STARKES STUDIUM.
PRIMA ZUKUNFT.

HOCHSCHULE HEILBRONN

TECHNIK WIRTSCHAFT INFORMATIK

Sicherheitstechnik, 8. Vorlesung (Safety Technology)

Campus Heilbronn

Campus Künzelsau
Reinhold-Würth-Hochschule

Campus Schwäbisch Hall

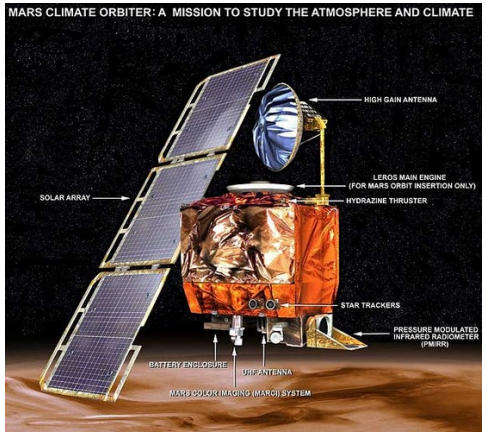
Fred Härtelt, Heilbronn

Beispiel (1999): Mars-Sonde der NASA

Mars Climate Orbiter: Absturz wegen Leichtsinnsfehler beim Rechnen

Nicht wegen einer technischen Panne, sondern weil die beteiligten Wissenschaftler in verschiedenen Maßeinheiten rechneten, ist die 125 Millionen teure Marssonde Climate Orbiter abgestürzt. Ein klassischer Schülerfehler führte bei der Übersetzung vom amerikanischen ins metrische Maßsystem zur peinlichsten Pleite der Nasa. Eine weitere Sonde ist vielleicht mit denselben Fehlberechnungen zum Mars unterwegs.

- Verlust des Kontakts mit der Sonde
- Zerstörung der Sonde durch zu dichte Atmosphäre
- Ursache: Marssonde war bereits zu nah am Mars (57 km anstelle 150 km)
- Zwei verschiedene Gruppen waren am Projekt beteiligt und rechneten mit unterschiedlichen Einheiten (m <-> inch)
- Mangelnde Erfahrung, Überlastung, schlechte Zusammenarbeit

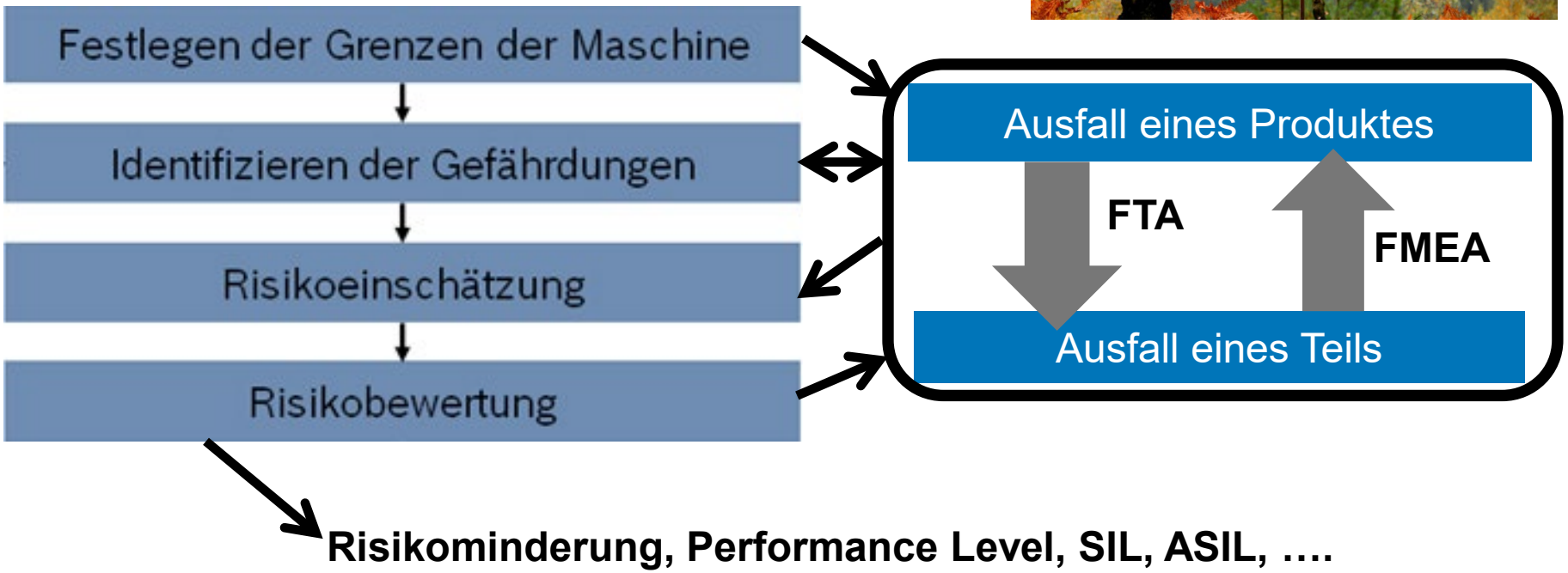


Quellen: www.spiegel.de, www.wikipedia.de

Sicherheitstechnik: zeitlicher Überblick

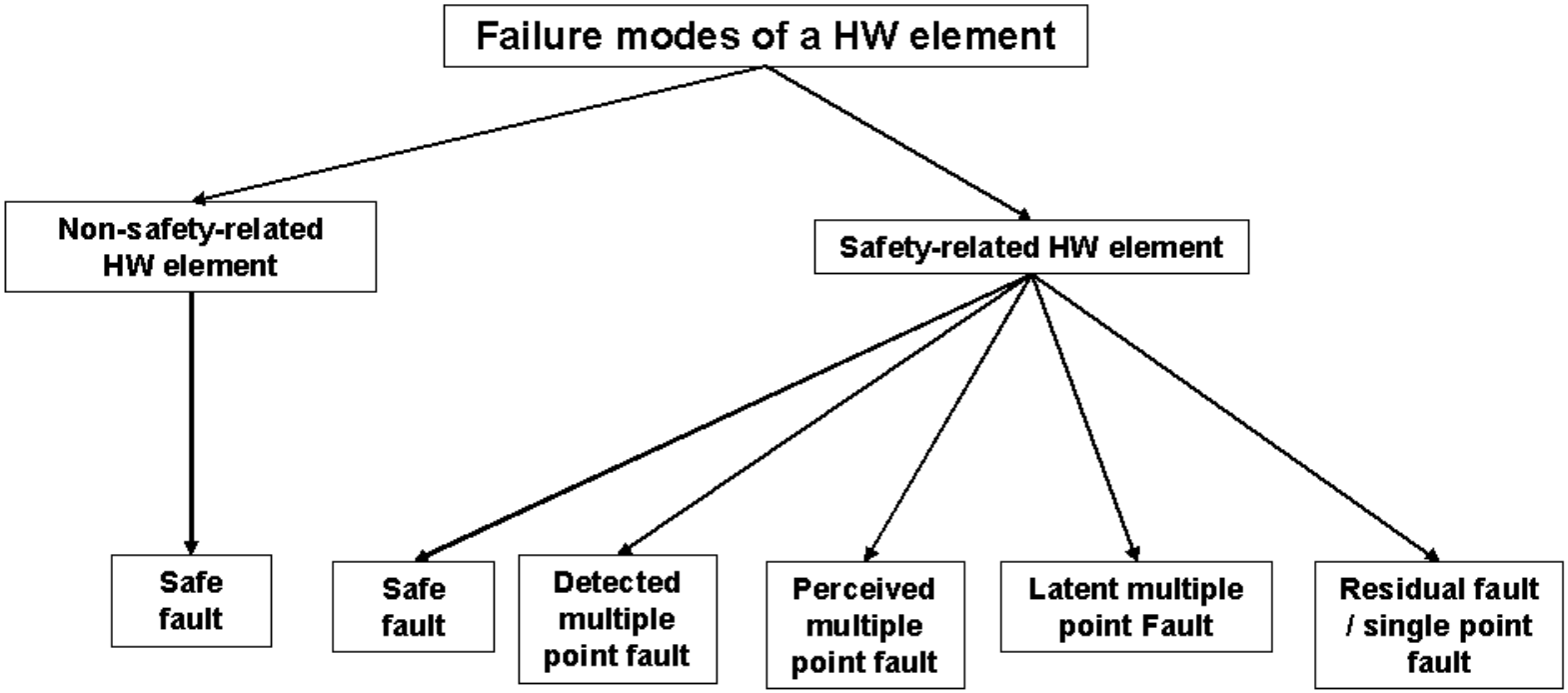
- 1. V: Definition Sicherheit, Normen und Vorschriften (14.03.2022)
- 2. V: Festlegung von Grenzen und Gefährdungen (21.03.2022)
- 3. V: Risikobeurteilung, -minimierung, Risikograph (28.03.2022)
- 4. V: Verteilungsfunktion, Ausfallraten, Fehlerbeherrschung (04.04.2022)
- 5. V: Fehlervermeidung, Fehlerentdeckung, FMEA (11.04.2022)
- Keine Vorlesung am 18.04.2022 (Ostermontag)
- Keine Vorlesung am 25.04.2022
- 6. V: Redundanz, Strukturierungsmaßnahmen, FTA (02.05.2022)
- 7. V: Berechnung von Ausfallraten, FMEDA, Aufgabenstellung Belegarbeit, **Einteilung der Gruppen** (09.05.2022)
- **8. V: Prozess vs. Technik, Besonderheiten HW/SW, Zuverlässigkeit SW Entwicklungsprozess, Bsp. Belegarbeit, Beginn der Gruppenarbeit (16.05.2022)**
- Rückfragen bezüglich Gruppenarbeit am 23.05., 30.05. und 13.06.2022 (WebEx)
- Abgabetermin der Gruppenarbeiten: **20.06.2022** (vor Beginn der Präsentationen)
- Präsentationstermine der Gruppen: **20.06.2022**

Sicherheitstechnik: Wiederholung



Risikominderung, Performance Level, SIL, ASIL, ….

Sicherheitstechnik: Wiederholung



Sicherheitstechnik: Wiederholung

FMEDA:

Vorbereitung einer FMEDA

1. Identifikation von relevanten Modulen/Teilen
2. Bestimmung der Fehlerraten
3. Bestimmung der Fehlermodi
4. Festlegung der Fehlerauswirkungen
5. Sortierung in Fehlerklassen
6. Entwicklung und Festlegung der Sicherheitsmechanismen
7. Bestimmung der „Failure Mode Coverage“
8. Kalkulation der Hardwaremetriken
9. Auswahl und Definition der Maßnahmen
10. Dokumentation und Präsentation

Sicherheitstechnik: Wiederholung

Cells Reviewed	Component Name	Description	Failure rate / FIT	Safety-related component to be considered in the calculations?	Failure Mode	Failure rate distribution	Failure effect (see FTA)	Failure Path	Failure mode that has the potential to violate the safety goal in absence of safety mechanisms ?	Safety mechanism(s) allowing to prevent the failure mode from violating the safety goal ?	Failure mode coverage wrt. violation of safety goal	Residual- or Single-Point Fault failure rate / FIT	Failure mode that may lead to the violation of safety goal in combination with an independent failure of another component ?	Detection means ? Safety mechanism(s) allowing to prevent the failure mode from being latent ?	Failure mode coverage wrt. Latent failures	Latent Multiple-Point Fault failure rate / FIT
reviewed	R3	Resistor	3	Yes	open	30			x		0	0,900			0	
reviewed					closed	10					0	0,000			0	
reviewed					drift 0,5	30					0	0,000			0	
reviewed					drift 2	30			x		0	0,900			0	
reviewed	R13	Resistor	2	Yes	open	90			x		0	1,800			0	
reviewed					closed	10			x		0	0,200			0	
reviewed	R23	Resistor	2	Yes	open	90					0	0,000			0	
reviewed					closed	10			x		0	0,200			0	
reviewed	C13	Capacitor	2	Yes	open	20			x		0	0,400			0	
reviewed					closed	80					0	0,000			0	
reviewed	C23	Capacitor	2	No	open	20					0	0,000			0	
reviewed					closed	80					0	0,000			0	
reviewed	WD	ASIC	20	Yes	Out stuck at 1	50					0	0,000	x		0	10,00
reviewed					Out stuck at 0	50					0	0,000			0	
reviewed	T71	IC	5,00	Yes	open circuit	50					0	0,000			0	
reviewed					short circuit	50			x	SM1	90	0,250	x	SM1_L	80	0,45
reviewed	R71	Resistor	2	Yes	open	90					0	0,000			0	
reviewed					closed	10					0	0,000	x		0	0,20
reviewed	R72	Resistor	2	Yes	open	90					0	0,000			0	
reviewed					closed	10					0	0,000	x		0	0,20
reviewed	R73	Resistor	2	No	open	90					0	0,000			0	
reviewed					closed	10					0	0,000			0	
reviewed	R74	Resistor	2	Yes	open	90					0	0,000	x		0	1,80
reviewed					closed	10					0	0,000	x		0	0,20
reviewed	I71	Resistor	5	No	open	70					0	0,000			0	
reviewed					closed	20					0	0,000			0	
reviewed	C71	Capacitor	2	Yes	open	20					0	0,000	x		0	0,40
reviewed					closed	80					0	0,000			0	
reviewed	R81	Resistor	2	No	open	90					0	0,000			0	
reviewed					closed	10					0	0,000			0	
reviewed	L1	LED	10	No	open	90					0	0,000			0	
reviewed					closed	10					0	0,000			0	
reviewed	µC	IC	100	Yes	all	50			x	SM4	90	5,000	x	SM4_L	100	0,00
reviewed					all	50					0	0,000			0	

Unterscheidung Prozess vs. Technik

- Prozess = z.B. organisatorische Maßnahmen (Wer ist verantwortlich? Wie ist dies in der Organisation implementiert?) und Qualitätsmaßnahmen

- Technik = Umsetzung technischer Art in Hardware und Software, die angemessen validiert und verifiziert werden (siehe Besonderheiten zwischen Hardware und Software)

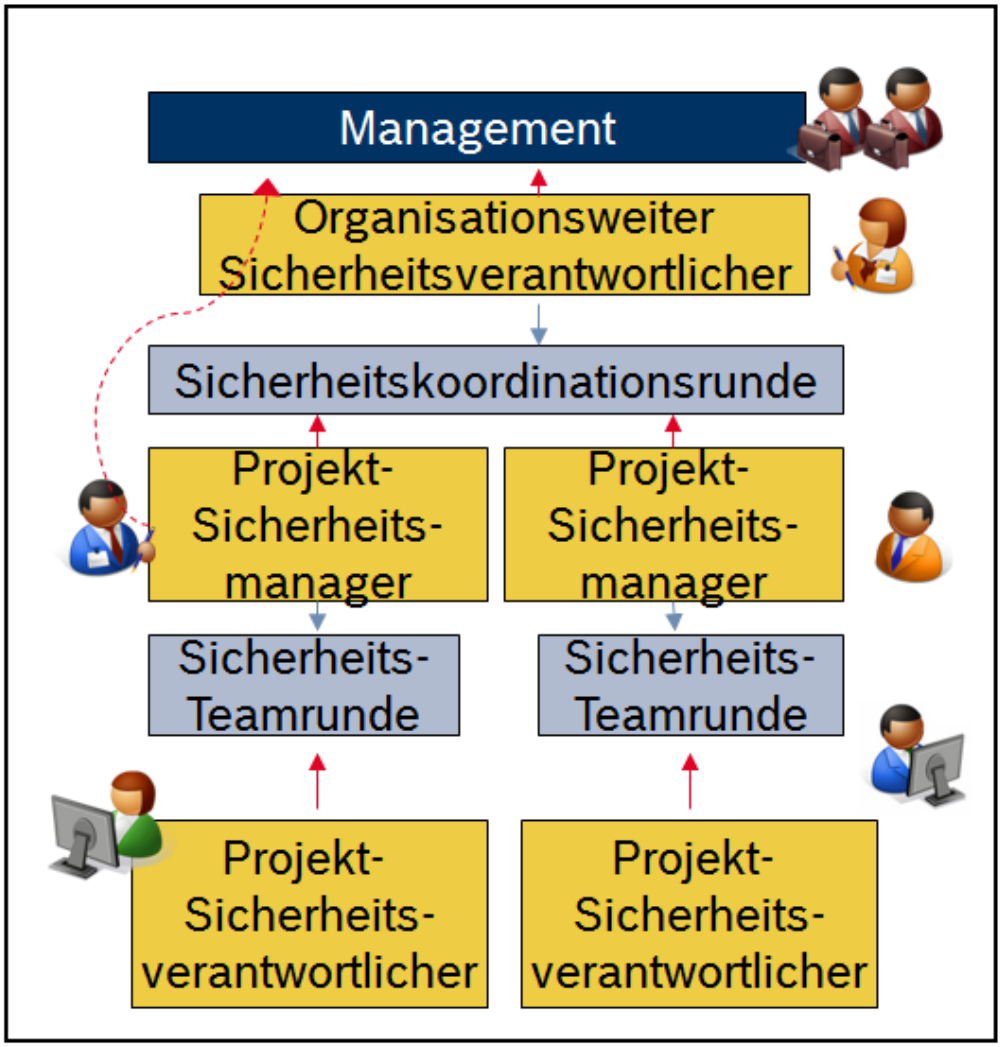
Prozess: Implementierungsbeispiele
10 Signale einer Kultur des „Sicheren Arbeitens“

- Kontinuierliche Prozessweiter-entwicklung
- Entscheidungen sind nachvollziehbar
- Intellektuelle Vielfalt wird zum Nutzen der Sicherheit verwendet
- Belohnungssystem favorisiert die Beachtung von Sicherheitsthemen
- Sicherheit hat die höchste Priorität (vor Kosten und dem Projektplan)
- Offene und frühzeitige Behandlung von Sicherheits- und Qualitätsthemen
- Belohnungssystem bestraft die Nichtbeachtung von Sicherheitsthemen
- Verantwortliche sind hinreichend qualifiziert
- Klare, definierte Prozesse
- Offene Kommunikation wird ermutigt

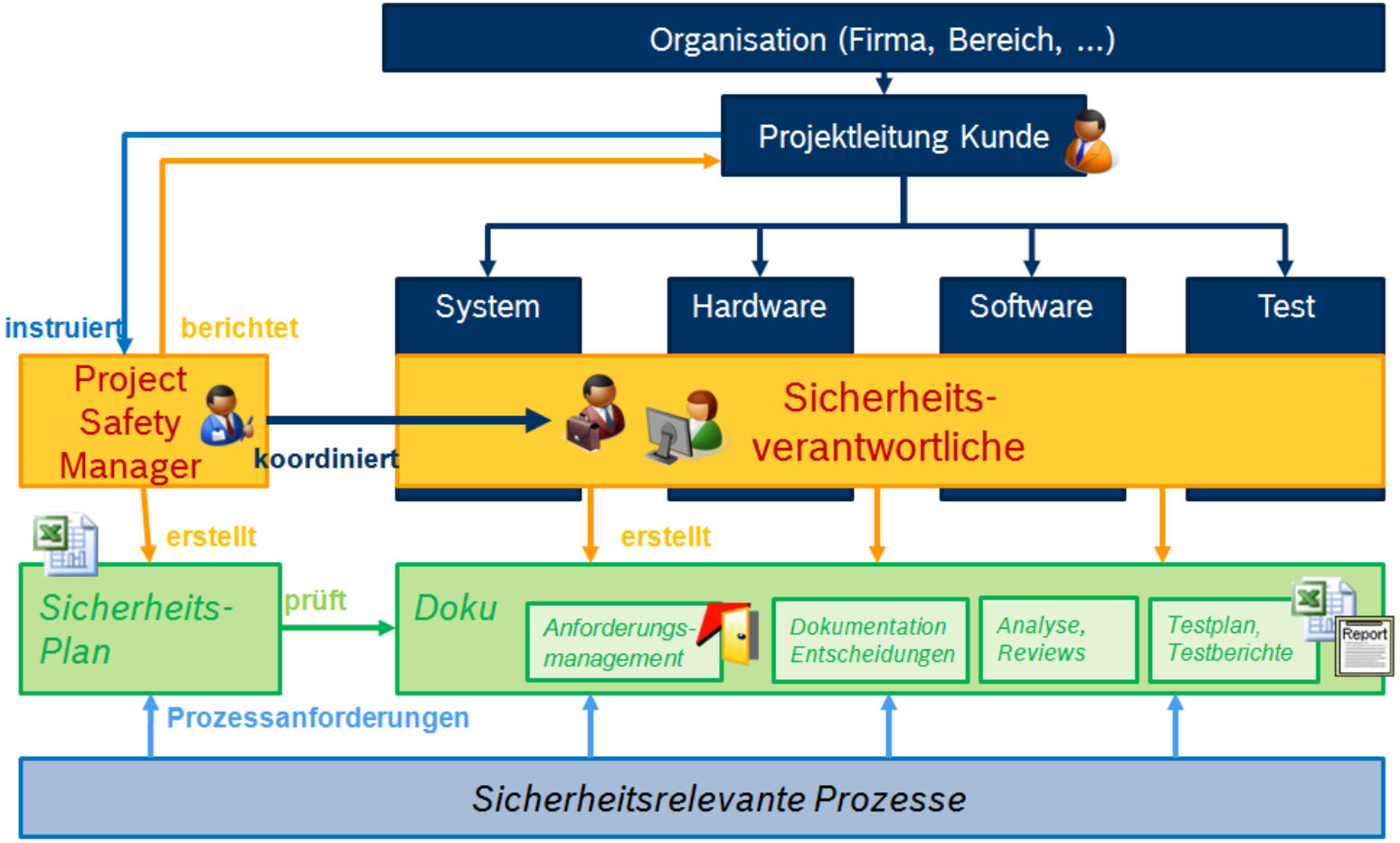
Prozess: Implementierungsbeispiele

Fragen	Ansatz
Ist ein Qualitätsmanagement- system implementiert?	• CMMI, ISO TS16949, etc.
Gibt es einen strukturierten Entwicklungsprozess nach beschriebenen Standards / Normen (Maschinenrichtlinie, ISO 13849)?	• Entwicklungsprozess definiert • Sind die Normen Bestandteil von “Quality Gates”?
Sind die Mitarbeiter hinreichend qualifiziert?	• Kompetenzmanagement bezogen auf Normen / Standards (Trainings)
Wird eine Kultur des sicheren Arbeitens und kontinuierlichen Verbesserung gelebt?	• Sicherheitsorganisation, Sicherheitssteuerkreise • Sicherheitsmanagement, Teams mit Sicherheitsverantwortlichen

Prozess: Implementierungsbeispiele (Organisation)



Prozess: Implementierungsbeispiele (Projekt)



Sicherheitstechnik
Inhalte

- Definition Sicherheit
- Aktuelle Normen und Vorschriften
- Methoden und Verfahren
  - Risikobeurteilung und –minderung, Risikograph
  - Verteilungsfunktionen, Ausfallraten, Fehlerbeherrschung und Vermeidung, Fehlerentdeckung, Redundanz
  - Strukturierungsmaßnahmen, FMEA, FTA, FMEDA u.a.
  - Unterscheidung Prozess vs. Technik
- Besonderheiten hinsichtlich Hardware und Software (Zuverlässigkeit SW Entwicklungsprozess)

Unterscheidung Prozess vs. Technik

- Typische Qualitätsmaßnahmen:
  - Maßnahmen in der Organisation (Rollen, Bewusstsein)
  - Sicherheitslebenszyklus, Prozesse
  - Sicherheitsanforderungen definieren (Traceability)
  - Sicherheitsanalysen verwenden (FMEA, FTA, …)
  - Dokumentation erstellen
  - Qualifizierung von SW-Tools
  - Assessments, Audits durchführen

Besonderheiten hinsichtlich Hardware und Software

- Zufällige Hardwarefehler vs. Systematische Hardware- und Softwarefehler
- Zufällige Hardwarefehler über probabilistischen Ansatz (siehe nächste Folie)
- Systematische Hardware- und Softwarefehler über vorgelagertes Qualitätsmanagement (siehe Prozess)

Besonderheiten hinsichtlich Hardware und Software

- Hardware
  - Redundanz (Bsp.: 3-Ebenen Modell, siehe Einstufung der Kategorie z.B. beim Performance Level), HW Layout, Überwachungsfunktionen, Metriken, Tests
  - Verwendung vorgeschriebener / genormter Elemente
  - Zertifizierung des Zulieferers
  - Verwendung von Methoden (z.B. FMEA, FTA, FMEDA) um Gefahren und Risiken zu ermitteln (als Bestandteil des Qualitätsmanagements)

Besonderheiten hinsichtlich Hardware und Software

Sicherheits-Integritätslevel (SIL)	Betriebsart mit niedriger Anforderungsrate PFD_{sys} (Low demand mode).
4	$\geq 10^{-5} \ldots < 10^{-4}$
3	$\geq 10^{-4} \ldots < 10^{-3}$
2	$\geq 10^{-3} \ldots < 10^{-2}$
1	$\geq 10^{-2} \ldots < 10^{-1}$

Die Tabelle zeigt die Abhängigkeit des Sicherheits-Integritätslevel von der mittleren Ausfallwahrscheinlichkeit bei Anforderungen einer Sicherheitsfunktion des gesamten sicherheitsbezogenen Systems (PFDsys). Betrachtet wird bei einem Wasserstandbegrenzer die Anforderung „Low demand mode", d.h. die Anforderungsrate an das sicherheitsbezogene System ist durchschnittlich einmal im Jahr.

Anteil ungefährlicher Fehler (SFF)	Fehlertoleranz der Hardware (HFT) für Typ B		
	0	1	2
< 60 %		SIL 1	SIL 2
60 % - < 90 %	SIL 1	SIL 2	SIL 3
90 % - < 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Die Tabelle gibt den erreichbaren Sicherheits-Integritätslevel in Abhängigkeit vom Anteil der ungefährlichen Ausfälle (SFF) und der Fehlertoleranz der Hardware (HFT) für sicherheitsbezogene Systeme an.

Besonderheiten hinsichtlich Hardware und Software

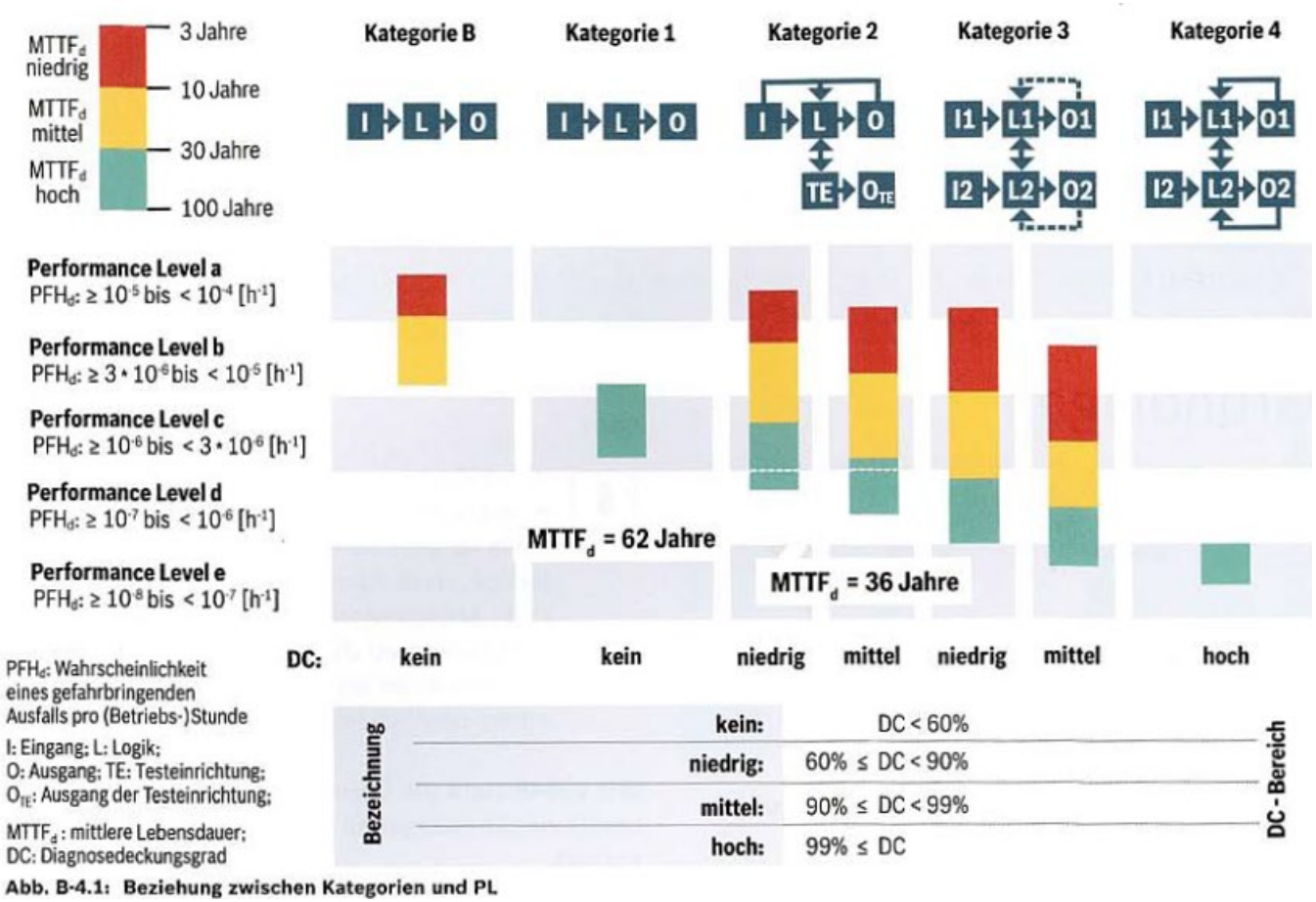


Abb. B-4.1: Beziehung zwischen Kategorien und PL

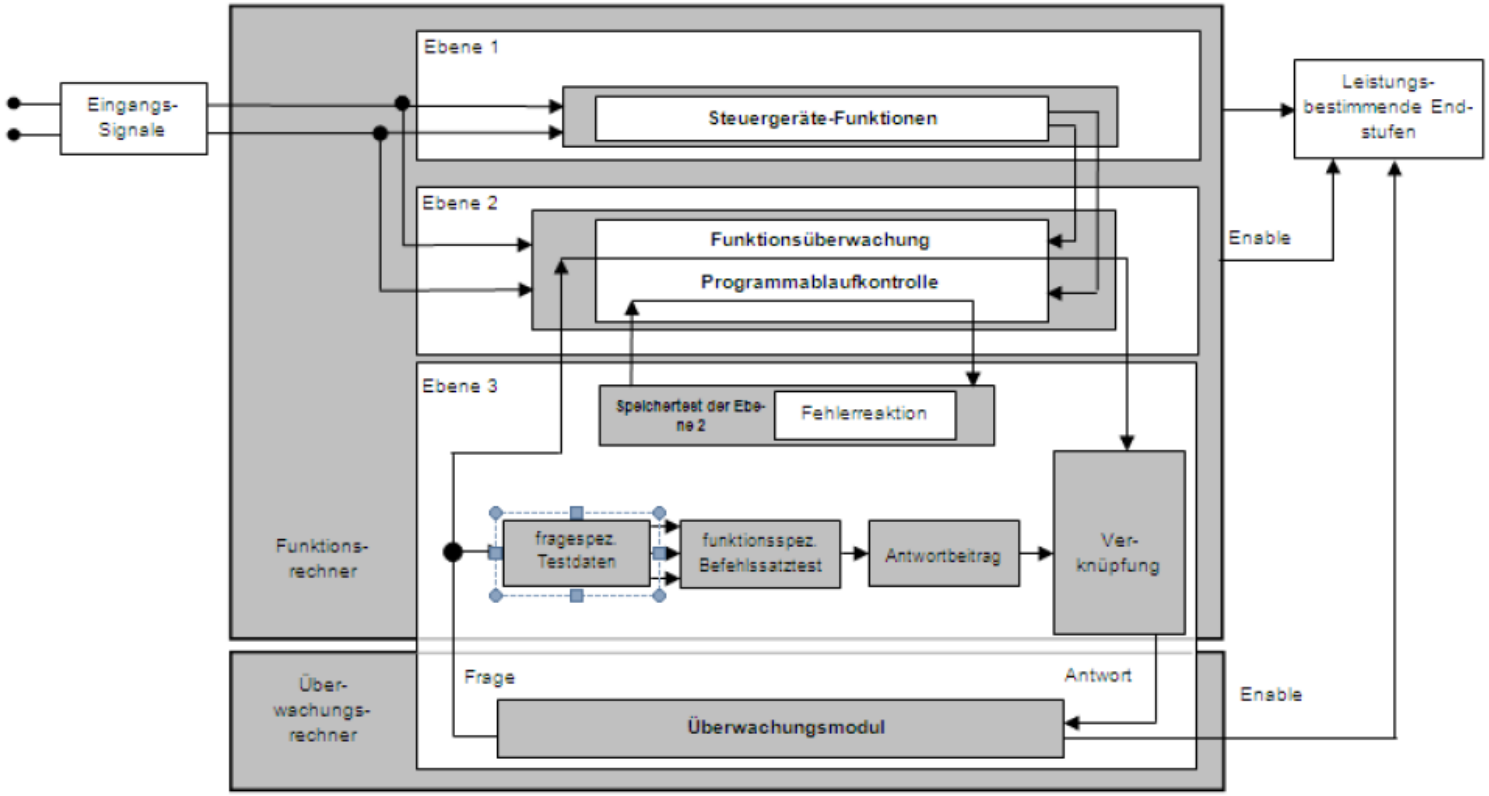
Besonderheiten hinsichtlich Hardware und Software

- Software
  - Einhaltung bestimmter Regeln / Standards (MISRA, Kodierrichtlinien)
  - Implementierung von Sicherheitssoftware auf verschiedenen Ebenen (z.B. 3-Ebenen Modell)
  - Zertifizierung von Tools (siehe Qualitätsmaßnahmen)
  - Verwendung geeigneter Analysetechniken
  - Reviews, …

Besonderheiten hinsichtlich Hardware und Software

Methods		ASIL			
		A	B	C	D
1a	Range checks of input and output data	++	++	++	++
1b	Plausibility check[a]	+	+	+	++
1c	Detection of data errors[b]	+	+	+	+
1d	External monitoring facility[c]	o	+	+	++
1e	Control flow monitoring	o	+	++	++
1f	Diverse software design	o	o	+	++

- Bsp.: 3-Ebenen-Modell



Quelle: AK EGAS

Besonderheiten hinsichtlich Hardware und Software

- Beispiele MISRA Kodierrichtlinien
  - Verschachtelte Kommentare vermeiden
  - Konstanten in einem vorzeichenlosen Kontext müssen ein bestimmtes Suffix verwenden
  - Gleitkommazahlen sollen nicht mit Vergleichsoperatoren getestet werden
  - „go to“ soll nicht verwendet werden
  - „magic numbers“ vermeiden und besser sinnvoll benannte Konstanten verwenden
  - Division durch Null verhindern
  - Compilerunabhängigkeit sicherstellen
  - …

Quelle: wikipedia

Besonderheiten hinsichtlich Hardware und Software

- Beispiele MISRA Kodierrichtlinien

Topics		ASIL			
		A	B	C	D
1a	Enforcement of low complexity[a]	++	++	++	++
1b	Use of language subsets[b]	++	++	++	++
1c	Enforcement of strong typing[c]	++	++	++	++
1d	Use of defensive implementation techniques	o	+	++	++
1e	Use of established design principles	+	+	+	++
1f	Use of unambiguous graphical representation	+	++	++	++
1g	Use of style guides	+	++	++	++
1h	Use of naming conventions	++	++	++	++

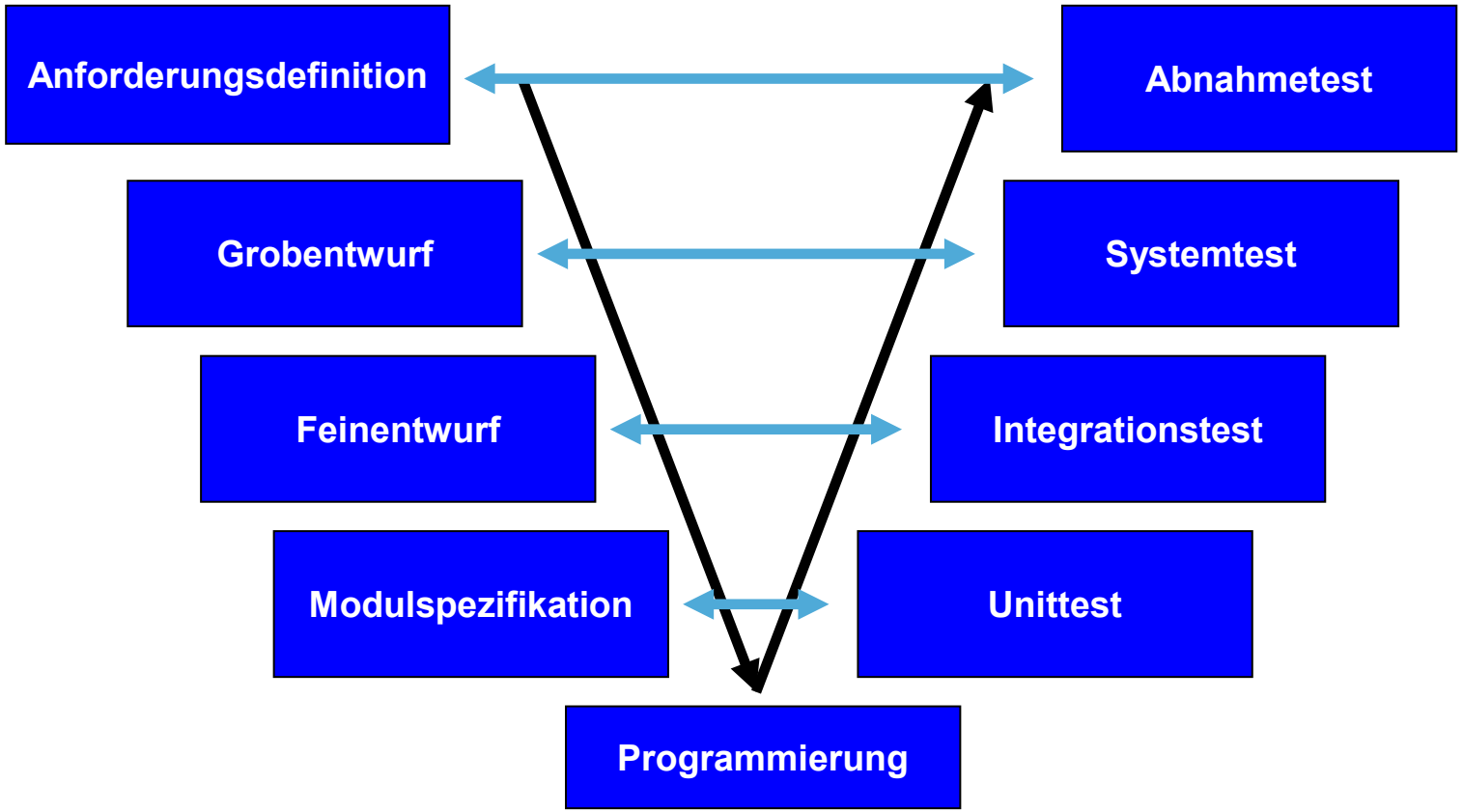
Quelle: ISO 26262

Besonderheiten hinsichtlich Hardware und Software

- Tests
  - Auswahl geeigneter Testverfahren um Software / Hardware testen zu können (z.B. Blackbox-, Whitebox-Verfahren)
  - Definition was wo und wie auf welcher Ebene (Modul, Integration, System) getestet wird
  - Ggf. Definition von Spezialtests um Sicherheitsfunktionen adäquat abtesten zu können
  - Anforderungsbasiertes Testen (Nachweis der Sicherheitsanforderungen)
  - Benutzen von gängigen Standards

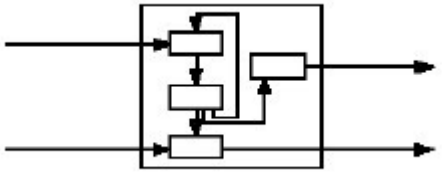
Besonderheiten hinsichtlich Hardware und Software

- V-Modell:



Besonderheiten hinsichtlich Hardware und Software

- **White-Box Test**
  - basiert auf expliziter Kenntnis des internen Aufbaus des Systems (also des Codes, der Beschreibung oder des Entwurfs)
- White-Box Methoden sind:
  - Strukturabdeckung
  - Codeüberdeckung
  - Anweisungsüberdeckung
  - Zweigüberdeckung
  - Entscheidungsüberdeckung
  - MC/DC
  - Pfadüberdeckung



Besonderheiten hinsichtlich Hardware und Software

White-Box Test

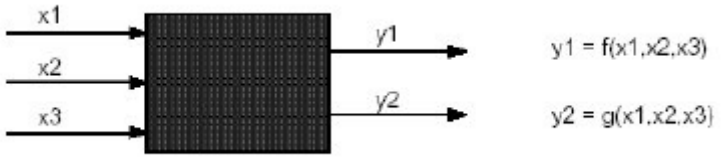
	Methods	ASIL A	ASIL B	ASIL C	ASIL D
1a	Statement coverage	++	++	+	+
1b	Branch coverage	+	++	++	++
1c	MC/DC (Modified Condition/Decision Coverage)	+	+	+	++

	Methods	ASIL A	ASIL B	ASIL C	ASIL D
1a	Function coverage[a]	+	+	++	++
1b	Call coverage[b]	+	+	++	++

Quelle: ISO 26262

Besonderheiten hinsichtlich Hardware und Software

- **Black-Box Test**
  - basiert auf dem System in der späteren Erscheinungsform (also funktionaler Spezifikation und Anforderungen)
  - Beurteilung auf Grund dessen, was das System können muss
- Black-Box Methoden sind:
  - Funktionsabdeckung
  - Äquivalenzklassenanalyse
  - Grenzwertanalyse
  - intuitive Testfallermittlung
  - Zufallstest
  - Fehlererwartung



Besonderheiten hinsichtlich Hardware und Software

Black-Box Test

	Methods	ASIL A	ASIL B	ASIL C	ASIL D
1a	Requirements-based test[a]	++	++	++	++
1b	Interface test	++	++	++	++
1c	Fault injection test[b]	+	+	+	++
1d	Resource usage test[c]	+	+	+	++
1e	Back-to-back comparison test between model and code, if applicable[d]	+	+	++	++

	Methods	ASIL A	ASIL B	ASIL C	ASIL D
1a	Analysis of requirements	++	++	++	++
1b	Generation and analysis of equivalence classes[a]	+	++	++	++
1c	Analysis of boundary values[b]	+	++	++	++
1d	Error guessing[c]	+	+	+	+

Quelle: ISO 26262

Sicherheitstechnik: Beispiel Bearbeitungsmaschine

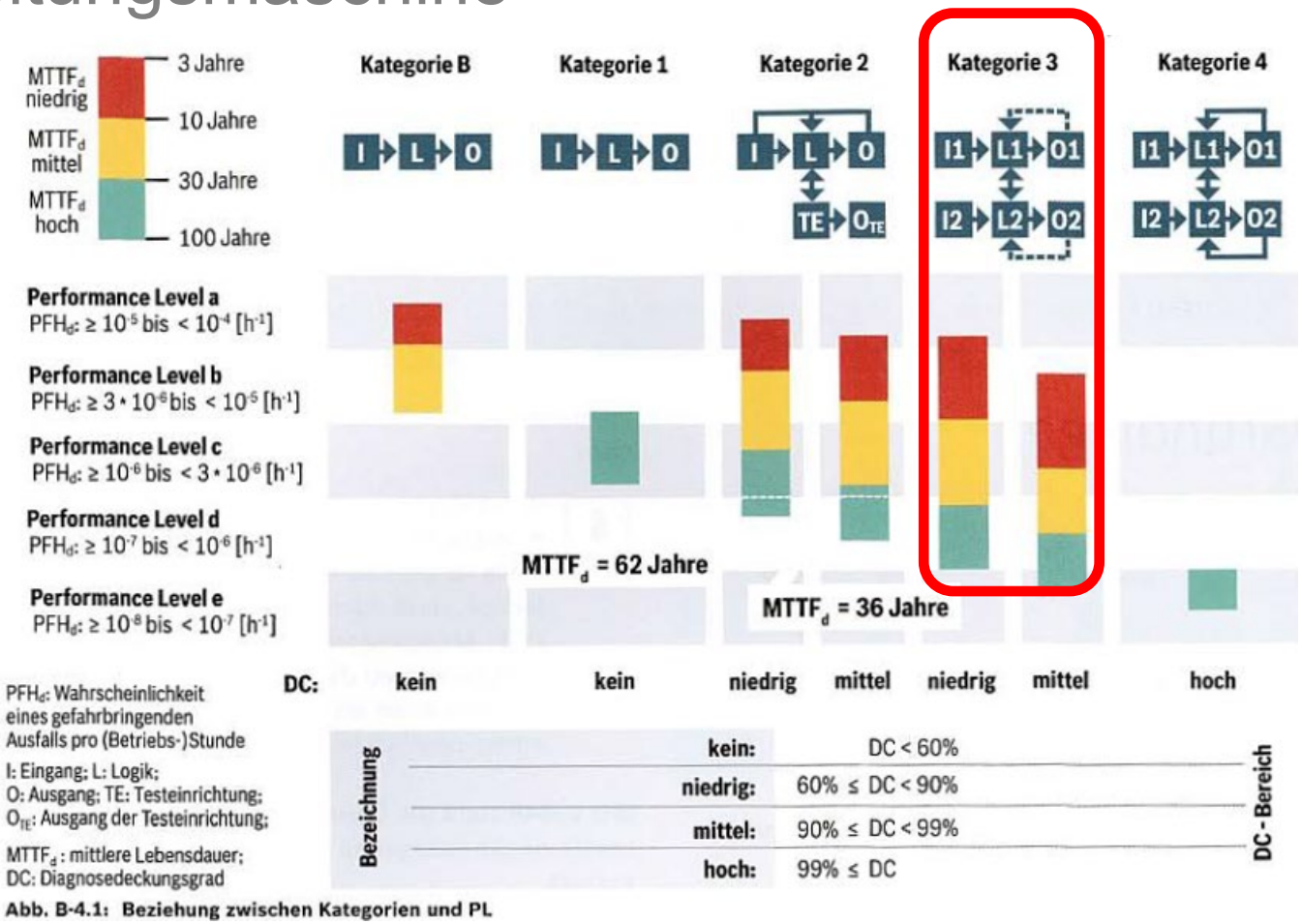
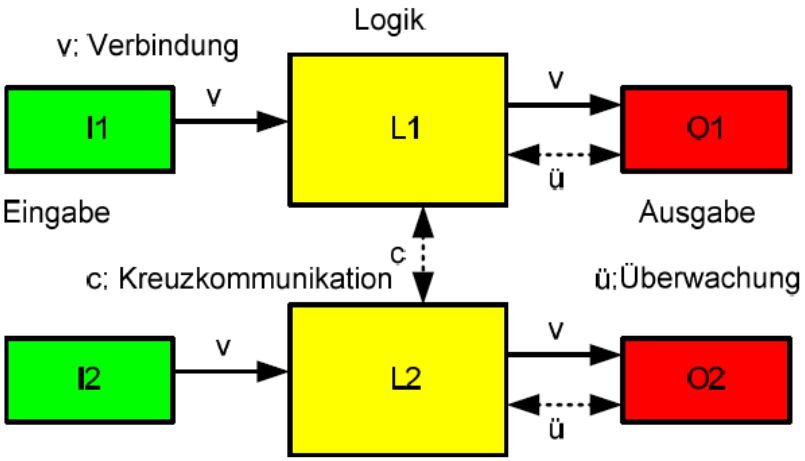
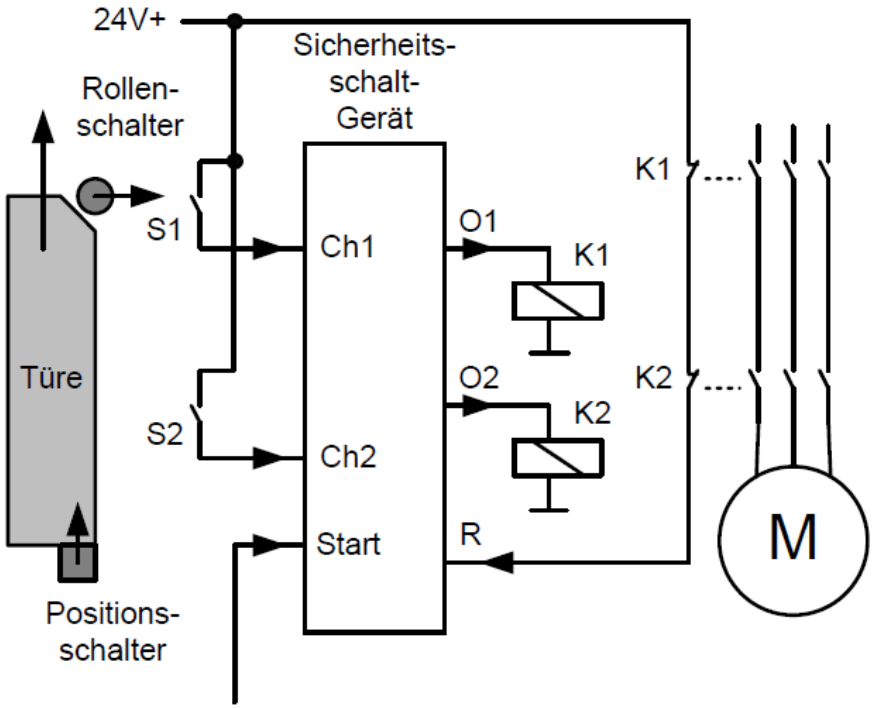


Abb. B-4.1: Beziehung zwischen Kategorien und PL

Quelle: innotec

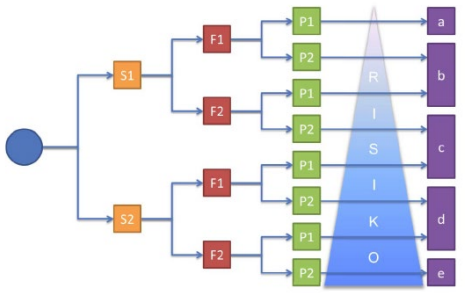
Sicherheitstechnik: Beispiel Bearbeitungsmaschine





Quelle: innotec

Sicherheitstechnik: Übung 10

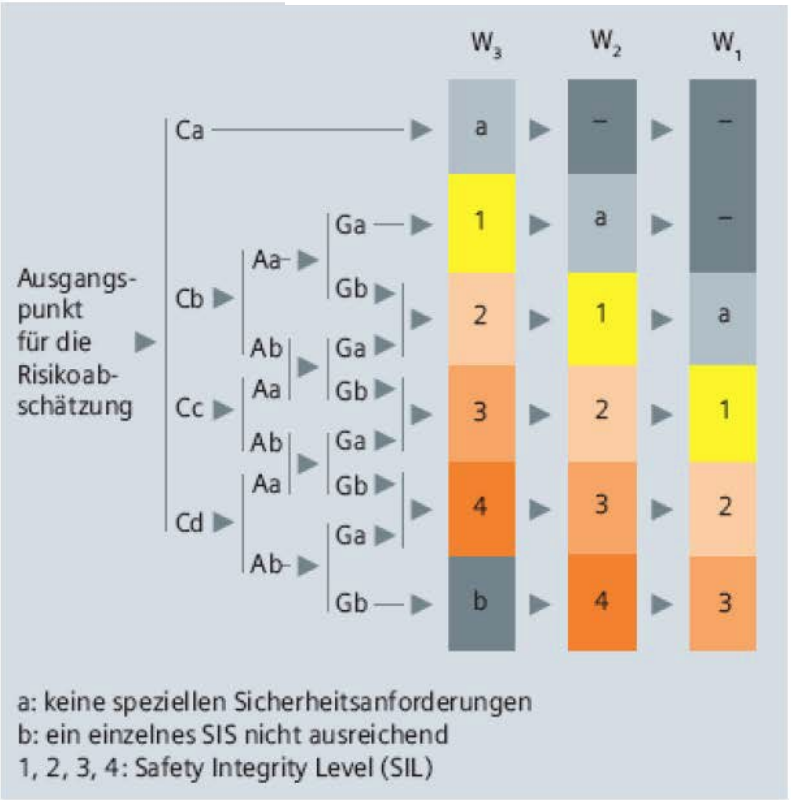


Schadensausmaß	
C_a	leichte Verletzung einer Person, kleinere schädliche Umwelteinflüsse
C_b	schwere Verletzungen oder Tod einer Person
C_c	Tod mehrere Personen
C_d	Tod sehr vieler Personen

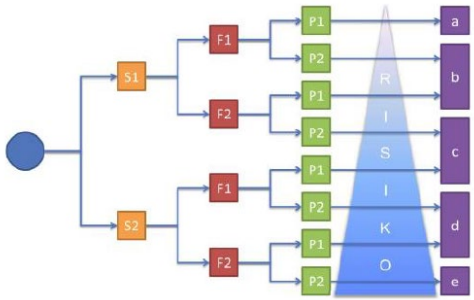
Aufenhaltsdauer einer Person im gefährlichen Bereich	
A_a	selten bis häufig
A_b	häufig bis dauernd

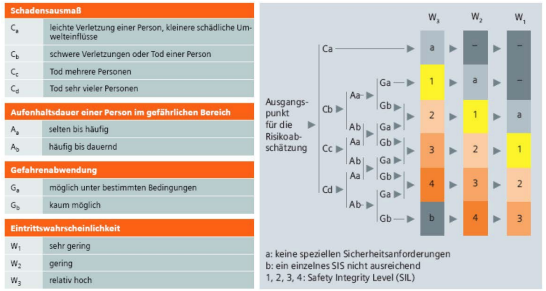
Gefahrenabwendung	
G_a	möglich unter bestimmten Bedingungen
G_b	kaum möglich

Eintrittswahrscheinlichkeit	
W_1	sehr gering
W_2	gering
W_3	relativ hoch



Sicherheitstechnik: Lösung Übung 10





Gefährdung	PL	SIL
Verletzung durch die Maschine bei geöffneter Tür (Maschine ist nicht stromlos -> sicherer Zustand verletzt) (Falls eine Person in das Werkzeug der Maschine eingreift, während diese sich dreht, sind schwerwiegende Verletzungen nicht auszuschließen)	S = 2 F = 2 P = 1 **PL = d**	C = Cb A = Ab G = Ga W = W3 **SIL = 2**

Sicherheitstechnik

Fragen?

Starkes Studium.
Prima Zukunft.

HOCHSCHULE HEILBRONN

TECHNIK WIRTSCHAFT INFORMATIK

Viel Erfolg!

Fred Härtelt, Heilbronn

Campus Heilbronn

Campus Künzelsau
Reinhold-Würth-Hochschule

Campus Schwäbisch Hall