BLOG/BILLINGHAM, UNITED KINGDOM | AUGUST 2021

Levelling Up Relief and Depressuring Assurance to Meet Functional Safety Best Practice

Blog by Paul Dumain, Process Engineering Team Leader, ABB

In a previous blog, I compared the detailed requirements for assurance of Safety Instrumented Systems (SIS) in IEC 61511 against the lack of equivalent requirements for mechanical pressure relief devices in common industry standards. This disparity seems alarming, given that the two systems often provide over-lapping and inter-dependent protection for process plants.

In this follow up blog, I'll explore the requirements of IEC 61511 in further depth and discuss how the same lifecycle approach can be applied to 'best practice' in pressure relief system design, operation and maintenance.

The Requirements of IEC61511.

IEC 61511 details four essential components for functional safety assurance of SIS;

- Verification
- Validation
- Functional Safety Assessments
- Functional Safety Audits

Verification

Verification is a process that IEC 61511 requires in every phase of the safety lifecycle, from the initial hazard identification through to the final decommissioning requirements. It is defined as the formal review and acceptance of process, procedures, documentation and testing results generated at each stage to ensure they're fit-for-purpose. IEC 61511 states that the verification techniques & measures, as well as the required independence of the verifier, may be based upon the complexity and novelty of the design, along with the required SIL level.

For mechanical pressure relief systems, verification best correlates to the formal checking and approval of pressure relief designs in the design phase, and the review and approval of inspection and maintenance reports during the operations phase. IEC 61511 states that the requirements for SIS verification should be clearly planned and recorded. This equates to a written checking and approval process for pressure relief design and maintenance, confirming for example:

- procedures, measures and techniques to be used
- when verification activities will take place
- the persons, departments and organizations responsible for verification, including required levels of independence
- identification of items to be verified
- identification of the information against which the verification is carried out
- the readability and audit-ability of documentation

Validation

In IEC 61511, 'validation' confirms that the installed and commissioned SIS meets the requirements detailed within the Safety Requirements Specification (SRS). This is achieved via Site Acceptance Testing (SAT).

Typical SAT 'best practice' for relief valves would include an initial bench based check of set pressure, followed by as-building checks to confirm the relief device is installed as per the design intent. Confirmation of actual depressuring times versus specification should be considered for depressuring systems.

Functional Safety Assessment (FSA)

IEC 61511 details a five stage FSA process, mapped across the safety lifecycle as follows:

Preceding IEC61511 Life Cycle Phases		IEC61511 FSA stage
1	Hazard and risk assessment	1
2	Allocation of safety functions to protection layers	
3	Safety requirements specifications	
4	Design and engineering	2
5	Installation, commissioning and validation	3
6	Operation and maintenance	4
7	Plant modifications	5
8	Decommissioning	

Table 1; Details of IEC61511 phases and FSA stages

FSA is intended to be a team activity, with participants from both technical and operations roles. IEC 61511 states that FSA teams should include at least one senior competent person not involved in the project design team (for stages 1, 2 and 3) or not involved in the operation and maintenance of the SIS (for stages 4 and 5). The FSA provides formal approval that the SIS meets the required risk reduction criteria. Particular emphasis is placed on FSA 3 within IEC 61511, as this the final FSA before the hazard being mitigated is present (typically before the process fluid is introduced to the facility). IEC 61511 also states that an FSA (Stage 4), should be carried out periodically during the operations and maintenance phase to ensure that these activities are being carried out accordance with the assumptions made during the design phase.

There isn't an obviously comparable activity to FSA within the typical pressure relief design, operation and maintenance lifecycle. That said, some operating companies implement a 'Design Verification Certificate' (DVC) process, which involves the final sign-off of relief designs by an independent and qualified person prior to use (i.e., at the equivalent point to FSA 3). Regarding the operations and maintenance based FSA 4, very few companies regularly review their relief designs during its operational life to ensure it is being operated and maintained as originally expected and therefore this is a major gap in comparison to SIS.

Functional Safety Audit

Within IEC 61511, a functional safety audit is a key verification activity intended to review the safety management system, auditing the associated policies and procedures to ensure that they are fit-for-purpose. Typical areas of review include assessment of the competence of responsible persons, management of change procedures, and the effective and timely resolutions of recommendations from FSAs. IEC 61511 states that audits should be completed by a person independent of the SIS delivery system, although the frequency of audits is not stipulated within the standard.

Again, there is no obvious parallel to relief design, although pressure relief procedures and philosophies may be audited as part of a wider quality assurance review, for ISO9001 for example. However there is nothing with common industry pressure relief standards which recommends a philosophy and procedural level audit.

The Missing Links

As outlined above, the largest gaps between the detailed and thorough functional safety assurance requirements for SIS and those commonly applied to mechanical pressure relief systems are associated with Functional Safety Audits and Assessments. These two activities are designed to ensure that systems are specified, designed, installed, operated, maintained and modified in a controlled and reviewed manner.

Therefore, the question must be asked, why does industry not apply the same focus and attention to implement an equivalent system for pressure relief systems?

ABB's Process Safety team provides expert process and functional safety knowledge and thought leadership to the process industries. The team offer bespoke, pragmatic solutions based on operational experience, best practice and regulatory feedback to ensure safe, smart and sustainable operations.

For further information please email me at paul.dumain@gb.abb.com

For further information see ABB pressure relief