Der Einsatz quantitativer Sicherheitsanalysen für den risikobasierten Test eingebetteter Systeme

Heiko Stallbaum, Andreas Metzger, Klaus Pohl

Software Systems Engineering

Institute for Computer Science and Business Information Systems (ICB)

University of Duisburg-Essen, Germany

www.sse.uni-due.de

Agenda

- **Einleitung und Motivation**
- Risikobasiertes Testen mittels quantitativer Sicherheitsanalysen
- Zusammenfassung und Ausblick

Testen und Sicherheitsanalysen

- Für eingebettetes System oftmals **Sicherheitsnachweis** gefordert
  - **Sicherheit** (Safety) ist Abwesenheit von **unakzeptablen Risiken**
    (vgl. [SAE96], [DIN03], [ISO09])
- **Risikobasiertes Testen**
  - **Produktrisiken** erforschen durch systematische Systemausführung
  - **Produktrisiken** explizit nutzen für Testplanung
- **Quantitative Sicherheitsanalysen**
  - **Produktrisiken** quantitativ analysieren auf Basis eines Systemmodells

Problem und Lösungsidee

- **Problem**
  - Risikobasiertes Testen erfordert Zusatzaufwand für Produktrisikobewertungen
- **Lösungsidee**
  - Separate Produktrisikobewertung obsolet machen durch Kombination von risikobasierten Testtechniken mit quantitativen Sicherheitsanalysen

Agenda

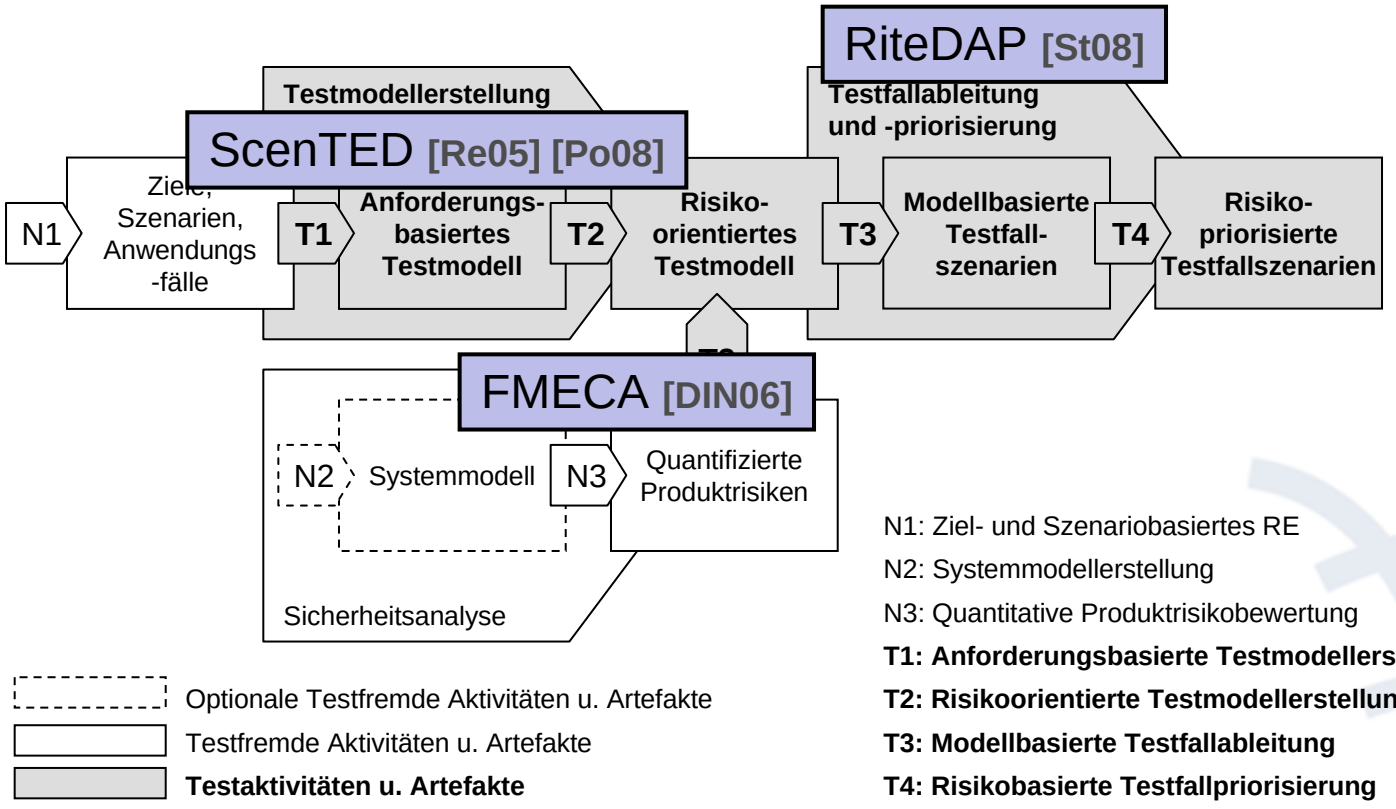
- Einleitung und Motivation
- **Risikobasiertes Testen mittels quantitativer Sicherheitsanalysen**
- Zusammenfassung und Ausblick

Überblick über den Ansatz

- **Anforderungsbasiert**
  - Anforderungen sind Basis für Testfallableitung
  - Ermöglicht systematischen Test des Systems gegen Anforderungen
- **Risikobasiert**
  - Produktrisiken sind Basis für Testfallpriorisierung
  - Ermöglicht systematischen Test entsprechend Produktrisiken
- **Modellbasiert**
  - Ableitung eines Testmodells aus Anforderungen
  - Annotation von Produktrisiken im Testmodell
  - Ableitung und Priorisierung von Testfällen aus Testmodell
  - Ermöglicht hohe Testautomatisierung

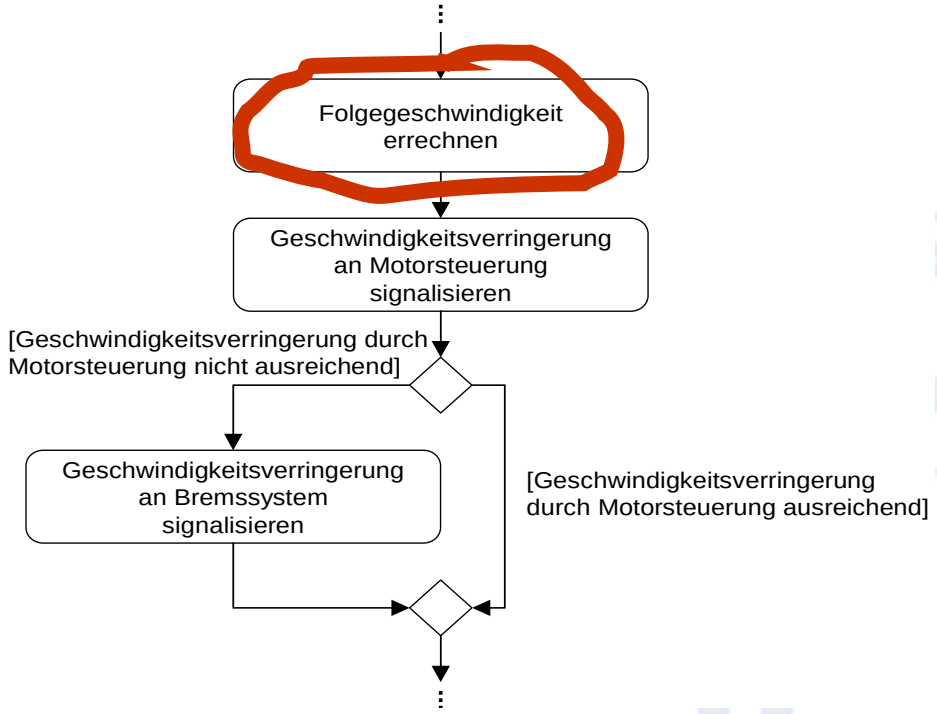
Risikobasiertes Testen mittels quantitativer Sicherheitsanalysen
Überblick über den Ansatz (2)

- Aktivitäten und Artefakte des Ansatzes



Risikobasiertes Testen mittels quantitativer Sicherheitsanalysen
Anwendung des Ansatzes

- Demonstration Anwendbarkeit am Beispiel **ACC-System** [Wi03]
- Beispielhafter **Anwendungsfall** „Geschwindigkeitsverringerung bei vorausfahrendem Fahrzeug innerhalb des Sicherheitsabstandes“
- Ausschnitt aus **anforderungs-basiertem Testmodell** zu betrachtetem Anwendungsfall



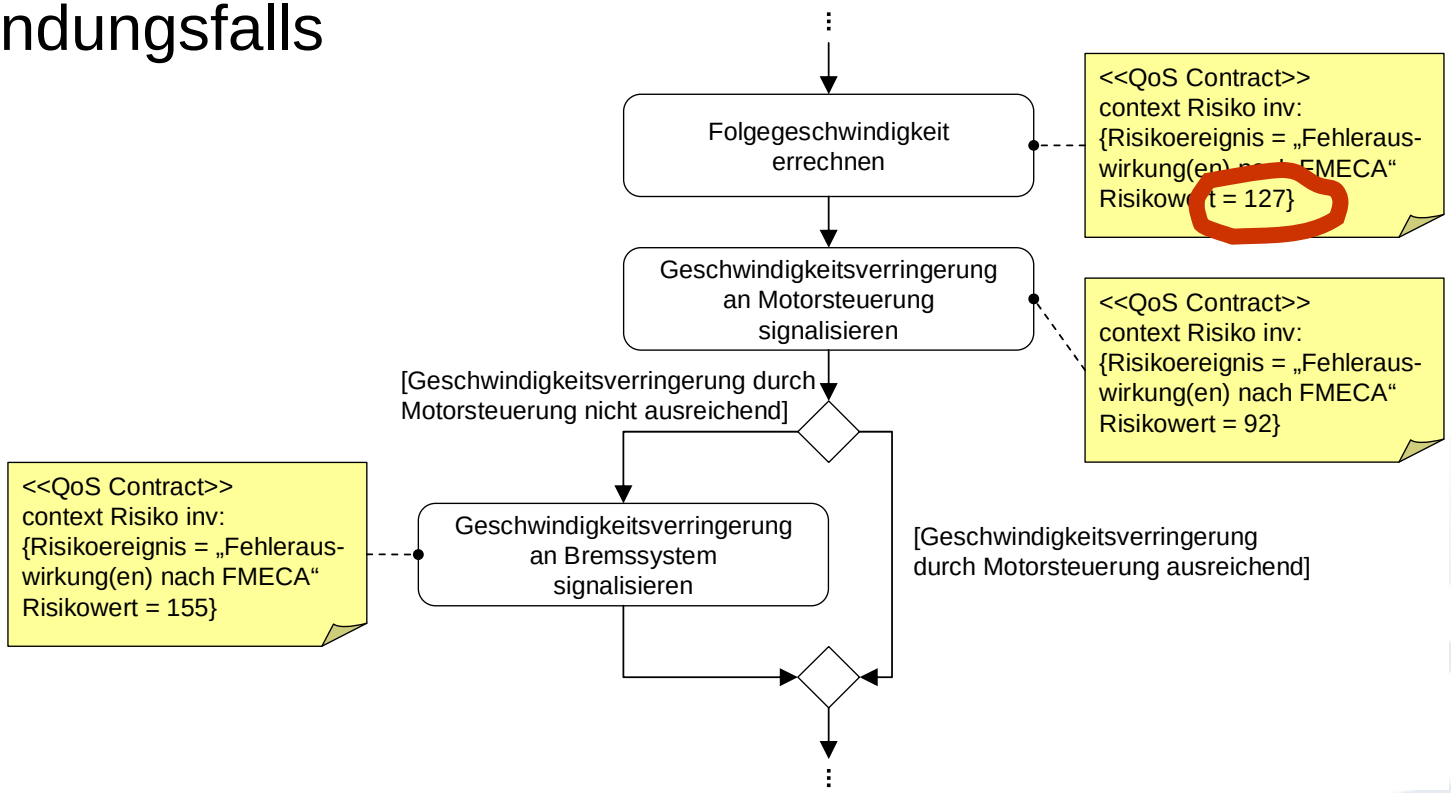
Risikobasiertes Testen mittels quantitativer Sicherheitsanalysen
Anwendung des Ansatzes (2)

- Ausschnitt aus **FMECA-Arbeitsblatt** zu einer Funktion des betrachteten Anwendungsfalls

Funktion / Anforder.	Fehlerart(en)	Fehlerauswrikung(en)	Schwere	Fehlerursache(n)	Auftreten	RPN
Folgegeschwindigkeit errechnen	Folgegeschwindigkeit kann nicht errechnet werden	Fahrzeug wird nicht verlangsamt und kollidiert mit vorausfahrendem Fahrzeug	10	Ist-Geschwindigkeit und / oder Abstand zum vorausfahrenden Fahrzeug liegen nicht vor	1	[illegible]
			10	Softwarefehler bei der Berechnung	2	20
	Folgegeschwindigkeit wird zu langsam errechnet	Fahrzeug wird verspätet verlangsamt und kollidiert mit vorausfahrendem Fahrzeug	10	Ist-Geschwindigkeit und / oder Abstand zum vorausfahrenden Fahrzeug liegen verspätet vor	1	10
			10	Softwarefehler bei der Berechnung	2	20
		Fahrzeug wird verspätet verlangsamt und kann Sicherheitsabstand nicht einhalten	4	Ist-Geschwindigkeit und / oder Abstand zum vorausfahrenden Fahrzeug liegen verspätet vor	1	4
			4	Softwarefehler bei der Berechnung	2	8
	Folgegeschwindigkeit wird zu hoch errechnet	Fahrzeug wird zu wenig verlangsamt und kollidiert mit vorausfahrendem Fahrzeug	10	Ist-Geschwindigkeit liegt falsch (zu niedrig) und / oder Abstand zum vorausfahrenden Fahrzeug falsch (zu groß) vor	3	30
			10	Softwarefehler bei der Berechnung	2	20
	Folgegeschwindigkeit wird zu niedrig errechnet	Fahrzeug wird stärker verlangsamt als zur Einhaltung des Sicherheitsabstandes notwendig	1	Ist-Geschwindigkeit liegt falsch (zu hoch) und / oder Abstand zum vorausfahrenden Fahrzeug falsch (zu klein) vor	3	3
			1	Softwarefehler bei der Berechnung	2	2

Risikobasiertes Testen mittels quantitativer Sicherheitsanalysen
Anwendung des Ansatzes (3)

- Ausschnitt aus **risikoorientiertem Testmodell** zum betrachteten Anwendungsfalls



- Hieraus **risikopriorisierte Testfallszenarien** automatisch ableitbar

Agenda

- Einleitung und Motivation
- Risikobasiertes Testen mittels quantitativer Sicherheitsanalysen
- **Zusammenfassung und Ausblick**

Zusammenfassung

- **Präsentiert wurde ein neuer Ansatz**
  - für den systematischen, risikobasierten Test eingebetteter Systeme
  - unter Verwendung quantitativer Sicherheitsanalysen
  - zur Verminderung des Zusatzaufwandes für Produktrisikobewertungen
  - mit hohem Automatisierungsgrad
- **Demonstriert wurde die Anwendbarkeit des Ansatzes**

Ausblick

- Evaluation der **Eignung und Anwendbarkeit von FMECA** im Rahmen des Testansatzes
  - Eignung und Anwendbarkeit von **FMECA für Software** umstritten
    - Ist z.B. Fehlzustandsbaumanalyse (FTA) geeigneter? [DIN07]
  - Frühe, **anforderungsbasierte FMECA** untypisch
    - Wie kann z.B. architekturbasierte FMECA verwendet werden?
- Evaluation des **Leistungsverhaltens des Testansatzes**
  - Leistungsverhalten von risikobasierten Tests bislang kaum empirisch untersucht

Zusammenfassung und Ausblick
Weitere Informationen

- **Forschungsprojekt**
  - **Software-Plattform Embedded Systems 2020**

  - Nationale Innovationsallianz
  - 21 Partner aus Forschung und Industrie
  - Förderung durch BMBF
  - Entwicklung einer Methodik zur durchgängig modellbasierten Entwicklung von eingebetteten Systemen
  - www.spes2020.de

- **Kontaktdaten**
  - **Heiko Stallbaum**
  - Software Systems Engineering
  - Universität Duisburg-Essen
    Schützenbahn 70
    45117 Essen
    Germany
  - Tel +49 (201) 183 - 4655
    Fax +49 (201) 183 - 4699
    Web www.sse.uni-due.de

    heiko.stallbaum@sse.uni-due.de

Referenzen

[DIN03] DIN EN 61508: Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer / programmierbarer elektronischer Systeme. DIN, Germany, 2003.

[DIN06] DIN EN 60812: Analysetechniken für die Funktionsfähigkeit von Systemen – Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA). DIN, Germany, 2006.

[DIN07] DIN EN 61025: Fehlerzustandsbaumanalyse. DIN, Germany, 2007.

[ISO09] ISO/DIS 26262: Road vehicles – Functional safety. ISO, Switzerland, 2009.

[Po08] K. Pohl: Requirements Engineering: Grundlagen, Prinzipien, Techniken. 2nd ed., dpunkt Verlag, 2008.

[Re05] A. Reuys, E. Kamsties, K. Pohl, S. Reis: Model-based System Testing of Software Prod-uct Families. In: Proc. of 17th CAiSE, Porto, Portugal, 2005, pp. 519-534.

[SAE96] ARP 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. SAE, 1996.

[St08] H. Stallbaum, A. Metzger, K. Pohl: An automated Technique for risk-based Test Case Generation and Prioritization. In: Proc. of 3rd AST, Leipzig, Germany, 2008, pp. 67-70.

[Wi03] H. Winner: ACC Adaptive Cruise Control. Robert Bosch GmbH, Stuttgart, 2003.