This paper will show a practical approach for applying to IEC 61511, Functional Safety in the process industry. What does end-user need to do to deal with functional safety management while designing safety instrumented functions and determine the Safety integrity level for the safety functions? It also covers the organizational responsibilities and examples of documentation to needed working in a lifecycle according to IEC61511. End-users are struggling every day with all the lifecycle activities connected to functional safety management. This includes activities from design, implementation, and operation though maintenance and repair of safety instrumented systems (SIS). The activities starts with the process hazard analysis and risk assessments which are typically done by the end-users who understand and know the process. The result of these activities gives a description of the required functionality and safety integrity for each safety function. The safety function is linked to a specific hazard or hazardous event. The end-user is always responsible for the safety integrity of the safety system in the plant. A lifecycle concept in the functional safety standards helps in a systematic way to deal with activities, responsibilities, and documentation needed between the different organizations involved. This paper will give examples of how to deal with the responsibilities between end-users and system integrators and how information can be structured in different type of documentation, like Safety plan, Verification &Validation plan and Safety Requirement Specification.
**What is safety?**

All aspects of safety are important, but safety can mean different things to different people. Some care is needed to understand the context and relationships, and to understand what is important to others.

When we discuss safety there are a number of different phrases in use, within the oil and gas industry, and there are also areas of overlap. Depending on the company and industry this may vary a little, but the following phrases are typically encountered:

![Figure 1: Overview of safety areas](image)

- **HSE/OHS – Health, Safety and Environment or Occupational Health and Safety**
  Occupational or Personal Safety – is concerned with the wellbeing of the individual in the workplace, primarily through the application of training and simple rules, procedures and protective measures. It doesn’t matter whether the workplace is an office, a manufacturing plant or an offshore platform. We often refer to this area of safety as the “management of slips, trips and falls”.

- **Process safety**
  Process Safety focuses on preventing fires, explosions and accidental releases of oil, gas and processes and facilities dealing with hazardous materials such as refineries, and oil and gas (onshore and offshore) production installations. Therefore process safety is very focused on maintaining containment. The term is used internationally, but there may be different words depending on industry and geographical location.

When it comes to the management of major accident risk, the oil, gas and petrochemical industry has certain special factors. The prevention of fires, explosions and accidental releases of hydrocarbons is clearly very important. However,
there are also other major risk factors present in offshore operations due to the special nature of the activities and its environment. These risk factors are typically associated with the weather, the sea conditions, the movement of materials and personnel and the lifting of heavy loads.

Product Safety
Product safety – product safety aims to ensure that any manufactured item or system is safe for its intended use. Design and manufacturing must therefore usually follow established rules and standards.

Functional safety
Functional Safety refers to the part of the overall safety that depends on a system or equipment operating correctly in response to its inputs. More specifically, the term is being used in relation to the application of the IEC 61508 Standard, covering the functional safety of electrical, electronic and programmable electronic safety-related systems. Even more specifically, in the context of the oil and gas industries, the term is referring to the application of IEC 61511, covering safety instrumented systems for the process industry sector. We are therefore referring to compliance with the safety standard that covers the specification, design, installation, testing and maintenance of safety instrumented systems that must reliably respond to plant conditions that may be hazardous and which must generate correct outputs to prevent or mitigate the consequences.

Human Factors and Safety Culture
Human error is involved in the majority of incidents and accidents. Even if not directly involved in the immediate incident, human error may well be present at some point in the event sequence – perhaps in the design, the manufacturing, or maintenance processes. The study of human factors and its relationship with safety processes, safety management and safety culture is therefore an important and wide ranging topic.

Hazard and Risk

In order to discuss functional safety management in more depth, we must first make sure we understand one or two fundamental definitions, Hazard and Risk

Hazards have the potential to cause us harm. This harm can occur through direct physical, injury - to us or others. It could also occur as an illness, either acute or chronic. Harm could also be caused indirectly, by damage to property, structure and machines, which in turn could then harm us.

Risk is the combination of the Severity of the harm and the Likelihood that that event might happen.

Severity is a measure of the degree or extent of the harm. This could range from a minor injury to a serious injury or even a fatality. In the extreme, the outcome of a major accident could result the loss of many lives, perhaps including innocent people who were not immediately involved in the activity or operation. The higher the severity, the more protective measures will be needed.

Likelihood tells us how frequently the event might happen. The higher the likelihood, the more protective measures will be needed.
Why safety system?

When the risk assessment concludes that existing risk reduction is not enough to reduce the risk to an acceptable level a Safety Instrumented System [SIS - 61511 terminologies] is very commonly used. This is popular because it is highly configurable and gives good risk reduction for the money.

What is the purpose of a safety system?

The purpose of a safety system is to reduce the risk and to keep the plant, people and business safe. The amount of risk reduction that an SIS can provide is represented by its Safety Integrity Level (SIL).

- SIL is defined as a range of Probability of Failure on Demand (PFD),
- Safe Failure Fraction (SFF) and
- Avoidance of Systematic failures which can be represented as the Systematic Capability for the each of the elements in the SIS.

What is a safety system?

A Safety Instrumented System (SIS) is a collection of sensors, controllers and actuators. It executes one or more Safety Instrumented Functions (SIFs) that are implemented for a common purpose.

The Safety Instrumented System (SIS) will together with other protection layers reduce the risk that a process may become hazardous to a tolerable level. The SIS does this by decreasing the frequency of unwanted accidents. SIS senses hazardous conditions and then takes action to move the process to a safer state, preventing an unwanted event from occurring.

So a safety system as we know it from oil & gas industry is in many cases a dormant system safeguarding the process control system. The control loop maintains a process variable within prescribed limits, while the SIS monitors a process variable and take action only when required.

The objective of IEC 61508 is to design a “safe safety system”

A safe safety system is tolerant to internal failure AND can execute the safety function OR it can’t carry out the safety function but it will notify operator via alarm.
Safety Lifecycle

The Analysis Phase - The safety lifecycle start at the concept phase and analyze the situation and document the safety requirements which gives an acceptable risk level

Design and Installation/Realization Phase - Then the requirements are translated into different risk reduction functions including a safety instrumented system with documented design, using appropriate hardware and software and design methods. The system must be evaluated and validated against the required integrity and functionality specification.

Operation and maintenance

Then the last phases are the Operation and maintenance. The operation and maintenance need to be done according to procedures, documenting the actual behavior of both the safety system and the plant demands for safety, to correct any deviation so that performance standards are maintained throughout the systems lifecycle.

Figure 3: SIS safety life-cycle phases and functional safety assessment stages (from IEC 61511)

In order to make sure we are doing the right things and also doing the things right; phase 9-11 go from concept phase to decommissioning.

The safety lifecycle is also a good way to ensure that all the organizations involved understand their role and responsibility and pass information and documentation between involved parties

How to know what we need?

Through the process hazard analysis most of the requirement for functionality and safety integrity is determined. This task is done by the end user / owner of the plant since the they understand the hazards of their process and they are experts on their own production process. There may be 3rd party experts or facilitators to join in the analysis phase. The
Objective of the Hazard and risk analysis is to identify the process hazards, estimate their risk (consequence/severity and likelihood) and decide if the risk is tolerable.

The result of the process hazard and risk assessment shall result in a verbal description of each safety loop/safety function to protect the plant including the following information. Each safety loop should protect for a specific hazard:

- A description of each identified hazardous event and the factors that contribute to it
- A description of the consequences and likelihood of the event
- Considerations of conditions and modes
- The determination of requirements for additional risk reduction
- A description of the measures taken to reduce or remove hazards and risk.
- Allocation of the safety functions to layer of protection
- Identification of those Safety functions applied as safety instrumented function

**Safety Requirement Specification (SRS)**

The result of the hazard and risk assessment is the input to the Safety Requirement Specification.

Definition of Safety Requirement Specification is defined in IEC 61511 – part 1, 3.2.78

“Specification that contains all the requirements of the safety instrumented functions that have to be performed by the safety instrumented systems”

The Objective of the Safety Requirement Specification is to specify all requirements of Safety Instrumented System (SIS) needed for detailed engineering and process safety information purposes. The requirement is grouped into functional and integrity requirement.

**The Functional Requirements** is a description of what the Safety Instrumented Function (SIF) shall do.

**The Integrity Requirements** is how well the SIF shall work – the level of confidence. How reliable the SIF must perform its duty.

Under is a list of some of the important functional requirements of the SRS. The complete list is found in IEC 61511 – part 1, Clause 10

- Description of the SIF
- Definition of the safe state
- Process inputs and their trip points
- Process parameters normal operating range
- Process outputs and their actions
- Relationship between inputs and outputs
- Selection of energize-to-trip and reenergize-to-trip
- Response time requirement
- Operator interface requirement
- Considerations for manual shutdown, and
- Considerations for bypass and override
• Action on loss of power to the SIS
• Response time requirements for the SIS to bring the process to a safe state
• Reset functions
The SRS should also contain these **integrity requirements**

• The required SIL for each SIF
• Requirements for diagnostics to achieve the required SIL Requirement for maintenance and testing to achieve the required SIL
• Reliability requirements if spurious trips may be hazardous

**Responsibilities**

The owner of the plant is responsible for safety, irrespectively who has done the design of the safety system. The owner need to make sure the different vendors follow the regulations and the chosen architecture and selected components meets the requirement.

The end-user often doesn’t have capabilities to verify all products used for the safety functions. By using certifies product according to IEC 61508 that means that a 3rd party (often TUV) has verified that the product comply to standard. A certified product addresses Electrical safety, environmental safety, EMC, User documentation and reliability analysis additional to functional safety according to IEC 61508.

**Documentation**

Since we work in lifecycle phases and we need to pass on information between different engineering disciplines it is important with documentation. Also the traceability and the need to always have up to date information / version control is important. Anything that can be stored and which can be properly identified can be used as documentation.

Typical documentations which are central for safety

• Hazop reports
• Safety Requirement Specification
• Functional Design Specification/Safety Analysis Report
• Safety plan/Safety Lifecycle Management Plan
• Test documents (Specifications & Records)
• Competence (Role descriptions & Competence requirements for each role)
• SIL Compliance report / SIL verification report

**Competence requirement and roles in a safety project**

The competence of people involved in safety projects is normative according to IEC 61511 (part 1, Clause 5.2.) In the planning phase of the safety system it is required to identify the competence needed, what is available in-house and what needs to be added.

There is a need for role descriptions and competence requirements for each role including requirement for education, training or experience. Competency is especially required with regards to functional safety and the technology used.
According to IEC 61511, a minimum, the following items should be addressed when considering the competence of persons, departments, organizations or other units involved in safety life-cycle activities:

- engineering knowledge,
- training
- experience appropriate to the process application

Example of roles in a project with are:

- Project Manager,
- Safety Lead Engineer/Functional Safety Manager
- Safety Engineers
- Safety Assessor

Even though the Project Manager does not always work with technical issues it is important that the management have an understanding for Functional Safety Management.

**Conclusion – Functional Safety**

To keep the plant safe it is not enough to use reliable hardware.

We need to look at

- What is the risk? And how can it be reduced?
- How to avoid failures?
- The entire lifecycle to be considered
- Work processes need to be established for each phase in the lifecycle

Importance of Competence should not be ignored

**SIL is applicable for a function not for a component alone**

**References**


WIN – WIN a MANAGERS GUIDE to FUNCTIONAL SAFETY, Curt Miller

IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems

IEC 61511Functional safety – Safety instrumented systems for the process industry sector