Functional Safety Management to DIN EN IEC 61511

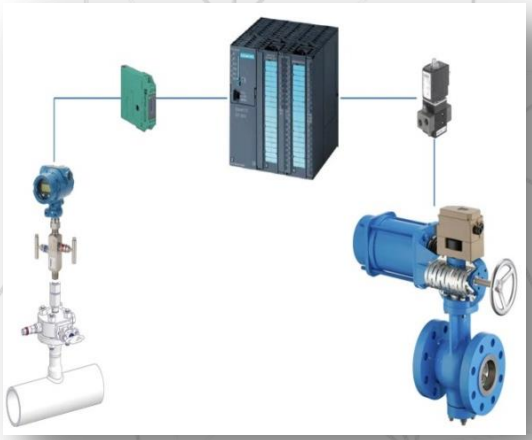
Contents

1. What is Functional Safety?

- Definition acc. to **61508-4**: „Part of the overall safety relating to the EUC and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities.“

  EUC = Equipment under Control

  E/E/PE = electric/electronic/programmable electronic



- Functional Safety is the risk reduction obtained from functions that are designed and implemented to maintain safe operation of a process.

  „The correct function of a protection system including sensors and final elements.“

- Functional Safety does not include: fire protection, explosion protection, workplace safety, inherent safety.

1. What is Functional Safety?

Extract from IEC 61511-1

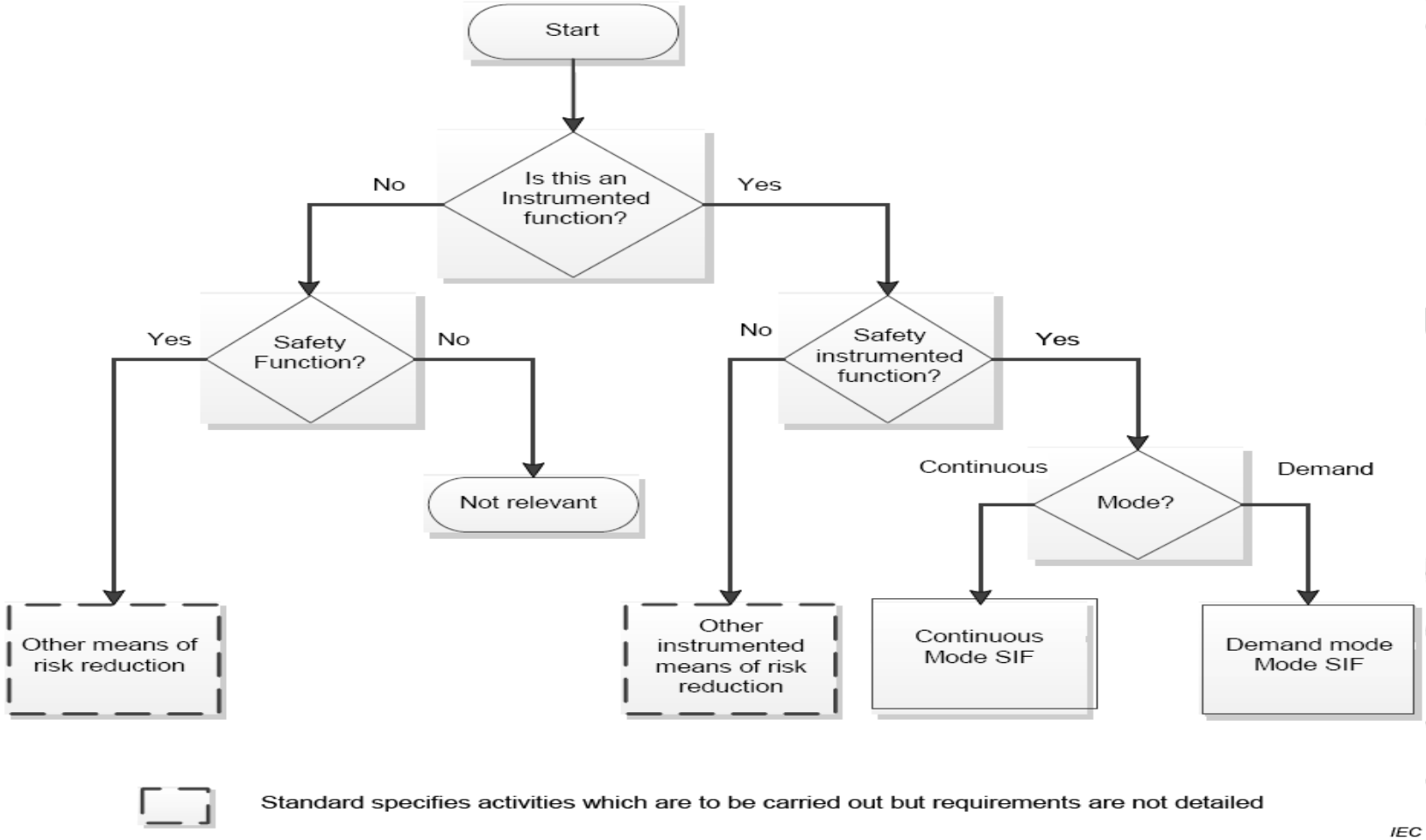
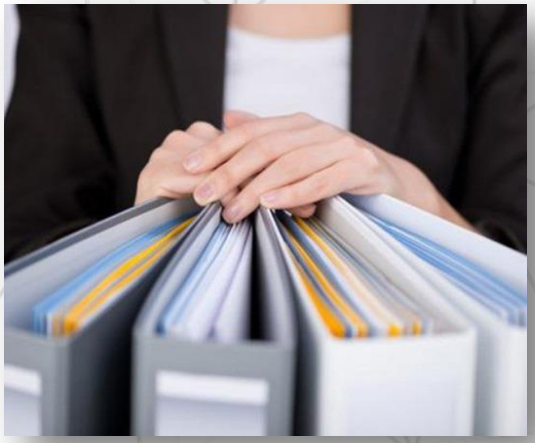


Figure 4 – Relationship between safety instrumented functions and other functions

2. Legal Framework

- EU-Safety Laws (z. B. SEVESO III, Machinery Directive) → National Laws → Regulations → generally recognised Best Engineering Practice (e.g. Standards) = Code Hierarchy

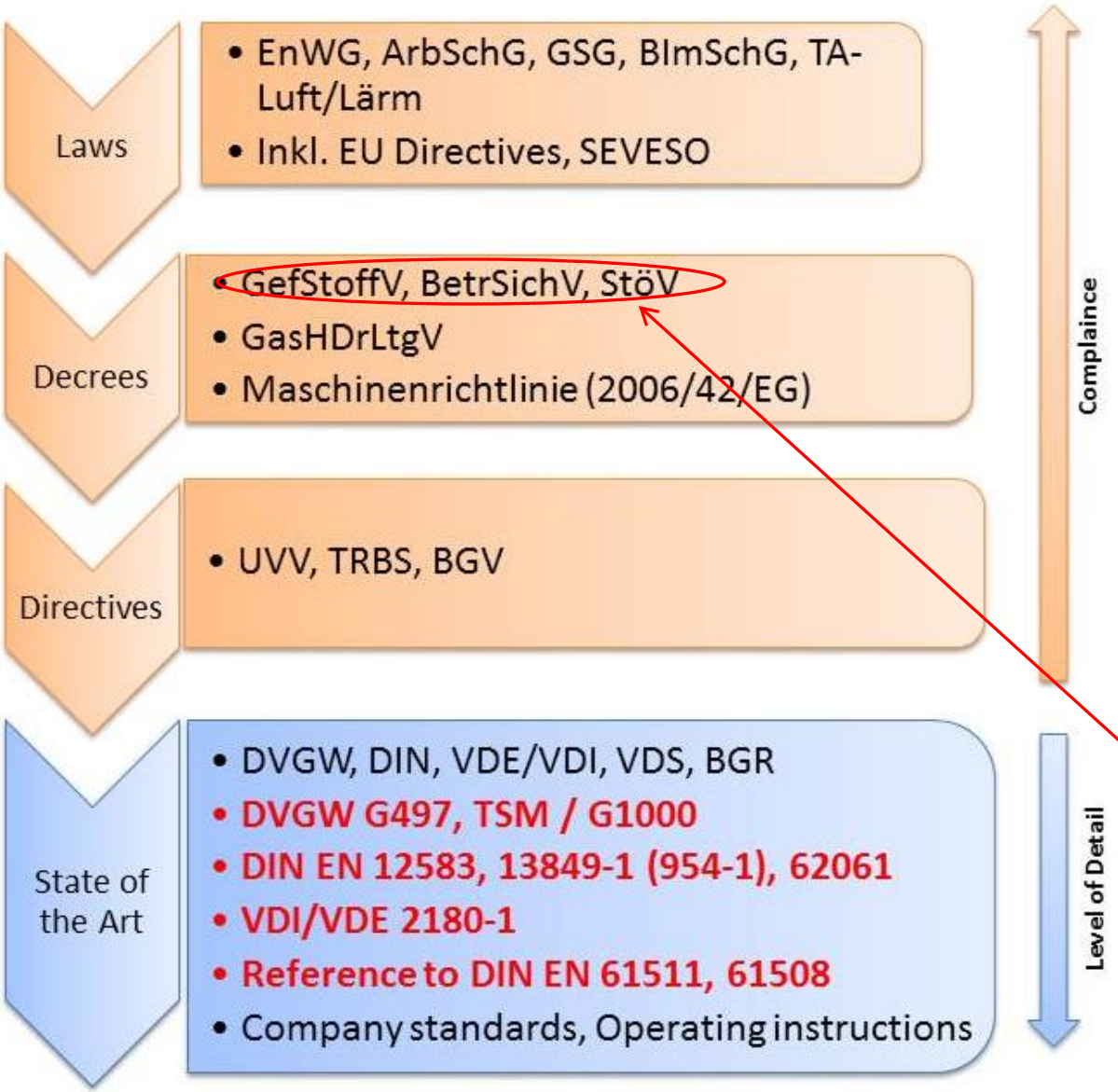


- Product Safety Act (ProdSV) for Manufacturers, resp. Working Conditions Act (ArbSchG) for End Users requires that Hazards have to be reduced to an acceptable minimum.

- According to ProdSV, a Hazard Analysis has to be carried out. The corresponding requirement acc. BetrSichV. is a Safety Assessment.

- Different safety-relevant codes are applied depending on Equipment or Plant type.

2. Legal Framework - typ. Gas Plant, Germany

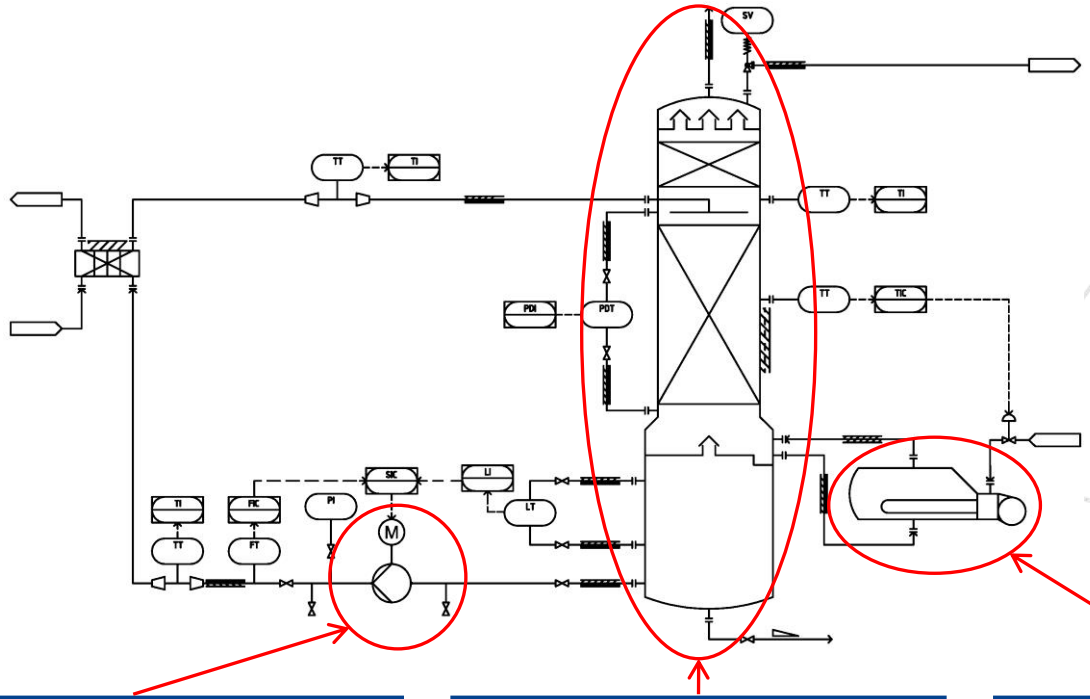


German legislation states that energy plants must be constructed and operated in such a way as to ensure technical safety.

Compliance with the generally accepted 'state of the art' is presumed if the DVGW technical rules have been complied with (§ 49 Abs. 2 EnWG, GasHdrLtgV §2 (2).

UK: COMAH 2015
US: OSHA CFR1910

2. Legal Framework

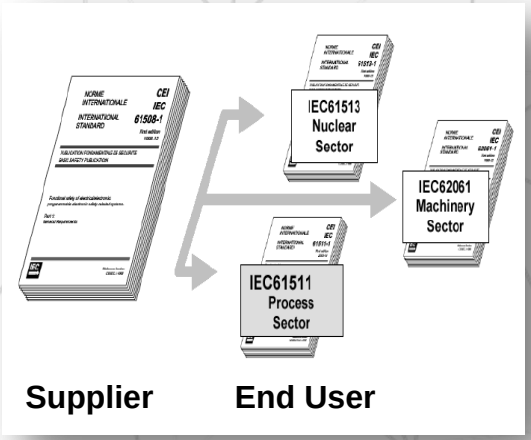


Machinery		Process	Fired Equipment
Machinery Directive 2006/42/EG		SEVESO III Directive12/18/EG (StöV, 12. BImSchV)	Pressure Equipment Directive 2014/68/EG
DIN EN 12100		Safety Case StöV 9	DIN EN 12952, 12953
DIN EN ISO 14121			DIN EN 230, 267, 298, 746
DIN EN 62061	DIN EN 13849	DIN EN 61511 (VDI/VDE 2180)	DIN EN 50156

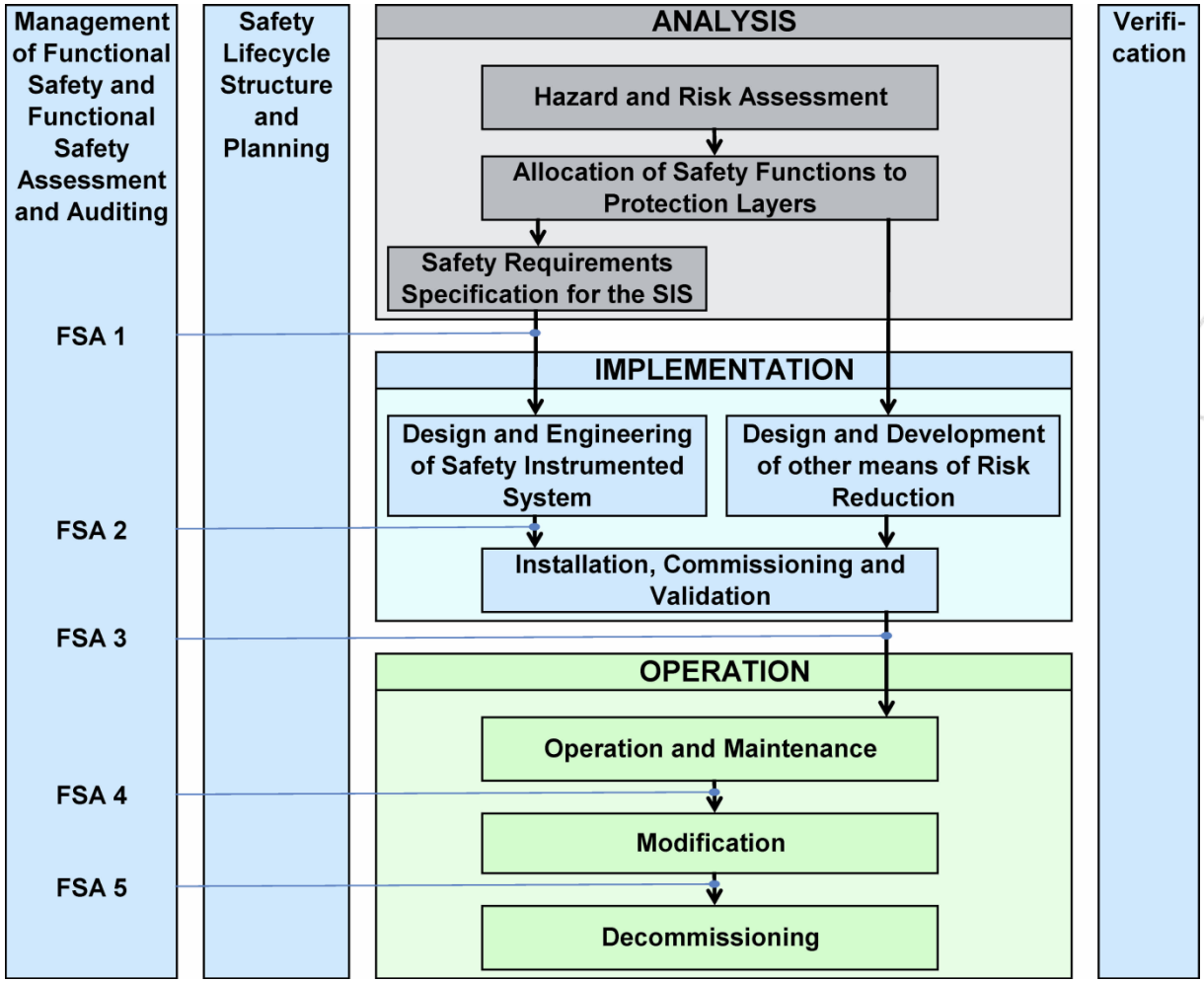
Functional Safety
Best Practice (RAGAGEP)

3. Safety Analysis – Responsibilities

- Hazard and Risk Analysis
  - Responsibility with Manufacturer/Installer
  - Analyses Hazards and their minimisation to an acceptable level for equipment/components
  - Basis of Safety Plan
  - Requirement of ProdSV (e.g. Machinery Dir., EN ISO 12100, DGRL, IEC 62061, VDMA 4315)
- Risk Assessment
  - End User is responsible for preparation/update during SLC
  - Assesses the Hazards during operation of the plant (functional)
  - Development of Safety Plan
  - Requirement of BetrSichV, ArbSchG, GefStofV
- Generally Accepted Best Practice
  - Safety-related systems have to be maintained according to Best Engineering Practice (e.g.12. BImschV (StörfallV), § 3)
  - In the case of an incident, the burden of proof to demonstrate compliance with BEP lies with the End User.
  - BEP for Functional Safety is given in DIN EN IEC 61508 and the derived sector standard (e.g. 61511)



4. SIS Safety Life Cycle acc. DIN EN IEC 61511-1

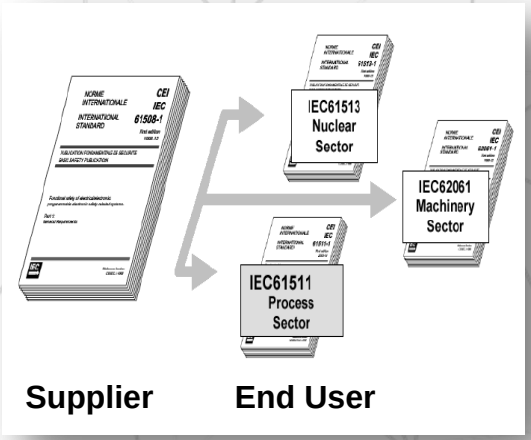


Suppliers and End Users shall have a Functional Safety Management System in place.

This shall be aligned to the Safety Life Cycle.

5. Status of the Norms

Functional safety – Safety instrumented systems for the process industry sector



- IEC 61511-1 Edition 2.0 2016-02
  - Part 1: Framework, definitions, system, hardware and application programming requirements
  - IEC 61511-1 Edition 2.1 2017-08 Amendment
- IEC 61511-2 Edition 2.0 2016-07
  - Part 2: Guidelines for the application of IEC 61511-1: 2016
- IEC 61511-3 Edition 2.0 2016-07
  - Part 3: Guidance for the determination of the required safety integrity levels

- German language adoption of the Norm through DKE/GK 914 (New Revision 02/2019!)
- Replaces: DIN EN 61511-1(VDE 0810):2005, Corrections2012-10 und 2017-11
- VDI/VDE 2180-1, 2, 3 was published in Feb. 2018

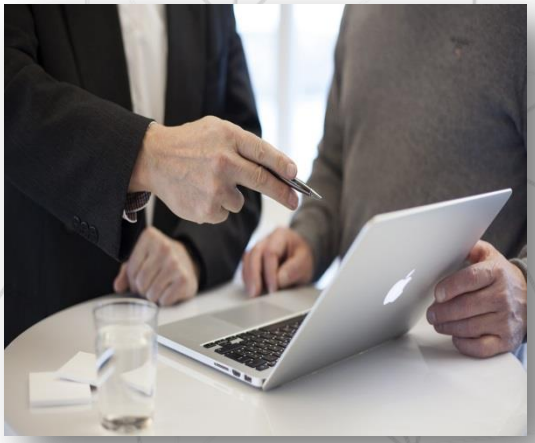
6. Changes in IEC 61511-1: 2016

- Requirements for the FSMS

  § 5.2.5.2

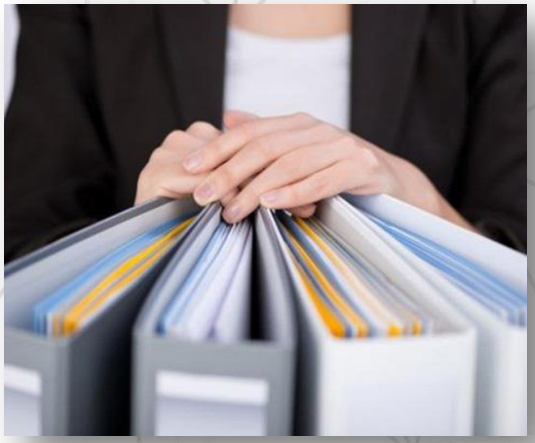
  – *If a supplier makes any functional safety claims for a product or service, which are used by the organization to demonstrate compliance with the requirements of this part of IEC 61511, the supplier shall have a functional safety management system. Procedures shall be in place to demonstrate the adequacy of the functional safety management system.*

  – *The functional safety management system shall meet the requirements of the basic safety standard IEC 61508-1:2010, Clause 6, or the functional safety management requirements of the standard derived from IEC 61508 to which functional safety claims are made.*



6. Changes in IEC 61511-1: 2016

- Requirements for Competency



§ 5.2.2.2

– *The following items shall be addressed and documented when considering the competence of persons, departments, organizations or other units involved in SIS safety life-cycle activities.*

– *a)..i)*

§ 5.2.2.3

– *A procedure shall be in place to manage competence of all those involved in the SIS life cycle. Periodic assessments shall be carried out to document the competence of individuals against the activities they are performing and on change of an individual within a role.*

6. Changes in IEC 61511-1: 2016

- Functional Safety Assessments (FSA)

§ 5.2.6.1.4

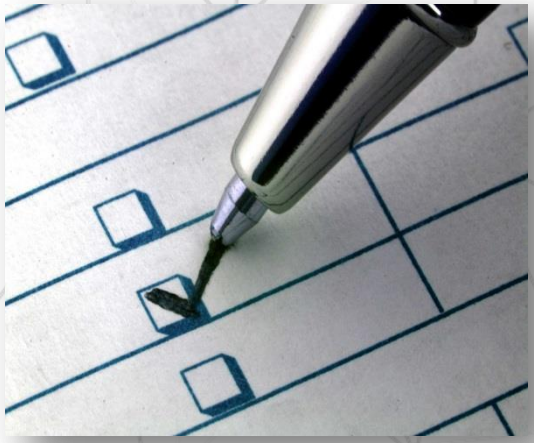
– *A FSA team shall review the work carried out on all phases of the safety life cycle prior to the stage covered by the assessment that have not been already covered by previous FSAs. If previous FSAs have been carried out then the FSA team shall consider the conclusions and recommendations of the previous assessments.*

§ 5.2.6.2.5

– *Management of change procedures shall be in place that identifies changes that will affect the requirements on the SIS (e.g., re-design of a BPCS, changes to manning in a certain area).*

6. Changes in IEC 61511-1: 2016

- Functional Safety Audit



§ 5.2.6.2

– *5.2.6.2.1 The purpose of the audit is to review information documents and records to determine whether the functional safety management system (FSMS) is in place, up to date, and being followed. Where gaps are identified, recommendations for improvements are made.*

– *5.2.6.2.2 All procedures identified as necessary resulting from all safety life-cycle activities shall be subject to safety audit.*

– *5.2.6.2.3 Functional safety audit shall be performed by an independent person not undertaking work on the SIS to be audited.*

6. Changes in IEC 61511-1: 2016

- Management of Change

§ 5.2.6.2.4

– *Management of change procedures shall be in place to initiate, document, review, implement and approve changes to the SIS other than replacement in kind (i.e., like for like, an exact duplicate of an element or an approved substitution that does not require modification to the SIS as installed).*

§ 5.2.6.2.5

– *Management of change procedures shall be in place that identifies changes that will affect the requirements on the SIS (e.g., re-design of a BPCS, changes to manning in a certain area).*

6. Changes in IEC 61511-1: 2016

- Security Risk Assessment

§ 8.2.4

– *A security risk assessment shall be carried out to identify the security vulnerabilities of the SIS.*

…

– *NOTE 1 Guidance related to SIS security is provided in ISA TR84.00.09, ISO/IEC 27001:2013, and IEC 62443-2-1:2010.*

– *NOTE 2 The information and control of boundary conditions needed for the security risk assessment are typically with owner/operating company of a facility, not with the supplier. Where this is the case, the obligation to comply with 8.2.4 can be with the owner/operating company of the facility.*

– *NOTE 3 The SIS security risk assessment can be included in an overall process automation security risk assessment.*

– *NOTE 4 The SIS security risk assessment can range in focus from an individual SIF to all SISs within a company.*

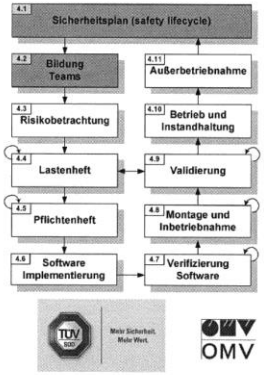
7. FSMS Key Requirements

- Preparation of a FSMP for the entire Safety Life Cycle
- Definition of Roles and Responsibilities (Matrix)
- Description how Functional Safety will be implemented
- Development of corresponding Procedures or cross-reference to existing Procedures
- Personal Competencies and Evaluation
- Planning of Functional Safety Assessments and Audits
- SIS Design Activities (Hard-und Software)
- Steps/Procedure for Verification und Validation of SIS Design
- Measurement of Performance (KPIs)
- Management of Change (MOC)
- Documentation requirements (dependent on SLC Phase)

8. What should be included in a FSMP?

- The 61511 Standard does not prescribe the format of a FSMP, however refers to 61508-1, § 6.
- 61508-1, Annex A gives an example of a documentation structure (complete documentation for SLC).
- PSC-Recommendation:
  - Basis IEC 61511-1: 2016
  - Overview document (FSMP) with reference to each SLC-phase
  - Cross-reference to existing company QM-Procedures (ISO-9001), or new procedures (to be prepared acc. to „Gap-Analysis“)
  - Define requirements for Qualifications and Competencies
  - Requirements for Documentation
  - Matrix of Responsibilities as per SLC
  - To be considered for applications in German-speaking countries: cross-reference to DIN EN 61511, VDI/VDE 2180

FSMP – Praxis Beispiel



8. Example FSMP for a Service Provider

TABLE OF CONTENTS

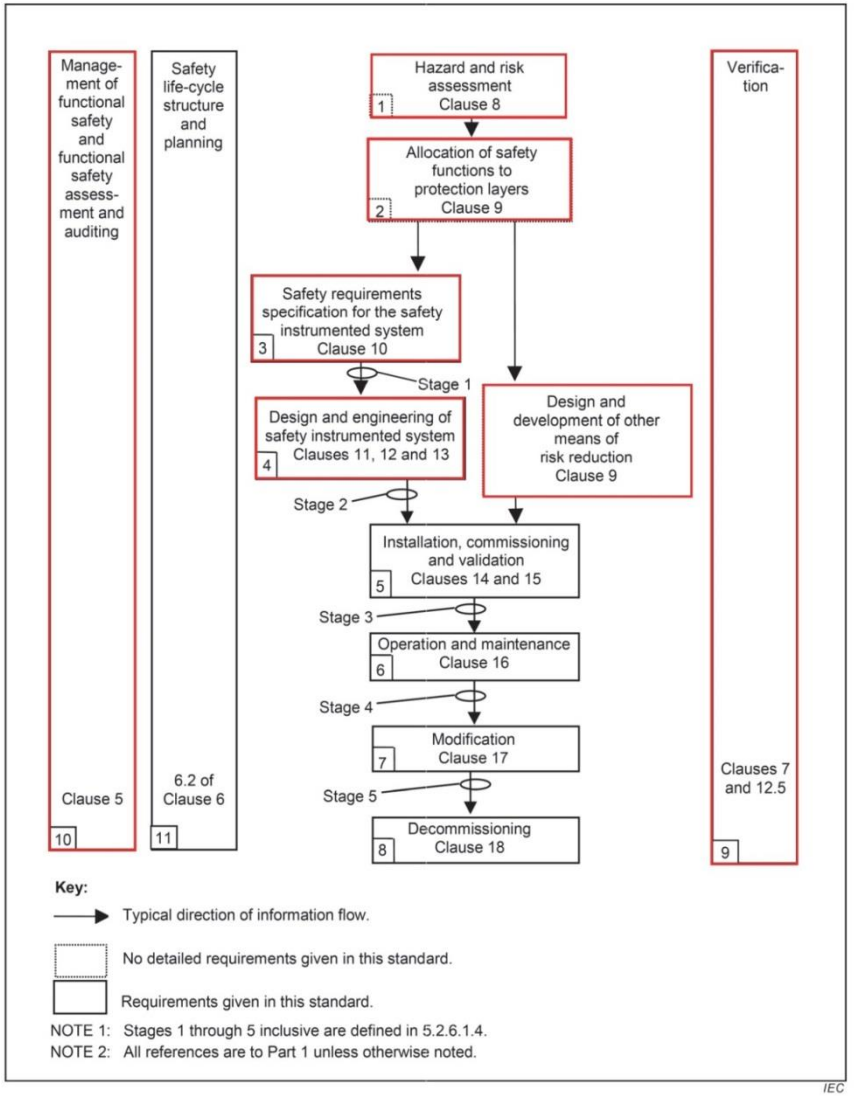


Figure 7 – SIS safety life-cycle phases and FSA stages

8. Example FSMP for a Service Provider – Responsibility Matrix

Safety life-cycle phase or activity		Objectives	Requirements Clause	Inputs	Outputs	Typical PSC Project-Specific Deliverables	Responsibility (R=Responsible, I= Input)					
Figure 7 box #	Title						OEM	Opera-tor	Desig-ner	Integra-tor	Contr-actor	PSC [1]
1	H&RA	To determine the hazards and hazardous events of the process and associated equipment, the sequence of events leading to the hazardous event, the process risks associated with the hazardous event, the requirements for risk reduction and the safety functions required to achieve the necessary risk reduction	Clause 8	Process design, layout, manning arrangements, safety targets	A description of the hazards, of the required safety function(s) and of the associated risk reduction	HAZOP/LOPA Methodology HAZOP/LOPA Report HAZOP/LOPA Close-Out List	I	I	I	-	-	R
2	Allocation of safety functions to protection layers	Allocation of safety functions to protection layers and for each SIF, the associated SIL	Clause 9	A description of the required SIF and associated safety integrity requirements	Description of allocation of safety requirements	SIL Methodology SIL Report	I	I	I	-	-	R
3	SIS safety requirements specification	To specify the requirements for each SIS, in terms of the required SIF and their associated safety integrity, in order to achieve the required functional safety	Clause 10	Description of allocation of safety requirements	SIS safety requirements; application program safety requirements	Safety Requirements Specification (incl. datasheet for each SIF) SRS updates during SLC	-	I	I	-	-	R
4	SIS design and engineering	To design the SIS to meet the requirements for SIF and their associated safety integrity	Clauses 11, 12, 13	SIS safety requirements Application program safety requirements	Design of the SIS hardware and application program in conformance with the SIS safety requirements; planning for the SIS integration test (FAT)	Detailed design documents (depending on scope of work) Engineering Management Plan (proj. specific) Management of Change Procedure (proj. specific)	R	I	R	R	R	I
5	SIS installation commissioning and validation	To integrate and test the SIS To validate that the SIS meets in all respects the requirements for safety in terms of the required SIF and their associated safety integrity	Clauses 14, 15	SIS design SIS integration test plan SIS safety requirements Plan for the safety validation of the SIS	Fully functioning SIS in conformance with the SIS safety requirements (SAT) Results of SIS integration tests Results of the installation, commissioning and validation activities	Inspection / Test Reports	R	I	I	R	R	I
6	SIS operation and maintenance	To ensure that the functional safety of the SIS is maintained during operation and maintenance	Clause 16	SIS safety requirements SIS design Plan for SIS operation and maintenance	Results of the operation and maintenance activities	Inspection / Test Reports Procedures (e.g. proof test)	-	R	-	-	-	I
7	SIS modification	To make corrections, enhancements or adaptations to the SIS, ensuring that the required SIL is achieved and maintained	Clause 17	Revised SIS safety requirements	Results of SIS modification	Inspection / Test Reports Verification Report	-	R	-	-	-	I
8	Decommissioning	To ensure proper review, sector organization, and ensure SIF remains appropriate	Clause 18	As built safety requirements and process information	SIF placed out of service		-	R	-	-	-	I
9	SIS verification	To test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase	Clause 7, 12.5	Plan for the verification of the SIS for each phase	Results of the verification of the SIS for each phase	Verification Procedure / Checklist Verification / Compliance Report	-	I	-	-	-	R
10	SIS FSA	To investigate and arrive at a judgement on the functional safety achieved by the SIS	Clause 5	Planning for SIS FSA SIS safety requirement	Results of SIS FSA	FSA Procedure / Checklist FSA Report	-	I	-	-	-	R
11	Safety lifecycle structure and planning	To establish how the lifecycle steps are accomplished	Clause 6.2	Not applicable	Safety plan	PSC's FSMP	-	R	-	-	-	I

9. Setup of a FSMS – Way Forward

1. Gap Analysis acc. IEC 61508/61511 Checklists

- Desk-top-Review of existing FSM-, QM-Procedures
- Compliance-Review and Interviews acc. to Checklist at Company premises
- Report, Presentation/Discussion of Recommendations

2. Preparation of the FSMP

- FSM-Plan: Table of Contents, Scope
- Agreement on SLC Responsibility Matrix and Activities
- Pragmatic way forward, cross-reference existing QM-Procedures as far as possible
- Define Priorities for the next steps, e.g. requirements for Training, preparation of missing documentation/procedures
- Road-Map“ for phased Compliance and timeframe for potential „Certification“ (if required)

Contact

PipeSystemConsult GmbH
Adelheidstraße 12
80798 Munich, Germany
Tel.: +49 (0)89 326 021 36
Fax: +49 (0)89 374 135 23
Mobile: +49 (0)1525 3011 991
E-Mail: info@pipesyscon.com
Internet: www.pipesyscon.com