Management der Funktionalen Sicherheit

KROHNE Academy „Automatisierungstechnik in der Prozessindustrie“

Fred Stay
2013-06-04/05

Medienpartner P&A

1. Warum brauchen wir ein FSM
2. Vermeidung/Beherrschung von Fehlern
3. Praxisbeispiel: Implementierung in 3 Schritten
4. Was Anwender eines FSM sagen

Management der Funktionalen Sicherheit

Agenda

Warum brauchen wir ein Management der Funktionalen Sicherheit?

Management der Funktionalen Sicherheit:

Eine Beschreibung der Managementtätigkeiten mit denen sichergestellt wird, dass die funktionalen Sicherheitsziele erreicht werden. Gemäß DIN EN 61511 besteht die Forderung ein entsprechendes Sicherheitsmanagement einzurichten.

Aber…. ist das wirklich etwas Neues?

Europäische Kommission über Sicherheits-Management-Systeme

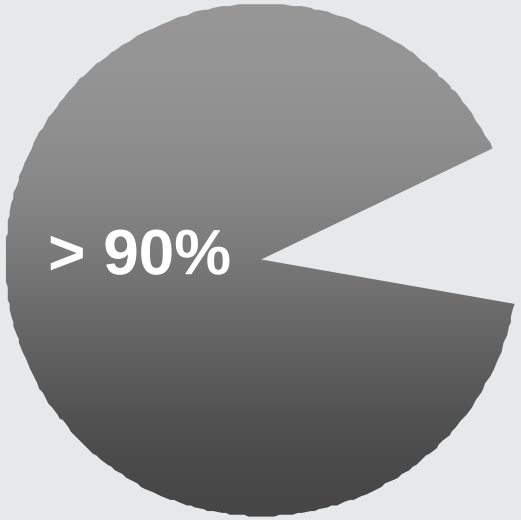
… eines der Hauptziele dieses Ausschusses ist die Verhinderung oder Reduzierung von Unfällen, die durch Management Faktoren ausgelöst werden. Innerhalb der europäischen Union waren seit 1982 bei über 90% aller Unfälle organisatorische Fehler der wesentliche ursächliche Faktor.

European Commission

European Civil Protection

Source: Chemical Accidents (Seveso II) - Legislation

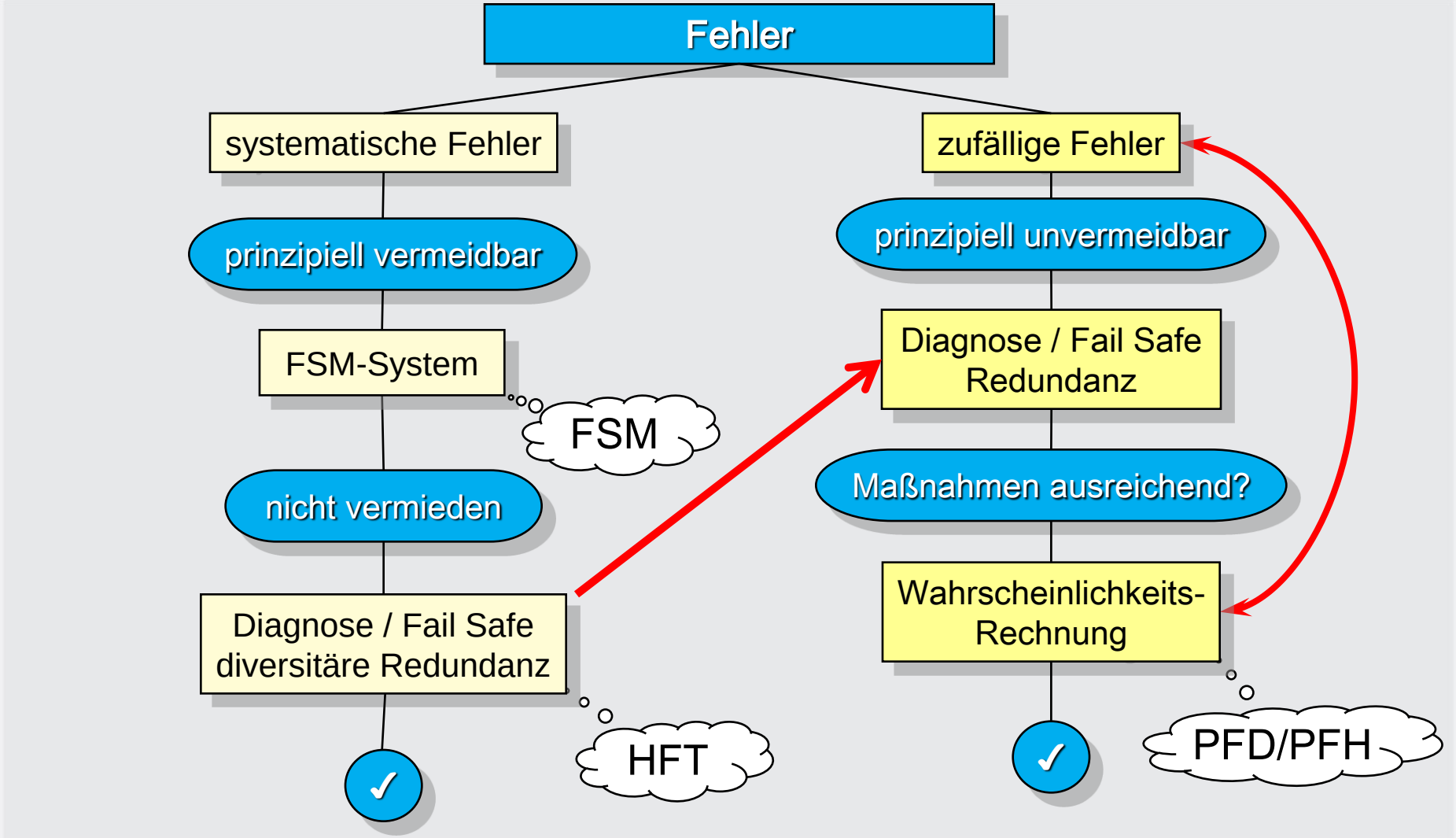
Unfälle verursacht durch Management Faktoren



(Die Seveso II Richtlinie wurde in Deutschland durch die Störfall-Verordnung - 12_ BImSchV umgesetzt)

Fehler vermeiden und beherrschen
Wo und wie hilft uns ein FSM?

Systematische und zufällige Fehler



Mit vielem Dank an Dr. Andreas Hildebrandt

Drei Komponenten der Sicherheitsintegrität

Management der Funktionalen Sicherheit (FSM)	• Vermeidung systematischer Fehler
Redundanz (HFT)	• Beherrschung systematischer und zufälliger Fehler
PFD-Berechnung	• Ermittlung der Wahrscheinlichkeit eines zufälligen Ausfalls

IEC 61511 (Vermeidung systematischer Fehler)

4 Übereinstimmung mit dieser Internationalen Norm

Für die Übereinstimmung mit dieser Internationalen Norm muss gezeigt werden, dass alle in den Abschnitten 5 bis 19 aufgestellten Anforderungen nach den festgelegten Kriterien erfüllt werden und damit die Zielsetzung des jeweiligen Abschnitts erreicht wird.

5 Management der funktionalen Sicherheit

5.1 Ziel

Das Ziel der Anforderungen dieses Abschnitts ist es, die erforderlichen Managementtätigkeiten zu beschreiben, mit denen sichergestellt wird, dass die funktionalen Sicherheitsziele erreicht werden.

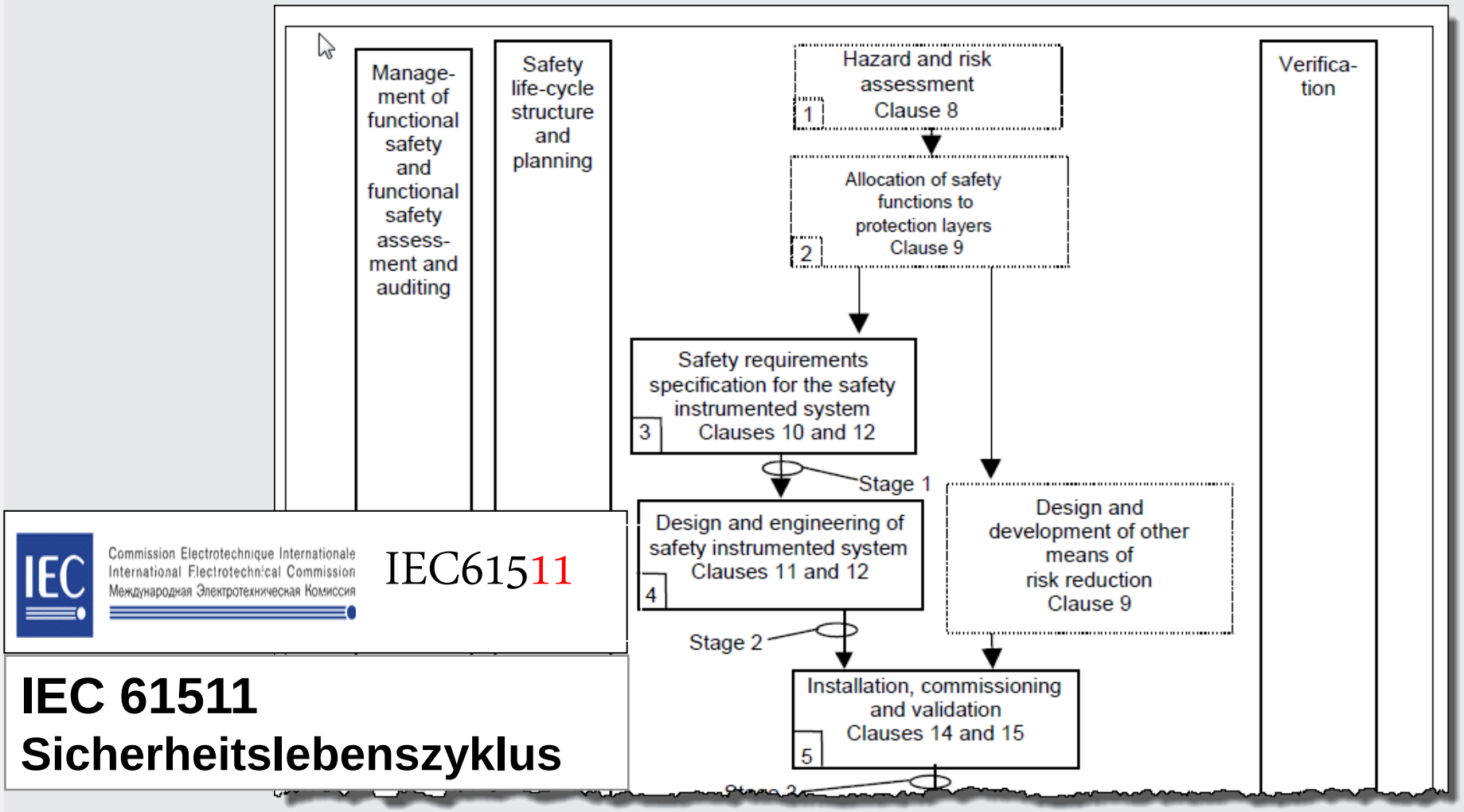
6 Anforderungen an den Sicherheitslebenszyklus

6.1 Ziele

Die Ziele dieses Abschnitts bestehen darin,

- die Phasen des Sicherheitslebenszyklus festzulegen und die damit verbundenen Anforderungen aufzustellen;
- die technischen Tätigkeiten in einem Lebenszyklus zu organisieren;
- sicherzustellen, dass eine geeignete Planung vorhanden ist oder entwickelt wurde, die sicherstellt, dass das SIS die Sicherheitsanforderungen erfüllt.

Sicherheitslebenszyklus
(Neue Standards als Richtlinie)



IEC 61511
Sicherheitslebenszyklus

Beherrschung zufälliger und systematischer Fehler

11.4 Anforderungen an die Hardware-Fehlertoleranz

11.4.1 Sensoren, Logiksysteme und Aktoren von sicherheitstechnischen Funktionen müssen eine Mindest-Hardware-Fehlertoleranz aufweisen.

ANMERKUNG 2 Die Mindest-Hardware-Fehlertoleranz wurde festgelegt, um mögliche Versäumnisse bei der Festlegung der sicherheitstechnischen Funktionen aufgrund der dem Entwurf der sicherheitstechnischen Funktion zugrunde liegenden Annahmen und aufgrund der Unsicherheit der Ausfallraten von Komponenten oder Teilsystemen in unterschiedlichen Prozess-Anwendungen auszugleichen.

Tabelle 6 – Mindest-Hardware-Fehlertoleranz von Sensoren, Aktoren und nichtprogrammierbaren Logiksystemen

SIL	Mindest-Hardware-Fehlertoleranz (siehe 11.4.3 und 11.4.4)
1	0
2	1
3	2
4	Es gelten besondere Anforderungen. Siehe IEC 61508

Erläuterung zur HFT und systematischen Fehlern

11.4 Anforderungen an die Hardware-Fehlertoleranz

11.4.1 Der traditionelle Ansatz bei der Auslegung eines Sicherheitssystems war bisher, sicherzustellen, dass kein Einzelfehler zu einem Ausfall der gewünschten Funktion führt. Systemarchitekturen mit einer 1oo2- oder 2oo3-Bewertung haben eine Fehlertoleranz von 1, da sie auf Anforderung auch dann funktionieren, wenn ein gefährlicher Fehler vorliegt. Solche Systeme wurden standardmäßig für Sicherheitssysteme verwendet, um sicherzustellen, dass sie ausreichend widerstandsfähig gegen zufällige Hardwareausfälle waren. Fehlertolerante Architekturen schützten auch gegen einen weiten Bereich systematischer Fehler (vorwiegend in der Hardware), da solche Fehler nicht notwendigerweise gleichzeitig auftreten.

Diese Norm erkennt, dass die Prozessindustrie für Sicherheitssysteme mehr als ein Leistungsniveau benötigt, und hat das Konzept der Sicherheits-Integritätslevel mit einer ansteigenden Leistungsfähigkeit übernommen, die von der erforderlichen Risikoreduzierung in einer bestimmten Anwendung abhängen.

EN 61511-2:2004

Wegen dieser unterschiedlichen Leistungsstufen ist es nicht länger sinnvoll, von allen Sicherheits-Integritätsleveln eine Fehlertoleranz zu erwarten. Bei der Auswahl einer Architektur für einen bestimmten Sicherheits-Integritätslevel ist es dagegen wichtig, sicherzustellen, dass sie gleichermaßen widerstandsfähig gegen zufällige Hardwarefehler und systematische Fehler ist. Um eine Widerstandsfähigkeit gegen zufällige Hardwarefehler sicherzustellen, fordert diese Norm, dass eine Zuverlässigkeits-Analyse durchgeführt wird.

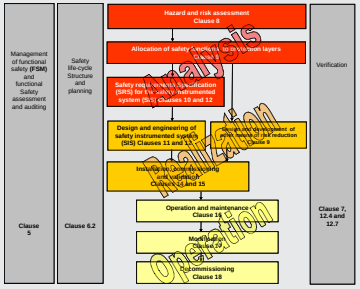
IEC 61511-2

FSM erhöht die Qualität der Funktionalen Sicherheit

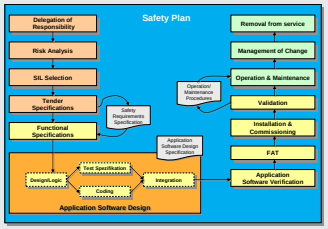
- Vermeidung systematischer Fehler
- Lebenszyklus-Ansatz (Organisation aller Aktivitäten über den gesamten Lebenszyklus einer Anlage)
- Unterschiedliche Maßnahmen zur Vermeidung von Fehlern
  - Personalqualifizierung
  - Verifikation
  - Validierung
  - Audits und Assessments
- Erweitertes Qualitätsmanagementsystem

FSM implementieren

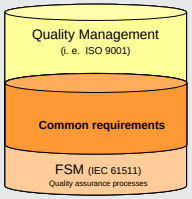
Wie lässt sich FSM implementieren?



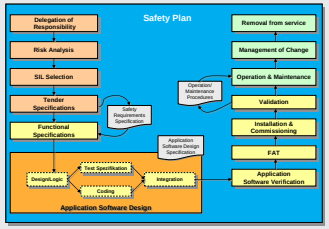
Standard



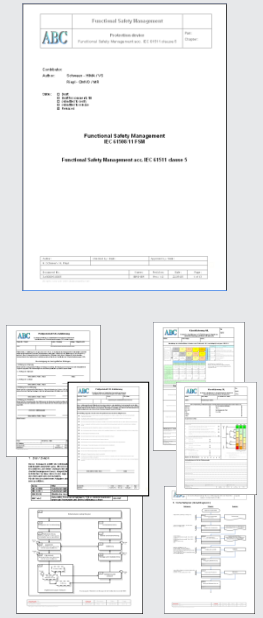
existierende Prozesse



Gap Analyse



Anpassen

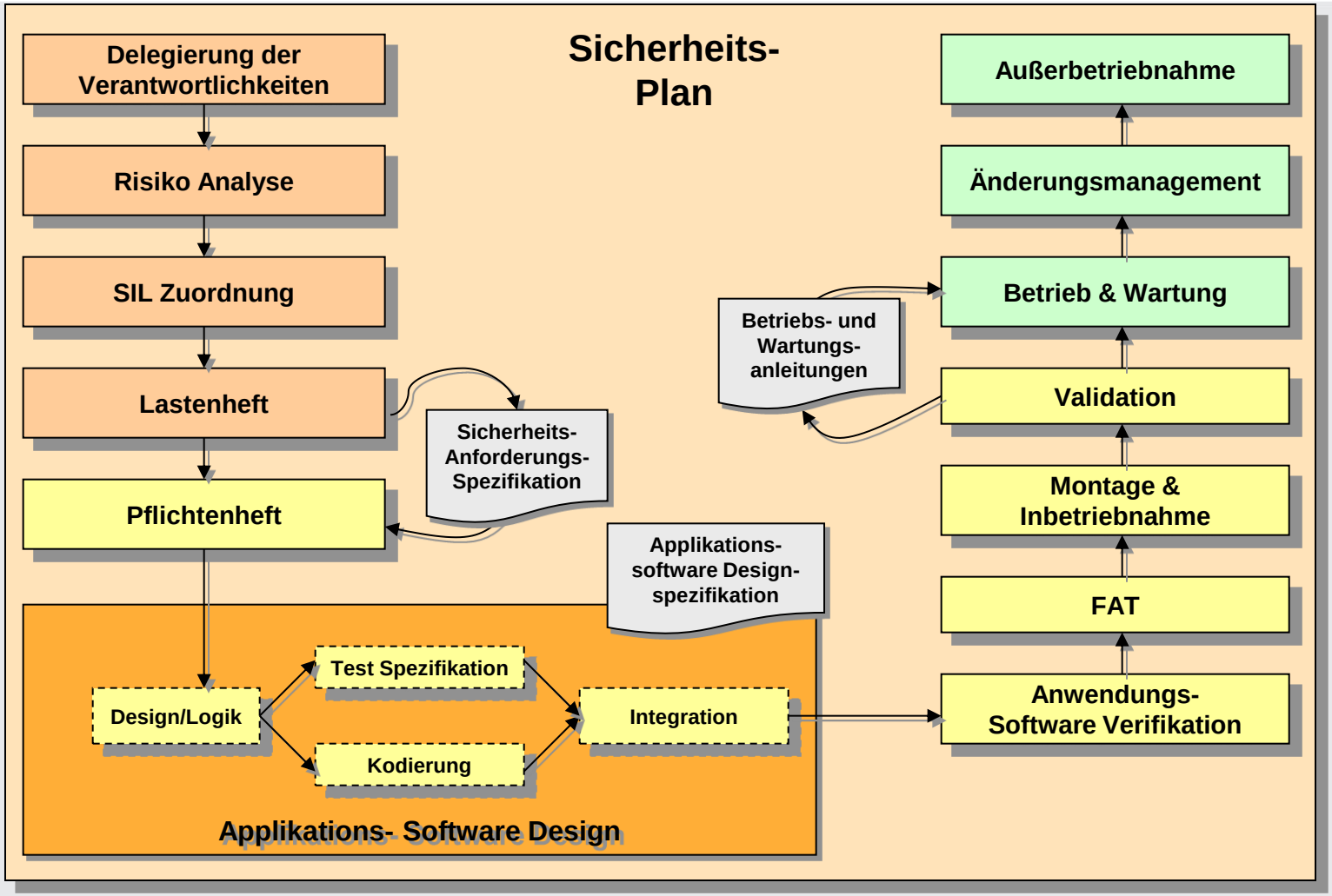


FSM Prozess

Implementierung – Schritt 1

(Analyse existierender Prozesse)

Graphische Darstellung aller relevanten Prozesse



Welche Probleme sind zu lösen?

Strukturiertes Vorgehen → jedoch flexibel reagieren

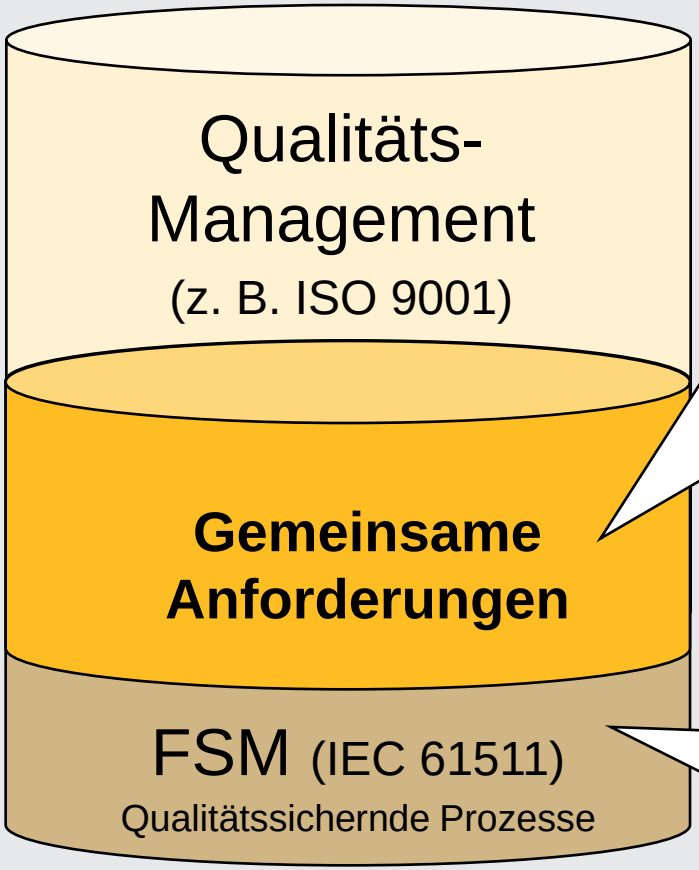
- Unterstützung durch das Management ist Voraussetzung
- Übersicht verschaffen, viele Prozesse sind existent, niemand kennt alle!
- Erste Übersicht in graphischer Darstellung erstellen
- Rechtzeitige Einbindung verantwortlicher Personen
- Workshop unterbrechen, wenn Informationen fehlen
- Das Team ist während der Analyse der jeweiligen Phasen anzupassen

Implementierung – Schritt 2

(Gap-Analyse)

Gap-Analyse

- **Analyse des existierenden QM Prozesses (Gap-Analyse)**



Identifikation von Überschneidungen z.B. Personalqualifikation, interne Audits, Dokumentenkontrolle, Wartung, Fehler Analysen, usw.

Identifikation der Gaps, Integration in bestehendes QM oder eigenes FSM System

Welche Probleme sind zu lösen?

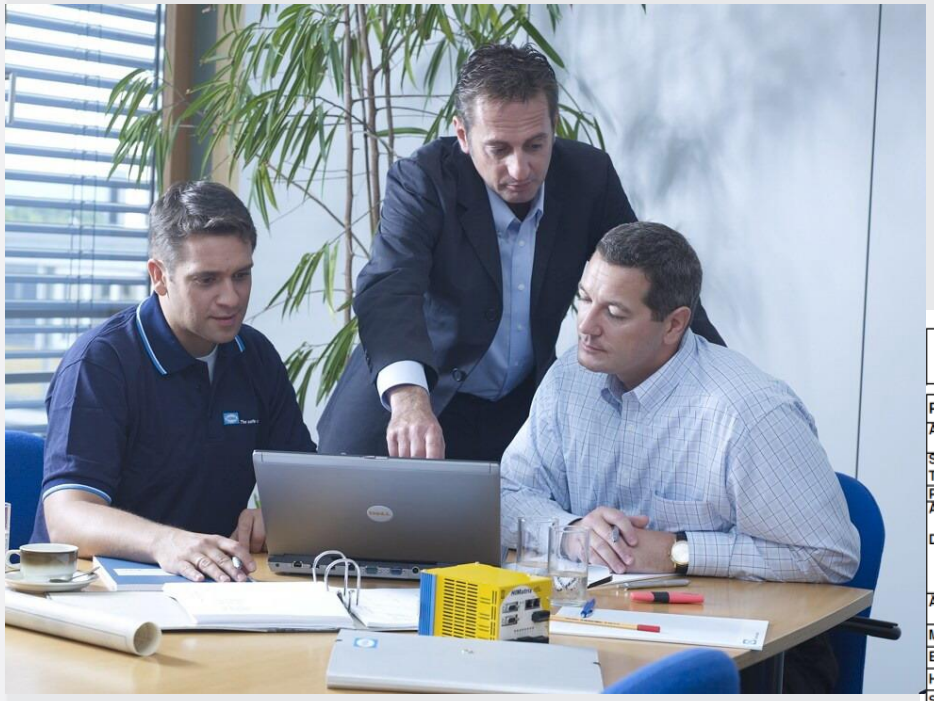
Strukturiertes Vorgehen → jedoch flexibel reagieren

- Identifizierung von Lücken (Gap) und Übereinstimmungen zwischen existierenden Prozeduren und Anforderungen aus IEC 61511
- Auch bei der Gap-Analyse muss das Team den zuständigen Bereichen angepasst werden
- Nach der Gap-Analyse muss die weitere Vorgehensweise festgelegt und die Prioritäten definiert werden.

Implementierung – Schritt 3

(Modifizierung der Prozesse)

Änderungsmanagement (MoC):
Prozedur unvollständig!



Überprüfung und
Modifikation der Prozeduren!

HIMA
P2 PE_ 186 C

Project Engineering
Change Request and Safety Review

Page 1 of 1
PE_186 (d)#1

Projekt:		**HIMA Projekt**		**CR #:**	
Änderungsanforderung, Auslöser: HIMA :		Unterschrift.:		Datum:	
System Beschreibung:					
Thema/Punkt: Software: ☐	Hardware: ☐	Dokument: ☐	Sicherheitsrelevant: JA NEIN		
Priorität: Dringend: ☐	eilig: ☐	Routine: ☐	Änderung einbringen bis:		
Änderungsbeschreibung: *(Detail Informationen siehe Anhang wenn nötig.)* Neue Anforderung: ☐	Geänderte Anforderung: ☐	Fehler ☐	Applikationsänderung ☐	Sonstiges: ☐	
Details:					

Änderungsanalyse: (Ausarbeitung von HIMA Projektbearbeiter. Siehe Anhang wenn nötig.) erhalten von: Datum:	**Dauer Std.**	**Ausgeführt Datum/Signum**	**Geprüft** Datum/Signum
Mechanisch:			
Elektrisch/Verdrahtung:			
Hardware:			
Software:			
Dokumente:			
Integration zu anderen Systemen:			
Genehmigung Kunde: von:			
Kunde Safety Review: *(Änderungen eingebracht entsprechend SRS Anforderung)* von:			

CR-beendet:
von PM: _____ Firma: _____ _____
Unterschrift Datum

Anforderungen an die Sicherheitsplanung:
- Der Sicherheitsplan

6.2 Anforderungen

6.2.1 In der Sicherheitsplanung muss ein Sicherheitslebenszyklus festgelegt werden, der die Anforderungen dieser Norm beinhaltet.

Tabelle 2 – Übersicht über den Sicherheitslebenszyklus eines SIS

Phase des Sicherheitslebenszyklus oder Tätigkeit		Ziele	Abschnitt oder Unterabschnitt der Anforderungen	Eingaben	Ergebnisse
Kastennummer in Bild 8	Titel				
1	Gefährdungs- und Risikobeurteilung	Festlegung von Gefährdungen und gefahrbringenden Ereignissen durch den Prozess bzw. die zugehörigen Einrichtungen, der Ereignisketten, die zu gefahrbringenden Ereignissen führen können, des damit verbundenen verfahrenstechnischen Risikos, der Anforderungen zur	8	Verfahrenstechnischer Entwurf, Auslegung, personelle Maßnahmen, Sicherheitsziele	Eine Beschreibung der Gefährdungen, der benötigten Sicherheitsfunktionen und der jeweiligen Risikominderung

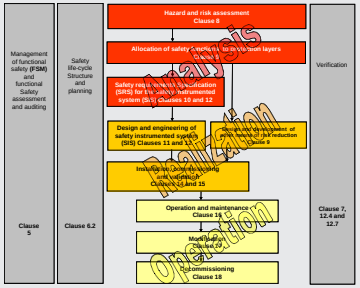
Welche Probleme sind zu lösen?

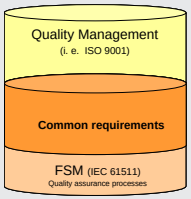
Strukturiertes Vorgehen → jedoch flexibel reagieren

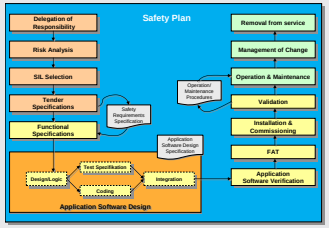
- Detaillierte Analyse einzelner Prozesse, notwendige Anpassungen / Ergänzungen festlegen
- Wenn möglich Ausarbeitung der Details durch den Betreiber
- Gemeinsamer Review der jeweiligen Modifikationen…

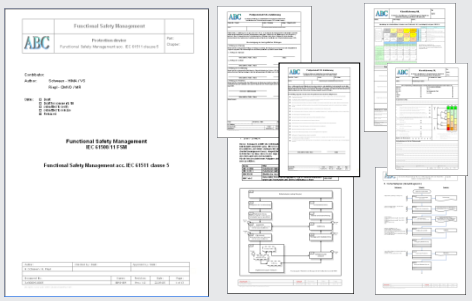
8 Zusammenfassung

Management der Funktionalen Sicherheit (FSM)









Standard | **Gap Analysis** | **Customize** | **FSM Prozess**

FSM stellt sicher, dass die richtigen Prozesse verwendet werden, um Funktionale Sicherheit zu erreichen.

Was Anwender zu FSM sagen

Anlagenbauer

- Globale Zuständigkeiten werden eindeutig definiert
- Berücksichtigung von Kundenvorgaben (Risikoeinstufung) bereits während der Angebotsphase
- Systematische Überprüfung der Prozesse und Abläufe
- Kostenersparnis durch Optimierung während der Analysephase sowie rechtzeitige Einbindung von Kundenanforderungen

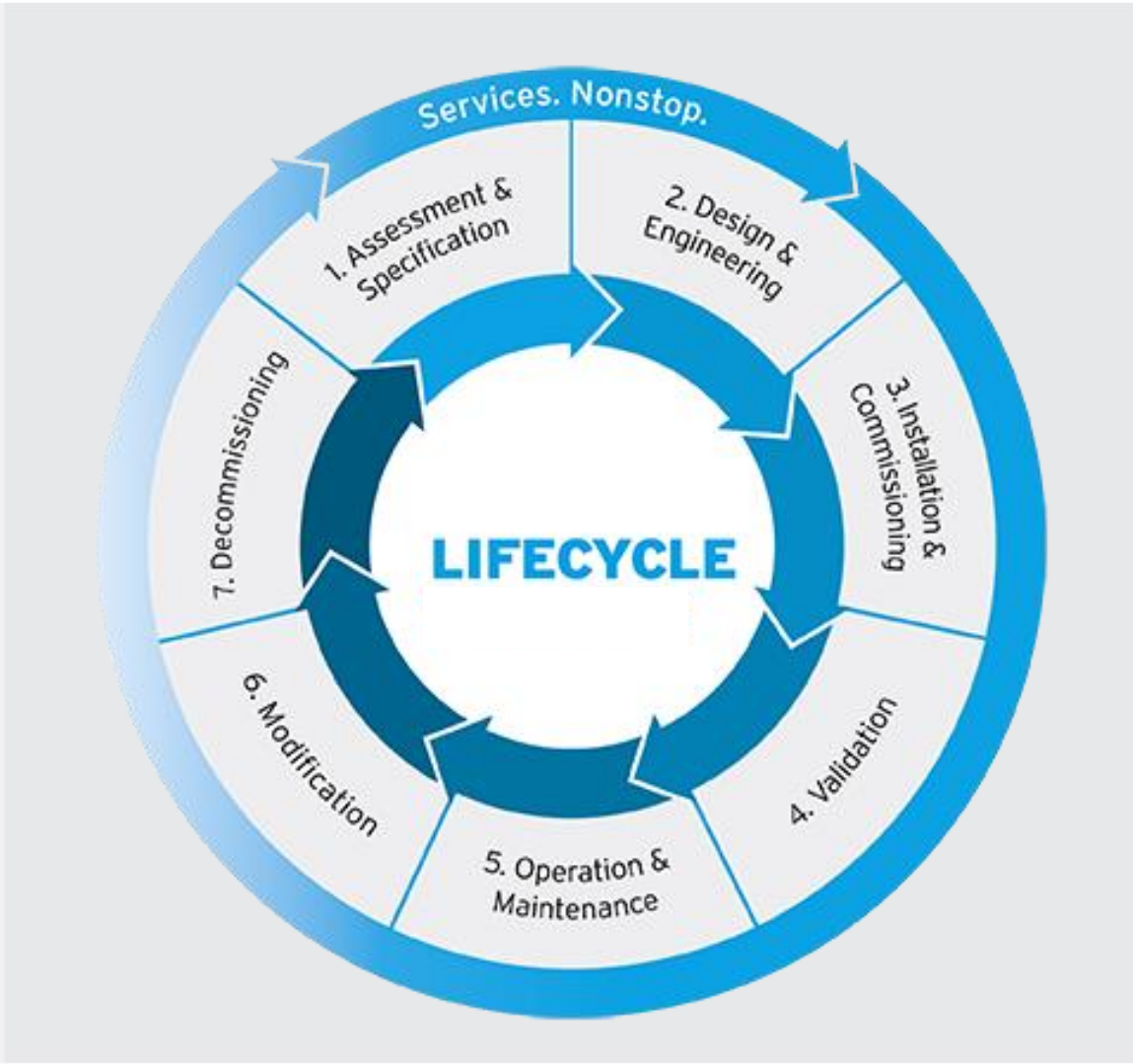
Anlagenbetreiber

- Spezifikation hat die größte Bedeutung
- Probleme werden aufgedeckt
- Erstellung von Details durch den Kunden erhöht die Akzeptanz
- Diverse Vorteile
  - Verbesserte Dokumentation / Bedienungsanleitungen
  - Reduzierte Schulungsaufwände
  - Führt zur Standardisierung

Anlagenbetreiber

- Kontrollierbare Qualität / Qualitätsverbesserung
  - Fehler werden erkannt und zugeordnet
  - Rückverfolgung des Prozesses
- Einbindung / Bekenntnis der Unternehmensleitung ist unumgänglich

FSM ist ein ganzheitliches Konzept



Fred Stay

Consulting

E-Mail: f.stay@hima.com


KROHNE
HIMA
SAFETY NONSTOP
PTB
PHOENIX CONTACT
Schneider Electric
FRIATEC
RHEINHÜTTE PUMPEN
TÜV NORD
SAMSON
RITTAL
EPLAN
Medienpartner
P&A
Vielen Dank für Ihre Aufmerksamkeit!