Functional Safety – How Compliant?

Nick Dawtry – Deputy Chief Inspector, Petroleum & Geothermal, WorkSafe NZ

Electrical, control, and instrumentation equipment and systems provide important prevention and mitigation measures against major incidents and accidents. The functionality and complexity of integrated systems is increasingly dependent of reliable systems. It has become more challenging to identify potential system issues that could lead to failure, with an increase on the reliance of complex software, electronic systems and automation to protect us from harm.

The Health and Safety at Work Act 2015, which is regulated by WorkSafe, requires that risks are reduced so far as is reasonably practicable (SFAIRP). The NZ petroleum legislation also uses the term as low as is reasonably practicable (ALARP) to mean essentially the same as SFAIRP.

Functional safety is the overall safety of a system or piece of equipment. It depends on the system or equipment operating correctly in response to its inputs, including the safe management of likely operator errors, hardware failures and environmental changes.

The functional safety lifecycle of equipment and systems involves the overall management, design, installation, operation, maintenance and modification of process safety systems that reduce the risk of a major accident.

These can include basic process control systems, safety instrumented systems and alarm systems.

The application of functional safety standards provides the duty holder a means to demonstrate equipment has been suitably designed, installed, operated and maintained to reduce risk as far as is reasonably practicable.

High Hazard installations operating under an accepted safety case document the standards applied to the installation or facility. While some duty holders claim to have systems that are compliant with recognised functional safety standards, WorkSafe's interactions within the industry has shown that the level of compliance against the elements of the functional safety lifecycle varies considerably.

As such, going forward, functional safety will be a focus point for WorkSafe in the High Hazard industries.

WorkSafe will be reviewing and assessing how duty holders manage functional safety against the benchmark standards, as a way to assess how their risks are being managed.

In particular, these standards include IEC 61511 Functional Safety (safety instrumented systems), IEC 62061 Functional Safety (Machinery), IEC 62682 Alarm Systems. Cyber security considerations are also important to keep integrated active systems available, these standards include IEC 62443 Cyber Security and ISO/IEC 27019 Information security management.

The expectation is that these benchmark standards should be applied either in full to installations built since the establishment of the benchmark standards or so as far as reasonably practicable to installations that pre-date their publication[1].

Regulatory Approach to the Duty Holder

Initially WorkSafe issues a set of questions to an operator and/or installation aligned to the elements of the functional safety lifecycle. The objective is to provide WorkSafe with a baseline to ascertain compliance against functional safety benchmark standards.

[1] The concept of Functional Safety has been in development since the early 1980's and subsequently refined and developed into a suite of recognised international standards (e.g. IEC 61508) since around 2002 along with the derived associated specific industry standards (e.g. IEC 61511 – Functional Safety for Process Industry Sector, IEC 62061 – Functional Safety of Machinery), though acknowledging that local/national variations may exist (e.g. ANSI/ISA 84.00.01).

The level, detail and quality of responses to the questions will allow WorkSafe to gauge duty holder compliance, and in turn provide an opportunity for WorkSafe to focus on which duty holders operations need reviewing and assessing. This will be derived using a risk ranking and prioritisation model.

Recognising most duty holders operate in the 'operation and maintenance' phases of the functional safety lifecycle, WorkSafe will be placing an emphasis on the adequacy of their Safety Instrumented Systems (SIS) to ensure they are managing risks appropriately.

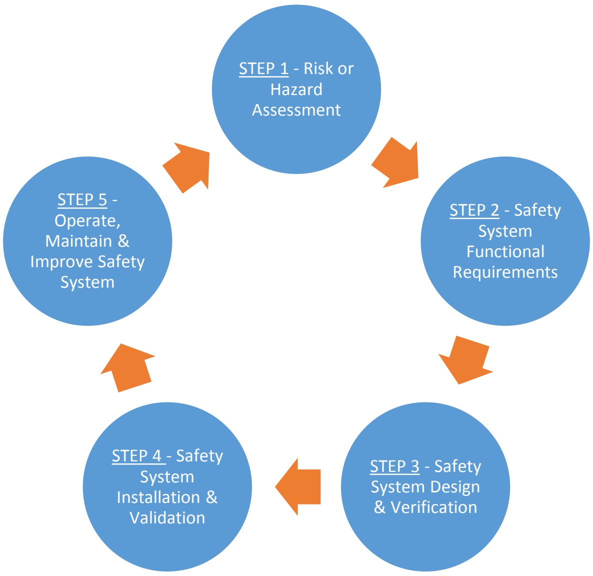
NZ legislation requires safety-critical elements on an installation to be suitable and where provided, remain in good repair and condition. Equipment and systems that are identified as safety-critical elements, for example safety instrumented systems, must be compliant.

Where duty holders systems pre-date the benchmark standards, often referred to as 'legacy systems', they will be required to undertake a gap analysis of their existing systems against the lifecycle phases of the benchmark standards[2].

Example of key areas of verification during inspection;

- Functional Safety Management system
- Hazard and Risk Assessment
- Engineering and Design
- Competence
- Operation, Maintenance & Inspection
- Verification
- Software
- Information and Documentation
- Management of Change
- Audit

Figure 1 – Functional Safety Lifecycle Overview


STEP 1 - Risk or Hazard Assessment
STEP 2 - Safety System Functional Requirements
STEP 3 - Safety System Design & Verification
STEP 4 - Safety System Installation & Validation
STEP 5 - Operate, Maintain & Improve Safety System

Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position or policy of any other IRF member.

[2] For offshore oil and gas applications, it is not uncommon for API RP 14C, ISO 10418 and IEC 61511 be specified, or in fact all to a certain extent. Consideration should be given to avoiding potential conflict between their prescriptive and risk-based approaches. ISO 10418 is very similar to API RP 14C but refers to IEC 61511 for safety instrumented functions. The goal setting regime within NZ does allow duty holders to take other action to ensure and demonstrate that risks relating to the use of safety related control and protection systems are reduced SFAIRP.