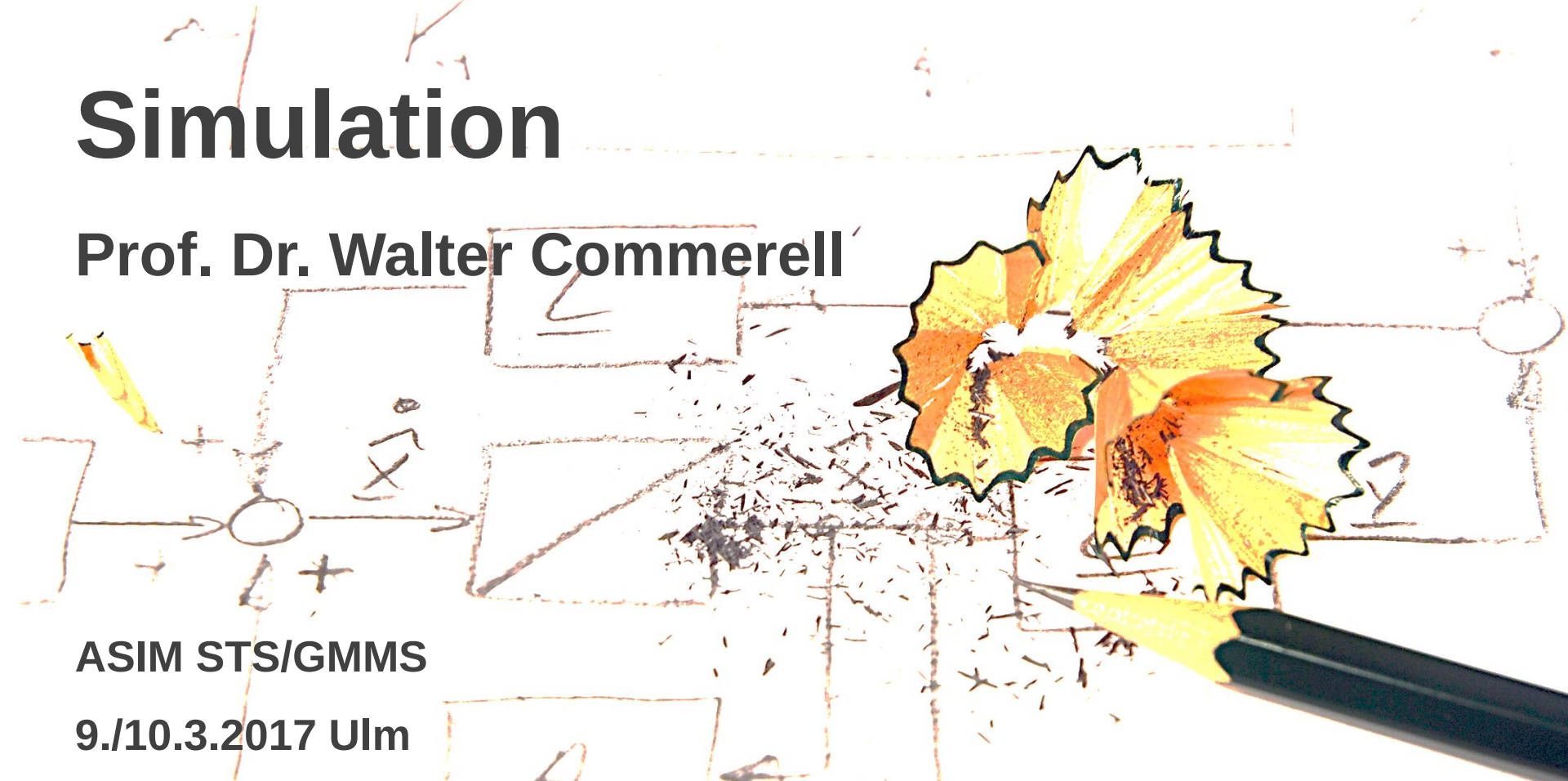
Steinbeis-Transferzentrum
System Design

Hochschule Ulm

Funktionale Sicherheit und Simulation

Prof. Dr. Walter Commerell



ASIM STS/GMMS

9./10.3.2017 Ulm

Inhalt

- Funktionale Sicherheit bei Fahrzeugen
- Simulative Anforderungen der ISO26262
- Optimaler Einsatz von Simulationsmodellen
- Zusammenfassung

Funktionale Sicherheit bei Fahrzeugen
Zielsetzung der ISO 26262

- Standardisiertes Vorgehen bei
  - der Entwicklung
  - der Produktion und
  - dem Betrieb
- Dadurch werden
  - Systematische Fehler vermieden,
  - Zufällige Fehler minimiert und
  - das Restrisiko minimiert.

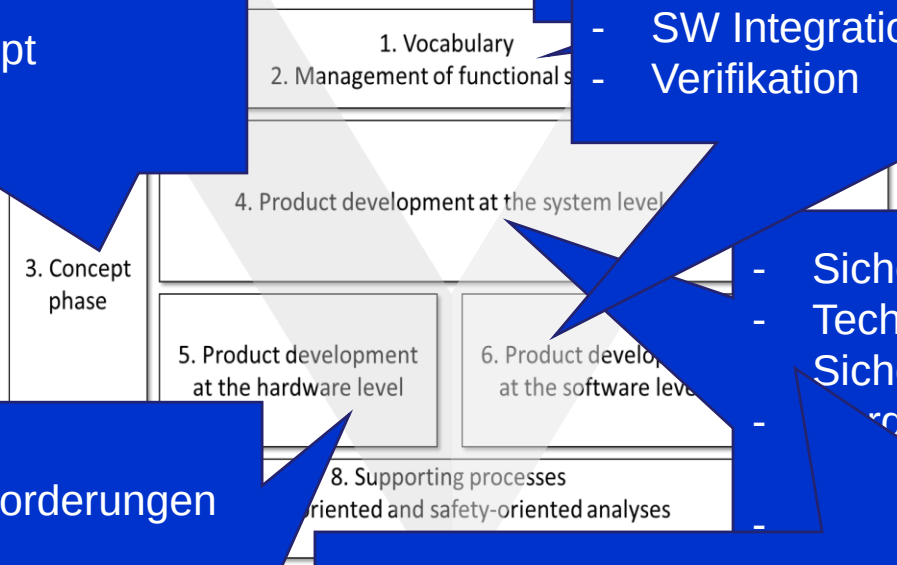
Betrachtung des gesamten Lebenszyklus

sichere Funktion

Funktionale Sicherheit bei Fahrzeugen Maßnahmen

- Einfluss Analyse
- Sicherheits plan
- Gefahren und Risikoanalyse => ASIL Level
- Sicherheitskonzept

- SW Sicherheitsanforderungen
- SW Architektur Design
- SW Design und Implementierung
- SW Integration und Test
- Verifikation



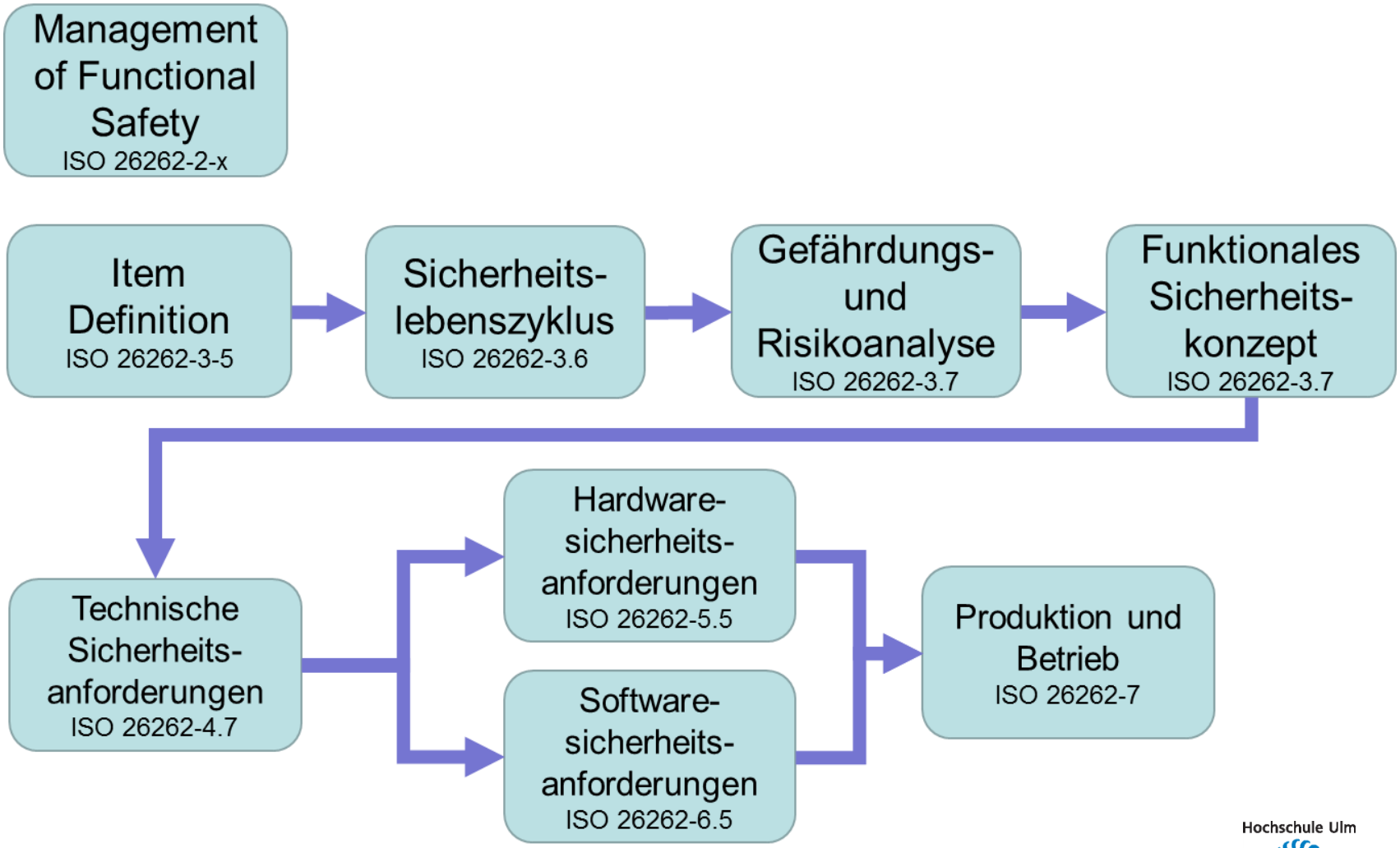
- Sicherheitsanforderungen
- Technisches Sicherheitskonzept
- rdware- Software
- telle
- ration und Test
- ntung

- HW Sicherheitsanforderungen
- HW Design
- Evaluierung der HS Metriken
- Evaluierung der Sicherheitsverletzungen durch zufällige Fehler
- HW Integration und Test

- Produktionsplanung
- Sicherheits-Wartungsplanung

Hochschule Ulm

Funktionale Sicherheit bei Fahrzeugen Vorgehen



Funktionale Sicherheit bei Fahrzeugen Vorgehen

- Einteilung der Funktion in Klassen
  - Schadensausmaß
  - Eintritts-wahrscheinlichkeit
  - Kontrollierbarkeit

	Severity class			
	S0	S1	S2	S3
Description	No injuries	Light and moderate injuries	Serve and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain) fatal injuries

	Probability class				
	E0	E1	E2	E3	E4
Description	Incredible	Very low probability	Low probability	Medium probability	High probability

	Controlability class			
	C0	C1	C2	C3
Description	Controllable in General	Simply Controllable	Normally Controllable	Difficult to control or uncontrollable

Funktionale Sicherheit bei Fahrzeugen Vorgehen

- Ermittlung des ASIL Levels

Serverity class	Probability class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

QM Quality Management

Simulative Anforderungen der ISO26262 Systemebene

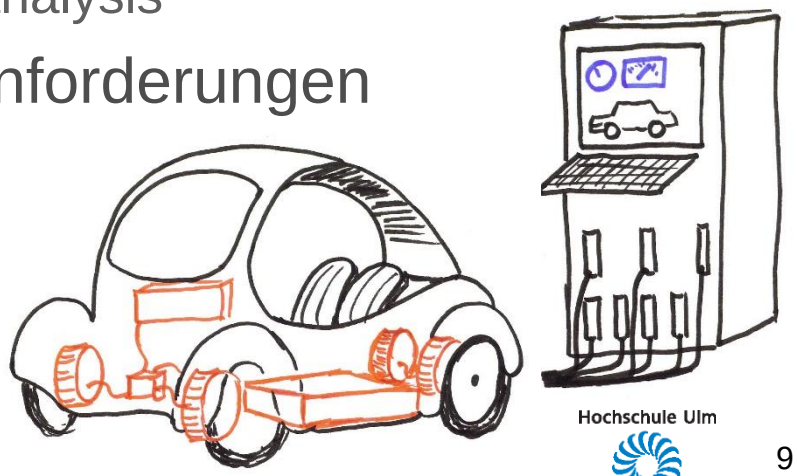
7.4.8	Verification of system design				
7.4.8.1	The system design shall be verified for compliance and completeness with regard to the technical safety concept using the verification methods listed in Table 3.	ASIL			
		A	B	C	D
	1a System design inspection	+	++	++	++
	1b System design walkthrough	++	+	o	o
	2a Simulation	+	+	++	++
	2b System prototyping and vehicle tests	+	+	++	++
	3 System design analyses see Table 1)	Inductive and/or deductive analysis			

++ highly recomended
+ recomended
o non recommendation for or against

Simulation ist für ASIL Level A und B empfohlen und für C und D sehr empfohlen
Alternative ist 2b => teuer und zeitaufwändig

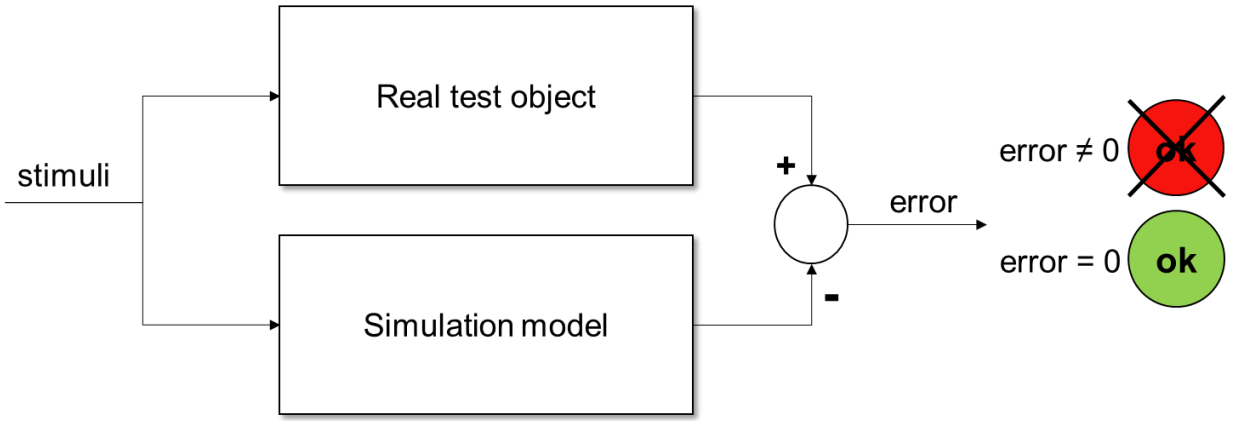
Simulative Anforderungen der ISO26262 Hard- Softwareebene

- Hardwareverifikation durch Simulation
  - Level B-D empfohlen
  - Alternative zum HW Prototyp
  - Vorteile bei der Fehlerinjektion
- Softwareverifikation durch Simulation
  - Alternative zu Walk-through, Inspection, Prototype, formal verif., Control flow, Data flow analysis
- Verifikation der Sicherheitsanforderungen
  - HiL Simulation



Simulative Anforderungen der ISO26262 HW SW Integration

- „Back to back“ Test ASIL A und B empfohlen, ASIL C und D sehr empfohlen

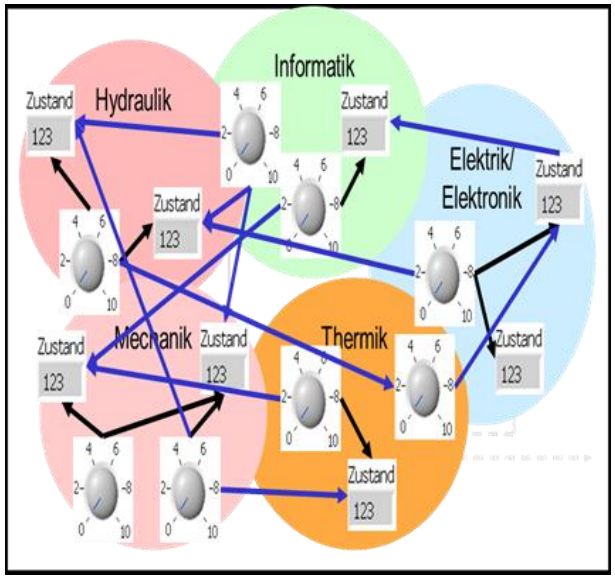


- Analyse des Zeitverhaltens der Sicherheitsmechanismen

Optimaler Einsatz von Simulationsmodellen
Simulatorauswahl

- Für umfassende Analysen und Test

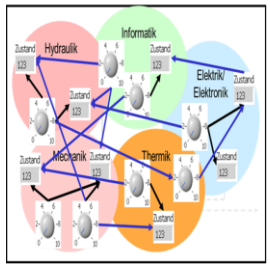
  Multi Domain Problem

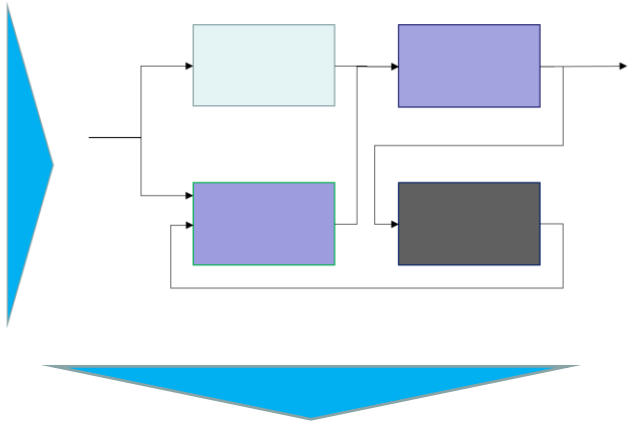


- Multidomain Simulation
  - Multidomain Simulator
  - Simulatorkopplung
  - Modellaustausch z.B. FMI

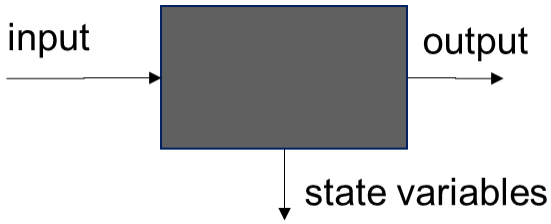
Optimaler Einsatz von Simulationsmodellen
Modellaufbau

- System - / Modellarchitektur
  - klar strukturiert
  - beherrschbar



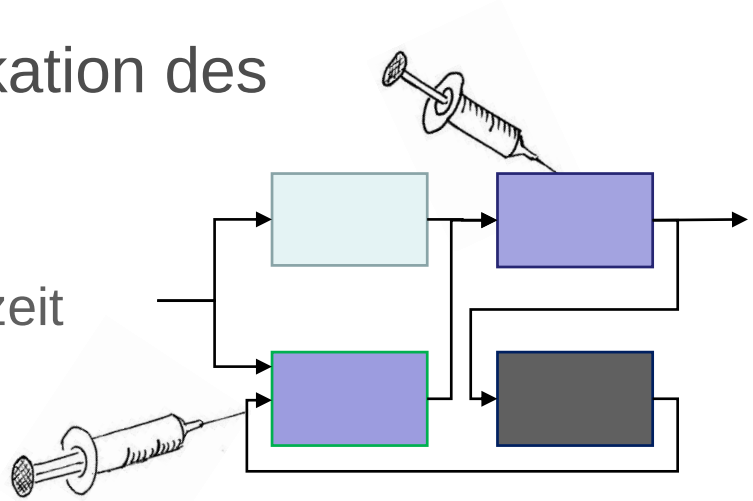


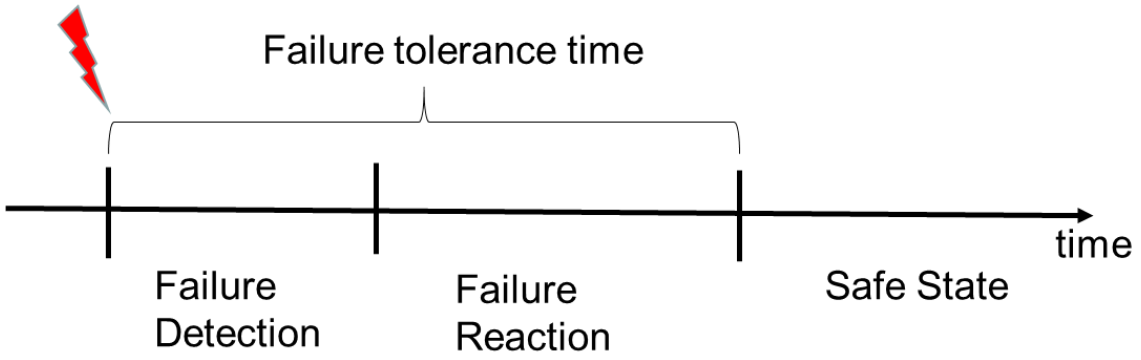
- Begrenzte Anzahl von Schnittstellen
- Messbare Zustandsgrößen



Optimaler Einsatz von Simulationsmodellen
Modellaufbau

- Simulationsmodell zur Verifikation des Sicherheitskonzeptes
  - Durch Fehlerinjektion
  - Verifikation der Fehlertoleranzzeit





Zusammenfassung

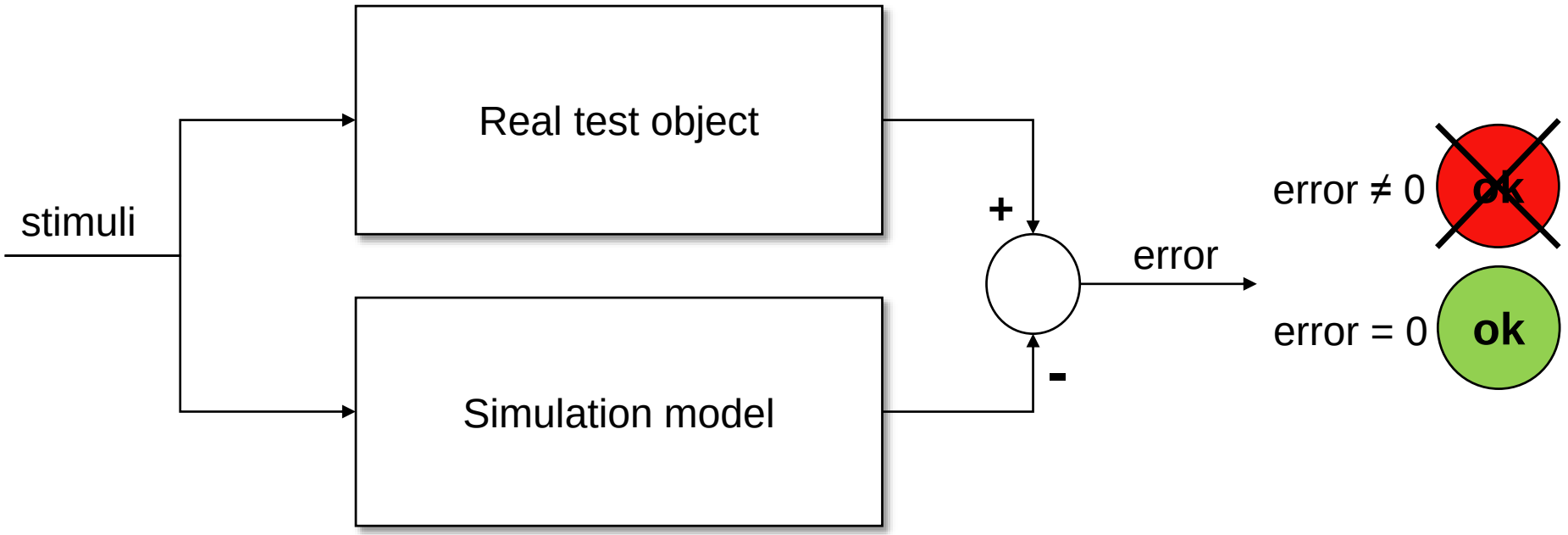
- Die Anwendung der Norm ISO 26262 Funktionale Sicherheit erfordert weit mehr als z.B. CMMI oder SPICE Anforderungen
- Auf Basis der Gefahren- und Risikobewertung erfolgt eine Einstufung in einen „Automotive Savety Integrity Level“ (ASIL) von A bis D (höchster)
- Die Norm fordert Maßnahmen und Prozessschritte anhand der ASIL Einstufung
- Simulationsmethoden bieten eine gute Alternative zu teuren Prototypaufbauten

Vielen Dank für die Aufmerksamkeit

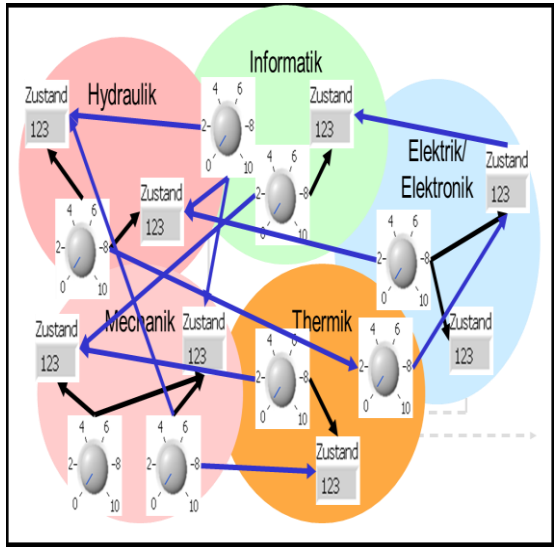
Prof. Dr. Walter Commerell
HS-Ulm
Institut Energie- und Antriebstechnik
Institut Fahrzeugsystemtechnik

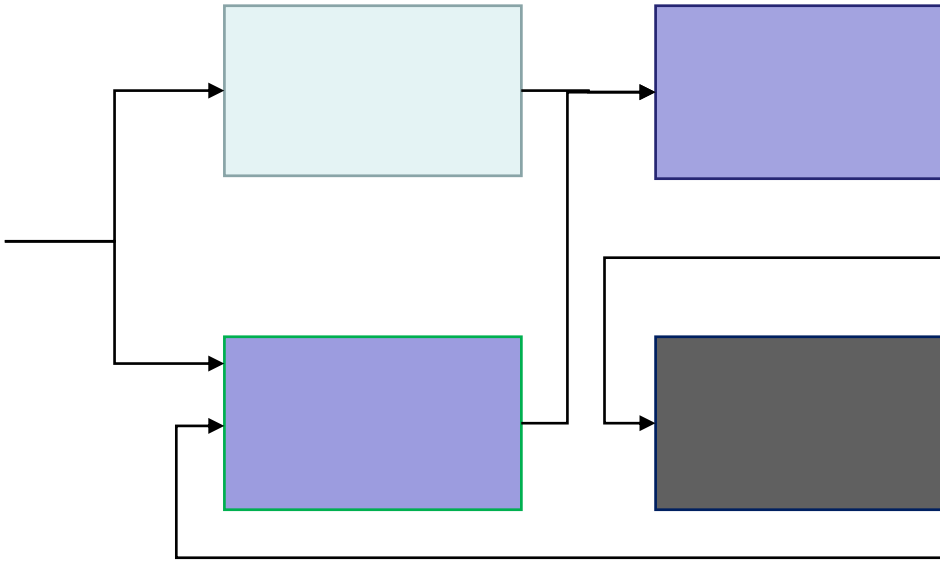
email: Commerell@hs-ulm.de

Simulative Anforderungen der ISO26262 HW SW Integration

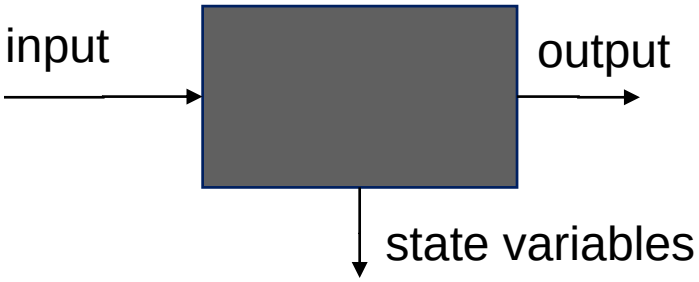


Optimaler Einsatz von Simulationsmodellen
Simulatorauswahl

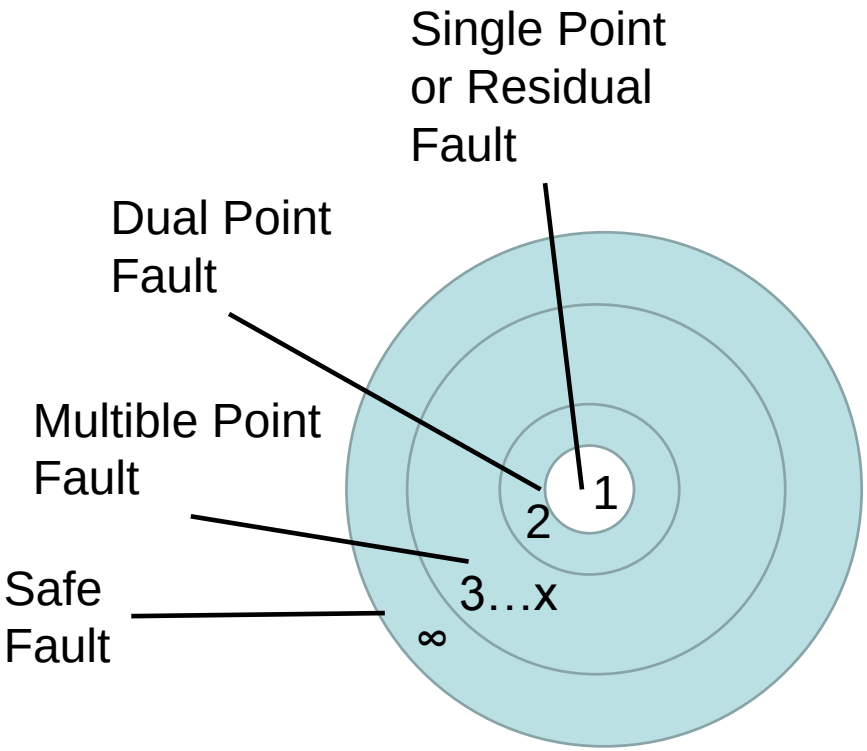




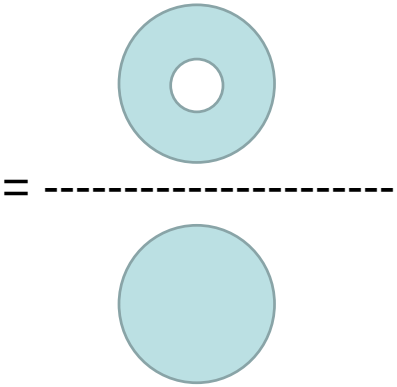
Optimaler Einsatz von Simulationsmodellen



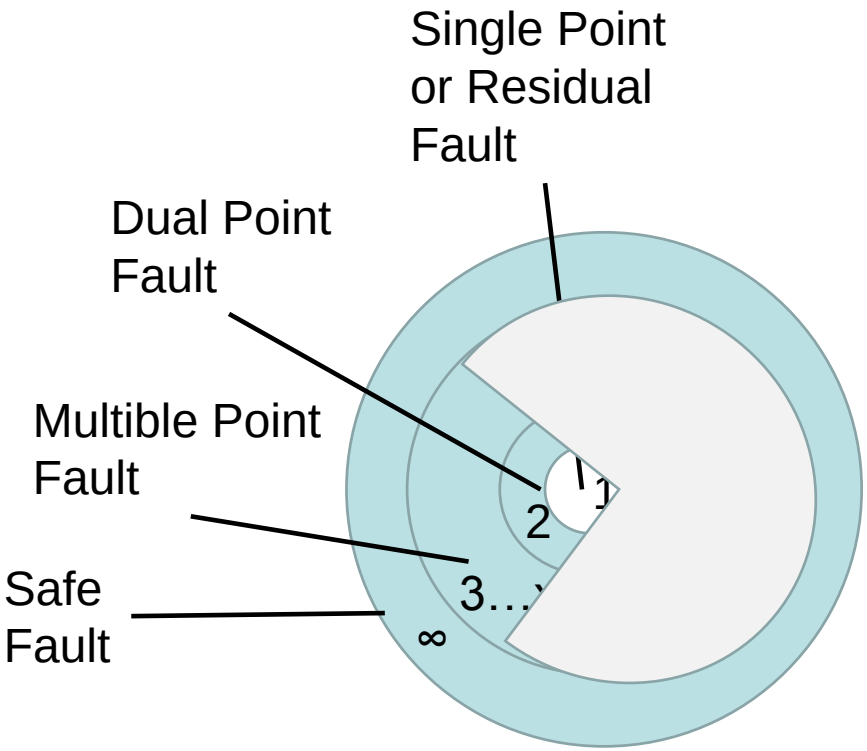
HW Fault Metric
Single Point Fault Metric



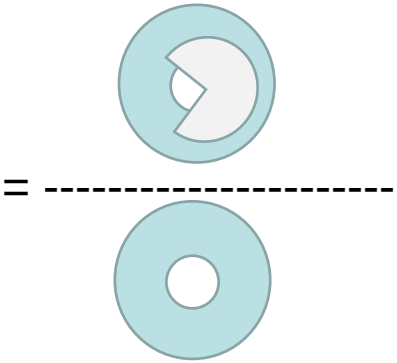
Single Point Fault Metric



HW Fault Metric
Latent Fault Metric



Latent Fault Metric



Optimaler Einsatz von Simulationsmodellen