SIEMENS

Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie

Datum/ Uhrzeit: 17.11.2010 / 18:00 Uhr

Ort: Technoseum Mannheim
(Landesmuseum für Technik
und Arbeit)
Museumsstraße, Mannheim

SIEMENS

Funktionale Sicherheit – Sicherh. Systeme für die Prozessindustrie

- Einführung zur Funktionalen Sicherheit
- Überlegungen zu Unfallursachen und Produkthaftung
- Übersicht zur IEC 61508
- Übersicht zur IEC 61511
- Management der Funktionalen Sicherheit
- Sicherheitslebenszyklus
- Zusammenstellung

Michael Stay

+49 (721) 595 4516 - office

+49 (160) 972 243 65 - mobile

michael.stay@siemens.com

76181 Karlsruhe (Germany)

Kurzprofil

1987 – 2000 HIMA Paul Hildebrandt, Engineering von sicherheitsgerichteten Steuerungen (BMS, ESD, F&G)

2000 – 2001 GE Harris, Entwicklung eines Sicherheitssystems für die Bahnindustrie (Heißläufer-Ortungsanlage)

2001 – 2007 Linde Engineering, Projektmanagement und Engineering MSR für Gas-, Helium- und Wasserstoffanlagen

- Asaluye, Iran – weltgrößte C2+ Recovery and Fraktionierung Anlage mit 3 Mio m^3/h
- SKIKDA, Algerien – Helium-Verflüssigung (16 Mio Nm^3 / Jahr)
  http://www.helison.ch/Helison_Prod/Helison_Prod-eng.htm
- CONCON, Chile – 46.000 m^3/h Wasserstoff-Anlage
  http://www.enap.cl/ingles/opensite_det_20051229181601.asp
- VLISSINGEN, Niederlande – m^3/h Wasserstoff-Anlage

Seit 2007 Siemens Industry IA AS SM MP 8, Partner Manager PCS 7 Process Safety

SIEMENS

Was versteht man unter „Funktionaler Sicherheit“?

Funktionale Sicherheit bezeichnet den Teil der Sicherheit eines Systems, der von der korrekten Funktion der sicherheitsbezogenen (Sub-)Systeme und externer Einrichtungen zur Risikominderung abhängt. Nicht zur funktionalen Sicherheit gehören u. a. elektrische Sicherheit, Brandschutz, Strahlenschutz.

Mit der Komplexität elektronischer, insbesondere programmierbarer Systeme steigt auch die Vielfalt der Fehlermöglichkeiten. Entsprechend fordert die Normenreihe IEC 61508 *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/ programmierbar elektronischer Systeme* die Anwendung diverser Methoden zur Vermeidung systematischer Fehler (das sind Fehler bei der Spezifikation, Implementierung etc. des Systems) und zur sicheren Beherrschung von Ausfällen und Störungen (oft durch physikalische Phänomene oder Bedienungsfehler).

SIEMENS

Funktionale Sicherheit – Sicherh. Systeme für die Prozessindustrie

- **Einführung zur Funktionalen Sicherheit**
- Überlegungen zu Unfallursachen und Produkthaftung
- Übersicht zur IEC 61508
- Übersicht zur IEC 61511
- Management der Funktionalen Sicherheit
- Sicherheitslebenszyklus
- Zusammenstellung

Definitionen

Sicherheit = **Freiheit von unvertretbaren Risiken**

Risiko = **Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt und dem Ausmaß dieses Schadens**

Schaden = **Verletzung oder der Tod von Menschen, katastrophale Auswirkung auf die Umwelt**

(vgl. IEC 61508, Teil 5, Anhang A)

Ziel ist es, das Risiko auf ein vertretbares Maß zu reduzieren !

Tolerierbares Risiko (Beispiel)

http://www.youtube.com/watch?v=6N4Cm01rszU

Was heißt vertretbares Risiko?

Vertretbar ist ein Risiko, wenn es von den potentiell Betroffenen (i. Allg. der Gesellschaft) akzeptiert ist

→ **gesellschaftlich akzeptiertes Risiko**

Was kann der Laie darunter verstehen?
Schutzziele werden durch die Gesellschaft vorgegeben. Es sind die Fragen zu beantworten, welche Sicherheit wir wollen und welche Sicherheit wir uns leisten können. Um Antworten zu finden, gilt es, akzeptable von nicht akzeptablen Risiken abzugrenzen. In der Praxis gehen wir heute von einem Grenzwert für ein akzeptiertes Risiko von 10–5 Toten/Jahr (0,00001 Tote/Jahr) aus. Dies entspricht der Todeswahrscheinlichkeit eines jungen Menschen in unserer Gesellschaft.

Zitat aus BAU & ARCHITEKTUR AUGUST 2010, S. 14

Was tun,
wenn die Akzeptanzgrenze überschritten wird?

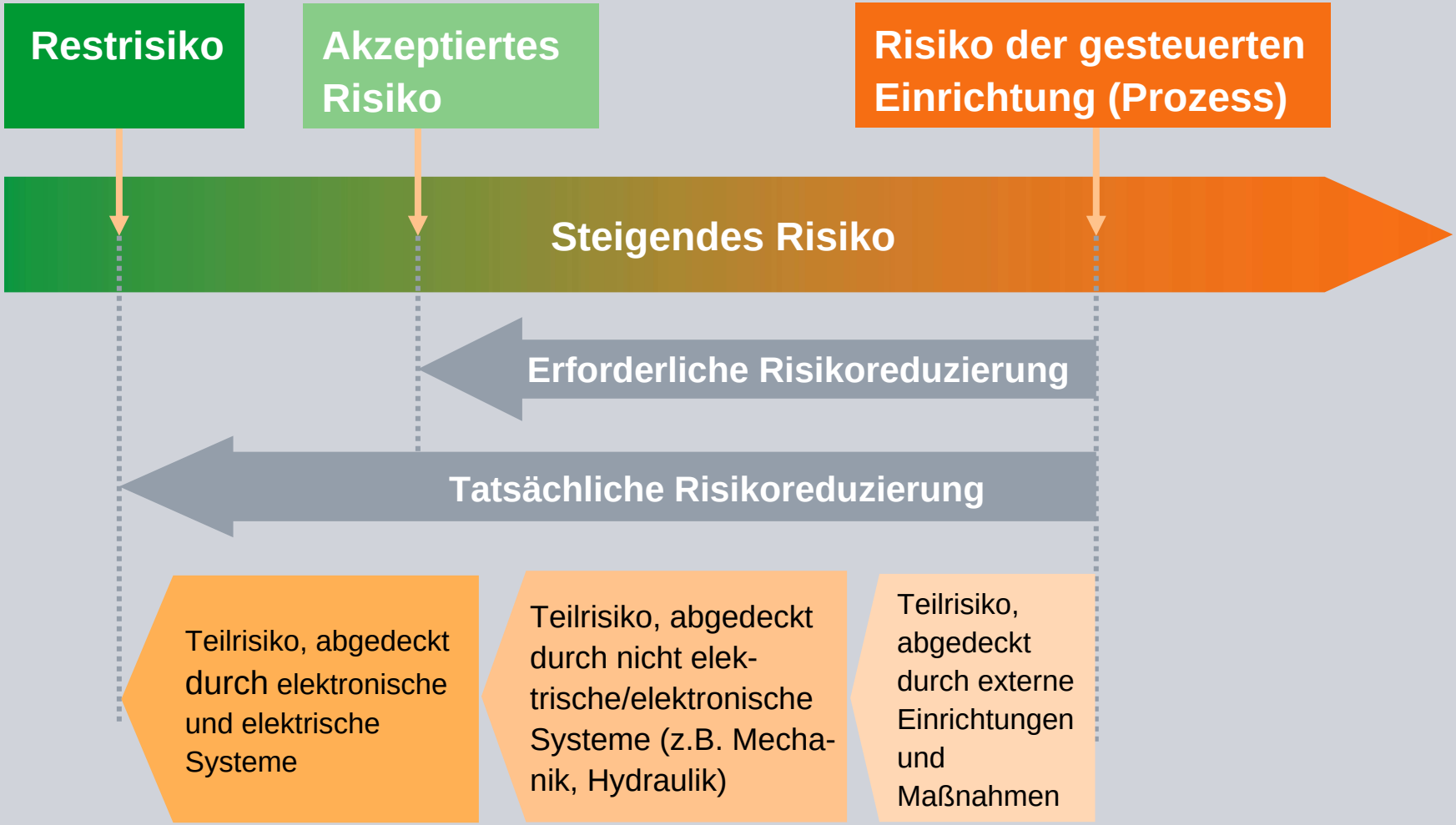
SIEMENS

Wird die Akzeptanzgrenze überschritten, so müssen Maßnahmen ergriffen werden diese zu erreichen bzw. zu unterschreiten

→ Risikoreduzierung erforderlich

Normen und Regeln der Technik beschreiben Maßnahmen zur erforderlichen Risikoreduzierung

Risikoreduzierung



Maß für die erforderliche Risikoreduzierung (IEC 61508)

SIEMENS

SIL = Safety Integrity Level

- 4-stufige Skala (SIL1 bis SIL4)
- Beschreibt das erforderliche Maß der Risikoreduzierung (SIL1 = niedrig, SIL4 = hoch)
- Ermittlung mittels anerkannter Methoden (Risikoanalyse)
- Erreicht durch die Summe von verschiedenen Maßnahmen, Methoden und Techniken

Aspekte zur Risikoreduzierung

Die Kombination aus Wahrscheinlichkeit und Schadensausmaß von gefährlichen Ereignissen darf das akzeptierte Risiko nicht überschreiten.

Anforderungen an die Zuverlässigkeit **sicherheitstechnischer Funktionen**, die zum Aufrechterhalten oder Erreichen der geforderten Sicherheit notwendig sind **= Funktionale Sicherheit**

Beherrschen von gefährlichen Ausfällen
während des Betriebes
→ **robustes Design**

Vermeiden systematischer Fehler bei Entwurf, Herstellung und Betrieb des Systems
→ **robuster Lebenszyklus**

Der „risiko-basierte Ansatz“

Die Vermeidung systematischer Fehler, sowie die Beherrschung systematischer und zufälliger Fehler in

„sicherheitstechnischen Funktionen“

senkt das zu erwartende **Risiko** auf ein akzeptiertes Maß.

Definition: Sicherheitstechnische Funktion

Abk.: SIF = Safety Instrumented Function

1. Fall:

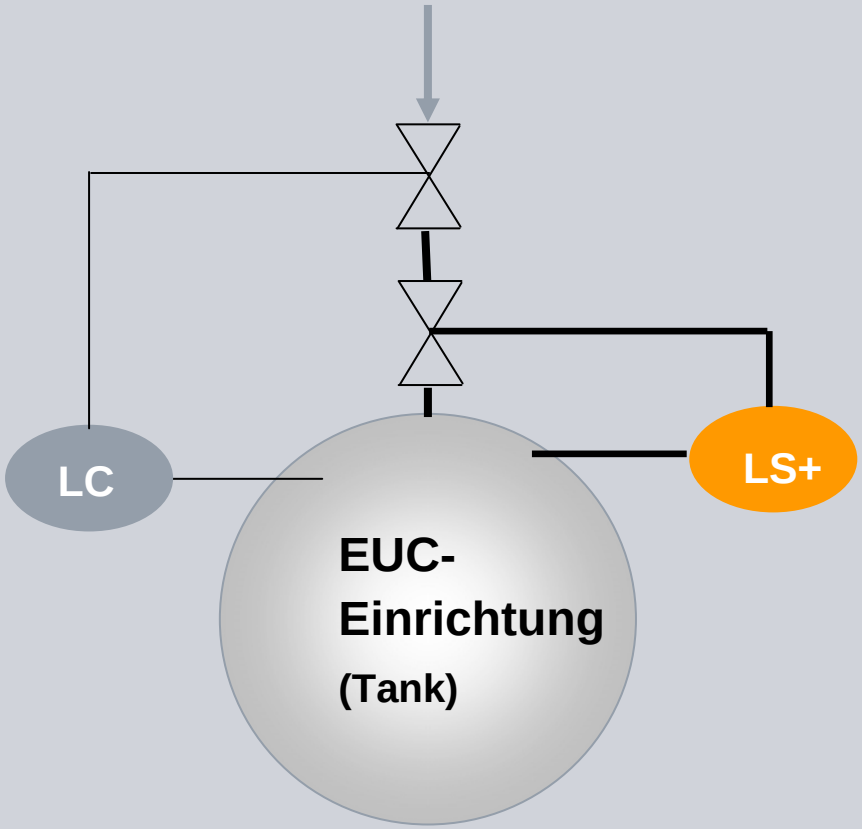
SIF
(Schutzfunktion)
Funktion überwacht und greift im Störfall ein.

EUC-Einrichtung
(Equipment Under Control)

2. Fall:

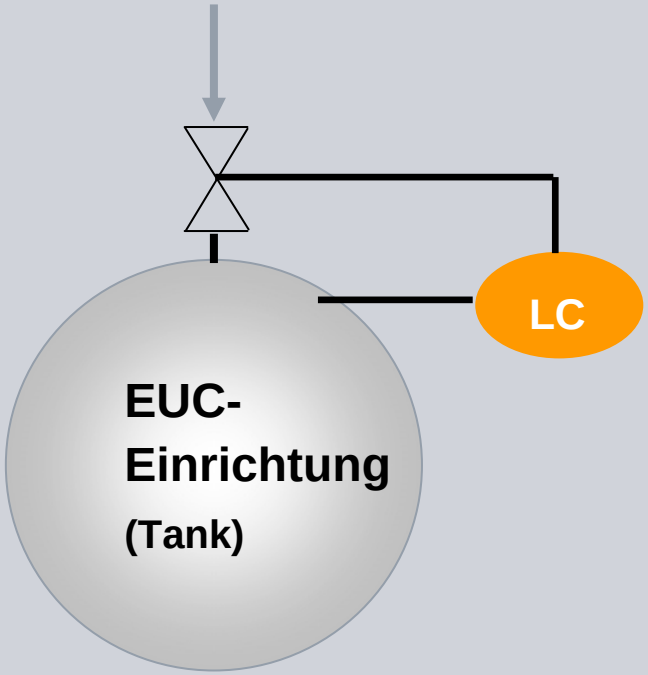
SIF
(Betriebsfunktion)
Ausgeführte Betriebsfunktion ist selbst die sicherheitstechnische Funktion (sicherheitstechnische Regelfunktion)

Beispiel: SIF (Schutzfunktion)



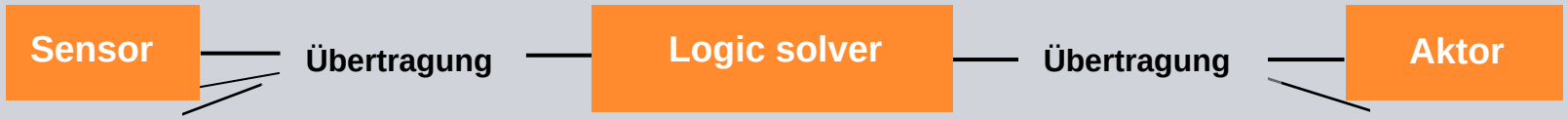
SIF:
Überwachen des Tanklevels (LS+) und schließen des Zulaufventils nur wenn Betriebseinrichtung versagt (Störung)

Beispiel: SIF (Betriebsfunktion)

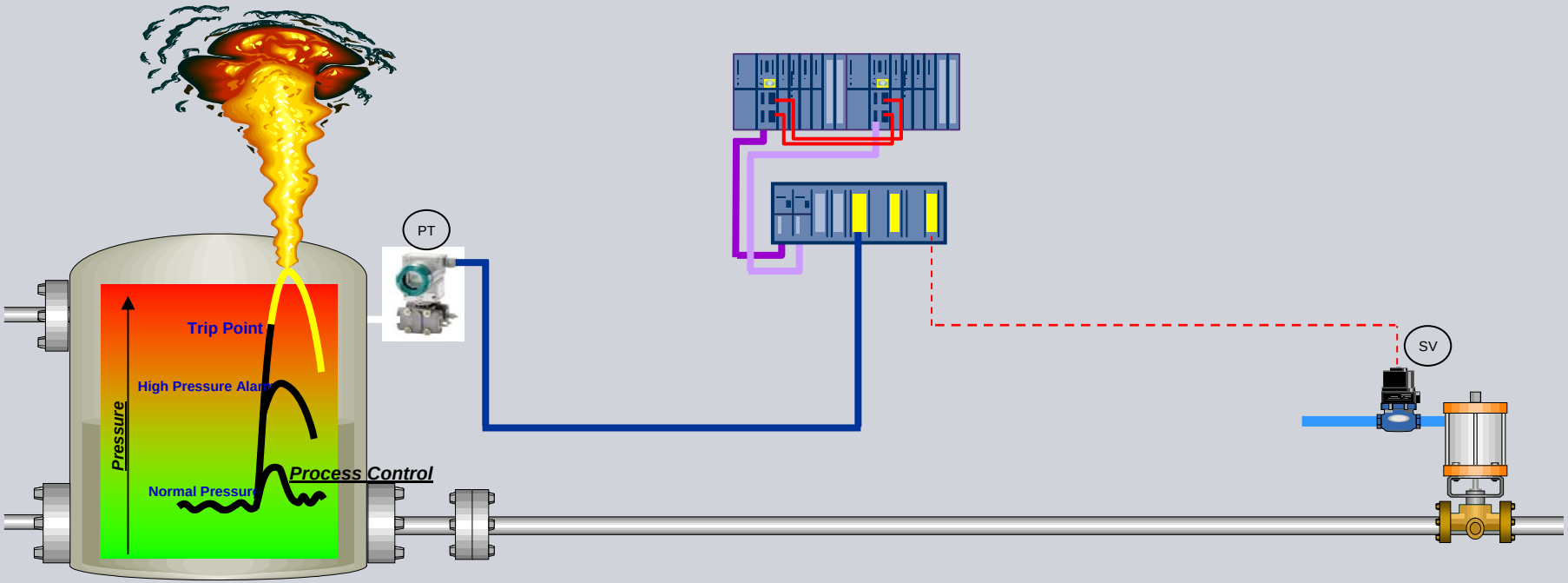


SIF:
Tanklevelregelung
ist sicherheitstechnische Regelfunktion
(Level muss in einem bestimmten
Bereich gehalten werden)

SIF Strukturierungselemente (Beispiel)



Informationen erfassen → **Informationen auswerten** → **Aktionen ausführen**



SIEMENS

Funktionale Sicherheit – Sicherh. Systeme für die Prozessindustrie

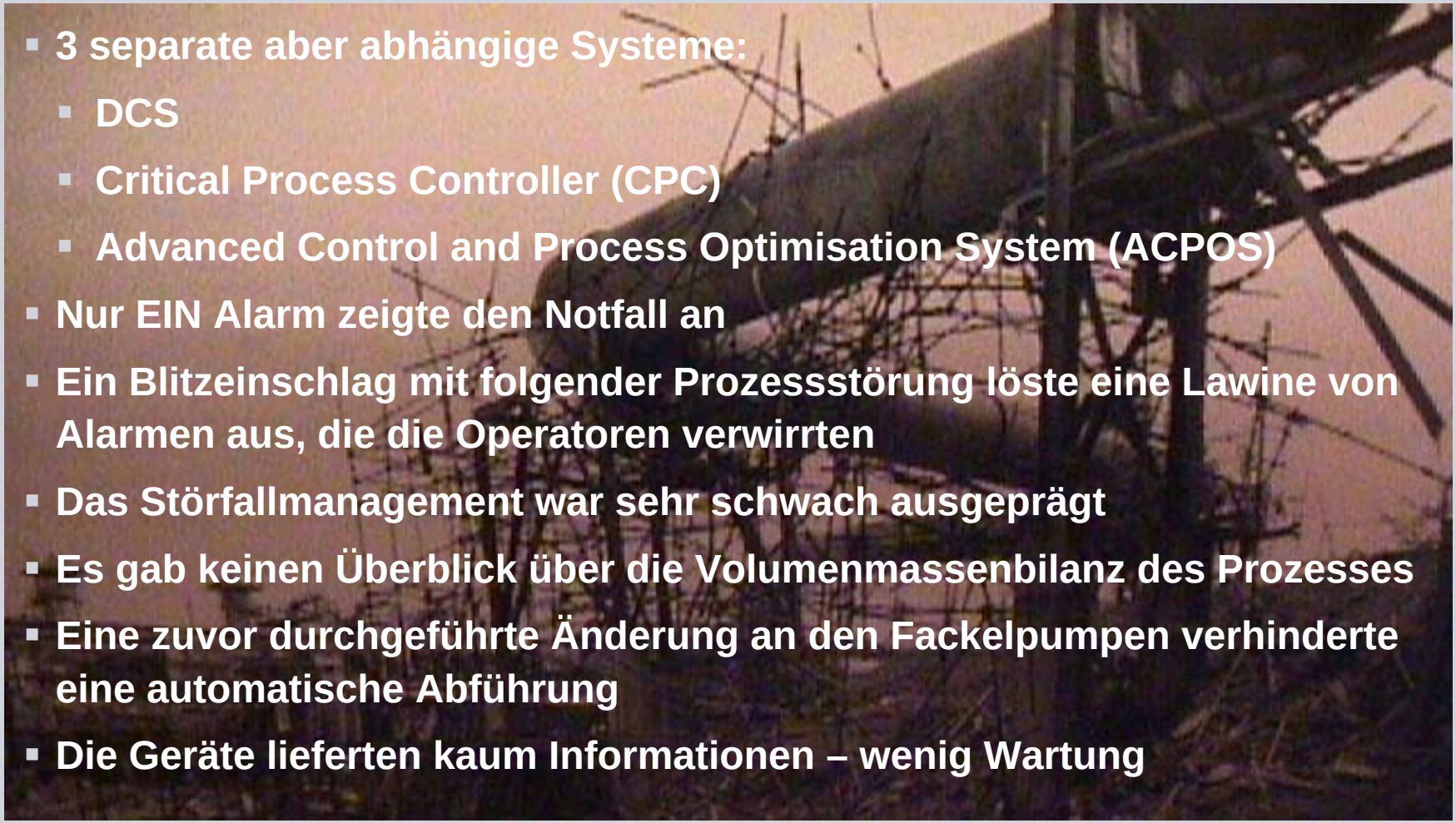
- Einführung zur Funktionalen Sicherheit
- **Überlegungen zu Unfallursachen und Produkthaftung**
- Übersicht zur IEC 61508
- Übersicht zur IEC 61511
- Management der Funktionalen Sicherheit
- Sicherheitslebenszyklus
- Zusammenstellung

Unfall in der Raffinerie Milford Haven UK – Juli 1994

SIEMENS

Unfall in der Raffinerie Milford Haven UK – Juli 1994 → Unfallursache

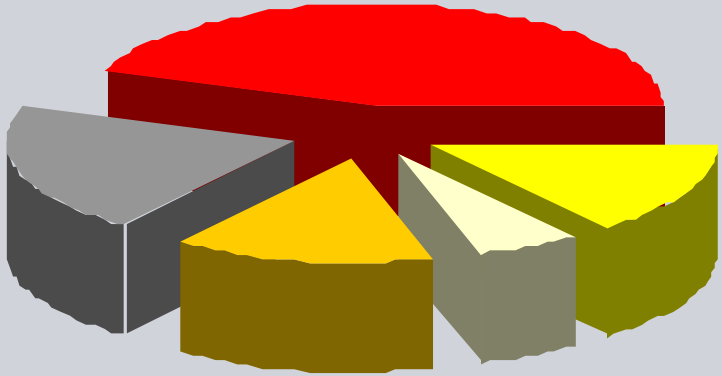
SIEMENS



- 3 separate aber abhängige Systeme:
  - DCS
  - Critical Process Controller (CPC)
  - Advanced Control and Process Optimisation System (ACPOS)
- Nur EIN Alarm zeigte den Notfall an
- Ein Blitzeinschlag mit folgender Prozessstörung löste eine Lawine von Alarmen aus, die die Operatoren verwirrten
- Das Störfallmanagement war sehr schwach ausgeprägt
- Es gab keinen Überblick über die Volumenmassenbilanz des Prozesses
- Eine zuvor durchgeführte Änderung an den Fackelpumpen verhinderte eine automatische Abführung
- Die Geräte lieferten kaum Informationen – wenig Wartung

Unfallursache
Störfallanalyse der Automatisierungssysteme

SIEMENS



Note : Based on 34 investigated incidents in the UK
Health and Safety Executive (GB): Out of Control. Why control systems go wrong and how to prevent failure. HSE Books 1995

Rechtslage

Sicherheitstechnische Funktionen

Gesetzliche Anforderungen für die Zulassung

Anforderungen aus Produkthaftungssicht (Stand der Technik)

Gesetzliche Anforderungen in der Prozessindustrie

Gesetze und Vorschriften müssen erfüllt werden, um die Zulassung für den Betrieb zu erwirken und aufrechtzuerhalten

Beispiele: (länderspezifisch)

Seveso-II-Richtlinie 96/82/EG	**Richtlinie 96/82/EG des Rates vom 9. Dezember 1996 zur Beherrschung der Gefahren bei schweren Unfällen mit gefährlichen Stoffen**
Bundes-Immis-sionsschutzgesetz: BImSchG.	**Gesetz zum Schutz vor schädlichen Umwelteinwirkungen durch Luftverunreinigungen, Geräusche, Erschütterungen und ähnliche ….**

Auslöser

Giftgasunfall in Chemieanlage in Seveso, Italien am 10. Juli 1976

Freisetzung von 2 kg hoch giftigen Dioxins

Auswirkungen:

- Schwere Verletzungen, Totgeburten und Tausende toter Tiere
- Bisher ca. 150 Mio € an gezahlten Entschädigungen

Explosion in BP Raffinerie Texas City, USA am 23. März 2005

Auswirkungen:

- 15 Tote und 170 Verletzte

Tankfarm Buncefield, 40 km nordwestlich von London, UK am 13. Dezember 2005

Eine Serie von Explosionen und darauf folgendem Feuer. Es dauerte zwei Tage um das Feuer in den betroffenen Tanks zu löschen.

Auswirkungen:

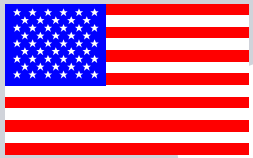
- 45 Verletzte, davon 2 schwer
- Schadensersatzansprüche von mehr als 700 Mio £

Anforderungen aus Produkthaftungssicht

„... Stand der Technik zum Zeitpunkt des Inverkehrbringens (=Inbetriebnahme) …“ ist relevant bei der Beurteilung in Produkthaftungsfällen

ProdHaftG

HSE
PES



ISA
S84

EWICS

DIN V 19250

DINV VDE0801

Arbeitsgruppen und nationale Normungsgremien waren an der Entwicklung einer weltweit gültigen Grundnorm für die Sicherheitstechnik beteiligt

Internationale Sicherheitsnormen beschreiben den Stand der Technik

SIEMENS

IEC Commission Electrotechnique Internationale International Electrotechnical Commission Международная Электротехническая Комиссия

IEC61508

Gültig für alle Industriebereiche

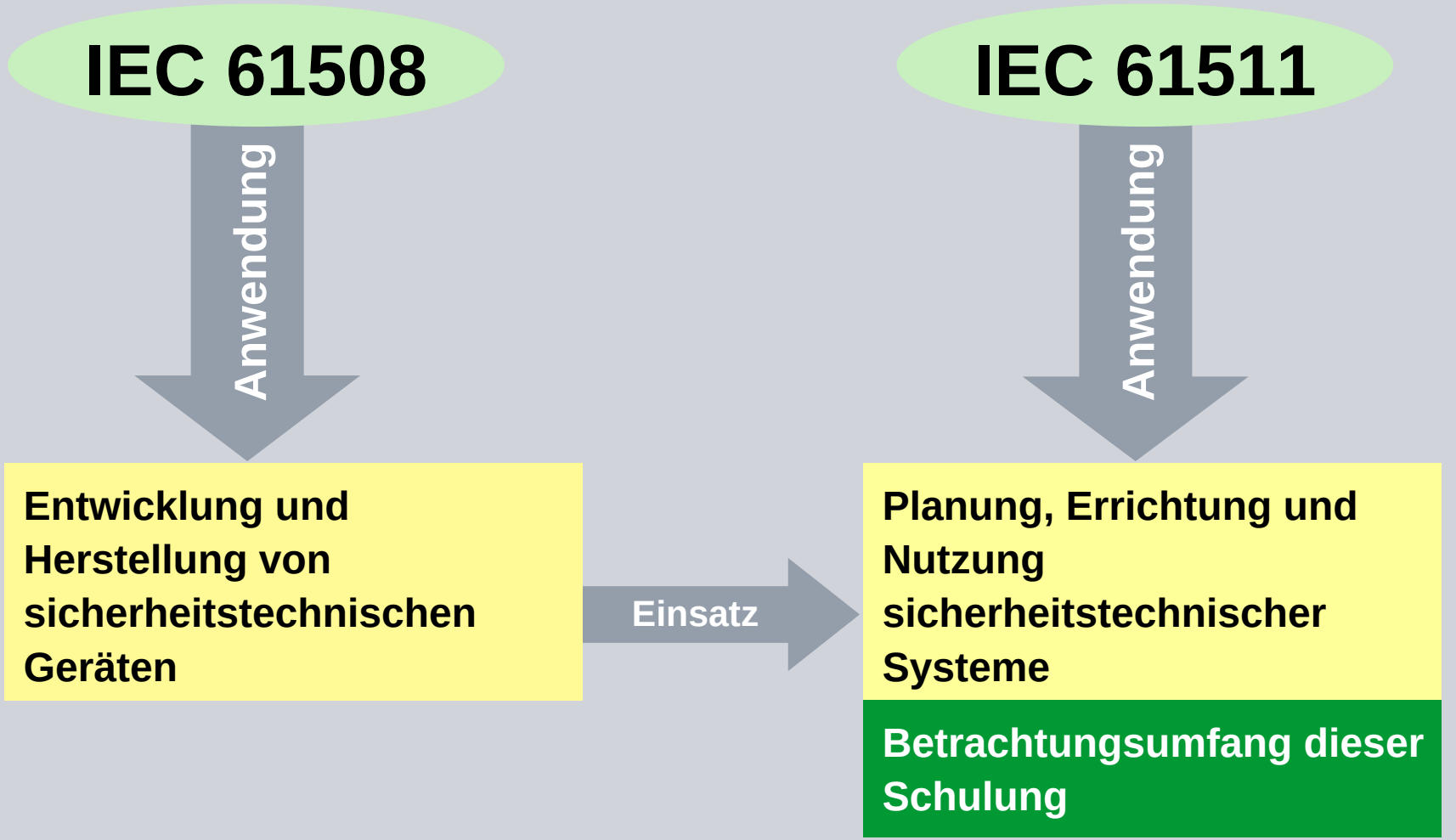
IEC Commission Electrotechnique Internationale International Electrotechnical Commission Международная Электротехническая Комиссия

IEC61511

Gültig für die Prozessindustrie

SIEMENS

Beziehung zwischen IEC 61508 und IEC 61511



Betrachtungsumfang

Funktionale Sicherheit

Vermeiden systematischer Fehler bei Entwurf, Herstellung und Betrieb sicherheitstechn. Funktionen

→ **robuster Prozess**

Beherrschen von gefährlichen Ausfällen während des Betriebes sicherheitstechnischer Funktionen

→ **robustes Design**

Anforderungen an die Planungsabläufe und Methoden

- **Kapitel 5:**
  Management der Funktionalen Sicherheit (FSM)
- **Kapitel 6:**
  Sicherheitslebenszyklus

Anforderungen an die technische Ausführung

- **Kapitel 6.4.1:**
  Architektur und HW-Zuverlässigkeit
- **Kapitel 6.4.2:**
  Anwendersoftware

SIEMENS

Funktionale Sicherheit – Sicherh. Systeme für die Prozessindustrie

- Einführung zur Funktionalen Sicherheit
- Überlegungen zu Unfallursachen und Produkthaftung
- Übersicht zur IEC 61508
- Übersicht zur IEC 61511
- **Management der Funktionalen Sicherheit**
- Sicherheitslebenszyklus
- Zusammenstellung

SIEMENS

Ziel des Managements der Funktionalen Sicherheit

Abk.: FSM = Functional Safety Management

Das FSM stellt den organisatorischen Rahmen zur

- Einführung,
- Aufrechterhaltung und
- Sicherstellung

aller **prozesstechnischen** und **technischen** Methoden und Maßnahmen dar, welche zur Erreichung der geforderten Funktionalen Sicherheit von sicherheitstechnischen Funktionen benötigt werden.

Aspekte zum FSM

Abk.: FSM = Functional Safety Management

- FSM-Struktur (FSM-System)
- Aufgaben des FSM
- Verifikation
- Beurteilung der Funktionalen Sicherheit

FSM-Struktur

	Projekt (Planung und Errichtung von sicherheitstechnischen Funktionen)	Betrieb (Betrieb und Instandhaltung von sicherheitstechnischen Funktionen)
FSM Ebene 1: projekt- / anlagenunabhängiges FSM	Übergeordnetes FSM der Planungsfirma	Übergeordnetes FSM des Betreibers
FSM Ebene 2: projekt- / anlagenabhängiges FSM	Projektspezifisches FSM (je Projekt)	Anlagenspezifisches FSM (je Anlage)

Aufgaben des FSM
(Ebene 1: projekt- / anlagenunabhängig)

SIEMENS

Projekt	Betrieb
Pflege und Verbesserung eines generischen Sicherheitsprozesses zur Planung sicherheitstechnischer Funktionen	Pflege und Verbesserung eines generischen Sicherheitsprozesses für Betrieb und Wartung sicherheitstechn. Funktionen
Überwachung des generischen Sicherheitsprozesses (Audits)	
	Beobachtung und Analyse von Fehlern im Betrieb, Vergleich mit den errechneten Werten aus der Planung
Ausbildungsplan für das Personal (Funktionale Sicherheit)	
Installation und Bewahrung eines Modifikationsprozesses während der Planung und Errichtung von Anlagen	Installation und Bewahrung eines Modifikationsprozesses während der Betriebes und der Wartung von Anlagen

Aufgaben des FSM
(Ebene 2: projekt- / anlagenabhängig)

SIEMENS

Projekt	Betrieb
Festlegung der durchzuführenden Planungsschritte gem. Sicherheitsprozess	Festlegung der durchzuführenden Sicherheitsaktivitäten während Betrieb und Wartung
Festlegung von Personen und deren Aktivitäten zur Funktionalen Sicherheit im Rahmen des Planungsprozesses	Festlegung von Personen und deren Aktivitäten zur Funktionalen Sicherheit im Rahmen des Betriebs- und Wartungsprozesses
Planung und Durchführung der Aktivitäten zur Beurteilung der Funktionalen Sicherheit (Safety Assessment s.a. folgende Seiten)	
Planung der Aktivitäten zur Verifikation und Validierung (FAT, SAT)	Planung der Aktivitäten zur Verifikation und Validierung (Proof Test)

Verifikation – Validierung

Verifikation

Tätigkeit, mittels Analyse und/oder Tests für jede Phase des Sicherheitslebenszyklus zu demonstrieren, dass die Ergebnisse der entsprechenden Phase den Zielen und Anforderungen für diese Phase entsprechen.

Validierung

Tätigkeit, mittels Tests zu demonstrieren, dass das sicherheitsrelevante System vor oder nach der Installation den Anforderungen der Sicherheitsspezifikation (SRS) entspricht.

Verifikation – Anforderungen

- Für jede Phase des Sicherheitslebenszyklus müssen die Verifikationsaktivitäten geplant werden.

- Als Nachweis, dass die jeweilige Phase zufriedenstellend verifiziert wurde, sind Informationen zu sammeln und zu dokumentieren.

Verifikation – Umsetzung

Verfahrensanweisung zum Verifikationsprozess (evtl. Erweiterung des Standard-Verfikationsprozesses)

Konkrete Planung im Safety-Plan

- Verantwortung
- Tätigkeit (Methodik)
- Dokumentation

Beurteilung der Funktionalen Sicherheit – Anforderungen

SIEMENS

engl.: Safety Assessment

- Festlegung von einer oder mehrerer Personen und/oder Organisationen, die die Beurteilung der Funktionalen Sicherheit durchführen. Mindestens eine vom Projekt unabhängige Person muss im Beurteilungsteam enthalten sein.

- Festlegung der Tätigkeiten zur Beurteilung der Funktionalen Sicherheit (i. Allg. Checklisten, Audits)

SIEMENS

Verfahrensanweisung zum Beurteilungsprozess (evtl. Erweiterung des Auditierungsprozesses)

Konkrete Planung im Safety-Plan

- Verantwortung
- Tätigkeit (Methodik)
- Dokumentation

Umsetzung FSM

FSM als Firmenstandard

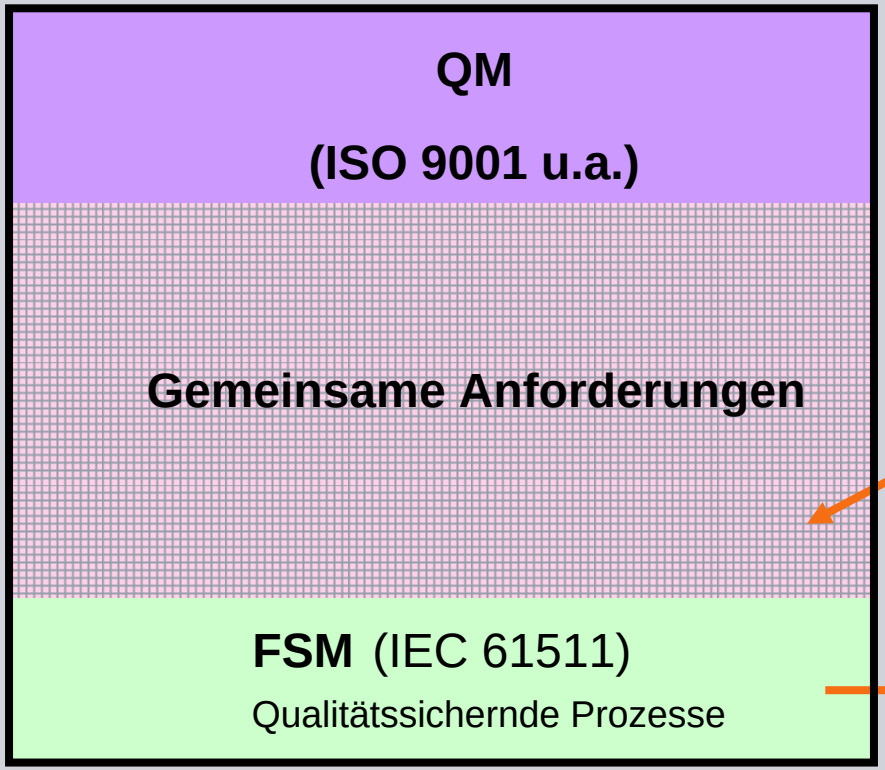
→ Integration innerhalb QM (Add on)

FSM auf Projekt- / Anlagenebene

→ **projekt- / anlagenspezifischer Safety-Plan**

FSM als Firmenstandard

Analyse der installierten QM-Prozesse (Gap Analysis)



Identifikation der Überschneidungen

z.B. Personalschulung, interne Audits, Dokumentenlenkung, Instandhaltung, Fehleranalyse etc.

Integration der „Add ons“ in das QM-System

FSM auf Projekt- / Anlagenebene

Installation eines geeigneten Planungs- und Überwachungsinstrumentes für Planungs-, Betriebs- und Wartungsphase

Einführung eines projektspezifischen **Safety-Plans** mit folgenden Inhalten:

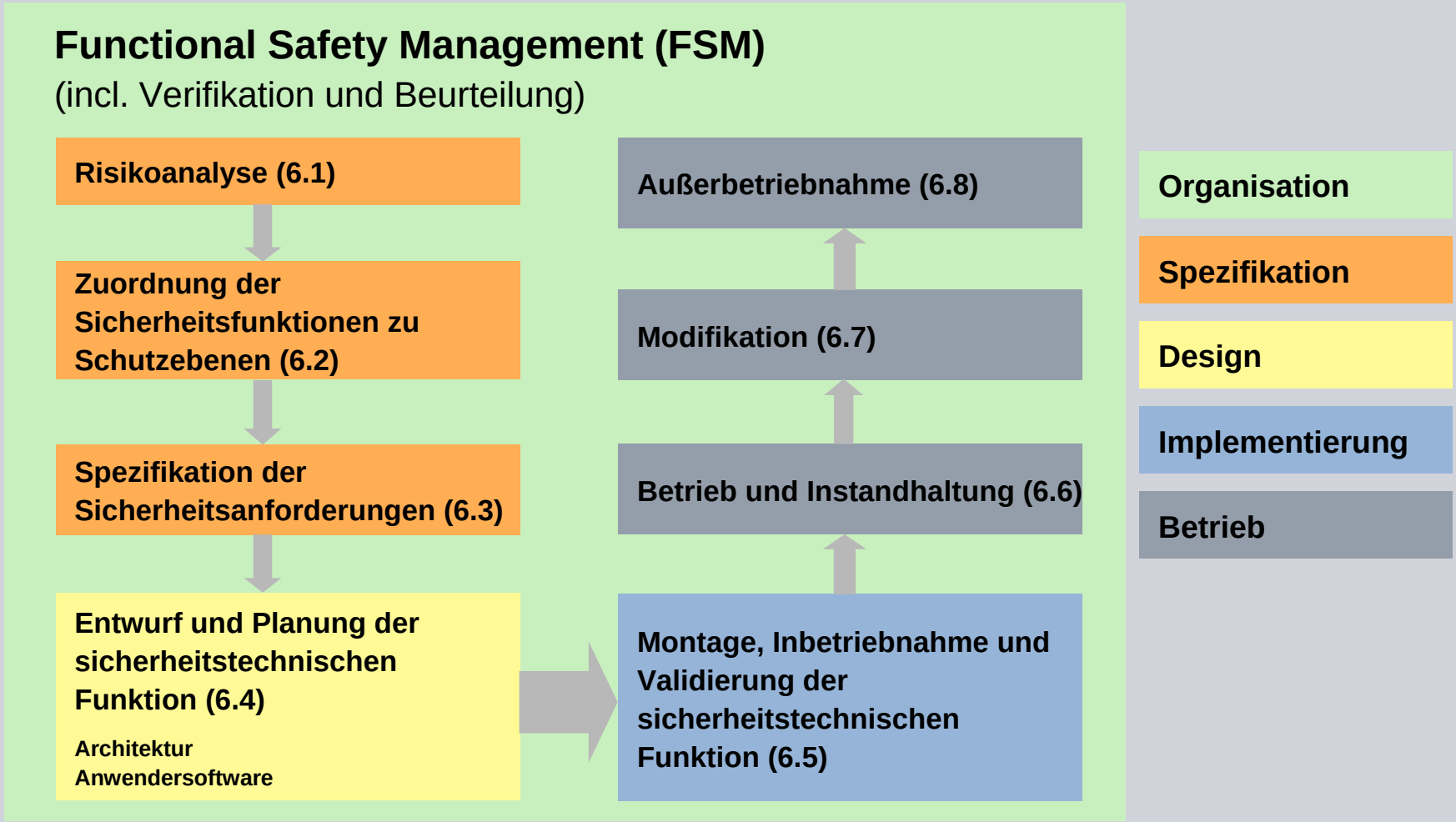
- Festlegung der Sicherheitsaktivitäten (Planung, Betrieb, Wartung)
- Referenzen zu den einschlägigen QM-Richtlinien
- Verantwortliche Abteilungen und Personen
- Verwendete Hilfsmittel und deren Qualifizierung
- Planung der Beurteilung, Verifikation und Validierung
- Planung der zu erstellenden Dokumentation
- ...

SIEMENS

Funktionale Sicherheit – Sicherh. Systeme für die Prozessindustrie

- Einführung zur Funktionalen Sicherheit
- Überlegungen zu Unfallursachen und Produkthaftung
- Übersicht zur IEC 61508
- Übersicht zur IEC 61511
- Management der Funktionalen Sicherheit
- **Sicherheitslebenszyklus**
- Zusammenstellung

Gesamter Sicherheitslebenszyklus nach IEC 61511



Übersicht Sicherheitslebenszyklus

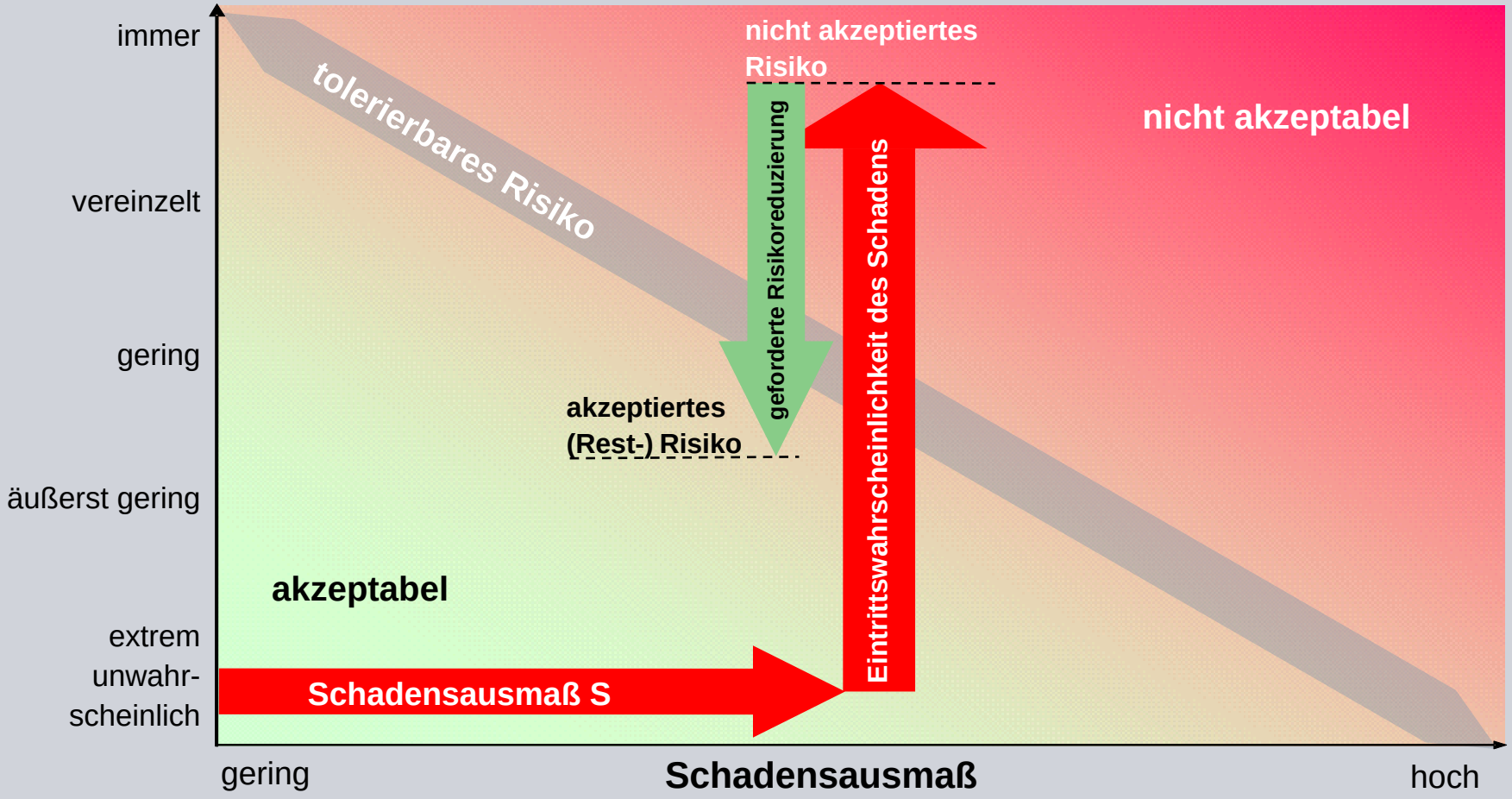
- **6.1 Risikoanalyse**
- 6.2 Zuordnung der Sicherheitsfunktion zu den Schutzebenen
- 6.3 Spezifikation der Sicherheitsanforderungen
- 6.4 Entwurf und Planung der sicherheitstechnischen Funktion
  - 6.4.1 Architektur und HW-Zuverlässigkeit
  - 6.4.2 Anwendungssoftware
- 6.5 Montage und Inbetriebnahme
- 6.6 Betrieb und Instandhaltung
- 6.7 Modifikation
- 6.8 Außerbetriebnahme

Ziel der Risikoanalyse

Ziele der Risikoanalyse sind:

- Ermittlung der Gefahren und der gefahrbringenden Ereignisse des Prozesses und der zugehörigen Betriebsmittel
- Ermittlung der Ereigniskette, die zu einem gefahrbringenden Ereignis führen kann
- Bestimmung des Prozessrisikos
- Aufstellung aller Anforderungen zur Risikoreduzierung
- Bestimmung der erforderlichen sicherheitstechnischen Funktionen zur Erreichung der geforderten Risikoreduzierung

Vorgehen bei der Risikoanalyse



Vorgehen bei der Risikoanalyse

- Identifikation der möglichen Gefahren
- Bestimmung des möglichen Schadensausmaßes (Konsequenz)
- Frage: Ist das zu erwartende Schadensausmaß akzeptabel? (Wahrscheinlichkeit?)
- Spezifikation der Maßnahmen zur Risikoreduzierung

Process Hazard Analysis (PHA)

Hinweis: HAZOP (Hazard and Operability Analysis) ist die meist verbreitete Methode für die Risikoanalyse von Prozessanlagen

Übersicht Sicherheitslebenszyklus

SIEMENS

- 6.1 Risikoanalyse
- **6.2 Zuordnung der Sicherheitsfunktion zu den Schutzebenen**
- 6.3 Spezifikation der Sicherheitsanforderungen
- 6.4 Entwurf und Planung der sicherheitstechnischen Funktion
  - 6.4.1 Architektur und HW-Zuverlässigkeit
  - 6.4.2 Anwendungssoftware
- 6.5 Montage und Inbetriebnahme
- 6.6 Betrieb und Instandhaltung
- 6.7 Modifikation
- 6.8 Außerbetriebnahme

Ziele der Zuordnung

Ziele der Zuordnung von Sicherheitsfunktionen zu Schutzebenen:

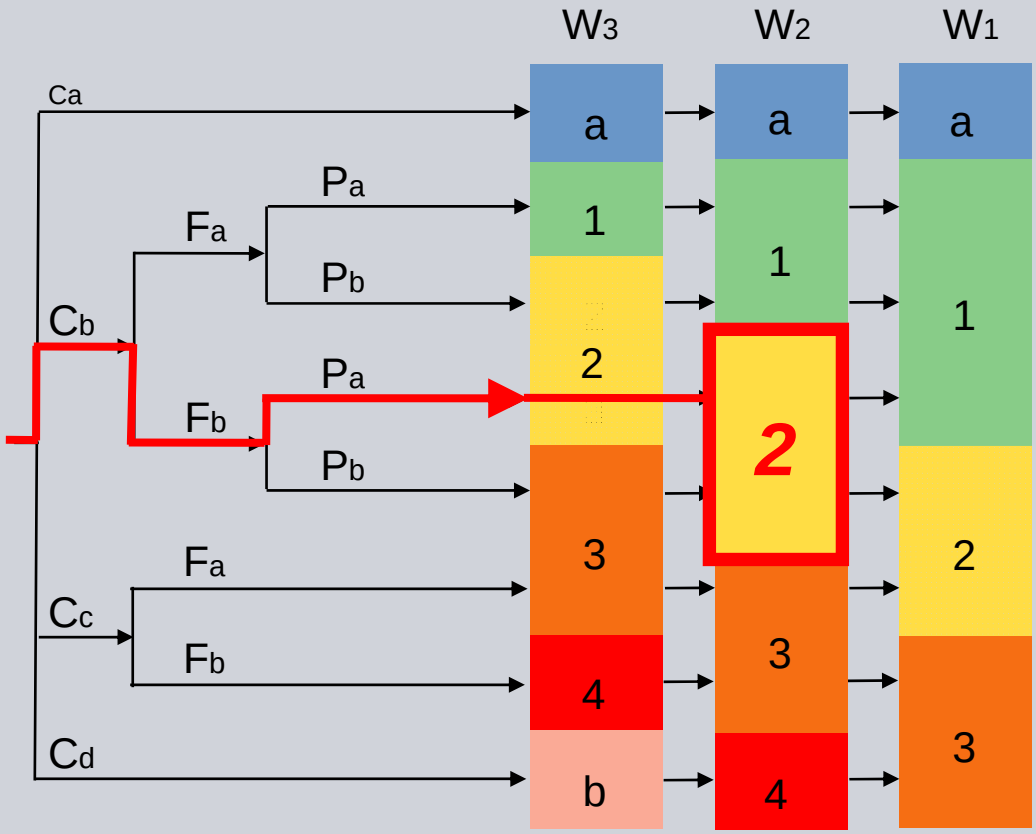
- Bestimmung, des Anteils der Risikoreduzierung jeder Maßnahme an der gesamten Risikoreduzierung

Methode: Layer of Protection Analysis (LOPA)

- Festlegung des jeweiligen Sicherheits-Integritätslevels zu jeder sicherheitstechnischen Funktion

Methode: Risikograph

Beispiel Ableitung SIL aus Risikograph



Safety Integrity Levels SIL

a = no special safety requirements
b = single safety system not sufficient

Consequence

Ca light injury
Cb serious permanent injury or death of one person
Cc death of several persons
Cd death of very many persons

Frequency and duration of stay

Fa rare to more frequent
Fb frequent to permanent

Risk Prevention

Pa possible under certain conditions
Pb almost impossible

Probability of Occurrence

W1 very slight
W2 slight
W3 relativ high

Übersicht Sicherheitslebenszyklus

SIEMENS

- 6.1 Risikoanalyse
- 6.2 Zuordnung der Sicherheitsfunktion zu den Schutzebenen
- **6.3 Spezifikation der Sicherheitsanforderungen**
- 6.4 Entwurf und Planung der sicherheitstechnischen Funktion
  - 6.4.1 Architektur und HW-Zuverlässigkeit
  - 6.4.2 Anwendungssoftware
- 6.5 Montage und Inbetriebnahme
- 6.6 Betrieb und Instandhaltung
- 6.7 Modifikation
- 6.8 Außerbetriebnahme

Spezifikation der Sicherheitsanforderungen

SIEMENS

Abk: SRS = Safety Requirements Specification

Spezifikation der Sicherheitsanforderungen

Anforderungen an die Sicherheitsfunktion

Anforderungen an die Sicherheitsintegrität

Alle für das Design von sicherheitstechnischen Funktionen erforderlichen Anforderungen sind zu spezifizieren

SRS – Anforderungen an die Sicherheitsfunktion

Beschreibung der sicherheitstechnischen Funktion(en)

→ R&I-Schema, Cause & Effect Diagrams, Prosatext

Definition des “Sicheren Zustandes”

→ Aufstellung der sicheren Prozesszustände, die durch die sicherheitstechnischen Funktionen erreicht werden sollen

Erforderliche Reaktionszeit zur Ereichung des sicheren Zustandes

→ erforderliche Zykluszeiten

Beschreibung der Mess-Signale und Grenzwerte

→ Instrumentenlisten, Alarm- und Schaltpunktlisten

Erforderliche Kriterien zur Erfüllung der sicherheitstechnischen Funktion

→ z. B. dichtes Schließen von Ventilen

SRS – Anforderungen an die Sicherheitsfunktion

Betriebliche Anforderungen

→ z. B. An- und Abfahren im Handbetrieb, Zurücksetzen nach Abschaltung,

Reaktion im Falle eines entdeckten Fehlers

Schnittstellen zu anderen betrieblichen Einrichtungen

→ z. B. Protokollierung

Mögliche gefahrbringende Kombinationen von Ausgangszuständen

Extremwerte aller Umweltbedingungen

→ EMV, Ex-Zonen, IP-Schutz etc.

SRS – Anforderungen an die Sicherheitsintegrität

Sicherheitsintegritätslevel (SIL) je sicherheitstechnischer Funktion

Geschätzte Rate der Anforderungen an die sicherheitstechnischen Funktionen und deren Auslöser

Anforderungen an das Intervall der Wiederholungsprüfungen (Proof-Testintervall T1)

→ Einfluss auf die Ausfallwahrscheinlichkeit (s. a. Kapitel 6.4.1)

Mittlere Reparaturzeit (MTTR = Mean Time To Reparation)

→ Einfluss auf die Ausfallwahrscheinlichkeit (s. a. Kapitel 6.4.1)

Übersicht Sicherheitslebenszyklus

SIEMENS

- 6.1 Risikoanalyse
- 6.2 Zuordnung der Sicherheitsfunktion zu den Schutzebenen
- 6.3 Spezifikation der Sicherheitsanforderungen
- **6.4 Entwurf und Planung der sicherheitstechnischen Funktion**
  - 6.4.1 Architektur und HW-Zuverlässigkeit
  - 6.4.2 Anwendungssoftware
- 6.5 Montage und Inbetriebnahme
- 6.6 Betrieb und Instandhaltung
- 6.7 Modifikation
- 6.8 Außerbetriebnahme

Entwurf und Planung (Design)

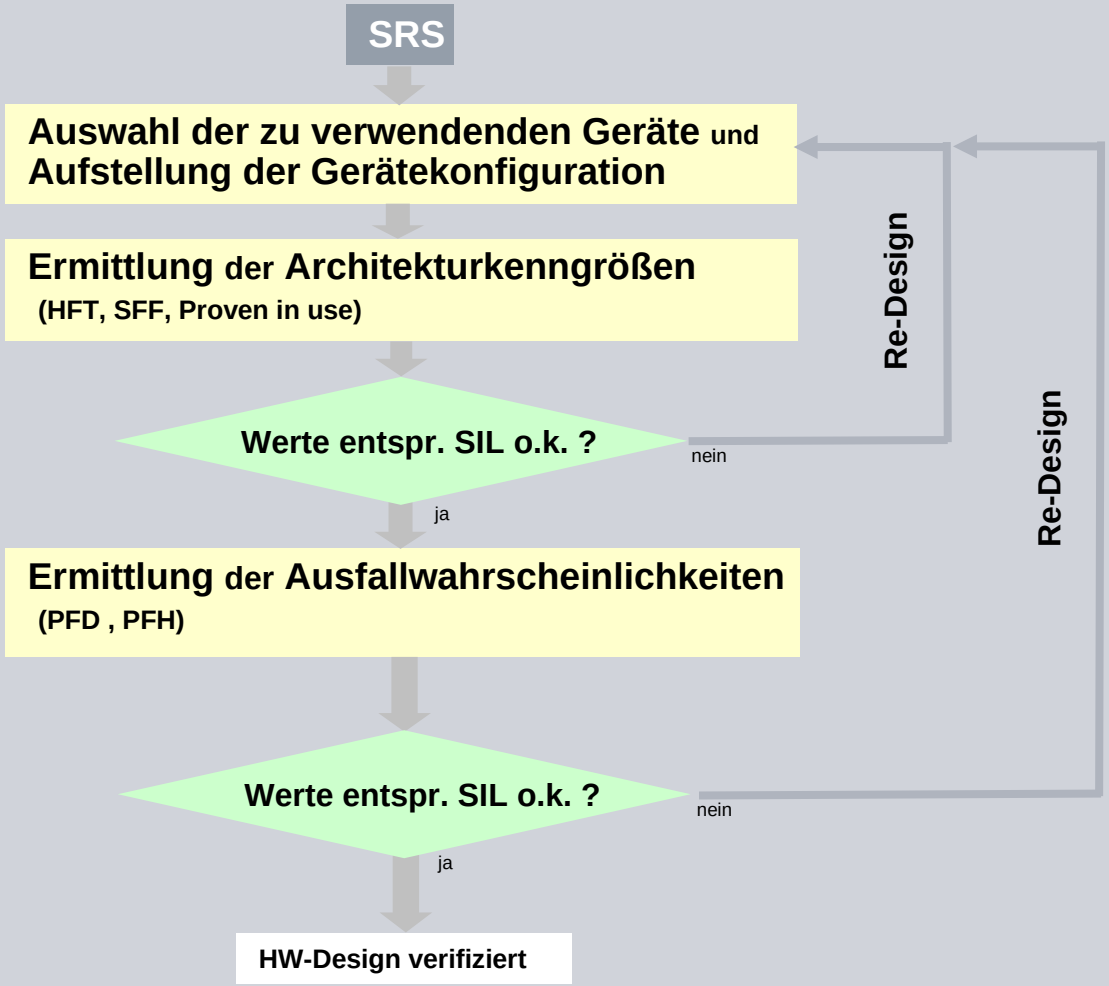
Spezifikation der Sicherheitsanforderungen

Design

Hardware	**Software**
▪ Architektur ▪ Zuverlässigkeit	▪ Anwendungssoftware ▪ Software-Hilfsmittel ▪ Embedded Software

Factory Acceptance Test (FAT)

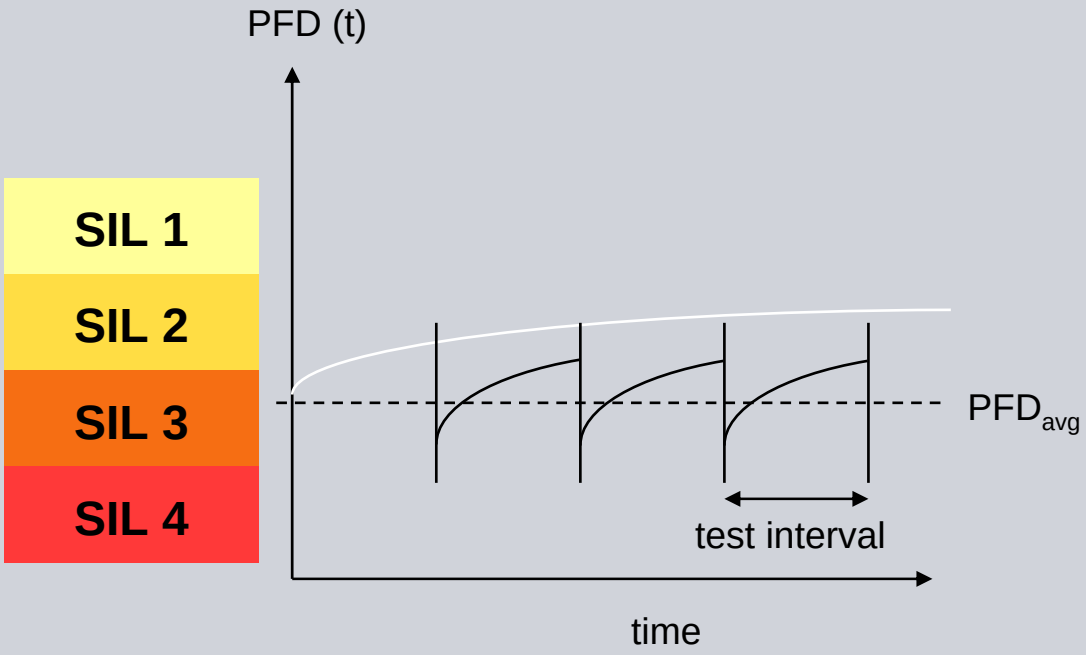
Typisches Vorgehen beim Design der Hardware



Was ist PFD?

Mit PFD wird die mittlere Ausfallwahrscheinlichkeit (PFDavg) bei Anforderung einer sicherheitstechnischen Funktion bezeichnet

Entsprechend SIL-Anforderung muss der PFD in einem bestimmten Intervall liegen muss.



Ausfallgrenzwerte PFD

Sicherheits-Integritätslevel: Ausfallgrenzwerte für eine Sicherheitsfunktion, die in der Betriebsart mit niedriger Anforderungsrate betrieben wird

Sicherheits-Integritätslevel	**Betriebsart mit niedriger Anforderungsrate** (mittlere Wahrscheinlichkeit eines Ausfalls der entworfenen Funktion bei Anforderung)
4	$\geq 10^{-5}$ bis $< 10^{-4}$
3	$\geq 10^{-4}$ bis $< 10^{-3}$
2	$\geq 10^{-3}$ bis $< 10^{-2}$
1	$\geq 10^{-2}$ bis $< 10^{-1}$

Definition: Betriebsart mit niedriger Anforderungsrate
Anforderung des sicherheitsbezogenen Systems nicht mehr als einmal pro Jahr und nicht größer als die doppelte Frequenz der Wiederholungsprüfungen

Grenzwerte für PFD (Average)

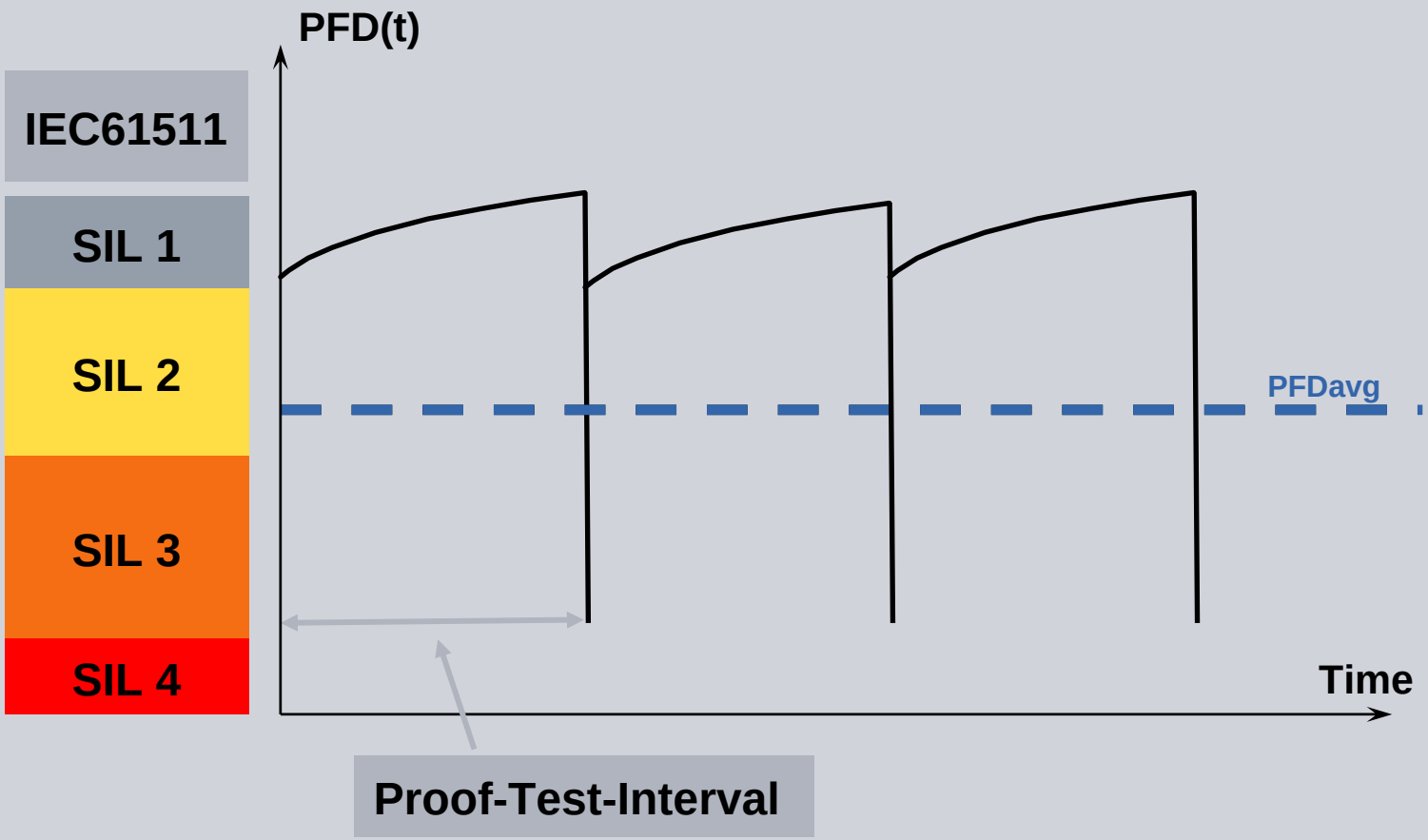
Abstand zw. Wiederholungsprüfungen (T_1)

Norm: Proof-Test-Interval

- **Zeitraum zwischen Wiederholungsprüfungen zur Aufdeckung „schlafender“ unerkannter Fehler.**
- **Angabe in Stunden [h]**
- **Wiederholungsprüfungen sollen das sicherheitsbezogene System möglichst nahe an den „Wie neu“-Zustand heranbringen.**

Proof-Test-Intervall
– Graphische Darstellung

SIEMENS

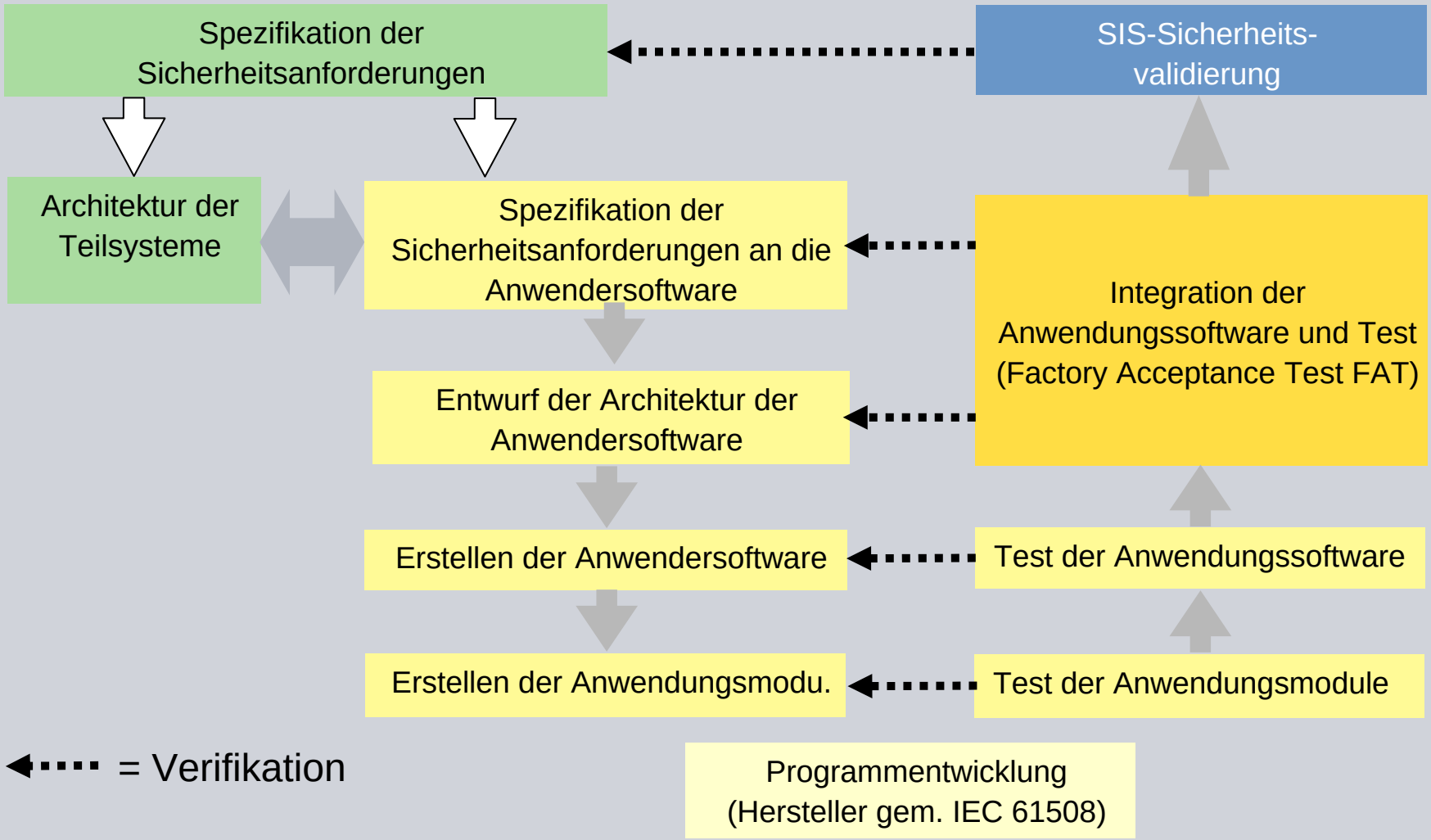


Übersicht Sicherheitslebenszyklus

SIEMENS

- **6.1** Risikoanalyse
- **6.2** Zuordnung der Sicherheitsfunktion zu den Schutzebenen
- **6.3** Spezifikation der Sicherheitsanforderungen
- **6.4 Entwurf und Planung der sicherheitstechnischen Funktion**
  - 6.4.1 Architektur und HW-Zuverlässigkeit
  - **6.4.2 Anwendungssoftware**
- **6.5** Montage und Inbetriebnahme
- **6.6** Betrieb und Instandhaltung
- **6.7** Modifikation
- **6.8** Außerbetriebnahme

Sicherheitslebenszyklus der Software



SIEMENS

Factory Acceptance Test (FAT)

Der FAT beschreibt den Integrationstest von HW und Anwender-SW, und wird deshalb auch als Systemabnahme bezeichnet

Aufgaben des FAT sind:

- Test von HW und Anwendersoftware vor Installation in der Zielanlage bzw. Ziel-SIF
- SW-Funktionen (Logik) kann bereits hier validiert werden. Dann sind entsprechend die Regeln der Validierung anzuwenden (Dokumentation)
- Möglichkeit Betriebspersonal miteinzubeziehen und damit auf spätere Bedienung vorzubereiten
- Übergabe (=Abnahme) des Teilsystems (i. Allg. Logiksystem) durch den Herstellers bzw. verantwortlichen Applikateur an den für die Montage und Inbetriebnahme verantwortlichen Partner (z. B. Kunde)

Übersicht Sicherheitslebenszyklus

SIEMENS

- 6.1 Risikoanalyse
- 6.2 Zuordnung der Sicherheitsfunktion zu den Schutzebenen
- 6.3 Spezifikation der Sicherheitsanforderungen
- 6.4 Entwurf und Planung der sicherheitstechnischen Funktion
  - 6.4.1 Architektur und HW-Zuverlässigkeit
  - 6.4.2 Anwendungssoftware
- **6.5 Montage und Inbetriebnahme**
- 6.6 Betrieb und Instandhaltung
- 6.7 Modifikation
- 6.8 Außerbetriebnahme

Validierung der sicherheitstechnischen Funktionen

Aspekte:

- Die Validierung entspricht dem erstmaligen “Proof-Test”
- Es werden die Sicherheitsanforderungen aus der SRS mittels Test bestätigt
- Die Validierung muss abgeschlossen sein, bevor die Anlage in Betrieb geht
- Die Validierung muss dokumentiert werden (Testprotokolle)
- Schnittstelle von Planung/Errichtung zu Betrieb

Link: Beipiel “Proof Test Protokoll”

Übersicht Sicherheitslebenszyklus

SIEMENS

- 6.1 Risikoanalyse
- 6.2 Zuordnung der Sicherheitsfunktion zu den Schutzebenen
- 6.3 Spezifikation der Sicherheitsanforderungen
- 6.4 Entwurf und Planung der sicherheitstechnischen Funktion
  - 6.4.1 Architektur und HW-Zuverlässigkeit
  - 6.4.2 Anwendungssoftware
- 6.5 Montage und Inbetriebnahme
- **6.6 Betrieb und Instandhaltung**
- 6.7 Modifikation
- 6.8 Außerbetriebnahme

Betrieb und Instandhaltung

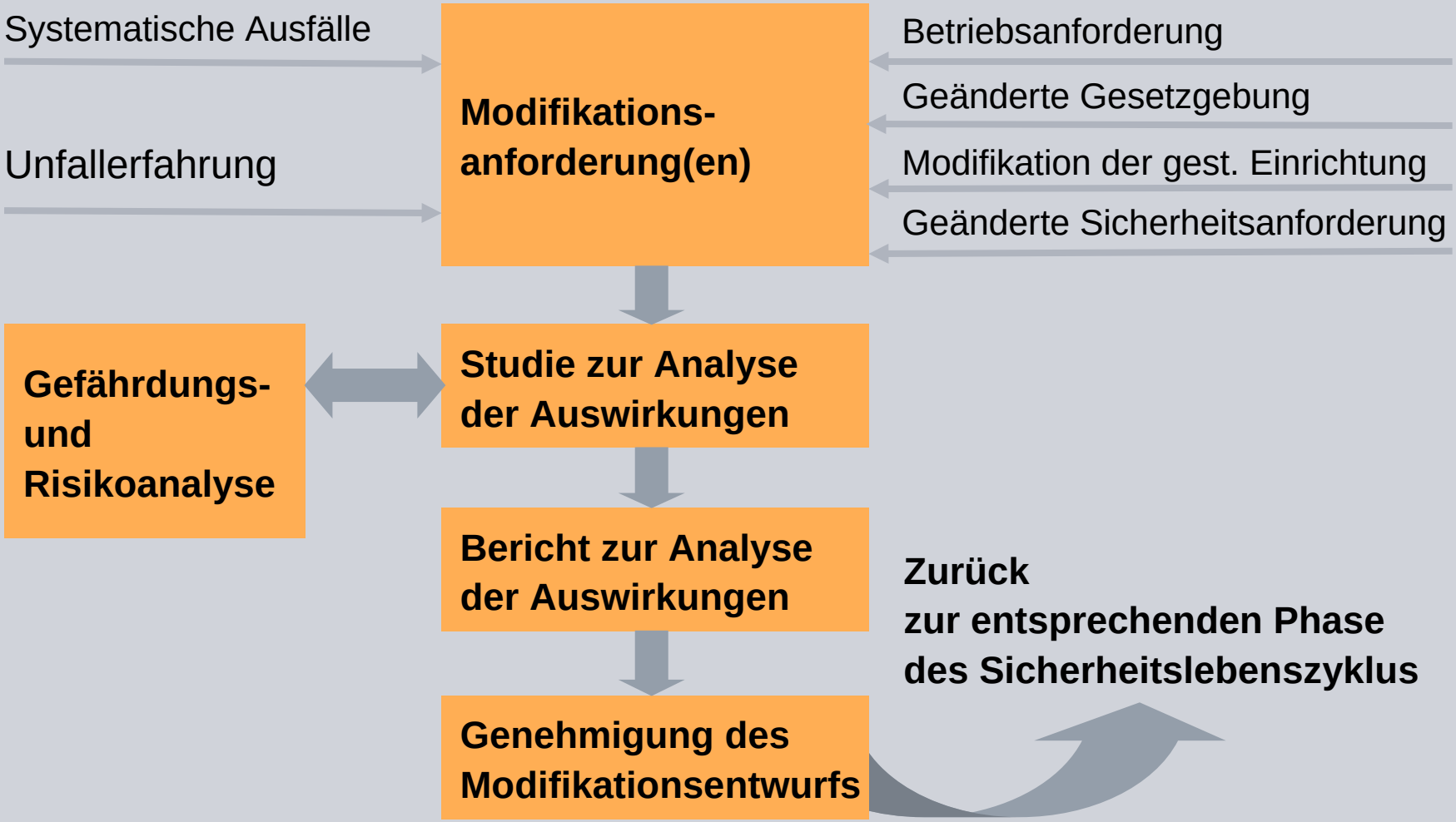
Aspekte:

- Die geforderte Zuverlässigkeit bzgl. Sicherheit muss während der gesamten Betriebszeit aufrecht erhalten bleiben.
- Die während der Planung festgelegten betrieblichen Aspekte (z. B. Ausbildung des Personals) müssen eingehalten werden
- Die während der Planung festgelegten Wartungsaktivitäten müssen durchgeführt werden
  (z. B. Proof-Test)
- Alle Aktivitäten müssen geplant und dokumentiert werden

Übersicht Sicherheitslebenszyklus

- 6.1 Risikoanalyse
- 6.2 Zuordnung der Sicherheitsfunktion zu den Schutzebenen
- 6.3 Spezifikation der Sicherheitsanforderungen
- 6.4 Entwurf und Planung der sicherheitstechnischen Funktion
  - 6.4.1 Architektur und HW-Zuverlässigkeit
  - 6.4.2 Anwendungssoftware
- 6.5 Montage und Inbetriebnahme
- 6.6 Betrieb und Instandhaltung
- **6.7 Modifikation**
- 6.8 Außerbetriebnahme

Modifikation



Vielen Dank für Ihre Aufmerksamkeit!

Michael Stay
+49 (721) 595 4516 - office
+49 (152) 226 299 23 - mobile
michael.stay@siemens.com
76181 Karlsruhe (Germany)