Management of functional safety
Guideline

Comments on this report are gratefully received by
Johan Hedberg
at SP Swedish National Testing and Research Institute
mailto:johan.hedberg@sp.se

Summary

This report is focusing on those parts of IEC 61511 that contain requirements on management of functional safety.

This report is one of the results of the research project SafeProd supported by VINNOVA (Swedish Agency for Innovation Systems). More information about the project could be found at www.sp.se/safeprod.

TABLE OF CONTENTS

1 Introduction

1.1 Purpose

This aim of this report is to be a support during the management of functional safety and give guidelines on management of functional safety in IEC 61511.

This report is only a guideline. In order to fulfil the requirements related to management of functional safety IEC 61511 must be used.

This report is one of the results of the research project SafeProd supported by VINNOVA (Swedish Agency for Innovation Systems). More information about the project could be found at www.sp.se/safeprod.

1.2 References

[1] IEC 61511-1 Functional safety- Safety instrumented systems for the process industry sector, Part 1: Framework, definitions, system, hardware and software requirements

[2] IEC 61511-2 Functional safety- Safety instrumented systems for the process industry sector- Part 2: Guidelines for the application of IEC 61511-1

[3] IEC 61511-3 Functional safety- Safety instrumented systems for the process industry sector- Part 3: Guidance for the determination of the required safety integrity level

[4] IEC 62061 Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems

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

1.3 Scope

This document gives guidelines on how to apply those parts in [1] that relates to management of functional safety.

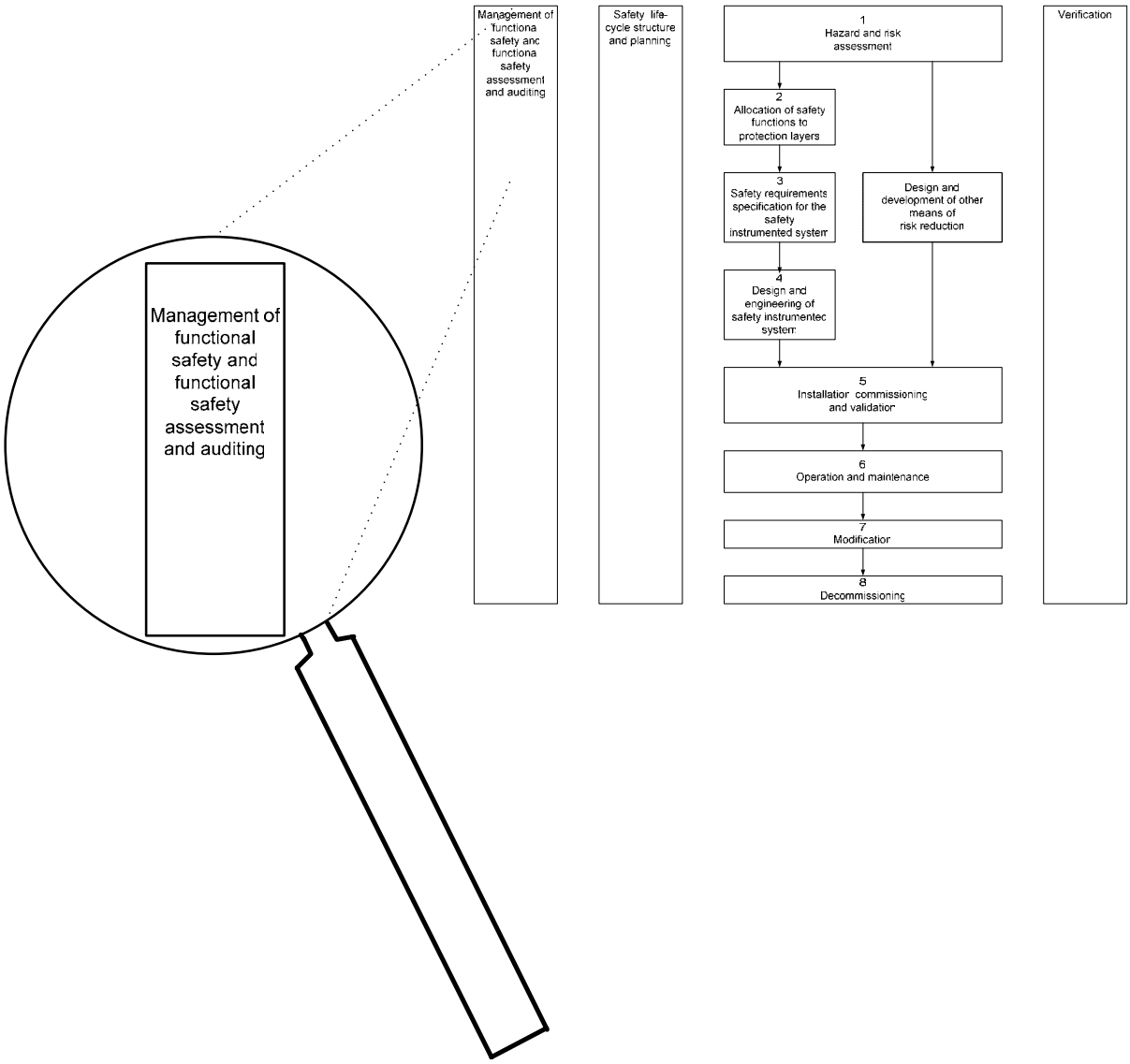


Figure 1. “Management of functional safety and functional safety assessment and auditing” life-cycle phase in [1]

The management of functional safety and functional safety assessment and auditing is one of the most central parts of the safety life cycle according to [1]. See figure 1.

1.4 Audience

Persons involved in design and engineering of safety instrumented systems.

2 Definitions and abbreviations

basic process control system (BPCS)
system which responds to input signals from the process, its associated equipment, other programmable systems and/or an operator and generates output signals causing the process and its associated equipment to operate in the desired manner but which does not perform any safety instrumented functions with a claimed SIL ≥ 1 (3.2.3 in [1])

component
one of the parts of a system, subsystem, or device performing a specific function (3.2.7 in [1])

continuous mode safety instrumented function
where in the event of a dangerous failure of the safety instrumented function a potential hazard will occur without further failure unless action is taken to prevent it (3.2.43.2 in [1])

demand mode safety instrumented function
where a specified action (for example, closing of a valve) is taken in response to process conditions or other demands. In the event of a dangerous failure of the safety instrumented function a potential hazard only occurs in the event of a failure in the process or the BPCS. (3.2.43.1 in [1])

device
functional unit of hardware or software, or both, capable of accomplishing a specified purpose (for example, field devices; equipment connected to the field side of the SIS I/O terminals; such equipment includes field wiring, sensors, final elements, logic solvers, and those operator interface devices hard-wired to SIS I/O terminals) (3.2.14 in [1])

diagnostic coverage (DC)
ratio of the detected failure rate to the total failure rate of the component or subsystem as detected by diagnostic tests. Diagnostic coverage does not include any faults detected by proof tests. (3.2.15 in [1])

final element
part of a safety instrumented system which implements the physical action necessary to achieve a safe state (3.2.24 in [1])

hardware safety integrity
part of the safety integrity of the safety instrumented function relating to random hardware failures in a dangerous mode of failure (3.2.29 in [1])

instrument

apparatus used in performing an action (typically found in instrumented systems) (3.2.38 in [1]) (3.2.72 in [1]).

logic solver
that portion of either a BPCS or SIS that performs one or more logic function(s) (3.2.40 in [1])

mode of operation
way in which a safety instrumented function operates (3.2.43 in [1])

module
self-contained assembly of hardware components that performs a specific hardware function (i.e., digital input module, analogue output module), or reusable application program (can be portion of a computer program that carries out a specific function (3.2.44 in [1])

non-programmable system
system based on non-computer technologies (i.e., a system not based on programmable electronics [PE] or software) (3.2.47 in [1])

programmable electronics
electronic component or device forming part of a PES and based on computer technology. The term encompasses both hardware and software and input and output units (3.2.55 in [1])

proof test
test performed to reveal undetected faults in a safety instrumented system so that, if necessary, the system can be restored to its designed functionality (3.2.58 in [1])

proven-in-use
when a documented assessment has shown that there is appropriate evidence, based on the previous use of the component, that the component is suitable for use in a safety instrumented system (3.2.60 in [1])

random hardware failure
failure, occurring at a random time, which results from a variety of degradation mechanisms in the hardware (3.2.62 in [1])

redundancy
use of multiple elements or systems to perform the same function; redundancy can be implemented by identical elements (identical redundancy) or by diverse elements (diverse redundancy) (3.2.63 in [1])

safe failure fraction
fraction of the overall random hardware failure rate of a device that results in either a safe failure or a detected dangerous failure (3.2.65.1 in [1])

safety configured logic solver

general purpose industrial grade PE logic solver which is specifically configured for use in safety applications in accordance with chapter 11.5 in [1] (3.2.40.1 in [1])

safety instrumented function (SIF)
safety function with a specified safety integrity level which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function (3.2.71 in [1])

safety instrumented system (SIS)
instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensor (s), logic solver (s), and final element (s) (3.2.72 in [1])

safety integrity level
discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems. Safety integrity level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest (3.2.74 in [1])

sensor
device or combination of devices, which measure the process condition (for example, transmitters, transducers, process switches, position switches) (3.2.80 in [1])

system
set of elements, which interact according to a design; an element of a system can be another system, called a subsystem, which may be a controlling system or a controlled system and may include hardware, software and human interaction (3.2.84 in [1])

target failure measure
intended probability of dangerous mode failures to be achieved in respect of the safety integrity requirements, specified in terms of either the average probability of failure to perform the design function on demand (for a demand mode of operation) or the frequency of a dangerous failure to perform the SIF per hour (for a continuous mode of operation) (3.2.87 in [1])

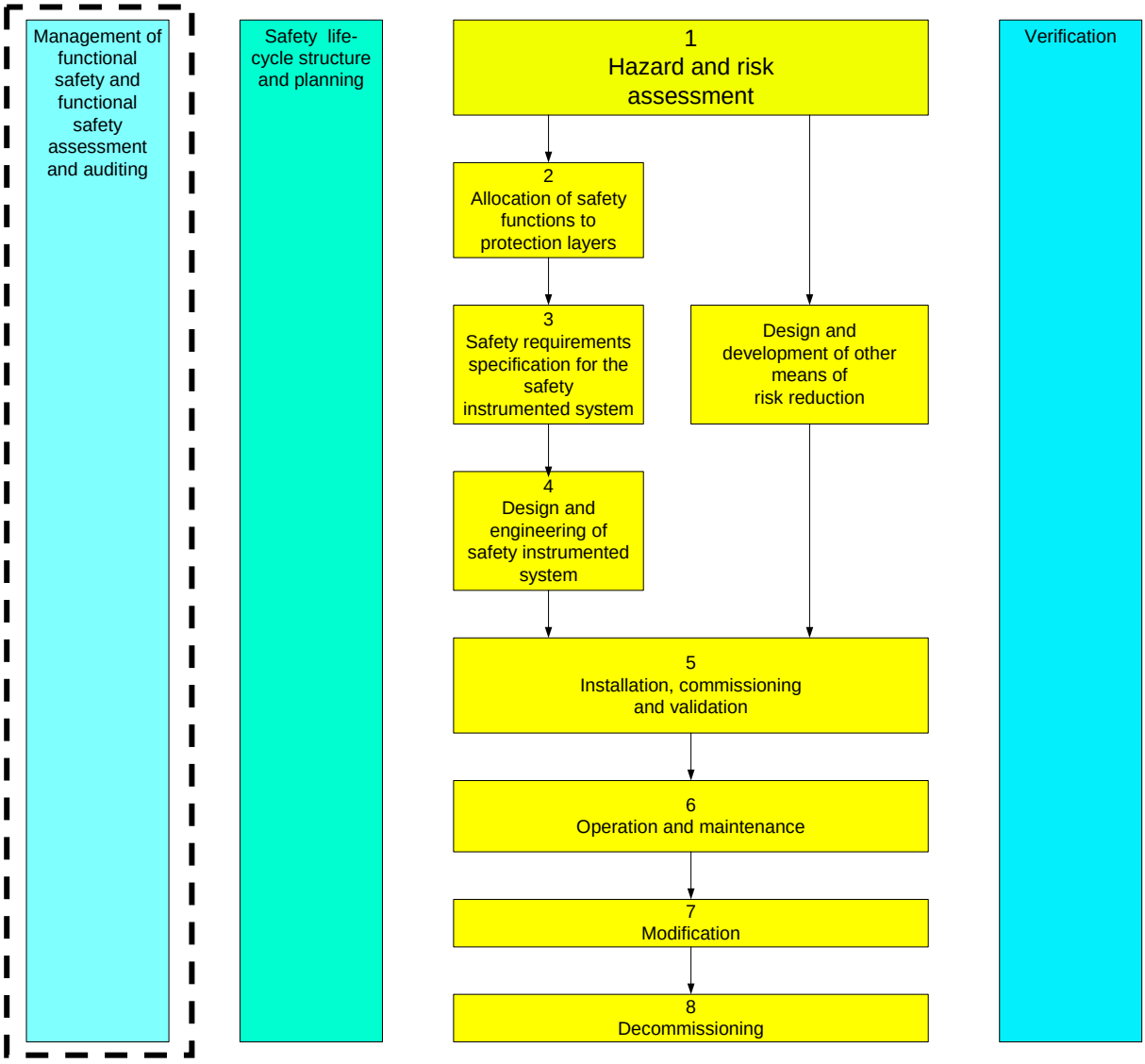
undetected/unrevealed/covert
in relation to hardware and software faults not found by the diagnostic tests or during normal operation (3.2.90 in [1])

Abbreviations:

CCF	Common Cause Failure
FMEDA	Failure Mode Effects and Diagnostic Analysis
PFD	Probability of Failure on Demand
SFF	Safe Failure Fraction
SIL	Safety Integrity Level
SIF	Safety Instrumented Function
SIS	Safety Instrumented System

3 Management of functional safety

Management of functional safety is one of the most important safety life cycles in [1], because if it the management is not handled correctly it will negatively influence all main life cycles (yellow marked in the below figure) in the overall safety lifecycle.



In [1] the requirements related to management of functional safety have been divided into the following categories:

- General requirements
- Organization and resources
- Risk evaluation, risk management and planning of the safety

- Implementing and monitoring
- Functional safety assessment
- Auditing and revision
- SIS configuration management

3.1 General requirements

- Strategies shall be developed, aiming on how to fulfil the safety requirements. The requirements in these strategies must be clear enough to make it possible to verify these at a later stage in the design
- These strategies must be communicated to all influenced persons at the company
- A safety management must be in place before start of design to guarantee that the design of the SIS/SIF is made in a correct way

3.2 Organization and resources

- Persons, departments and organizations responsible for the different safety life cycles shall be identified
- Organizations responsible for review/assessment of the different safety life cycles shall be identified
- Important to check that persons involved in the different safety life cycles have got correct competence for their assigned work, for instance:

- engineering knowledge about the process
- engineering knowledge about use of safety systems
- knowledge about different safety analysis methods
- requirements from the authorities

3.3 Risk evaluation, risk management and planning of the safety

- Hazard shall be listed and hazardous events shall be identified. The need for risk reduction shall be investigated for each hazardous event by estimating its consequence and frequency (more information about hazard and risk analysis could be found in chapter 8 in [1]
- The hazard and risk analysis shall consider both risks related to personal safety and environment. In some situations it could also be important to consider economical risks
- Risk management is an iterative process that must be updated continuously when the design is changed

3.4 Implementing and monitoring

- Procedures shall be implemented to support follow-ups and modifications when faults are detected in any safety life cycle, for instance during:
- Hazard and risk analysis
- Review of independent third party
- Verification and validation activities
- Incidents and accidents that occurs after the SIS is installed
- Organizations responsible for any safety life cycle shall only use sub suppliers that have got quality management systems
- Procedures shall be developed to check that the final safety system is in accordance with the original requirements put on it

3.5 Functional safety assessment

- A procedure for functional safety shall be defined and applied. This procedure is necessary to define to be able to handle these requirements in an efficient way
- A certain group responsible for functional safety assessment shall be defined. It is important that this group has got knowledge about both the present process application but also the used technology (including used safety systems)
- This group shall at least consist of one person with long experience in the specific area which has not been involved in the project
- Below follows some examples on aspects to be taken into consideration when planning to perform a functional safety assessment
- scope of the functional safety assessment
- knowledge areas that must be covered by the persons that shall participate
- how to present the result of the functional safety assessment
- summary of which authorities that participate in the functional safety assessment
- the independence of the group
- The safety procedure defined shall describe at which points in the safety life cycle a functional safety assessment shall be performed
- In some situation it could be necessary to perform additional functional safety assessments after the SIS is commissioned, for instance
- when new hazards and hazardous events are identified
- after modifications
- The scope of the functional safety assessment is based on:
- the total size of the project
- complexity
- defined safety integrity level
- total project time
- Potential hazardous events that could occurif an accident occurs
- To which degree the used design principles has been used in earlier projects
- Requirements from the authorities

- Figure 8 in [1] gives examples on stages in the overall safety life cycle when it is suitable to perform a functional safety assessment
- If functional safety assessment is not performed at those stages described in Figure 8 in [1] it shall as a minimum be performed before the hazards are being present and this functional safety assessment shall at least consider those aspects described in chapter 5.2.6.1.4 in [1]
- Also tools used during the development and production of the safety instrumented system shall be considered by the group working with functional safety, for more information see chapter 5.2.6.1.5 in [1]
- The result of the functional safety assessment with all its comments shall be available when necessary
- The group responsible for the functional safety assessment shall, when needed, have access to all relevant information/documentation related to the design of the safety related system

3.6 Auditing and revision

- Procedures shall be developed that describes in which way audits are used. This shall for instance describe:
- how often audits are performed
- independence between those persons performing the audits and those persons performing the design of the safety instrumented system
- how these audits are documented and which kind of follow-up activities that will be performed if some kind of problem is identified

- A management system that handles modifications shall be developed and it shall at least cover the following aspects:
- how to initiate that you want to perform a change
- how to perform the change
- how to approve the change

3.7 SIS configuration management

- Procedures related to configuration management shall be developed, where for instance the following aspects shall be specified
- at which phase ,in the overall safety life cycle, formal configuration checking shall be implemented
- Procedures to uniquely identify all includedparts in a component (both hardware and software)
- How to detect non-original components during services and how to avoid that these components will be re-used