PLATO AG
Funktionales Sicherheitsprojekt & System-FMEA

Umsetzung in einem Datenmodell

Claudia Lange

Die PLATO AG auf einem Blick

Software- und Dienstleistungsunternehmen mit

- Methoden- und Softwarelösungen für den Entwicklungsprozess technischer Produkte
- 20 Jahren Markterfahrung in den Branchen Automobil, Medizintechnik, Pharma und Maschinenbau
- 50 Mitarbeitern
- 80.000 verkauften Lizenzen
- und mehr als 600 Kunden

PLATO AG – ist bekannt für…

- … **früher:** FMEA
- … **gestern:** wissensbasiertes Risikomanagement mit Integration in die Unternehmensprozesse
- …**heute:** Integration von entwicklungsbegleitenden Qualitätsmethoden in
  - die Unternehmensprozesse
  - eine IT – Datenlandschaft / -basis

PLATO Softwarelösungen auf einen Blick

PLATO Engineering

- Risikomanagement ➡ PLATO SCIO™ - Risk and Knowledge Management
- Anforderungsmanagement ➡ PLATO SCIO™ - Matrix
- Änderungsmanagement ➡ PLATO SCIO™ - DRBFM
- **NEU: Methodenintegration** ➡ **PLATO SCIO™ - Methods**

PLATO Compliance

- Maßnahmenmanagement ➡ PLATO AQTIO™
- Dokumentenmanagement ➡ PLATO XERI™
- Auditmanagement ➡ PLATO AUDIT

Methodenanwendung im Entwicklungsprozess „V-Model“

Anerkannte QM-Methoden
für den Entwicklungsprozess:

QFD

FMEA

FMECA

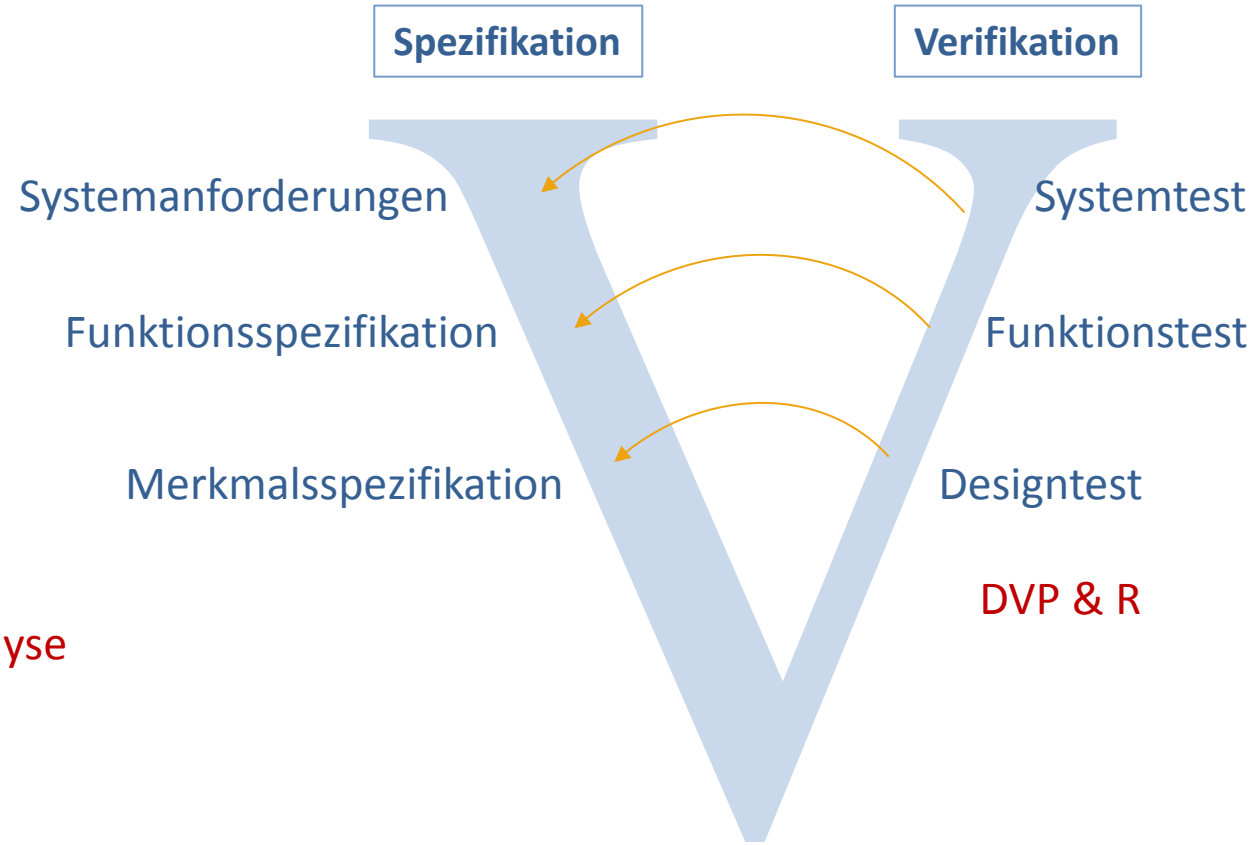
FMEDA

HACCP

Branchenspezifische
Risikoanalyse

Gefahrenanalyse

……



Methodenanwendung im Entwicklungsprozess „V-Model“

Anerkannte QM-Methoden für den Entwicklungsprozess:

QFD

FMEA

FMECA

FMEDA

HACCP

Branchenspezifische Risikoanalyse

Gefahrenanalyse

……

Das Problem

- Methodenvielfalt
- Unterschiedliche Verantwortlichkeiten im Unternehmen
- Keine Vernetzung zwischen den Methoden
  - keine Kommunikation zwischen den Abteilungen
  - kein Datenmanagement (IT)

Die Folgen

- Doppelarbeit
- Dateninkonsistenz: z.B.: Sicherheitsziele aus der Gefahrenanalyse landen nicht in der Anforderungsanalyse
- Fehler am Produkt oder im Herstellprozess werden zu spät erkannt => hohe Kosten
- Wissensmanagement in interdisziplinären Teams wird ausgehebelt

Anerkannte QM-Methoden für den Entwicklungsprozess:

QFD

FMEA

FMECA

FMEDA

HACCP

Branchenspezifische Risikoanalyse

Gefahrenanalyse

……..

Die Lösung

- Durchgängiges Methoden- und Datenkonzept von der Anforderungsanalyse bis zur Produktion
- Durchgängiges Datenmodell verbindet anerkannte QM-Methoden für den Entwicklungsprozess
- Durchgängiger Nachweis dass Anforderungen umgesetzt werden

Zentrales System-Modell für alle Methoden

Spezifikation

Systemanfor-derungen

Risiko

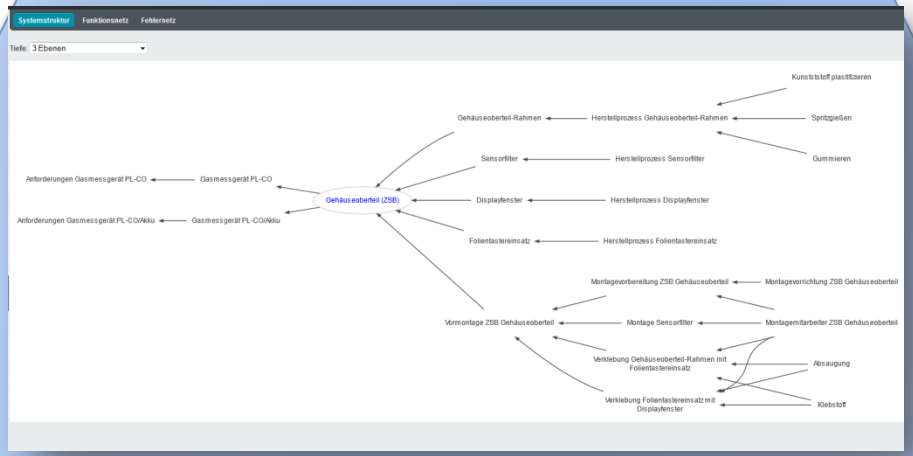
Funktions-spezifikation

Risiko

Merkmals-spezifikation

Risiko

System-Modell



Engineering-Daten
Systemnetz
Funktionsnetz
Fehlernetz
Traces-Netz

Verifikation

Systemtest

Funktionstest

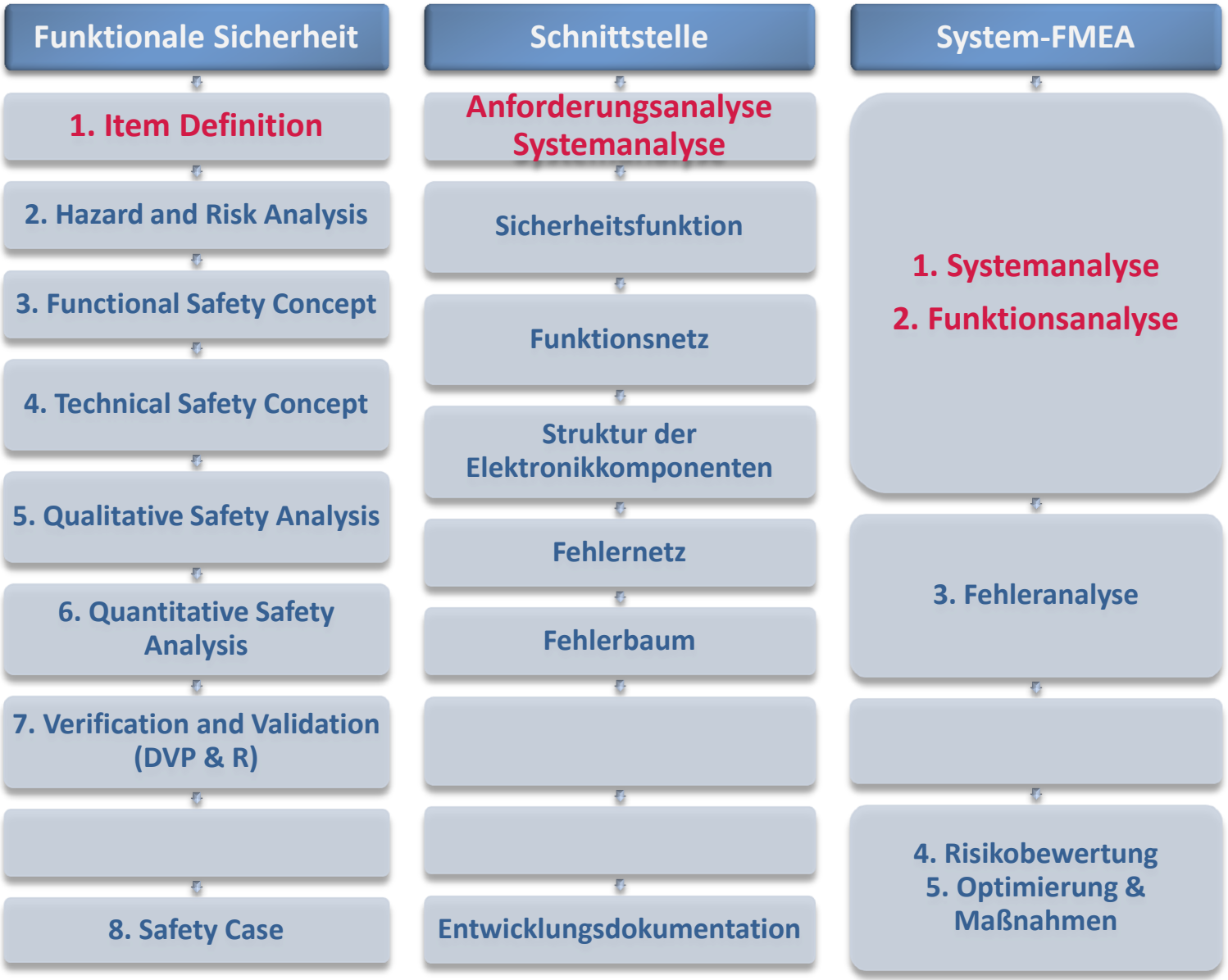
Designtest

Der Ablauf


Funktionale Sicherheit
1. Item Definition
2. Hazard and Risk Analysis
3. Functional Safety Concept
4. Technical Safety Concept
5. Qualitative Safety Analysis
6. Quantitative Safety Analysis
7. Verification and Validation (DVP & R)
8. Safety Case

Beispiel “Fahrerassistenzsystem KFZ”

1. Item Definition



1. Item Definition

Beschreibung der / Link auf die

- **Funktionalen Anforderungen**
- Nicht-Funktionalen Anforderungen
- Systemarchitektur
- Schnittstellen
- Betriebszustände

Formblatt: **Item Definition**

Item Attribute	Item Description
Funktionale Anforderungen	Die Funktionalen Anforderungen liegen in dem Top-Systemelement "**Fahrer-Assistenz-Systeme (ADAS)**" Der Link verweist auf die erste Funktion.
Nicht-Funktionale Anforderungen	Die Nicht-Funktionalen Anforderungen liegen in dem Top-Systemelement "**Nicht-Funktionale Anforderungen**"
Systemarchitektur	
Interaktionen	
Betriebszustände	Betriebszustände sind in dem entsprechenden Katalog auf Projektebene abgelegt.

Beispiel: **Funktionale Anforderungen an ein Fahrerassistenzsystem im KFZ**

Kurzbezeichnung / Funktion	ID	ASIL	Anforderungsbeschreibung	Fehlermöglichkeiten	Status	Zielmarkt
Erkennung von Objekten und Ereignissen	A1		Objekte auf der Fahrbahn sollen in einem Abstand von 40 m erkannt werden.	Objekterkennung zu spät.	Offen	Europa, USA
Erkennung von Fußgängern	A2		Fußgänger auf der Fahrbahn sollen in einem Abstand von 40 m erkannt werden.	Objekterkennung zu spät.	Offen	Europa, USA
Müdigkeit erkennen	A6		Gesichtsüberwachung soll Müdigkeit erkennen.	Müdigkeitserkennung findet nicht statt.	Abgeschlossen	Europa, USA
Spurwechel unterstützen	A4		noch zu definieren		Undefiniert	Europa, USA
Abstandsregelung bieten	A5		PKW darf vorgegebenen Abstand zum vorderen Fahrzeug nicht unterschreiten. 	Abstandregelung löst zu früh aus. Abstandregelung löst zu spät aus. Abstandregelung gibt falsche Werte Abstandregelung löst ungewollt aus	Abgeschlossen	Europa, USA

1. Item Definition

Beschreibung der / Link auf die

- Funktionalen Anforderungen
- **Nicht-Funktionalen Anforderungen**
- Systemarchitektur
- Schnittstellen
- Betriebszustände

Formblatt: **Item Definition**

Item Attribute	Item Description
Funktionale Anforderungen	Die Funktionalen Anforderungen liegen in dem Top-Systemelement "**Fahrer-Assistenz-Systeme (ADAS)**" Der Link verweist auf die erste Funktion.
Nicht-Funktionale Anforderungen	Die Nicht-Funktionalen Anforderungen liegen in dem Top-Systemelement "**Nicht-Funktionale Anforderungen**"
Systemarchitektur	
Interaktionen	
Betriebszustände	Betriebszustände sind in dem entsprechenden Katalog auf Projektebene abgelegt.

Beispiel: **Nicht-Funktionale Anforderungen an ein Fahrerassistenzsystem im KFZ**

Kurzbezeichnung / Funktion	ID	ASIL	Anforderungsbeschreibung	Fehlermöglichkeiten	Status	Zielmarkt
Bedienkomfort			Spracherkennung (Mehrsprachigkeit) und einfache Steuerung durch den Fahrer	Fahrzeug entspricht nicht dem allgemeinen Ansprüchen an Komfort	Offen	Europa,USA, Asien
Unterstützung des Fahrers			Einparkhilfe, Schnittstellen zu Google+ und Facebook, Geographische Daten mit Sachdatenbezug	Fahrzeug entspricht nicht dem allgemeinen Ansprüchen an Komfort	Undefiniert	Europa, USA, Asien
Sicherheitsaspekte				Gefährdung von Personen und Auftreten von Sachschäden	Offen	Europa, USA, Asien
Steigerung des Fahrkomforts				Fahrzeug und Fahrverhalten sind wenig komfortabel	Abgeschlossen	Asien
Verbesserung der Ökonomie			Benefit für den Fahrer (Kosten/Nutzen) 	Fahrzeug wird als unwirtschaftlich angesehen	Offen	Europa, USA

1. Item Definition

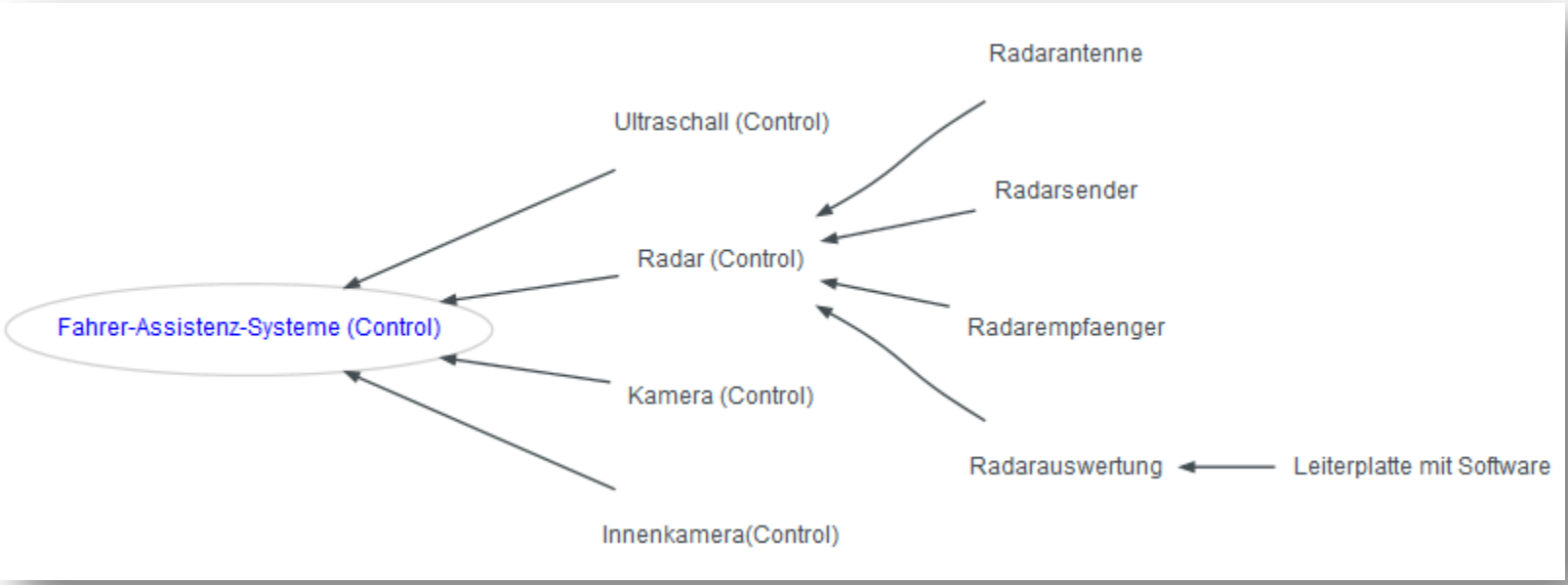
Beschreibung der / Link auf die

- Funktionalen Anforderungen
- Nicht-Funktionalen Anforderungen
- **Systemarchitektur**
- Schnittstellen
- Betriebszustände

Formblatt: **Item Definition**

Item Attribute	Item Description
Funktionale Anforderungen	Die Funktionalen Anforderungen liegen in dem Top-Systemelement "**Fahrer-Assistenz-Systeme (ADAS)**" Der Link verweist auf die erste Funktion.
Nicht-Funktionale Anforderungen	Die Nicht-Funktionalen Anforderungen liegen in dem Top-Systemelement "**Nicht-Funktionale Anforderungen**"
Systemarchitektur	
Interaktionen	
Betriebszustände	Betriebszustände sind in dem entsprechenden Katalog auf Projektebene abgelegt.

Beispiel: **Systemarchitektur**



1. Item Definition

Beschreibung der / Link auf die

- Funktionalen Anforderungen
- Nicht-Funktionalen Anforderungen
- Systemarchitektur
- Schnittstellen
- **Betriebszustände**

Formblatt: **Item Definition**

Item Attribute	Item Description
Funktionale Anforderungen	Die Funktionalen Anforderungen liegen in dem Top-Systemelement "**Fahrer-Assistenz-Systeme (ADAS)**" Der Link verweist auf die erste Funktion.
Nicht-Funktionale Anforderungen	Die Nicht-Funktionalen Anforderungen liegen in dem Top-Systemelement "**Nicht-Funktionale Anforderungen**"
Systemarchitektur	
Interaktionen	
Betriebszustände	Betriebszustände sind in dem entsprechenden Katalog auf Projektebene abgelegt.

1. Item Definition

Beispiel: **Betriebszustände**

Fahrsituation (Operational situation)
Fahren Zone 30
Fahren Stadtverkehr
Fahren Landstraße
Fahren Autobahn
Parken

Formblätter und Netze

liegen in **einer Datenbank** und stehen für

die „Item-Definition“ => Funktionales Sicherheitsprojekt

und

„System- und Funktionsanalyse“ => FMEA Projekt

stets aktuell zur Verfügung!

2. Hazard and Risk Analysis

Identifizieren und Klassifizieren von Gefahrensituationen und Ableiten der Schutzziele!

Beispiel: **Gefahrenanalyse**

Fahrer-Assistenz-Systeme (ADAS)

Bearbeiter	plato	Letzte Änderung	Mi 23.01.2013 15:14
Kommentar			

Gefährdung	Fahrsituation	E	Folgen	S	Kontrollierbarkeit	C	ASIL	ASIL res.	Schutzziel	Sicherheitsfunktion
Unmotivierter Bremsvorgang	Fahren Zone 30	E4	Fahrer erschrickt und führt Lenkbewegung aus / latente Unfallgefahr	S1	Am Fahrbahnrand stoppen	C1	QM	C	Unmotivierten Bremsvorgang ausschlissen	Unmotivierten Bremsvorgang sicher ausschließen
	Fahren Landstraße	E4	Fahrer erschrickt und führt Lenkbewegung aus / erhöhte Unfallgefahr	S2	Keine Kontrolle	C3	C			
	Fahren Stadtverkehr	E4	Fahrer erschrickt und führt Lenkbewegung aus / erhöhte Unfallgefahr	S2	Keine Kontrolle	C3	C			

Fahrsituation (Operational situation)
Fahren Zone 30
Fahren Stadtverkehr
Fahren Landstraße
Fahren Autobahn
Parken

Fahrsituationen kommen aus dem Katalog „Betriebszustände“!

Identifizieren und Klassifizieren von Gefahrensituationen und Ableiten der Schutzziele!

Beispiel: **Gefahrenanalyse**

Fahrer-Assistenz-Systeme (ADAS)

Bearbeiter	plato	Letzte Änderung	Mi 23.01.2013 15:14
Kommentar			

Gefährdung	Fahrsituation	E	Folgen	S	Kontrollierbarkeit	C	ASIL	ASIL res.	Schutzziel	Sicherheitsfunktion
Unmotivierter Bremsvorgang	Fahren Zone 30	E4	Fahrer erschrickt und führt Lenkbewegung aus / latente Unfallgefahr	S1	Am Fahrbahnrand stoppen	C1	QM	C	Unmotivierten Bremsvorgang ausschlissen	Unmotivierten Bremsvorgang sicher ausschließen
	Fahren Landstraße	E4	Fahrer erschrickt und führt Lenkbewegung aus / erhöhte Unfallgefahr	S2	Keine Kontrolle	C3	C			
	Fahren Stadtverkehr	E4	Fahrer erschrickt und führt Lenkbewegung aus / erhöhte Unfallgefahr	S2	Keine Kontrolle	C3	C			

ASIL Einstufungen werden nach ISO/DIS 26262 berechnet!

Identifizieren und Klassifizieren von Gefahrensituationen und Ableiten der Schutzziele!

Beispiel: **Gefahrenanalyse**

Fahrer-Assistenz-Systeme (ADAS)

Bearbeiter	plato	Letzte Änderung	Mi 23.01.2013 15:14
Kommentar			

Gefährdung	Fahrsituation	E	Folgen	S	Kontrollierbarkeit	C	ASIL	ASIL res.	Schutzziel	Sicherheitsfunktion
Unmotivierter Bremsvorgang	Fahren Zone 30	E4	Fahrer erschrickt und führt Lenkbewegung aus / latente Unfallgefahr	S1	Am Fahrbahnrand stoppen	C1	QM	C	Unmotivierten Bremsvorgang ausschlissen	Unmotivierten Bremsvorgang sicher ausschließen
	Fahren Landstraße	E4	Fahrer erschrickt und führt Lenkbewegung aus / erhöhte Unfallgefahr	S2	Keine Kontrolle	C3	C			
	Fahren Stadtverkehr	E4	Fahrer erschrickt und führt Lenkbewegung aus / erhöhte Unfallgefahr	S2	Keine Kontrolle	C3	C			

Sicherheitsfunktionen gehen mit ASIL Einstufung automatisch in die Anforderungsanalyse, d.h. sie stehen

- in den Funktionalen Anforderung der Item-Definition => Funktionales Sicherheitsprojekt
- in der Top-Ebene der System-FMEA => FMEA Projekt

2. Hazard and Risk Analysis

Kurzbezeichnung / Funktion	ID	ASIL	Anforderungsbeschreibung	Fehlermöglichkeiten	Status	Zielmarkt
Erkennung von Objekten und Ereignissen	A1		Objekte auf der Fahrbahn sollen in einem Abstand von 40 m erkannt werden.	Objekterkennung zu spät.	Offen	Europa, USA
Erkennung von Fußgängern	A2		Fußgänger auf der Fahrbahn sollen in einem Abstand von 40 m erkannt werden.	Objekterkennung zu spät.	Offen	Europa, USA
Müdigkeit erkennen	A6		Gesichtsüberwachung soll Müdigkeit erkennen.	Müdigkeitserkennung findet nicht statt.	Abgeschlossen	Europa, USA
Spurwechel unterstützen	A4		noch zu definieren		Undefiniert	Europa, USA
Abstandsregelung bieten	A5		PKW darf vorgegebenen Abstand zum vorderen Fahrzeug nicht unterschreiten. 	Abstandregelung löst zu früh aus. Abstandregelung löst zu spät aus. Abstandregelung gibt falsche Werte Abstandregelung löst ungewollt aus	Abgeschlossen	Europa, USA
Unmotivierten Bremsvorgang sicher ausschließen		C		Bremsung ausgelöst, wenn kein Objekt vorhanden ist.	Undefiniert	

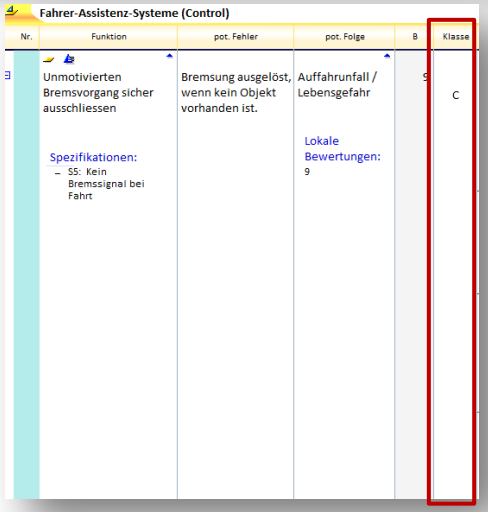
Ergebnis aus der Gefahrenanalyse fließt automatisch in die Anforderungsanalyse ein!

=> so stehen sie im Funktionsnetz für System-FMEA **UND** funktionalen Sicherheitskonzept

System- und Funktionsanalyse mit Sicherheitsfunktion

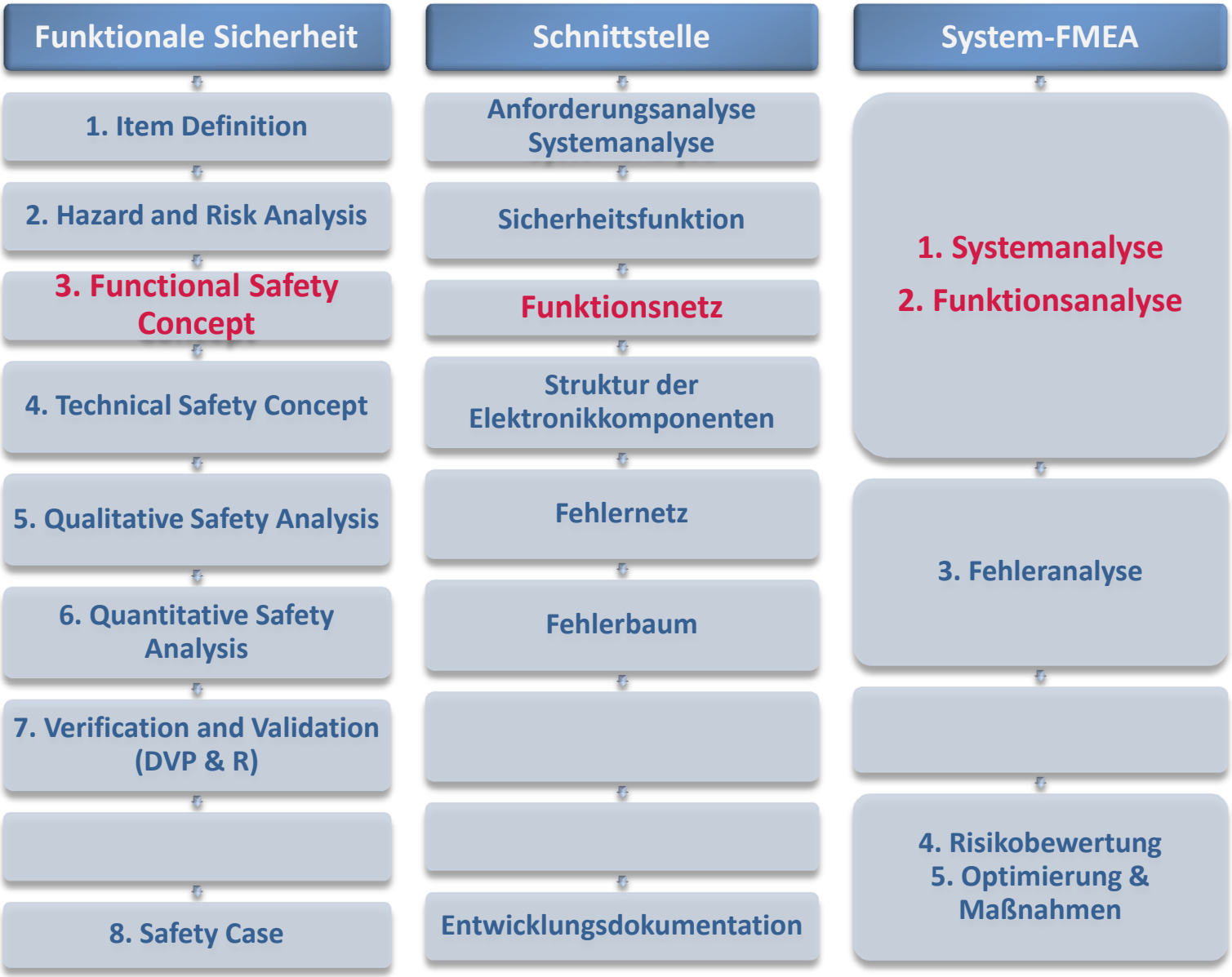
Beispiel: **Matrix-Analyse**

Fahrer-Assistenz-Systeme (ADAS)	Erkennung von Objekten und Ereignissen	Erkennung von Fußgängern	Müdigkeit erkennen	Spurwechel unterstützen	Abstandsregelung bieten	Unmotivierten Bremsvorgang sicher ausschliessen
Ultraschall					X	X
Radar	X	X		X		X
Kamera	X	X				X
Innenkamera			X			



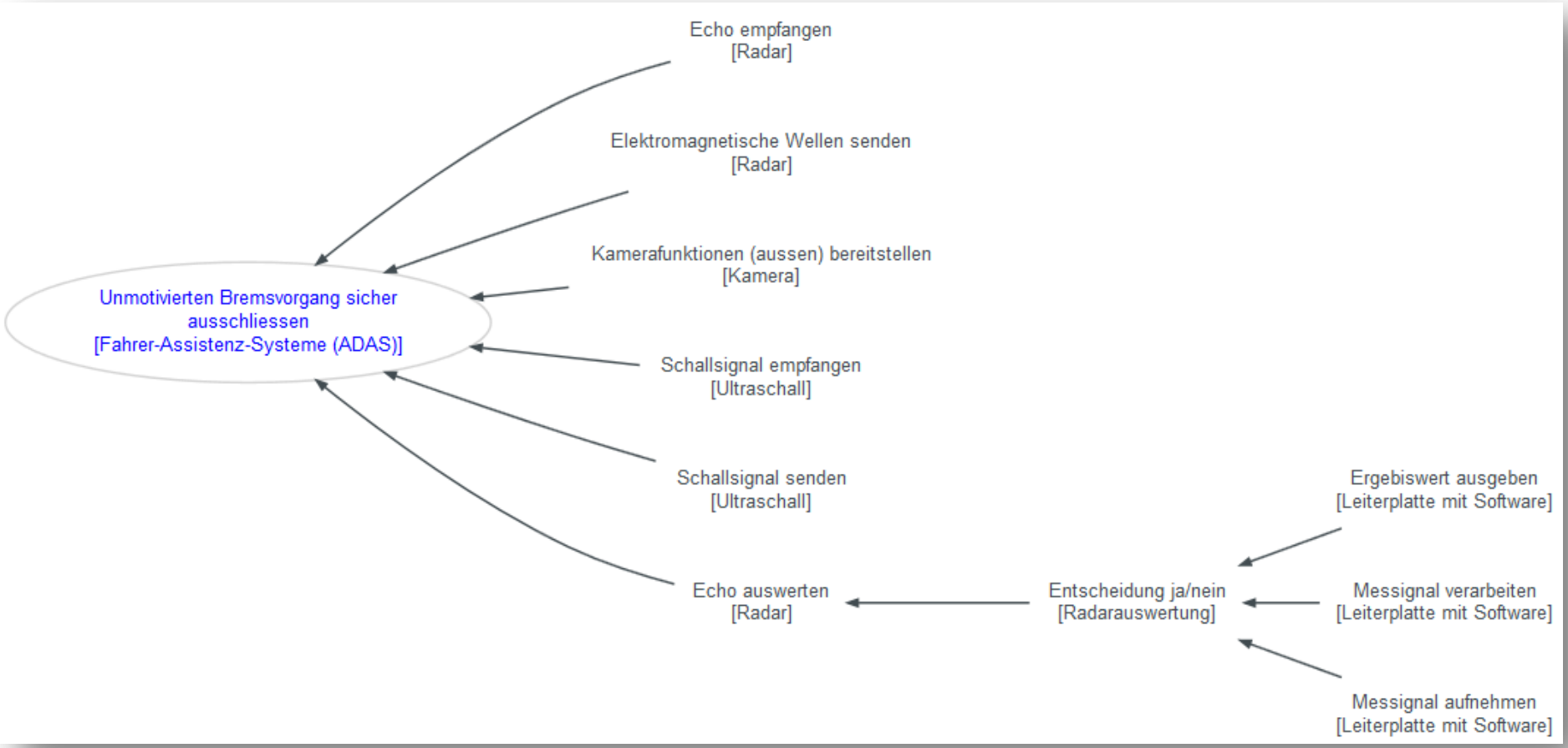
Radar	Unmotivierten Bremsvorgang sicher ausschliessen [Fahrer-Assistenz-Systeme (ADAS)]		
	Elektromagnetische Wellen senden	Echo empfangen	Echo auswerten
Radarantenne	X	X	
Radarsender	X		
Radarempfaenger		X	
Radarauswertung			X

3. Functional Safety Concept

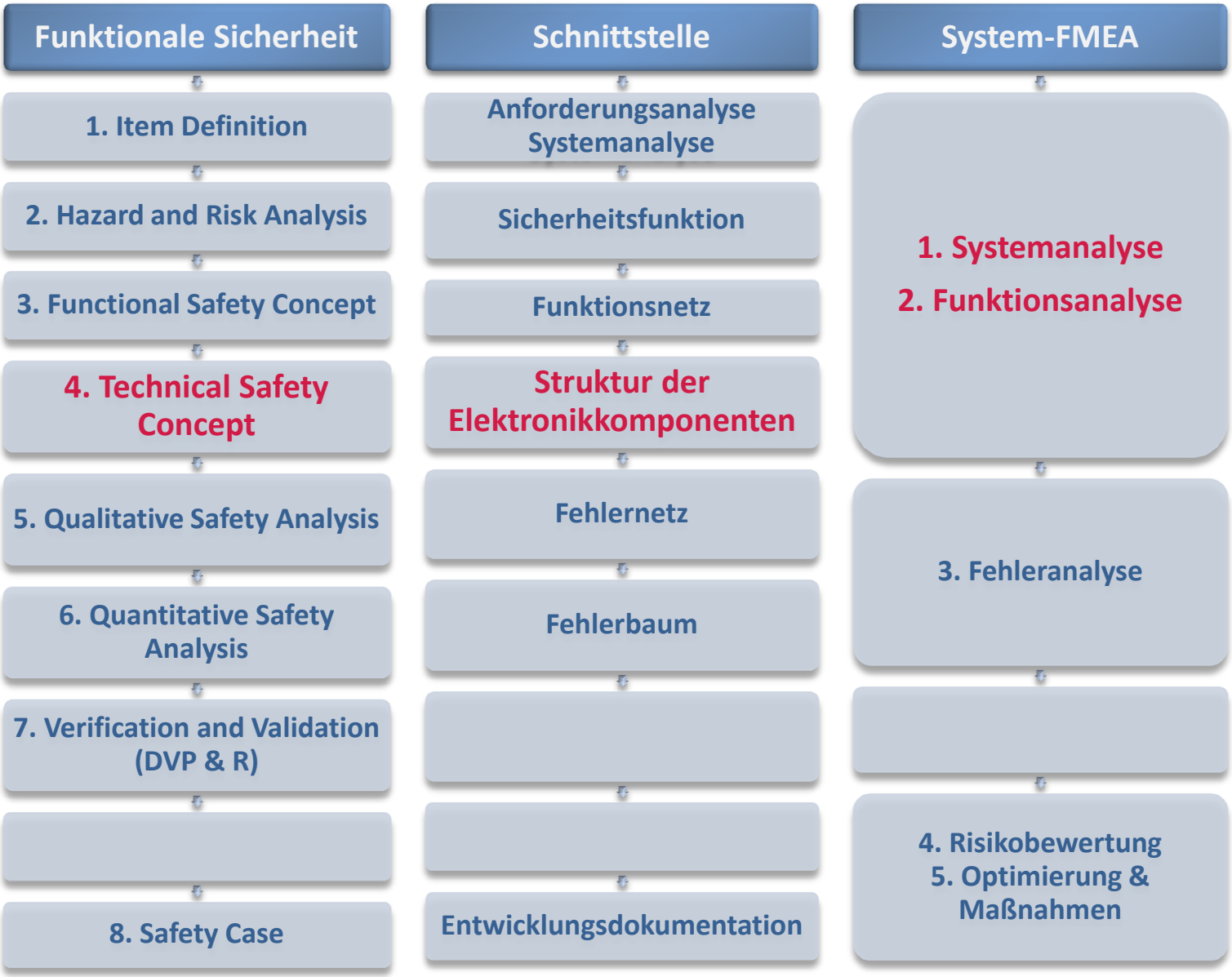


Konzept zur funktionalen Umsetzung der Sicherheitsfunktion (FUSI + FMEA)

Beispiel: **Funktionsnetz**



4. Technical Safety Concept

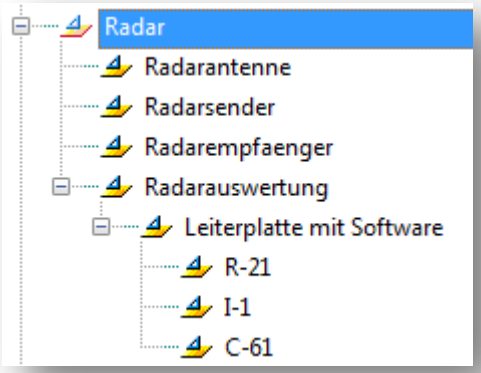


Konzept zur technischen Umsetzung der Sicherheitsanforderung (FUSI + FMEA)

Beispiel: **Matrix-Analyse**

Fahrer-Assistenz-Systeme (ADAS)	Erkennung von Objekten und Ereignissen	Erkennung von Fußgängern	Müdigkeit erkennen	Spurwechel unterstützen	Abstandsregelung bieten	Unmotivierten Bremsvorgang sicher ausschliessen
Ultraschall					X	X
Radar	X	X		X		X
Kamera	X	X				X
Innenkamera			X			

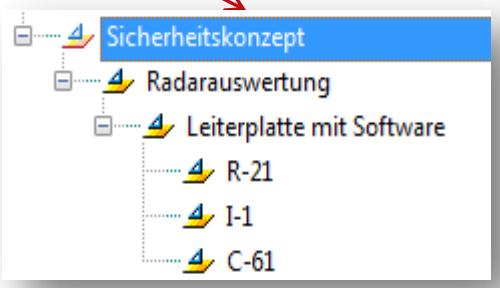
Beispiel: Systemarchitektur **Radar** für die System-FMEA:
=> alle zuliefernden Systemelemente werden gelistet



Konzept zur technischen Umsetzung der Sicherheitsanforderung (FUSI + FMEA)

Beispiel: **Matrix-Analyse**

Fahrer-Assistenz-Systeme (ADAS)	Erkennung von Objekten und Ereignissen	Erkennung von Fußgängern	Müdigkeit erkennen	Spurwechel unterstützen	Abstandsregelung bieten	Unmotivierten Bremsvorgang sicher ausschliessen
Ultraschall					X	X
Radar	X	X		X		X
Kamera	X	X				X
Innenkamera			X			
Technisches Sicherheitskonzept	X	X	X			X



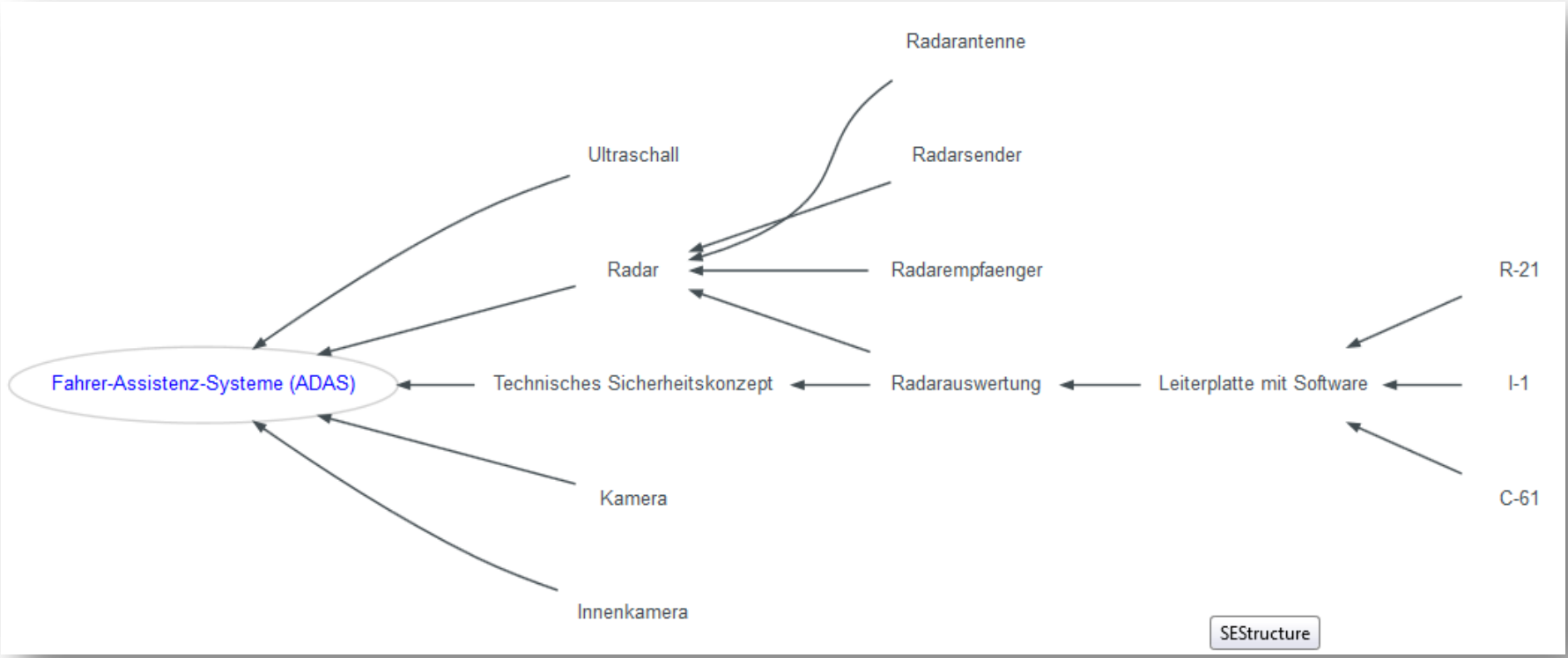
Beispiel: Systemarchitektur für das Sicherheitskonzept:

=> Nur die dem Sicherheitskonzept zuliefernden Komponenten werden gelistet

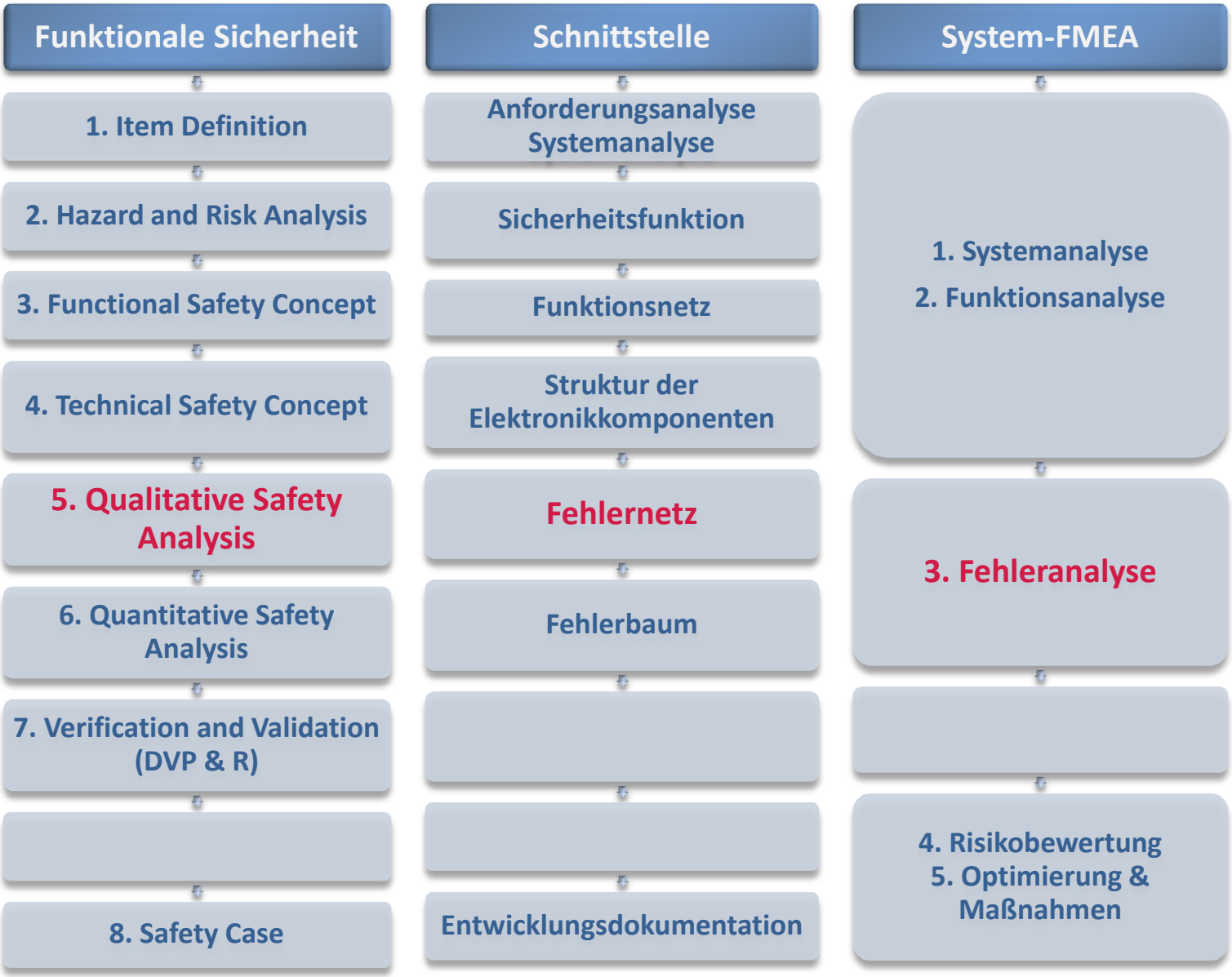
=> Identische Systemelement werden mehrfach (in beiden Projekten) angezeigt

Konzept zur technischen Umsetzung der Sicherheitsfunktion (FUSI + FMEA)

Beispiel: **Systemstruktur**

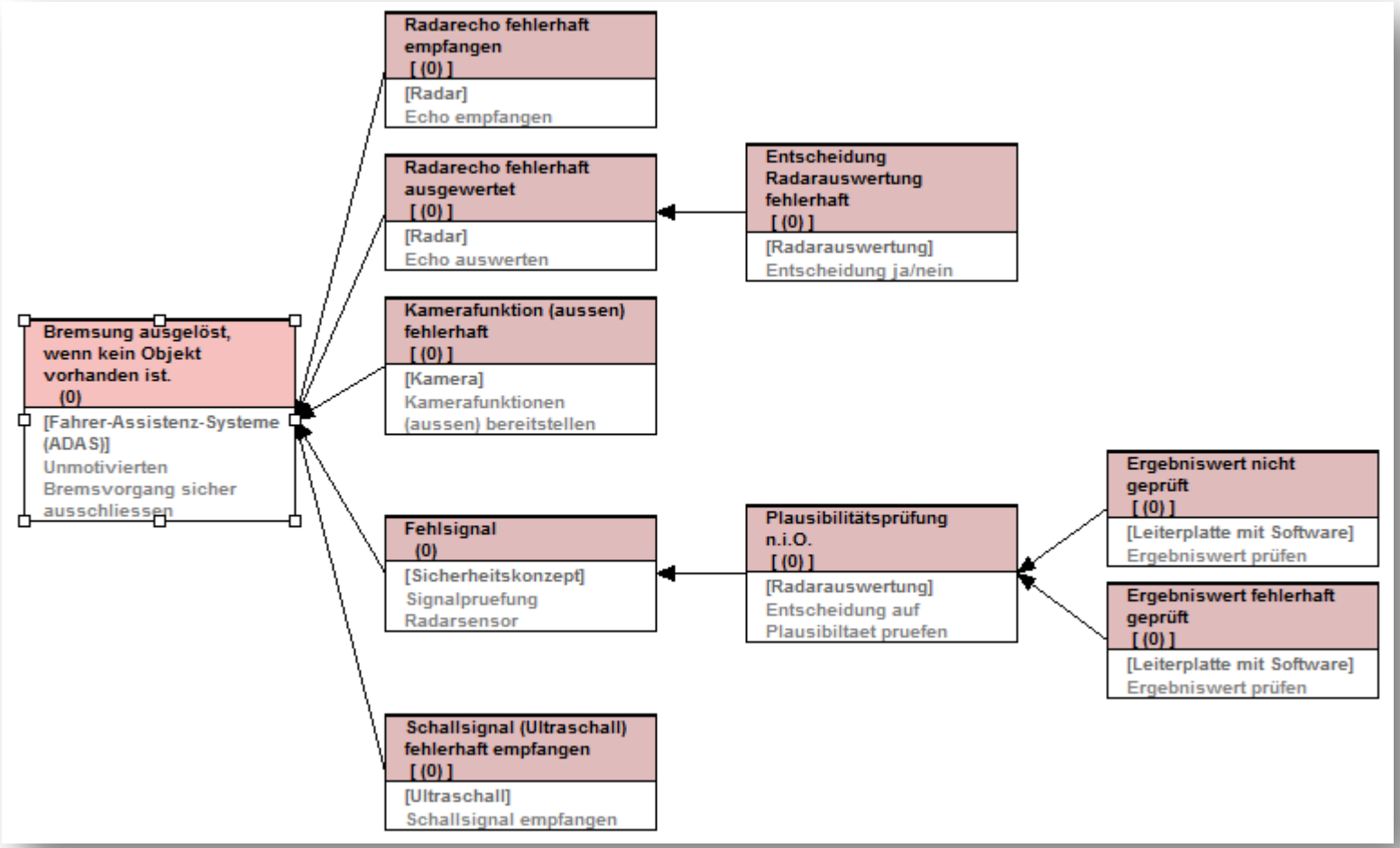


5. Qualitative Safety Analysis



Nachweisführung, dass das Design die Sicherheitsziele erfüllt (Fehlernetz, FMEA).

Beispiel: **Fehlernetz**

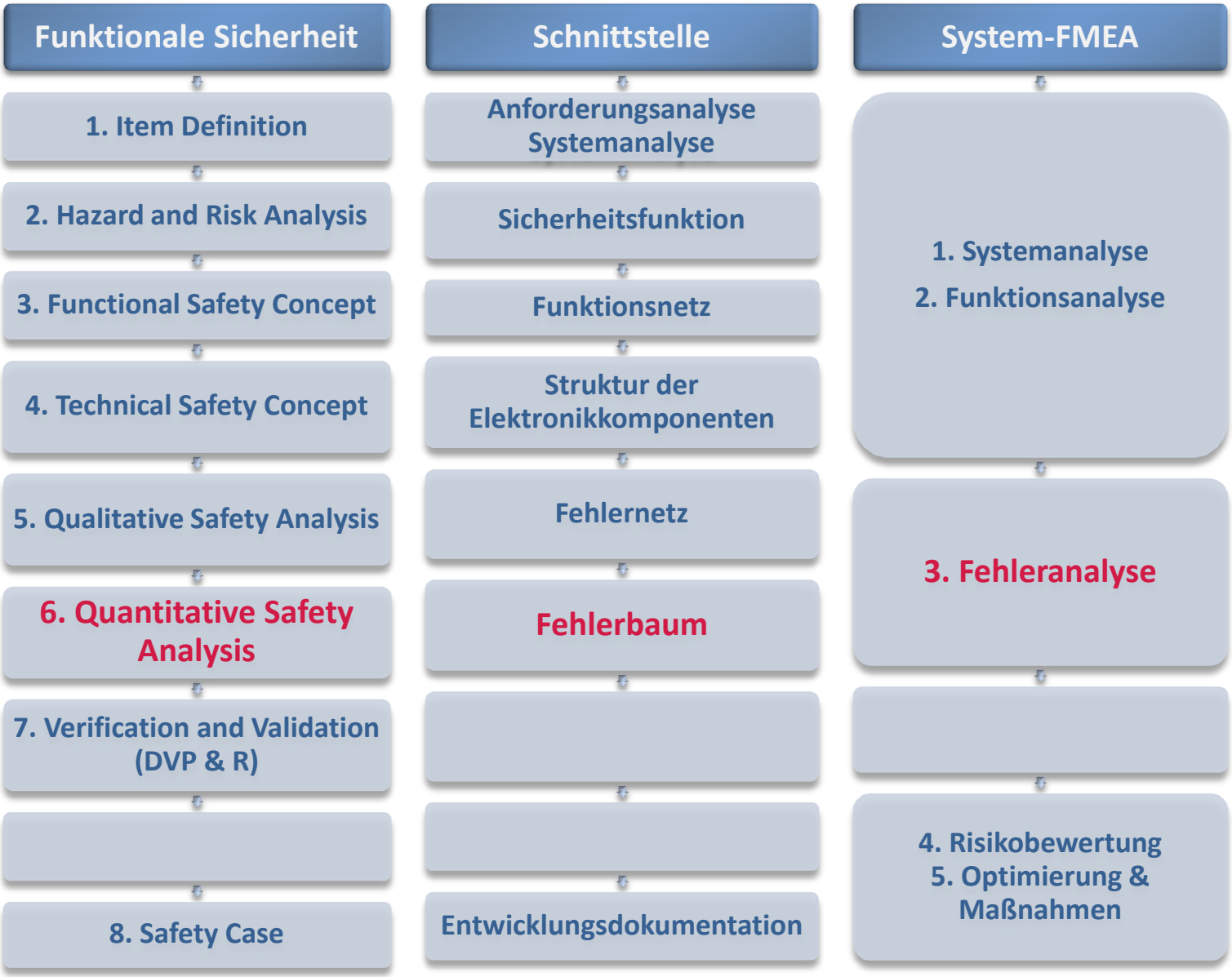


Fehlerverknüpfungen werden in das FMEA Formblatt übernommen

Fahrer-Assistenz-Systeme (ADAS)

Nr.	Funktion	pot. Fehler	pot. Folge	B	Klasse	Ursache(n)	A	V-Maßnahme(n)	P-Maßnahme(n)	E	RPZ
	Abstandsregelung bieten										
	Unmotivierten Bremsvorgang sicher ausschliessen Spezifikationen: – S5: Kein Bremssignal bei Fahrt	Bremsung ausgelöst, wenn kein Objekt vorhanden ist.	Auffahrunfall / Lebensgefahr	9	C	Schallsignal (Ultraschall) fehlerhaft empfangen Herkunft: Ultraschall	Stand: 07.05.2013 5	keine	DVP	3	135
						Radarecho fehlerhaft empfangen Herkunft: Radar	Stand: 07.05.2013 3	keine	DVP	3	81
						Radarecho fehlerhaft ausgewertet Herkunft: Radar	Stand: 07.05.2013 2	Funktionales Sicherheitskonzept	DVP	3	54
						Kamerafunktion (aussen) fehlerhaft Herkunft: Kamera	Stand: 07.05.2013 4	keine	DVP	3	108

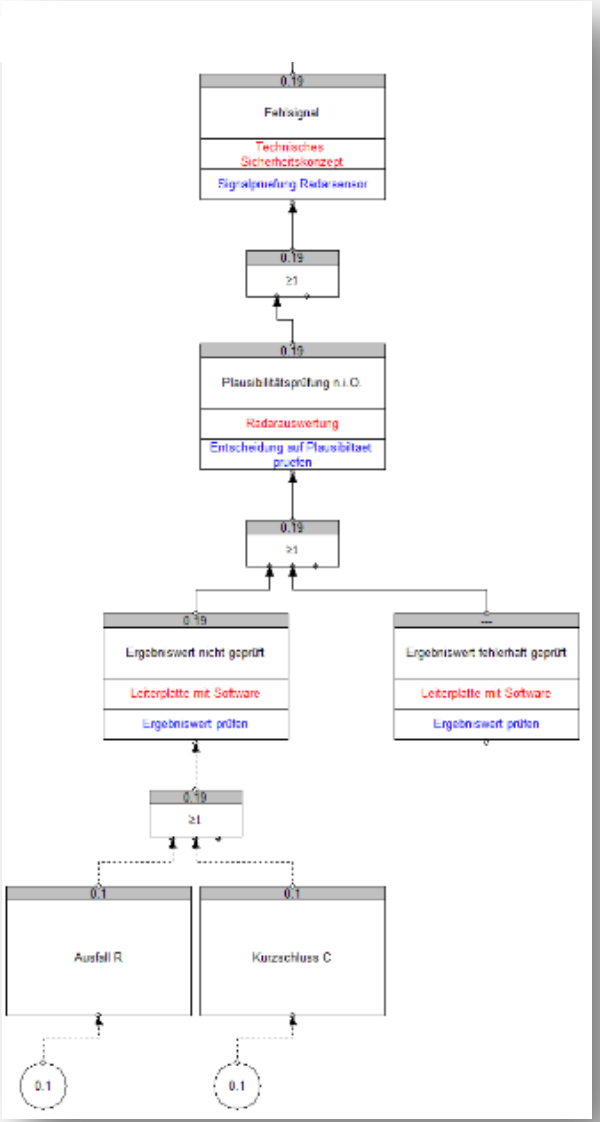
6. Quantitative Safety Analysis



6. Quantitative Safety Analysis

Berechnung der Wahrscheinlichkeit, dass die Sicherheitsfunktion ausfällt.

Beispiel: **Fehlerbaum**



6. Quantitative Safety Analysis

Berechnung der Wahrscheinlichkeit, dass die Sicherheitsfunktion ausfällt, bzw. dass der Ausfall nicht frühzeitig erkannt wird

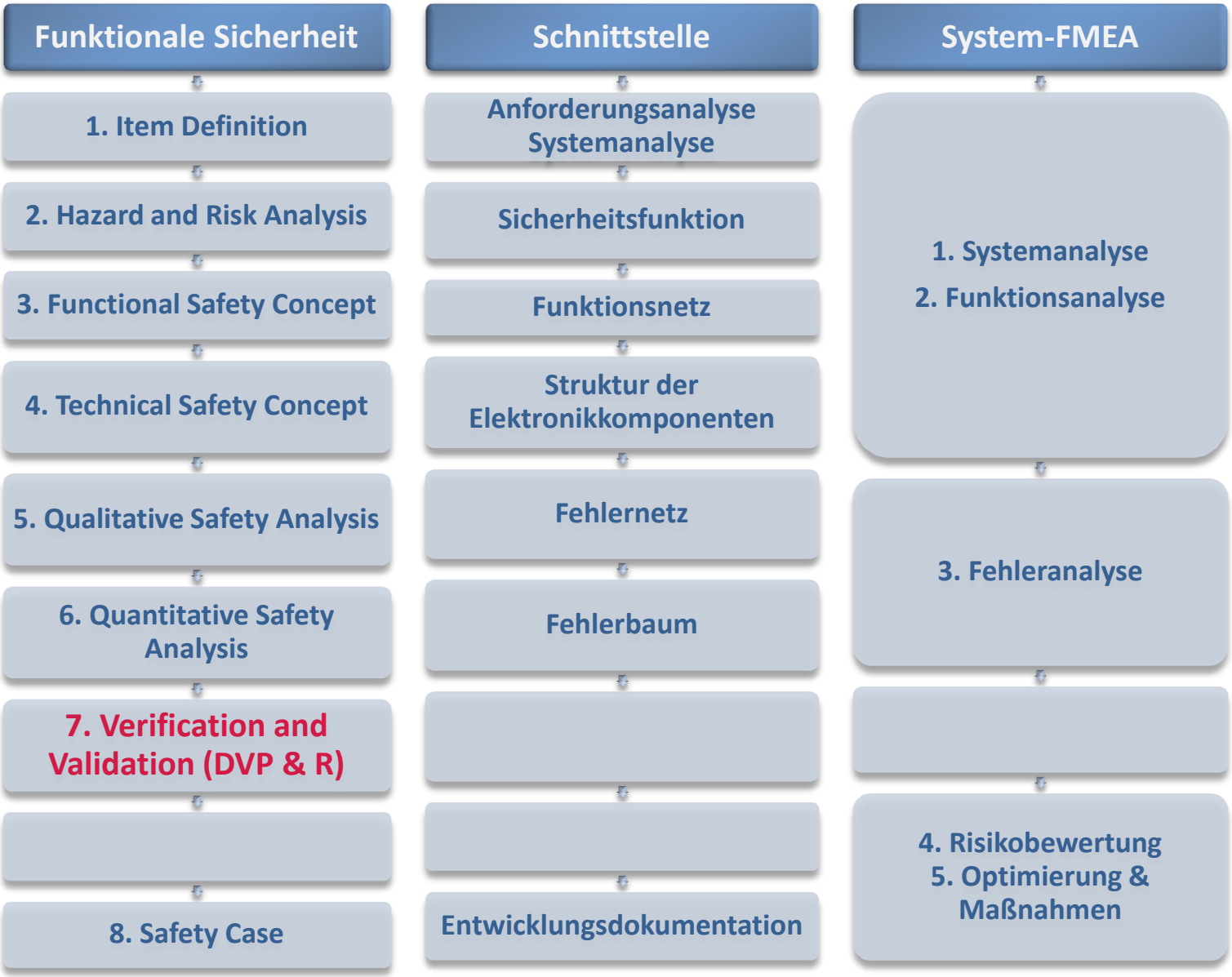
Beispiel: **FMEDA**

Systemelement	Komp.Typ	FIT	Sicherheitsrel. Komp.	Funktion	Fehlerart	Verteilung der Fehlerrate	Fehler verletzt Sicherheitsziel	Sicherheitsmechanismus für Sicherheitsziel	Fehlerabdeckung	FIT - Residual oder Single-Point
R-21	R	2	SR	R-21	open	90.0 %	☑		99.0 %	0.018
					closed	10.0 %	☑	SM 2	99.0 %	0.002
I-1	I	4	NSR	I-1	closed	20.0 %	☑	SM 2	99.0 %	0.008
					open	70.0 %	☑	SM 2	99.0 %	0.028
					drift 2	5.0 %	☐		0.0 %	-
					drift 0,5	5.0 %	☑	SM 2	99.0 %	0.002
C-61	T	5	SR	T-61	short circuit	10.0 %	☑	SM 3	90.0 %	0.05
					open circuit	90.0 %	☐		0.0 %	-

Total failure rate	11	**∑1**	0.11	**∑2**	0
Total Safety Related	7	**Single Point Faults Metric**	98.4%	**Latent Faults Metric**	100%
Total Not Safety Related	4				

ASIL C ist erfüllt!

7. Verification and Validation (DVP & R)



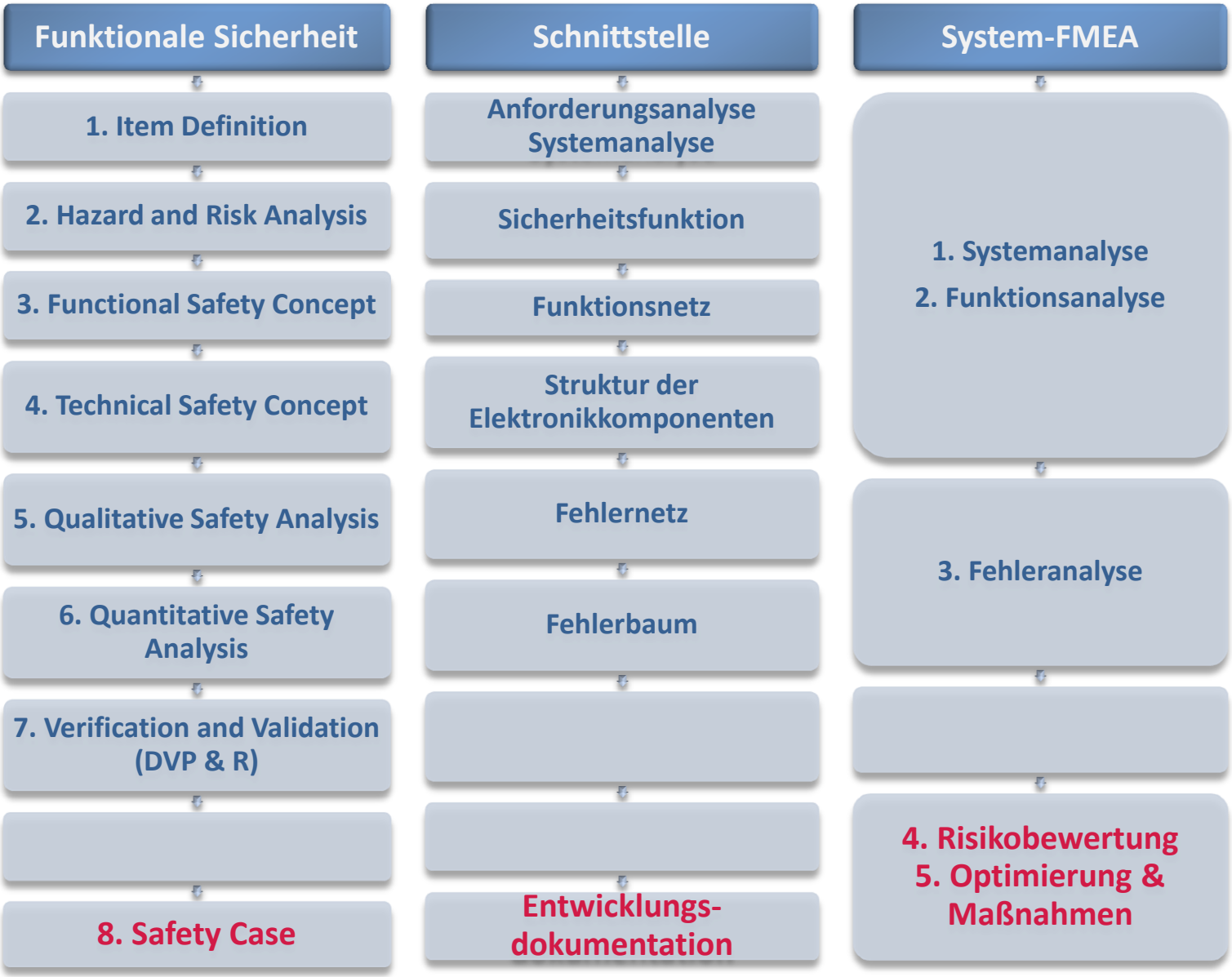
Prüfen und Nachweisen, dass alle (Sicherheits-)Funktionen korrekt umgesetzt wurden!

Beispiel: **DVP&R**

Funktion		Testplan				Testdurchführung					
Anforderung / Funktion	ASIL	Abnahmekriterium / Soll-Größe	Testmethode	Test	Beschreibung	Start	Ende	Verantw.	Stichprob. soll	Stichprob. ist	Ergebnis
Unmotivierten Bremsvorgang sicher ausschließen	C	S5: Kein Bremssignal bei Fahrt	Dauerfahrt mit Signalüberwachung	Stadtfahrt	Fahrt durch die Lübecker Innenstadt	25.01.2013	30.01.2013	Plato			OK
Erkennung von Objekten und Ereignissen		S1: Entfernung 40 m (Max: 42 / Min: 0)	Simulation der Fahrsituation								
		S2: Geschwindigkeit <= 2 ms	Geschwindigkeitsmessung durch Testskript								

Sämtliche Anforderungen und Spezifikationen erscheinen automatisch im DVP!

8. Safety Case



Der Sicherheitsnachweis wird erbracht durch die Gestaltung eines strukturierten, schlüssigen, vollständigen und überzeugenden Systems und den Beweis dass alle Sicherheitsziele und zugehörigen Vorschriften erfüllt sind.

Ausblick:

- Erbringung des Nachweises mit SCIO™ Methods, dass alle Gefährdungen, die ermittelt wurden und einen ASIL C oder D haben, sicher abgedeckt sind
- Nachweis ist Bestandteil der Entwicklungsdokumentation

Fazit

- Funktionales Sicherheitsprojekt und Erstellung der System FMEA durchgängig in einem Datenmodell
- Daten werden methodenspezifisch erfasst und anderen Methode zur Verfügung gestellt
- Formblätter und Datenaustausch können kundenspezifisch angepasst werden
- Normenkonformität durch Vorgabekataloge
- Darstellung komplexer Zusammenhänge in Netzen
- Daten sind themenspezifisch abruf- und darstellbar (Netze, Formblätter, Berechnungen)

So kommen wir ins Gespräch …

Auf der Control 2013: PLATO AG, Halle 1, Stand 1616

Per Telefon: +49.451.930 986-05

Per Email : info@plato.de