Management der funktionalen Sicherheit nach DIN EN IEC 61511

Gliederung

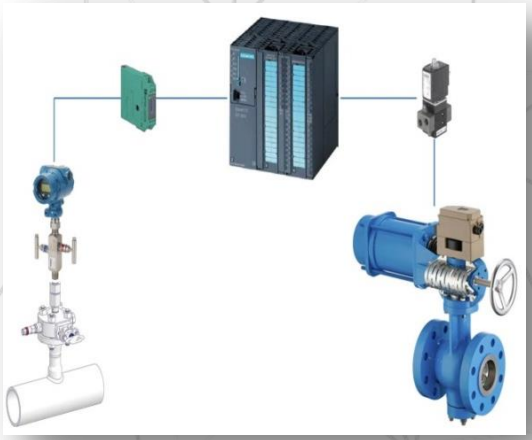
1. Was ist funktionale Sicherheit?
2. Rechtliche Rahmenbedingungen
3. Sicherheitsbetrachtung – Zuständigkeiten
4. SIS-Sicherheitslebenszyklus gem. DIN EN IEC 61511-1
5. Stand der Normung
6. Neuerungen der IEC 61511-1: 2016
7. FSMS Schlüsselanforderungen
8. Was sollte im FSMP enthalten sein? (Beispiel FSMP)
9. Aufsetzen eines FSMS – Vorgehensweise

1. Was ist funktionale Sicherheit?

- Definition nach **61508-4**: „Teil der Gesamtsicherheit, bezogen auf die EUC und das EUC-Leit- oder Steuerungssystem, der von der korrekten Funktion des sicherheitsbezogenen E/E/PE-Systems und anderer risikomindernder Maßnahmen abhängt.“

  EUC = Equipment under Control

  E/E/PE = elektrische/elektronische/programmierbare elektronische



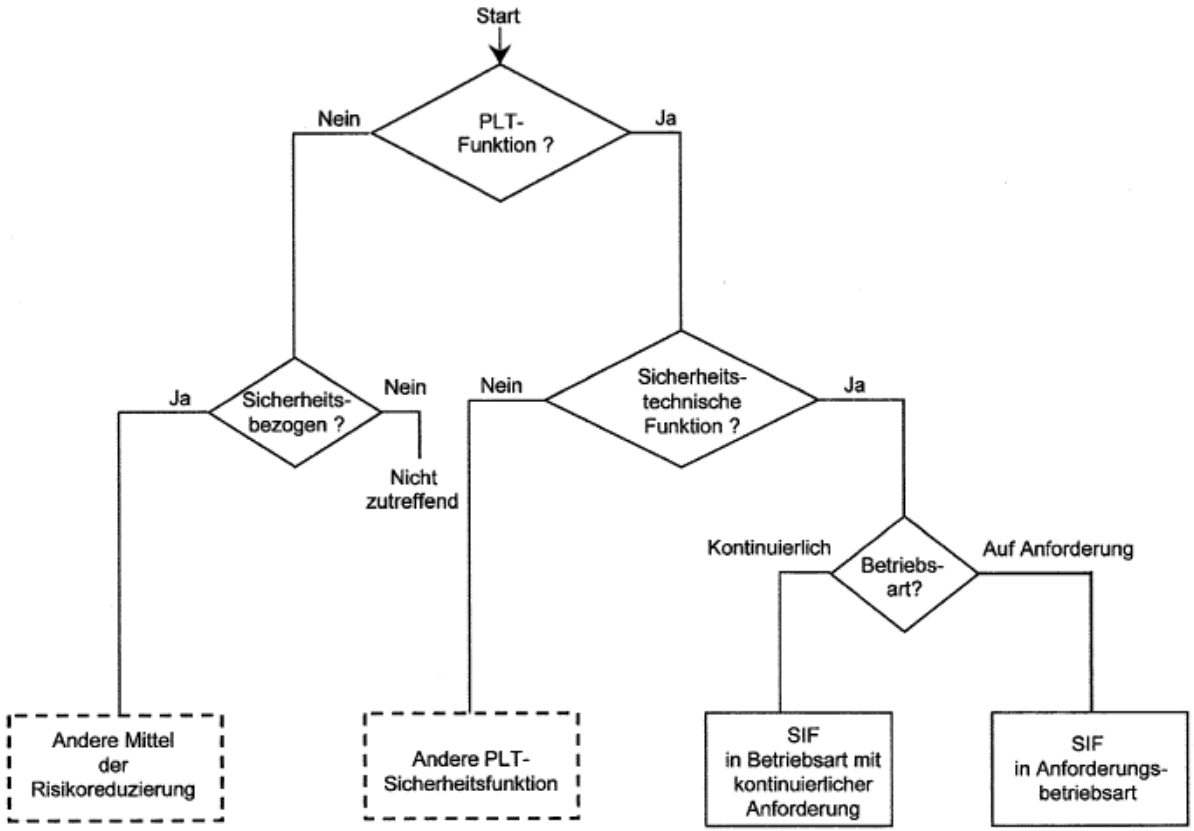
- Die funktionale Sicherheit ist die Risikominimierung, die von den Funktionen bereitgestellt wird, die implementiert wurden, um den sicheren Betrieb des Prozesses zu gewährleisten.

  „Die korrekte Funktion eines Schutzsystems inklusive der Sensoren und Aktoren.“

- Nicht zur funktionalen Sicherheit gehören u. a. Brandschutz, Ex-Schutz, Arbeitsschutz, inhärente Sicherheit.

1. Was ist funktionale Sicherheit?

Auszug aus DIN EN 61511-1

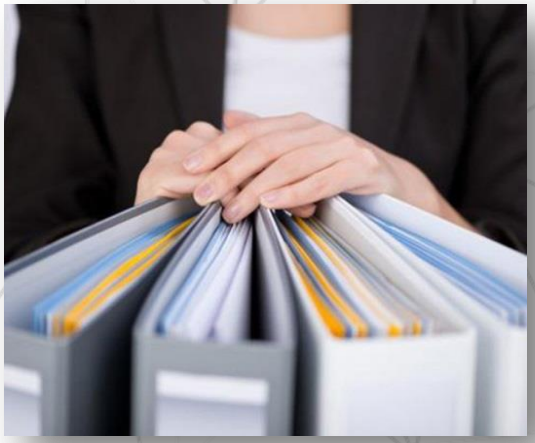


Die Norm legt auszuführende Tätigkeiten fest, die Anforderungen an diese sind jedoch nicht im Einzelnen dargestellt.

Bild 4 – Zusammenhang zwischen sicherheitstechnischen und anderen Funktionen

2. Rechtliche Rahmenbedingungen

- EU-Sicherheitsgesetze (z. B. SEVESO III, Maschinenrichtlinie) → nationale Gesetze → Verordnungen → allgemein anerkannte Regeln der Technik (z. B. Normen) = Normenhierarchie

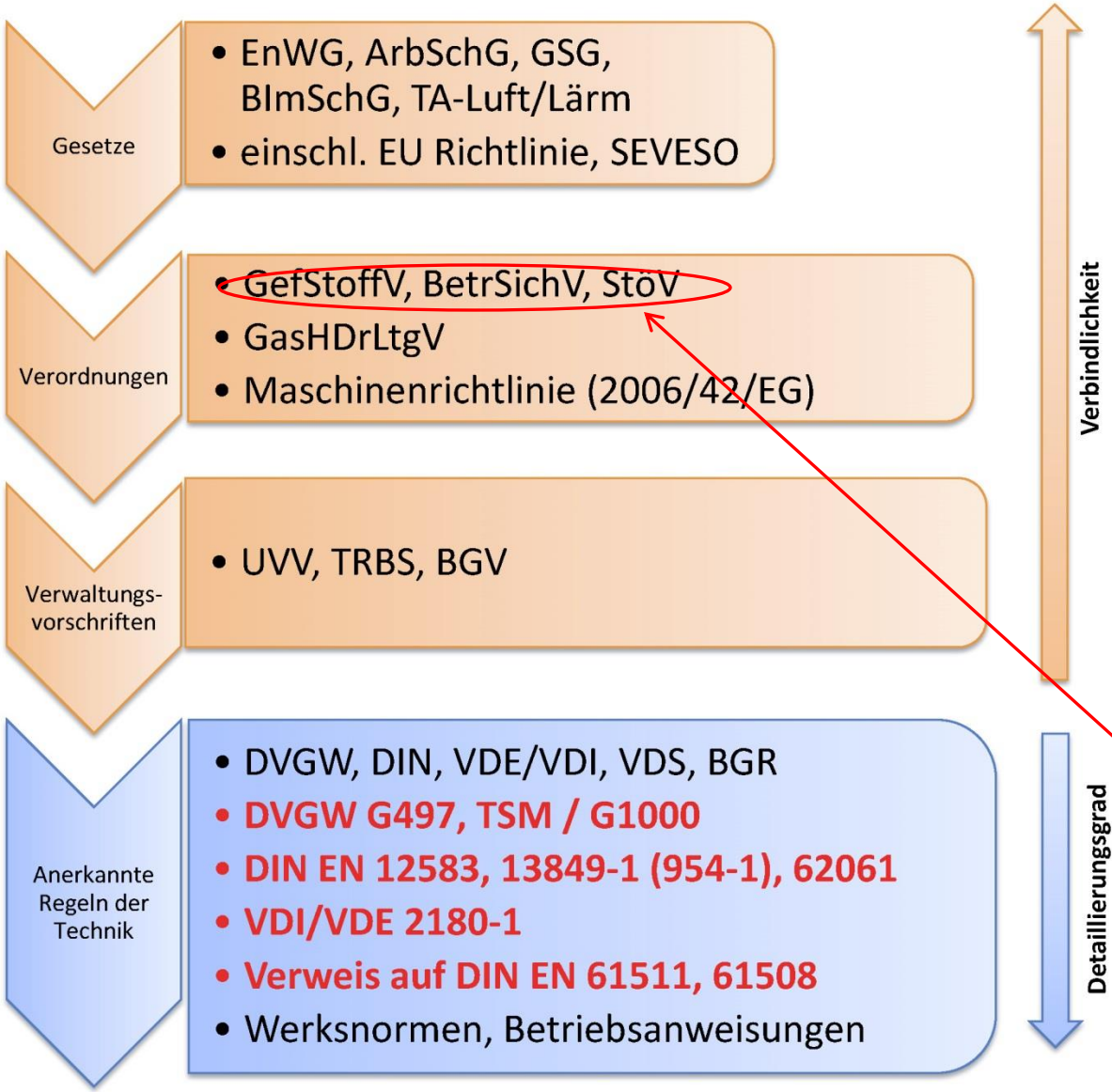


- Das Produktsicherheitsgesetz für Hersteller, bzw. das Arbeitsschutzgesetz für Betreiber verlangt, Sicherheitsrisiken auf ein akzeptables Minimum zu reduzieren.

- Gemäß ProdSV muss eine Gefahrenanlyse, bzw. gem. BetrSichV eine Sicherheitsbetrachtung, durchgeführt werden.

- Abhängig von Geräte-, bzw. Anlagentyp werden unterschiedliche sicherheitstechnische Normen verwendet.

2. Rechtliche Rahmenbedingungen - typ. Gasanlage, Deutschland

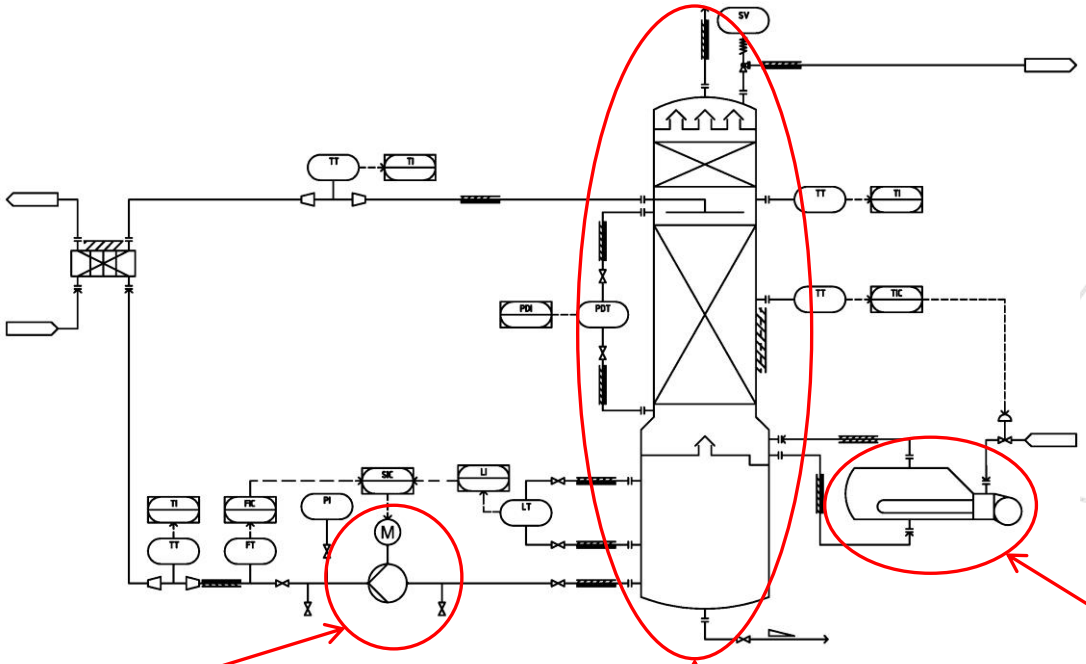


Die Gesetzgebung gibt vor, dass Energieanlagen so zu errichten und betreiben sind, dass die technische Sicherheit gewährleistet ist.

Die Einhaltung der allgemein anerkannten Regeln der Technik wird vermutet, wenn die technischen Regeln des DVGW eingehalten worden sind (§ 49 Abs. 2 EnWG, GasHdrLtgV §2 (2).

UK: COMAH 2015
US: OSHA CFR1910

2. Rechtliche Rahmenbedingungen

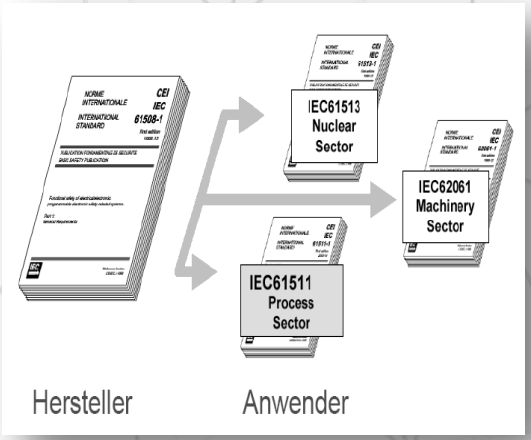


Maschinentechnik		Verfahrenstechnik	Feuerungstechnik
Maschinenrichtlinie 2006/42/EG		SEVESO III Richtlinie 12/18/EG (StöV, 12. BImSchV)	Druckgeräterichtlinie 2014/68/EG
DIN EN 12100		Sicherheitsbericht StöV 9	DIN EN 12952, 12953
DIN EN ISO 14121			DIN EN 230, 267, 298, 746
DIN EN 62061	DIN EN 13849	DIN EN 61511 (VDI/VDE 2180)	DIN EN 50156

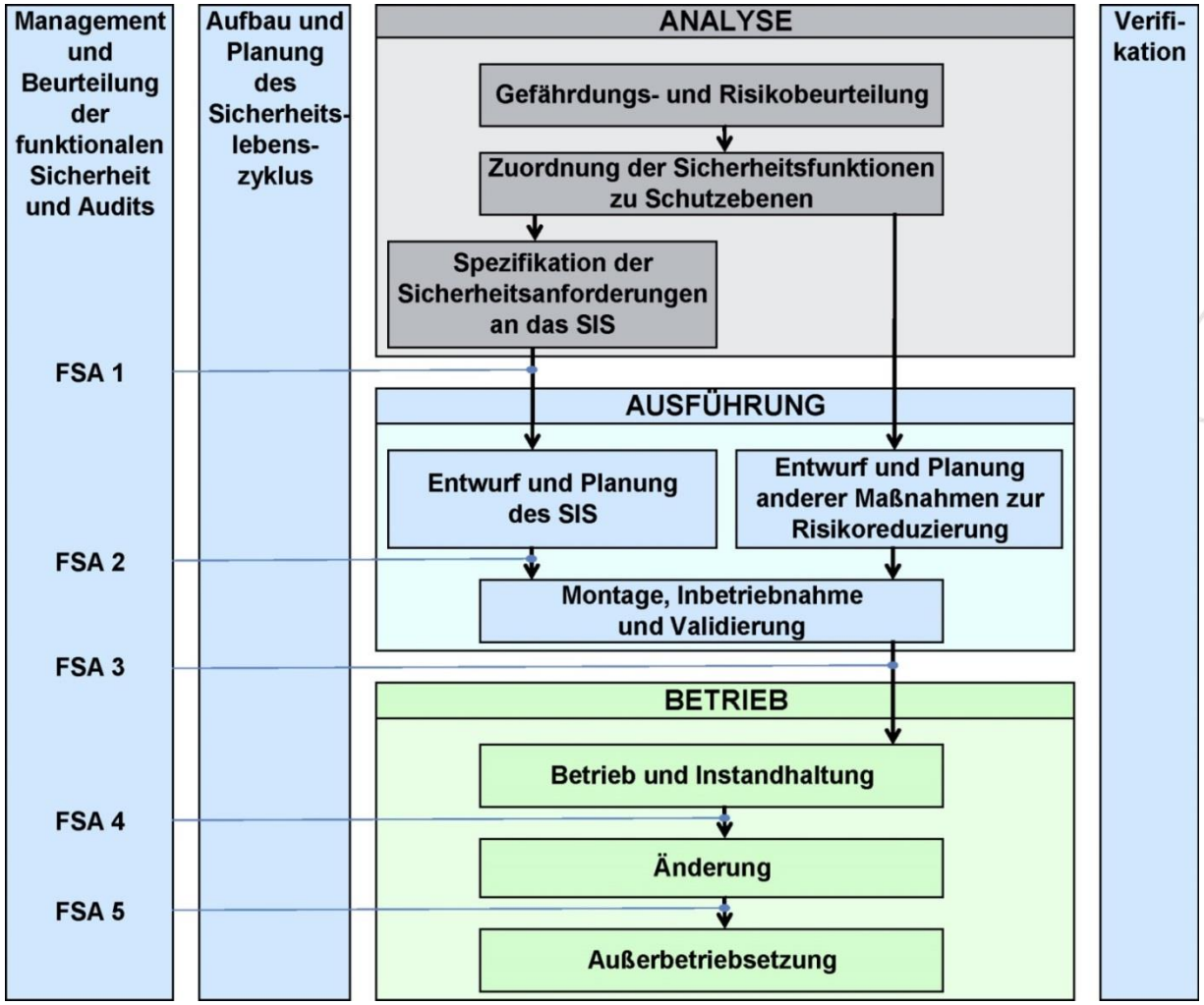
Stand der Sicherheitstechnik

3. Sicherheitsbetrachtung – Zuständigkeiten

- Risiko- und Gefahrenanalyse
  - Hersteller/Errichter ist verantwortlich
  - betrachtet Gefahren und deren Minderung für das/die Teil/Komponente
  - Grundlage eines Sicherheitskonzeptes
  - Forderung der ProdSV (z. B. Maschinenrichtlinie, EN ISO 12100, DGRL, IEC 62061, VDMA 4315)
- Gefährdungsbeurteilung
  - Betreiber ist verantwortlich für die Erstellung/Aktualisierung während des Lebenszyklus
  - betrachtet die Gefahren beim Umgang mit der Anlage (funktional)
  - Erweiterung des Sicherheitskonzeptes
  - Forderung der BetrSichV, ArbSchG, GefStofV
- Anerkannte Regeln der Technik
  - Sicherheitseinrichtungen sind am Stand der Sicherheitstechnik zu halten (z. B. nach 12. BImschV (StörfallV), § 3)
  - Im Falle eines Störfalles und einer Schuldzuweisung liegt die Beweislast für das Einhalten der Regeln der Technik beim Anwender.
  - Stand der Sicherheitstechnik ist in der DIN EN IEC 61508 bzw. in der abgeleiteten Normen abgebildet (z.B. 61511)



4. SIS-Sicherheitslebenszyklus gem. DIN EN IEC 61511-1

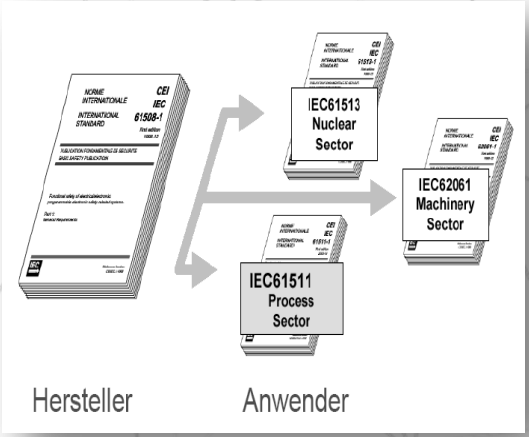


Hersteller und Anwender sollen ein Managementsystem der funktionalen Sicherheit einführen.

Dies orientiert sich am Sicherheitslebenszyklus.

5. Stand der Normung

Functional safety – Safety instrumented systems for the process industry sector

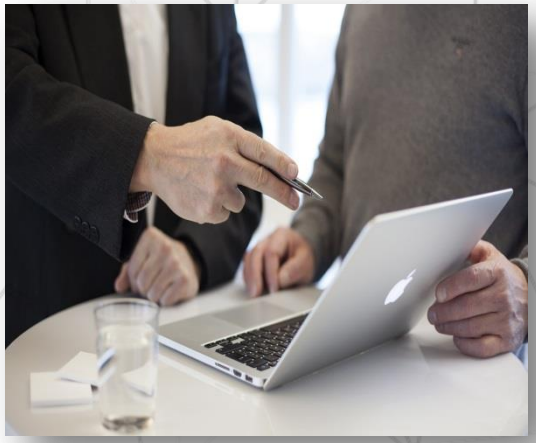


- IEC 61511-1 Edition 2.0 2016-02
  - Part 1: Framework, definitions, system, hardware and application programming requirements
  - IEC 61511-1 Edition 2.1 2017-08 Amendment
- IEC 61511-2 Edition 2.0 2016-07
  - Part 2: Guidelines for the application of IEC 61511-1: 2016
- IEC 61511-3 Edition 2.0 2016-07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

- Deutsche Übernahme der Norm durch DKE/GK 914 (Neue Ausgabe 02/2019 veröffentlicht!)
- Erstezt: DIN EN 61511-1(VDE 0810):2005, Korrekturen 2012-10 und 2017-11
- VDI/VDE 2180-1, 2, 3 wurden im Feb. 2018 neu veröffentlicht

6. Neuerungen der IEC 61511-1: 2016

- Anforderungen an FSMS



§ 5.2.5.2

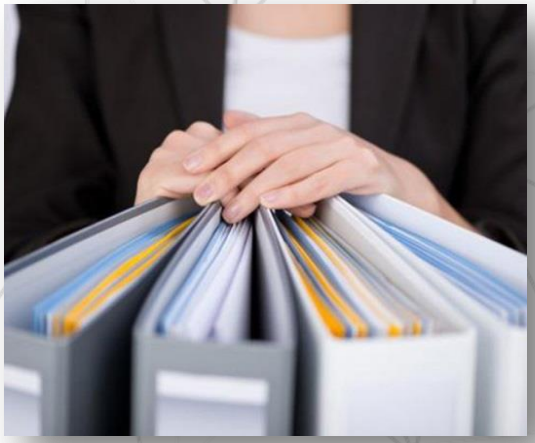
– *If a supplier makes any functional safety claims for a product or service, which are used by the organization to demonstrate compliance with the requirements of this part of IEC 61511, the supplier shall have a functional safety management system. Procedures shall be in place to demonstrate the adequacy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

Zusammenfassung auf Deutsch: Lieferanten, die für ihre Produkte und Dienstleistungen funktionale Sicherheit in Anspruch nehmen, müssen ein zusätzliches Management-System für funktionale Sicherheit vorweisen.

6. Neuerungen der IEC 61511-1: 2016

- Anforderungen an Kompetenzen



§ 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.*

Zusammenfassung auf Deutsch: Es ist sicherzustellen, dass über den gesamten Lebenszyklus für die jeweilige Tätigkeit qualifizierte Personen eingesetzt werden. Diese Qualifizierung ist zudem regelmäßig zu prüfen und aufzufrischen. Dieses Management der vorgehaltenen Kompetenzen ist zu dokumentieren.

6. Neuerungen der IEC 61511-1: 2016

- Beurteilungen der funktionalen Sicherheit (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.*

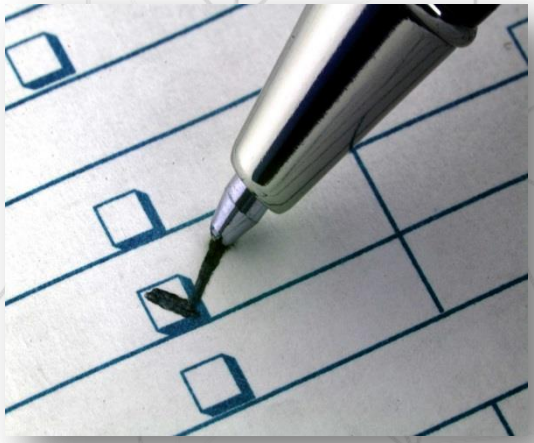
§ 5.2.6.2.5

– *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).*

Zusammenfassung auf Deutsch: Assessments zur funktionalen Sicherheit sollen begleitend zum Lebenszyklus erfolgen. Dabei ist das Management von Änderungen zu beachten. Während des Betriebs sind regelmäßig Assessments zur funktionalen Sicherheit durchzuführen. Es gibt erweiterte Anforderungen bzgl. Kriterien und Teilnehmer. FSA Stufe 3 und 4 werden als obligatorisch angesehen (FSA-3 vor der Einführung von Gefahrstoffen und FSA-4 während des Betriebs).

6. Neuerungen der IEC 61511-1: 2016

- Audit der funktionalen Sicherheit



§ 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.*

Zusammenfassung auf Deutsch: Unabhängige Audits sollen durchgeführt werden. Bei diesen Audits ist zu prüfen, ob die erforderliche Dokumentation je nach SLC-Phase verfügbar ist. Wo Lücken identifiziert werden, werden Empfehlungen für Verbesserungen gegeben.

6. Neuerungen der IEC 61511-1: 2016

- Änderungsmanagement

§ 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).*

Zusammenfassung auf Deutsch: Die Anforderungen an das Änderungsmanagement im gesamten Lebenszyklus eines Sicherheitssystems wurden erweitert. Änderungen und deren Verifikation müssen Teil der Sicherheitsplanung sein. Es ist sicherzustellen, dass alle betroffenen Dokumente bei Änderungen aktualisiert werden.

6. Neuerungen der 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.*

Zusammenfassung auf Deutsch: Es muss eine Risikobewertung zur IT-Sicherheit durchgeführt werden. Eingeschlossen sind PLT-Sicherheitseinrichtungen, PLT-Betriebseinrichtungen und sonstige verbundene Systeme. Es sind sämtliche Risiken zu identifizieren und zu beschreiben, die zu Sicherheitsvorfällen führen können.

7. FSMS Schlüsselanforderungen

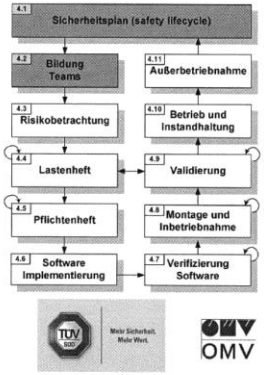
- Erstellung eines FSMP für den gesamten Sicherheitslebenszyklus
- Definition der Rollen und Verantwortlichkeiten (Matrix)
- Beschreibung, wie funktionale Sicherheit durchgeführt wird
- Erstellung von entsprechenden Prozeduren und/oder Verweise auf bestehende Prozeduren
- Personalkompetenzen und Bewertungen
- Durchführung von Audits und Bewertungen der funktionalen Sicherheit
- SIS Design-Aktivitäten (Hard-und Software)
- Schritte/Verfahren für die Verifikation und Validierung des SIS-Designs
- Leistungsmessung (KPIs)
- Management of Change (MOC) einbinden
- Dokumentationsanforderungen (abhängig von SLC-Phase)

8. Was sollte im FSMP enthalten sein?

- Der Standard 61511 gibt das Format eines FSMPs nicht an, sondern verweist auf 61508-1, § 6.
- Der Anhang in 61508-1 gibt ein Beispiel einer Dokumentationsstruktur (Gesamte Doku für SLC).
- PSC-Empfehlung:
  - Basis IEC 61511-1: 2016
  - Übersichtsdokument (FSMP) mit Bezug auf jeden Schritt des SLC
  - Querverweise auf bestehende QM-Verfahren (ISO-9001), bzw. neu zu erstellende FSM-Verfahren (anhand „Gap-Analyse“)
  - Anforderungen an Qualifikation und Kompetenz
  - Anforderungen an die Dokumentation
  - Matrix der Zuständigkeiten gem. SLC
  - Zu überlegen: Querverweise auf DIN EN 61511, VDI/VDE 2180

FSMP – Praxis Beispiel

Inhalt
1 Ziel / Zweck
2 Begriffe und Abkürzungen
3 Geltungsbereich
4 Organisation im Sicherheitslebenszyklus
4.1 Sicherheitsplan (safety lifecycle)
4.2 Delegation der Verantwortung
4.2.1 Planungsteam
4.2.2 Beurteilungsteam
4.3 Risikobetrachtung
4.3.1 Betrachtung der Risiken im Rahmen der HAZOP
4.3.2 Zuordnung des Geltungsbereich der jeweiligen NORM
4.3.3 Einstufung der Sicherheitstechnischen Systeme (SIS)
4.4 Erstellung des Lastenheft
4.5 Erstellen des Pflichtenheft
4.6 Implementierung der Software
4.7 Verifizierung der Software
4.8 Montage und Inbetriebnahme
4.9 Validierung
4.10 Betrieb und Instandhaltung
4.11 Außerbetriebnahme
5 Änderungsmanagement
6 Prüfungen im Sicherheitslebenszyklus
6.1 Zweck
6.2 Durchzuführende Prüfungen
6.2.1 Prüfung des Lastenheft
6.2.2 Prüfung des Pflichtenheft
6.2.3 Verifizierung der Software
6.2.4 Überprüfung der ordnungsgemäßen Durchführung von Montage und IBN
6.2.5 Validierung
7 Auditierung (Prüfung betrieblicher Qualitätsmerkmale)
7.1 Zweck
7.2 Planung und Durchführung (Mindestanforderungen)
7.2.1 Delegieren der Verantwortlichkeiten
7.2.2 Festlegen des Umfang
7.2.3 Festlegen der Häufigkeit
7.2.4 Durchführung des Audits
7.2.5 Dokumentation und Auswertung der Ergebnisse
8 Mitgeltende Unterlagen
9 Änderungsdienst
10 Requirement-Index



8. Beispiel FSMP eines Dienstleisters

TABLE OF CONTENTS

1 Approvals, control and amendment 3

2 Scope and Exclusions 3

2.1 General 3

2.2 Scope 3

2.3 Functional Safety Policy and Measurable Targets 4

2.4 Definitions 5

2.5 Abbreviations 5

3 Functional Safety Management System 6

3.1 General 6

3.2 Responsibilities 7

3.3 FSM Activities to be carried out by PSC 7

3.3.1 Hazard and risk assessment 7

3.3.2 Allocation of safety functions to protection layers 8

3.3.3 Preparation of the Safety Requirements Specification (SRS) 8

3.3.4 Design and engineering of safety instrumented systems 8

3.3.5 Verification, validation, functional safety assessment, audit 9

3.3.6 Auditing 10

3.3.7 Support services during installation, commissioning, testing (FAT, SAT), operation, maintenance, modification and decommissioning 10

4 Competency Requirements 11

5 Documentation Requirements 11

APPENDIX 1 – Index of PSC quality system procedures 12

APPENDIX 2 – SLC Matrix showing PSC responsibilities and activities 13

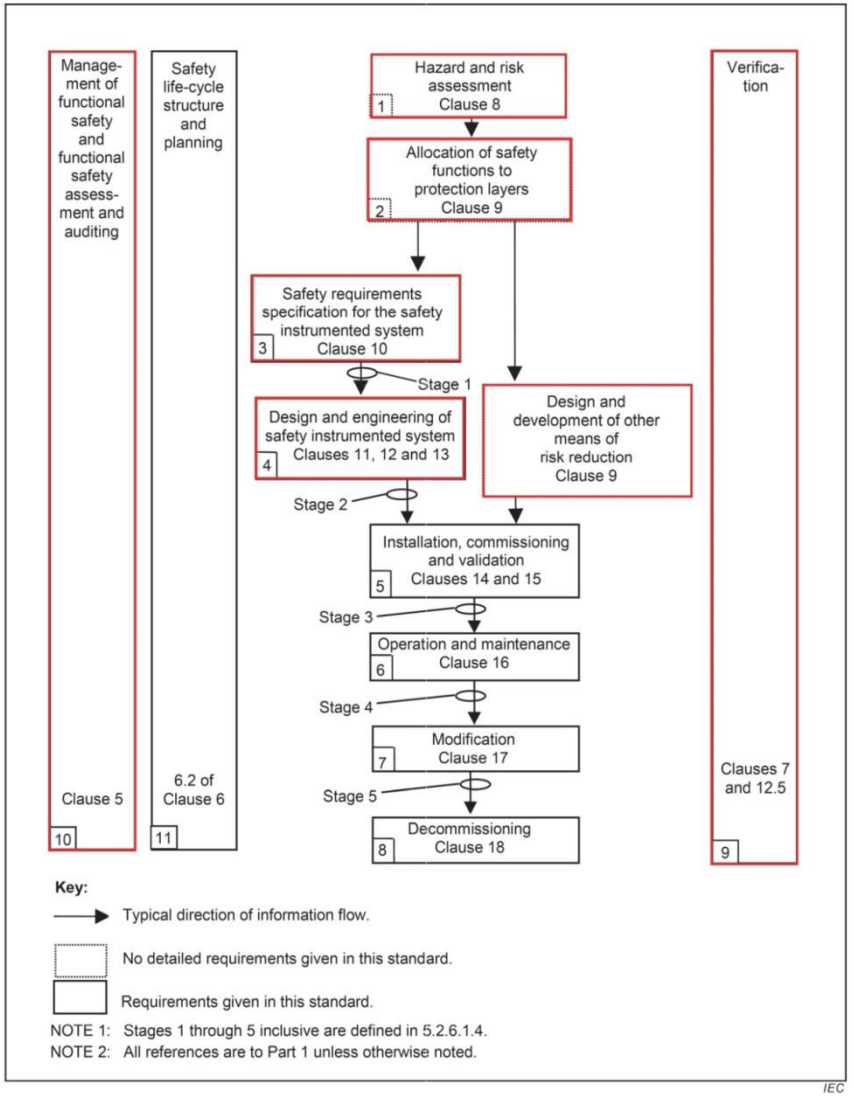


Figure 7 – SIS safety life-cycle phases and FSA stages

8. Beispiel FSMP eines Dienstleisters – Zuständigkeitsmatrix

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 lest (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 lest 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. Aufsetzen eines FSMS – Vorgehensweise

1. Gap-Analyse gem. IEC 61508/61511 Checkliste

- Desk-top-Review bestehender FSM-, QM-Verfahren
- Compliance-Review und Interviews gem. Checkliste vor Ort
- Bericht, Präsentation/Diskussion der Empfehlungen

2. Erstellung eines FSM-Plans

- FSM-Plan: Inhaltsverzeichnis, Umfang
- Abstimmung der Matrix der SLC-Zuständigkeiten und Aktivitäten
- pragmatischer Ansatz, so weit wie möglich auf bestehende QM-Verfahren verweisen/zurückgreifen
- Prioritäten für die nächsten Schritte, z. B. dringende Anforderungen für UK-Projekt, Bedarf an Schulung/Weiterbildung, fehlende Dokumentation/ Procedere
- „Road-Map“ für phasenweise Compliance und Zeitrahmen für eine „Zertifizierung“

Kontakt

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