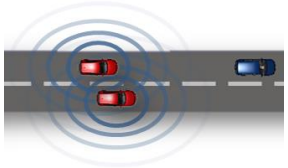
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 643921.

Online Absicherung kooperativer Autonomer Fahrzeuge

Daniel.Hess@DLR.de

Sicherheit hoch-automatisierter Fahrzeuge

Herausforderung:
Komplexität der Umgebung, des Systems, der Interaktion den zwischen Systemen



[Kölner Stadtanzeiger]

[www.motormobiles2.de]

[techrepublic.com]

N. Kalra and S. M. Paddock, 2016: *440 million km test drive, to show with 95% reliability that an automated vehicle causes less accidents than an average human driver [1]*

Offline Absicherung:
Auf ***relevante*** Szenarien beschränken

Online Absicherung:
Auf ***ein*** Szenario beschränken (das aktuelle)

(?)

Idee Online Absicherung

Wann ist eine mögliche Handlung eines Fahrzeugs sicher?

➔Wenn das Fahrzeug nach Ausführung der Handlung garantiert in einen sicheren Zustand überführt werden kann.

Vorschlag:

- Invariante: Existenz eines Notfallmanövers (endet in sicherem Zustand)
- Sicherheitsgarantie des Notfallmanövers:
  - Nachweis der physischen Ausführbarkeit des Notfallmanövers, worst-case Annahmen zur Dynamik des Ego-Fahrzeugs
  - Worst-case Annahmen zum Verhalten anderer Verkehrsteilnehmer

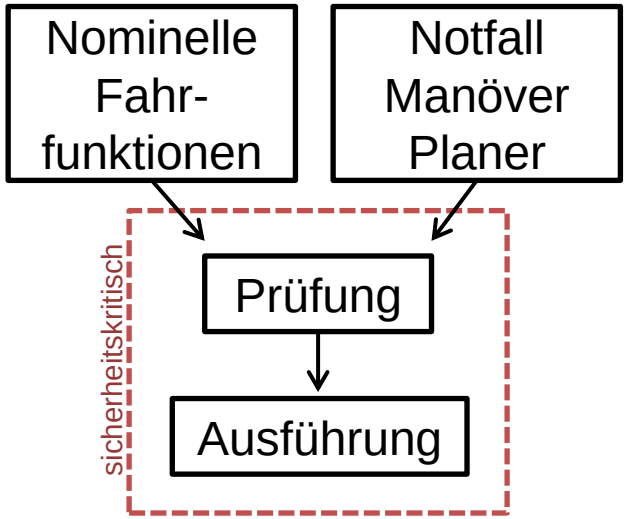


Abb. 1: Architektur Konzept

Vorgehensweise Online Absicherung

Vorgehensweise Online Absicherung

Offline: Konformantes Fahrzeugmodell erzeugen → **Offline:** Sicheren Manöver Automaten berechnen → **Online:** Notfall Manöver planen & Ausführung prüfen → Invariante Sicherheit

Conformance Testing

Fahrverhalten ⊆ Nicht-deterministisches Modell mit beschränkten Störungen

Abb. 2: Aufzeichnung von Testfahrten [2,3]

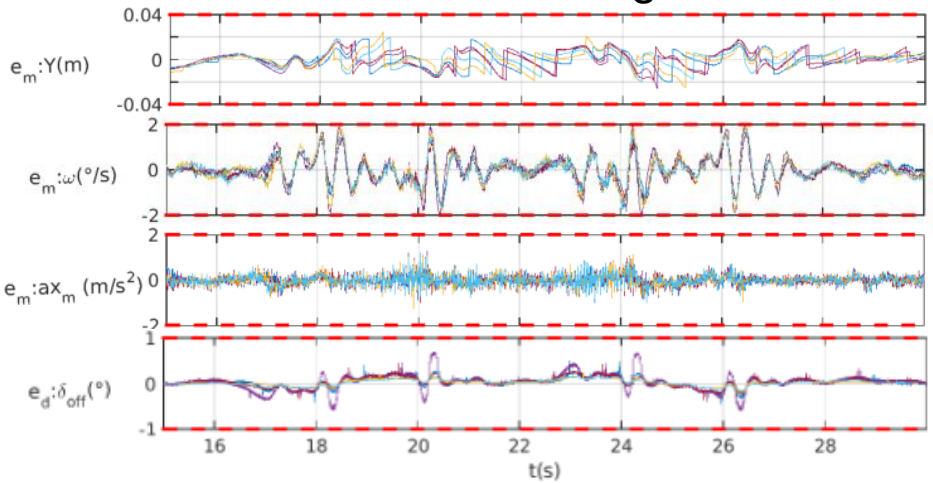


Abb. 3: Rekonstruierte Störungen und Fehler-Schranken eines Einspurmodells [2,3]

Vorgehensweise Online Absicherung

Offline: Konformantes Fahrzeugmodell erzeugen → **Offline:** Sicheren Manöver Automaten berechnen → **Online:** Notfall Manöver planen & Ausführung prüfen → Invariante Sicherheit

Erreichbarkeits Analyse

Nicht-deterministisches Modell mit beschränkten Störungen

Sicherer Manöver Automat:
-Deterministische Manöver Ausführung
-Garantierte maximale Abweichungen

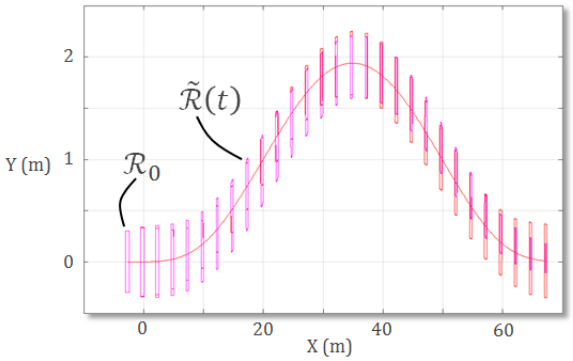


Abb. 4: Erreichbarkeitsmengen für einen Doppelspurwechsel [4]

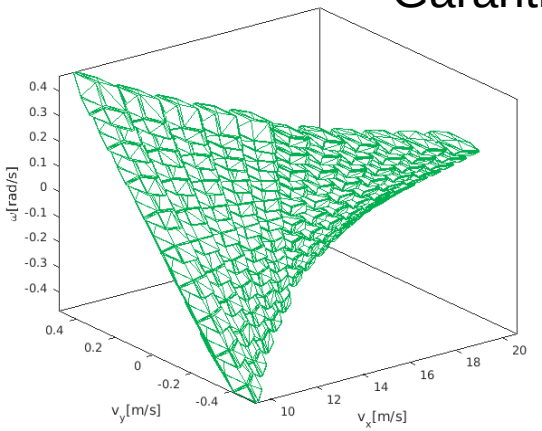


Abb. 5: Mengen der zulässigen Einstiegspunkte für Notfallmanöver [5]

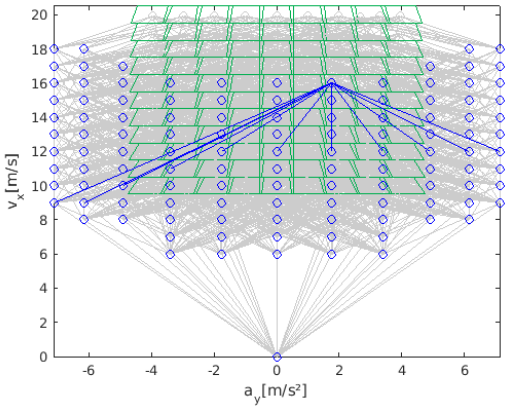


Abb. 6: Sichere Notfallmanöver Teilstücke [5]

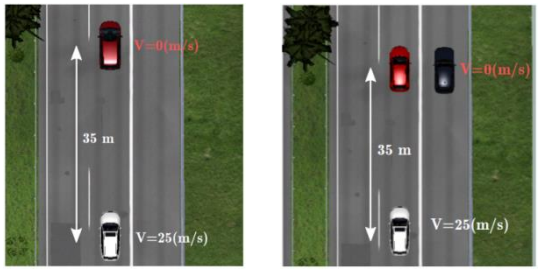
Vorgehensweise Online Absicherung

Offline: Konformantes Fahrzeugmodell erzeugen → **Offline:** Sicheren Manöver Automaten berechnen → **Online:** Notfall Manöver planen & Ausführung prüfen → Invariante Sicherheit

Graphensuche über sicheren Manöverautomaten

➔ Notfallmanöver mit Ausführungsgarantie, Schranken für maximale Abweichung

➔ Prüfung gegen konservatives Umweltmodell



(a) Scenario 1 (b) Scenario 2

	Senario 1				Senario 2			
	AWA*		SHA*		AWA*		SHA*	
Solution	1st	Last	1st	Last	1st	Last	1st	Last
Time [ms]	18	21	3	23	31	51	3	36
# Invalid Nodes	179	240	3	77	599	755	3	222
Memory	42	61	563	723	58	108	387	548
Epsilon Value	4	1.22	4	1.10	4	1.43	4	1.20

Abb. 7: Testszenarios und Performance [6]

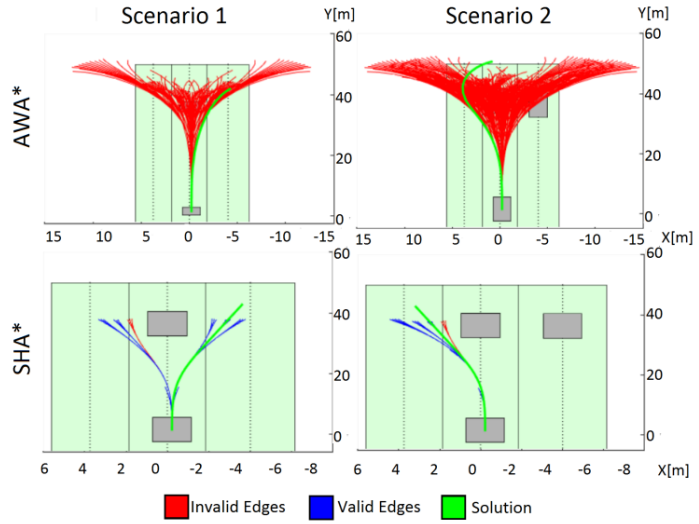


Abb. 8: Notfallmanöver Planung [6]

Online Absicherung & Vernetzung

Idee: Explizite Absprache (C2X) von Nebenbedingungen kooperativer Manöver

Kooperation anfordern:

- Bei Zustimmung: Konservative Vorhersagen einschränken

Kooperation zustimmen:

- Zusätzliche Nebenbedingungen: Auf Kompatibilität mit Notfallmanöver prüfen

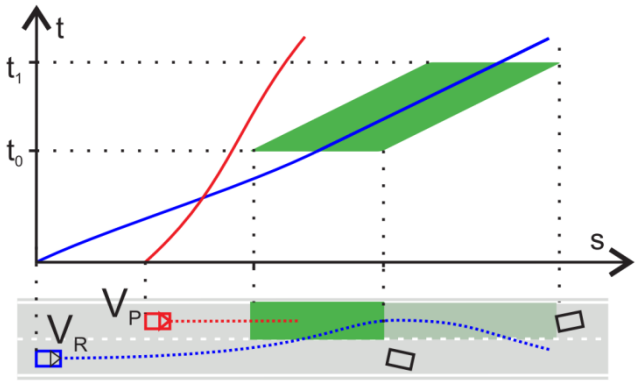
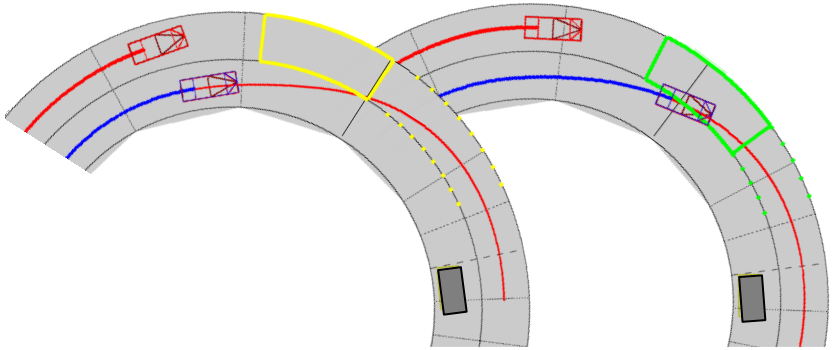


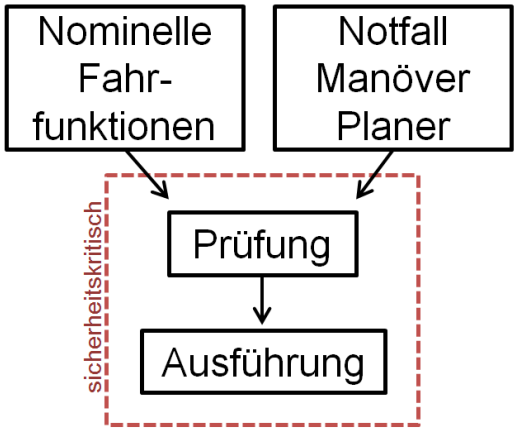
Abb. 8: Nebenbedingungen für kooperativen Spurwechsel [7]



(a) Reservierung (b) Durchführung

Abb. 9: Ablauf eines kooperativen Spurwechsels

Diskussion und Ausblick



- Möglichkeiten durch Online Absicherung
  - Viele Steuerungsmodule können als *operation-critical* statt *safety-critical* betrachtet werden (Entwicklungskosten, Testaufwand, Over-the-air-updates)
  - Standardisierung von Notfallmanövern, herstellerspezifisches nominelles Fahrverhalten?
  - Standardisierung von kooperativen Fahrfunktionen schwierig => Sicherheitskritische Rahmenbedingungen standardisieren?
- Kombination mit Szenario-basiertem Testen: Notfallmanöver sollten das letzte Netz sein.
  - Durch Szenario-basiertes Testen sicherstellen, dass Notfallmanöver in unkritischen Situationen nicht auftreten

- Demo „Kooperativer, automatisierter Spurwechsel“ (UnCoVerCPS)

  ➔ 5.9.2018 FIF-Event

Referenzen

[1] N. Kalra and S. M. Paddock: „How many miles of driving would it take to demonstrate autonomous vehicle reliability?“, RAND Corporation, CA, Tech. Rep., 2016. online

[2] M. Hartung, D. Heß, R. Lattarulo, J. Oehlerking, J. Pérez, A. Rausch: „D5.2 – Report on Conformance Testing of Application Models“, Tech. Rep., EU project UnCoVerCPS, 2017.

[3] B. Schürmann, D. Heß, J. Eilbrecht, O. Stursberg, F. Köster, M. Althoff: „Ensuring drivability of planned motions using formal methods.“ In Intelligent Transportation Systems (ITSC), IEEE 20th International Conference on, 2017.

[4] D. Heß, B. Schürmann, M. Forets, G. Frehse: „D3.2 – Report on Precomputation of Reachable Sets and Advances in Reachability Analysis.“, Tech. Rep., EU project UnCoVerCPS, 2017.

[5] D. Heß, C. Löper, T. Hesse: „Safe Cooperation of Automated Vehicles.” In: AAET Automatisiertes & Vernetztes Fahren, ITS Automotive Nord, 2017.

[6] J. Salvado, L. Custódio, D. Heß: „Contingency planning for automated vehicles.“ In: International Conference on Intelligent Robots (IROS), IEEE, 2016.

[7] D. Heß, R. Lattarulo, J. Pérez, J. Schindler, T. Hesse, F. Köster: „Fast maneuver planning for cooperative automated vehicles.“ In: Intelligent Transportation Systems (ITSC), IEEE 21st International Conference on, 2018. (accepted)