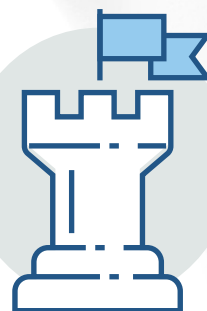




SAFE AND SOUND



Ton Beems, Yokogawa Europe, the Netherlands, explains how compliance with IEC-61508 and IEC-61511 standards can be ensured through the operational phase of the safety lifecycle.



Much effort and attention is taken to develop and design a safety instrumented system (SIS) so that it is compliant with the IEC-61508 and IEC-61511 standards. First a hazard and operability study (HAZOP) is carried out; then the safety instrumented functions (SIFs) are assigned a safety integrity level (SIL), and, in many cases, this is confirmed in a so-called SIL verification.

The safety system is only one of several 'layers of protection' in a plant, alongside, for example, a rigid review of the design and control of the process. Another layer is the mechanical layer where pressure relief valves, rupture disks and break-pins can reduce the frequency of hazards coming from the process. Finally, should something go wrong despite the other three layers of protection, the 'mitigation' layer is there to reduce the consequences.

In a previous article published in *Hydrocarbon Engineering*, Mark Hellinghuizer and Ton Beems pointed out that functional safety systems are designed on the assumption that any danger is likely to originate in the process rather than any external sources.¹ However, system and network security is becoming increasingly important

– something that is substantiated by the latest edition of IEC-61511.

Safety requirement specification

After SIL verification has been completed, the scope for the different layers of protection is clear and responsibility can be allocated to vendors or suppliers. However, for the SIS layer, the IEC standards require a little more in the shape of a special safety requirement specification (SRS), which is targeted at the suppliers of the safety system. Once this is completed, the SIS supplier, contractor or system integrator can start the engineering of the SIS.

This process is designed to be structured and well documented, with every document written evaluated by a competent reviewer (someone other than the author) and everything that is built (whether hardware or application programs) is thoroughly tested by a competent tester (similarly, someone other than the engineer). At the end of this process, the client accepts or declines the safety system during a factory acceptance test. This test is a validation of the SRS, in which all intermediate verifications are checked along with document reviews, internal testing,

phase of the system. The backbone of this training will be the safety lifecycle, as defined in IEC-61508 and IEC-61511, with every step in the lifecycle forming a training module or chapter (Figure 2). The rest of this article summarises these elements and their relevance, both before and during the operational phases.

Of common importance for all phases are the following:

- **Competence:** who is on site? Which companies? Which people? Which hierarchy between the companies? If this is known, then one checks if all personnel are proven to be competent for the job.
- **Documentation:** during the full safety lifecycle there must be a so-called 'auditable trail'; who did what? When? How? What was the outcome? Who authorised what? Who engineered what? And so on. A 'watertight' auditable trail demonstrates a good systematic capability for site organisation.
- **Testing:** since safety functions cannot be tested 'live' in most site installations (because they will shut down the process), as much testing as possible has to be carried out beforehand. For functional safety, this involves comprehensive management of change procedures, in which all errors or malfunctions are documented and their safety-related impacts reviewed in a process known as 'impact analysis'.

Site installation

As mentioned before, it is important to know which companies are involved. Does someone responsible on site have the complete overview of all companies and company representatives? Is there documented evidence that all personnel on site are competent? Does everybody understand their individual responsibility for their part of the job? Is there a formal site acceptance test certificate for every vendor to ensure the formal handover from the supplier to the end-user?

Commissioning

The field devices will be connected and tested, and, in most cases, also verified by an independent certification organisation who looks over the shoulder of the personnel who perform the checks. When all loops for a particular SIF have been tested, the total function can be tested. This phase requires co-ordination, overview and, if dangerous situations can occur, a fully operational permit to work system.

Overall site validation

Before the hazards are introduced into the system, the standards require it to be validated. Depending on the SIL of the safety functions, an independent person (SIL 1), an independent department (SIL 2) or an independent organisation (SIL 3) should carry out this validation. The validator looks both backwards and forwards:

- **Backwards:** have all verifications been completed? Are the personnel competent? The personnel may ask for another SIF function test, for example, to see for themselves if the SIF actually works within the SRS.
- **Forwards:** is the organisation on site ready for the future? Are all procedures for operation, maintenance, proof-testing and modifications in place? And, are the people that remain on site competent?

Operations

The plant is now up and running. If the distributed control system (DCS) controls the process within the operational envelopes, then the safety system has an easy job. With skilled operators and good procedures, it may have an easy job for many months, even years. However, after a year of not closing down, who can guarantee that a critical valve will fully close within the specified time interval? During the operational phase, it is important that deviations from normal operation are registered and investigated. These situations must be studied by competent personnel and if this results in modifications, a good impact analysis has to be carried out and all intermediate steps of the lifecycle have to be repeated again for the changed part(s).

Maintenance

As with everything else, maintenance must be well documented: who did what? When and where? What were the circumstances? Should an incident happen onsite, one of the first things an insurance company will check will be the maintenance records to see if proper maintenance was neglected. Again, identifying that there is a need for clear procedures and documentation as standard tools.

Proof-testing

During the initial system engineering, calculations of 'probability of a failure on demand' (PFD) will have been made to prove that the SIFs are compliant with the required SIL level. Multiple devices will have been used to prove the hardware fault tolerance required for a certain SIL level, and the systematic capability of the organisation responsible for the engineering will have been checked. But for the PFD average, these calculations are based on a so-called proof-test interval. In other words, if one does not test their SIF, the risk for dangerous undetected failures increases year-by-year, and soon the SIL level will be unattainable.

So, onsite personnel have to be aware of individual proof-test intervals for individual SIFs, and these tests have to be conducted, recorded and compared with previous tests to ensure something dangerous has not crept into the safety function over the years. Moreover, a proof-test for a valve involves more than just partial closing, which will only prove that the valve will move slightly but offers no guarantee that the valve will fully close. The only option is a full-stroke test, which means that a (partial) shutdown is required. Again, should something occur on site, this is the first thing that insurance companies will look at, and if there is no evidence that proper proof-testing took place then they will have a valid reason for abstaining from paying out.

Modifications

The procedure for modifications follows a familiar pattern: modifications, impact analysis, procedures, engineering, testing offline, acceptance test offline, implementation at site, commissioning, testing, acceptance test on site, overall validation and then back into operation. Management of change is the key phrase here, with documentation, auditable trail, and competent people.



Figure 3. Yokogawa training course for personnel in the operational phase of a safety system(s).

Decommissioning/disposal


As the Bhopal disaster in 1984 demonstrates, it is important to ensure that decommissioning and disposal is carried out in a structured way, with procedures, an auditable trail, and competent personnel.

Filling the gap

There are many reasons for people in the operational phase of a safety system to be proven competent. As stated previously, TÜV Rheinland noted this gap and asked its course providers to set up a training programme to fill the gap. Yokogawa accepted the challenge because it also recognised this gap in site competency, and decided to create a new training schedule focused on the personnel in the operational phase (Figure 3). This was piloted recently for technicians from three leading end-user organisations: Gate LNG terminal, Shell and NAM, to see if it was the correct approach and to discover where there was scope for improvement to make it fit for purpose. The participants provided Yokogawa with good comments and information, which has been taken on board and will aid in the implementation of an updated plan. Yokogawa aims to have this training programme ready for the public from June 2017.

Conclusion

When realising a functional SIS to the IEC-61508 and IEC-61511 standards, much attention is paid to competency during the SIS realisation phase (an average of five years), but not enough to competency during the operational phase (20 years or more).

The IEC standards are calling for '(re)training and (re)assessing', a situation recognised by TÜV Rheinland, who has asked course providers to set up a training programme especially for those involved in the operational phase of the system. The core of this training is the safety lifecycle as defined by the standards, and this article describes the resultant training programme and its implementation to date. 

References

1. BEEMS, T. and HELLINGHUIZER, M., 'Secured against sabotage', *Hydrocarbon Engineering*, (July 2014), pp. 38 – 44.

Together facing a brighter tomorrow

At Yokogawa, we believe the sky's the limit. And to reach beyond today's horizons, we work step-by-step with you to make the unimagined a reality. That's how we move forward, through the synergy of co-innovation partnership. Join hands with us, and together we can sustain a brighter future. Yokogawa: Building a better tomorrow with you today.

Co-innovating tomorrow™

Please visit www.yokogawa.com/eu

