negative. Finally, all assessments require timely and satisfactory resolution of recommendations. For example, SCAI functional defects found during the stage 3 assessment must be resolved, or compensating measures put in place, prior to startup.

As the process industry has evolved, automation has taken a crucial role in the normal control of the facility and the protection of personnel, the environment, and facility assets. The sustainability of safe automation is essential to the successful, productive and safe operations of these plants. Automation management of change, alarm management, verification and validation, functional safety assessments, periodic audits, and bypass controls are widely acknowledged as critical management systems for safe

SIS-TECH.COM

operation. Defects in these management systems appear with unfortunate frequency in process safety incident reports. Robust execution of FSA can help identify and correct such systematic errors, reducing the chance that they will contribute to loss events. Timely execution of FSA can also help in preserving limited project resources from costly rework. To be effective, these reviews require sufficiently independent and competent personnel and strong support from senior management to ensure that recommendations are resolved in a timely and effective manner.

Click here to read the full paper.