TÜVRheinland®
Risktec

RISKworld / The Newsletter of Risktec Solutions / Autumn 2018 p2-3

An introduction to functional safety assurance

If you've ever wondered what's meant by the term functional safety assurance, you're not alone. Simply put, functional safety assurance is the process by which we ensure that safety-related systems do what we need them to do, when we need them to do it, so that risk is maintained at tolerable levels. But what does this mean in practice?

The originating standard for functional safety is IEC 61508, which applies to Electrical, Electronic and Programmable Electronic (E/E/PE) safety-related systems. This is a generic standard with industry-specific variations developed from it, including IEC 61511 for the process industry, for example.

Although functional safety assurance principles can be applied to all types of equipment, the term is usually used in connection with E/E/PE systems, for instance railroad signalling, or trip logic for stopping pumps or isolating valves automatically.

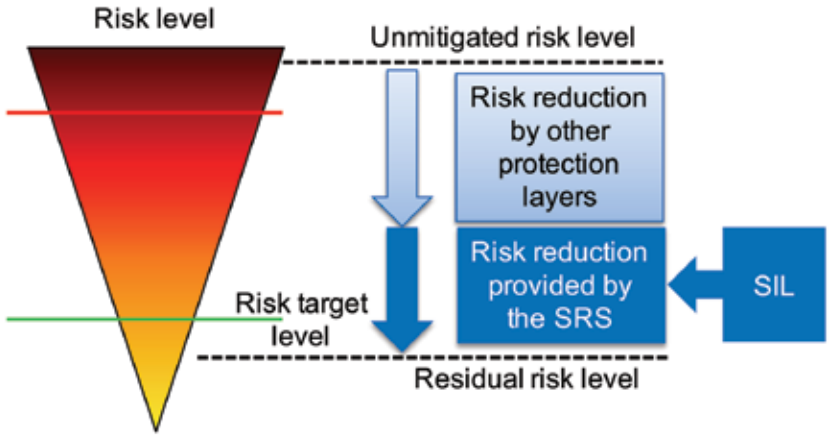

Figure 1 - Risk reduction by safety-related systems

WHAT IS IT?

Functional safety assurance comprises five main activities:

1. Determine safety function and integrity requirements
2. Design system to achieve requirements
3. Verify that design fulfils requirements
4. Validate that functional safety activities have been undertaken correctly
5. Ongoing activities to support the integrity of the system

Unlike some standards which tend to be relevant to a single step of the risk management process, functional safety assurance covers a number of these steps. It may seem like a lot of additional work but, if properly planned for, it can be integrated into existing risk management and design activities with relatively minimal extra effort.

1. DETERMINE REQUIREMENTS

At this stage the project defines the concept design and carries out risk assessment to determine:

- The required safety function
- The level of risk reduction required of the safety function

This is typically presented as a safety requirements specification, which details the functionality and risk reduction requirements of the

Safety-Related System (SRS), and then maps that risk reduction to an equivalent Safety Integrity Level (SIL), as illustrated by Figure 1. This step if often called 'SIL determination' or 'SIL assignment'.

The requirements specification should also include requirements relating to testability, maintainability and independence (from other safeguards and fault causes), as well as the specific functionality in the event of detected failure, to help inform the design process.

Optioneering should be conducted to identify the most effective means of achieving the required risk reduction and arrive at the As Low As Reasonably Practicable (ALARP) solution. For example, it might be simpler and cheaper to fit a key-controlled padlock on an enclosure, rather than design a bespoke E/E/PE SIL-rated interlock.

2. DESIGN SYSTEM

The system proposed to deliver the safety function must then be designed, based on the safety requirements specification and the relevant standard from the IEC 61508 series, which considers factors such as architectural constraints, minimisation of systematic failures and fault detection, and supports the overall demonstration of integrity. This ensures that not only will the SRS reliably perform the required safety function, it will also be suitably robust, rigorously designed and tolerant to faults such that confidence in its correct function is assured.

3. VERIFY DESIGN

At this step the design is critically reviewed against the requirements, typically including reliability analysis to demonstrate that the required risk reduction has been achieved, i.e. 'SIL verification'. Verification must also confirm that the full range of safety requirements have been achieved, e.g. that appropriate redundancy, diversity and robustness have been incorporated into the design.

4. VALIDATE/CERTIFY DESIGN

The validation process is often undertaken by independent parties to ensure objective analysis. The intent of this step is to audit the overall process to confirm that appropriate functional safety assurance tasks were planned for and undertaken when required by suitably competent people, to an appropriate standard and quality. This will initially focus on a high level, but will drill down into specific detailed analysis as required. Equipment manufacturers will often seek formal recognition of the design's validation in the form of 'SIL certification' by an accredited certifying body.

5. ONGOING SUPPORT

The requirements of functional safety do not end once the design is verified and validated. The system must still be installed, tested, maintained, monitored and managed so that it continues to perform as intended and that the assumptions and claims of the assurance process as a whole remain valid.

SO WHAT CAN GO WRONG?

Although at a high level the functional safety assurance process is relatively simple, there are some common pitfalls, which are equally applicable to risk management activities more generally. For example:

- Activities not anticipated or planned
- Work not undertaken by competent persons
- Poor traceability between hazards, requirements and design
- Ill-defined or missing safety requirements specification
- Weak or missing design evidence
- Key design ALARP decisions not documented

CONCLUSION

In the right hands, functional safety assurance is a mature, standardised process for designing, delivering and operating fit-for-purpose E/E/PE safety-related systems and their associated safety justification.

Contact: Kevin Charnock
kevin.charnock@risktec.tuv.com