Aktionspläne zur Erlangung eines sicheren Zustandes bei einem autonomen Stauassistenten

Markus Hörwick, Dr. Karl-Heinz Siedersberger, 15.4.2010

Agenda

- Problemstellung
- Stauassistent: automatisches oder autonomes FAS?
- Strategie eines Sicherheitskonzepts für ein autonomes FAS
- Systemgrenzenüberwachung beim autonomen STA
- Fail-Safe-Zustand eines autonomen STA
- Aktionspläne zur Erlangung eines sicheren Zustandes bei einem autonomen STA
- Zusammenfassung

Problemstellung

- Zukünftige Fahrerassistenzsysteme (FAS) übernehmen neben der Längs- auch die Querführung
- Fahrer wird sich von seiner Überwachungsaufgabe zurückziehen
- Fahrer muss nur noch selten, aber in sehr kritischen Fällen eingreifen
- Ausbleibende oder falsche Fahrerreaktion ist sehr wahrscheinlich („Ironies of Automation“ [1])

[1] L. Bainbridge, “Ironies of Automation,” *Automatica*, vol. 19, no. 6, 1983, S. 775-779.

Stauassistent: automatisches oder autonomes FAS?

- Stauassistent (STA): FAS übernimmt im Stau (v < 60km/h) auf Autobahnen und großen Ringstraßen vollständig die Längsführung und die Querführung innerhalb der eigenen Fahrspur [2]

- Zwei Ausprägungen denkbar
  - Vollautomatischer STA

    keine/ wenige Nebenbeschäftigungen erlaubt

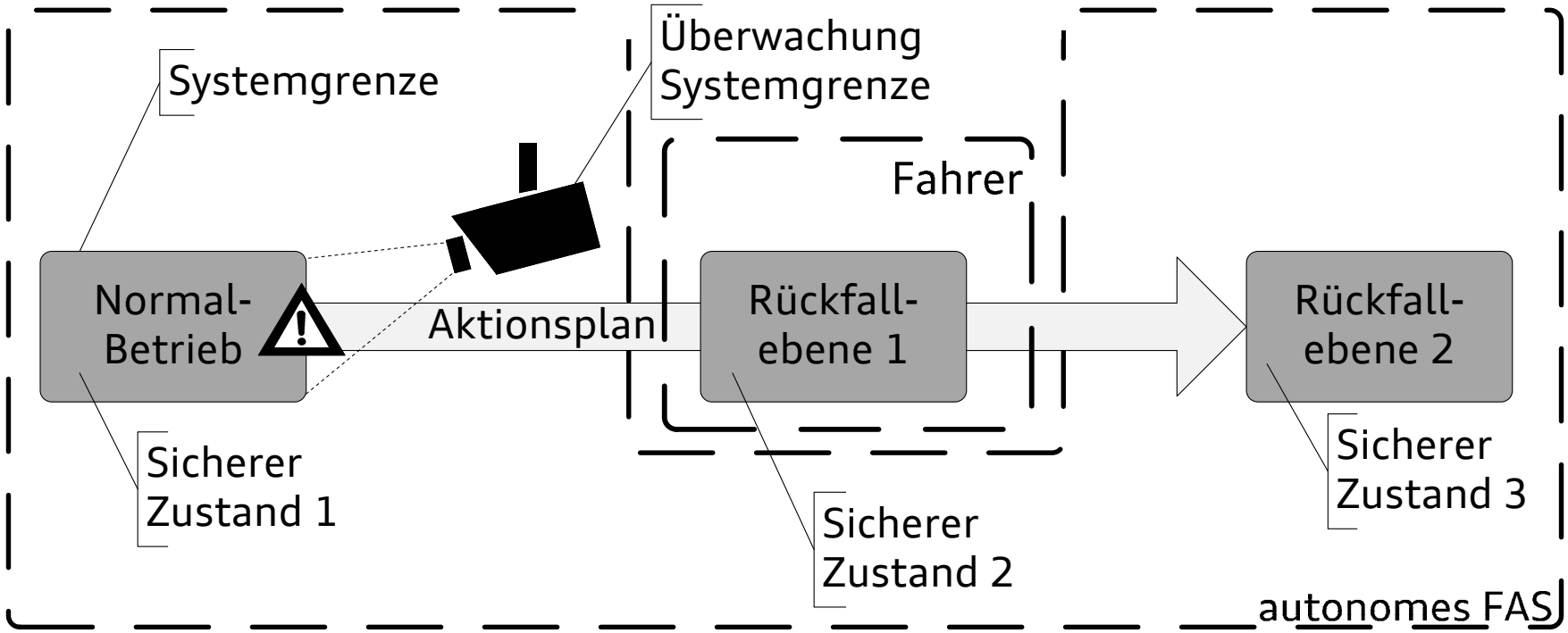
    Fahrereingriffe in seltenen Fällen noch notwendig
  - Autonomer STA

    Nebenbeschäftigungen erlaubt

    Keine Fahrereingriffe mehr notwendig

[2] T. Schaller, „Stauassistenz - Längs- und Querführung im Bereich niedriger Geschwindigkeit," Dissertation, Lehrstuhl für Fahrzeugtechnik (FTM), Technische Universität München, Garching, 2009.

Strategie eines Sicherheitskonzepts für ein autonomes FAS



Quelle: [3]

[3] M. Hörwick, K.-H. Siedersberger, „Strategy and Architecture of a Safety Concept for Fully Automatic and Autonomous Driving Assistance Systems," *Proc. of the 2010 IEEE Intelligent Vehicles Symposium*, Juni 2010, zur Veröffentlichung eingereicht.

Strategie eines Sicherheitskonzepts für ein autonomes FAS

- *"If no mechanical back-up exists after failure of electronics, only an action by other electronics (...) can bring the vehicle (...) to a safe state, i.e. (...)* ***active fail-safe****."* [4]

- Begriffe aus der Eisenbahntechnik
  - Sicherer Zustand: *„Zustand, der die Sicherheit weiterhin bewahrt"* [5]
  - Rückfallebenen: mehrere sichere Zustände in hierarchischer Ordnung [6, S. 161f.]

- Fazit: 3 sichere Zustände bei einem autonomen FAS
  - FAS-Normalbetrieb
  - Manueller Betrieb (Fahrer)
  - Automatisch ansteuerbare Fail-Safe-Zustand

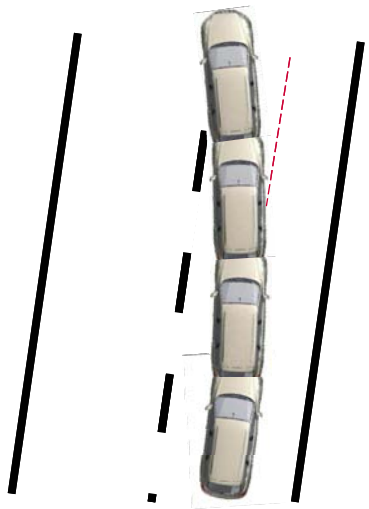
[4] R. Isermann, *Fault Diagnosis Systems: An Introduction from Fault Detection to Fault Tolerance*. 1. Aufl., Berlin: Springer-Verlag, 2005, S. 352.

[5] DIN EN 50129, *Bahnanwendungen. Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme. Sicherheitsrelevante elektronische Systeme für Signaltechnik*. 2003, S.12.

[6] W. Fenner, P. Naumann, J. Trinckauf, *Bahnsicherungstechnik. Siemens Aktiengesellschaft (Hrsg.)*. 2. Aufl., Erlangen: Publicis Corporate Publishing, 2003.

Systemgrenzenüberwachung beim autonomen STA [3]

- Ausfälle von Hardware oder Software
- Funktionsgrenzen
- Negative externe Einflüsse
- Funktionale Plausibilität



Fail-Safe-Zustand eines autonomen STA

- Was kommt als automatisch ansteuerbarer Fail-Safe-Zustand in Frage?

- Eisenbahntechnik
  - *„zumeist der Stillstand (...) als sicherer Zustand definiert“*, allerdings außerhalb von Tunneln [7]
  - Stillstand als sicherer Zustand für Züge [8], [6, S. 147]

- Fahrzeugtechnik
  - *“(...) typische Beispiele für sichere Zustände (...) der Haltezustand von Verkehrssystemen”* [9]
  - *„For automobiles, (...) a **safe state is stand still** (...) **at a nonhazardous place**.“* [4]

[7] H. Geyer, D. Prostrednik, „Sicherheit von Schienenfahrzeugen aus technischer Perspektive,“ *Elektrotechnik & Informationstechnik*, vol. 123, no. 9, 2006, S. 388-395.

[8] E. Anders, „Ein Beitrag zur ganzheitlichen Sicherheitsbetrachtung des Bahnsystems,“ Dissertation, Fakultät Verkehrswissenschaften, Technische Universität Dresden, 2008, S. 58.

[9] W. Halang, R. Konakovsky, *Sicherheitsgerichtete Echtzeitsysteme*. 1. Aufl., München: Oldenbourg-Verlag, 1999, S. 8.

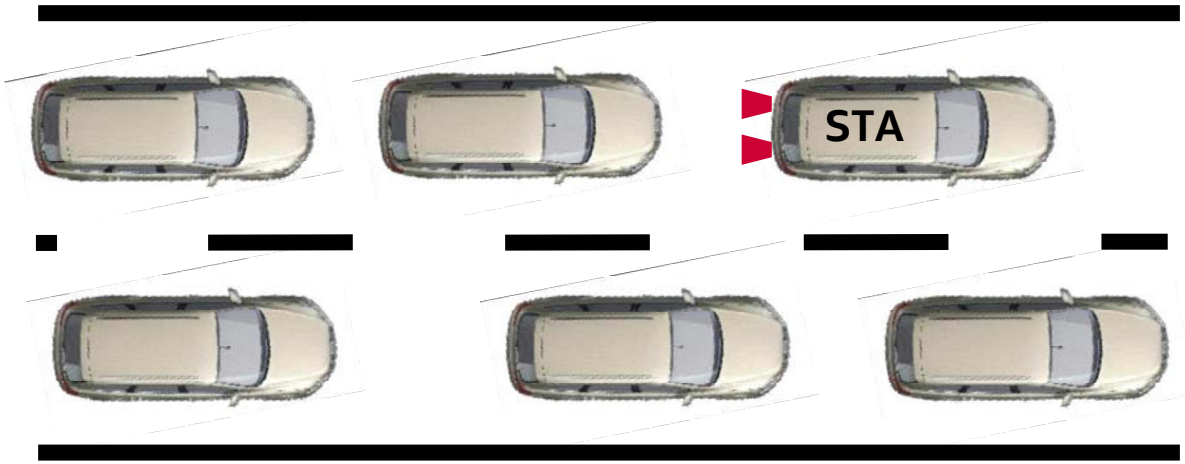
Fail-Safe-Zustand eines autonomen STA

- STA
  - **Stillstand** als anzustrebender **Zustand**!
  - **Eigene Fahrspur** als anzustrebender Ort für den Stillstand!

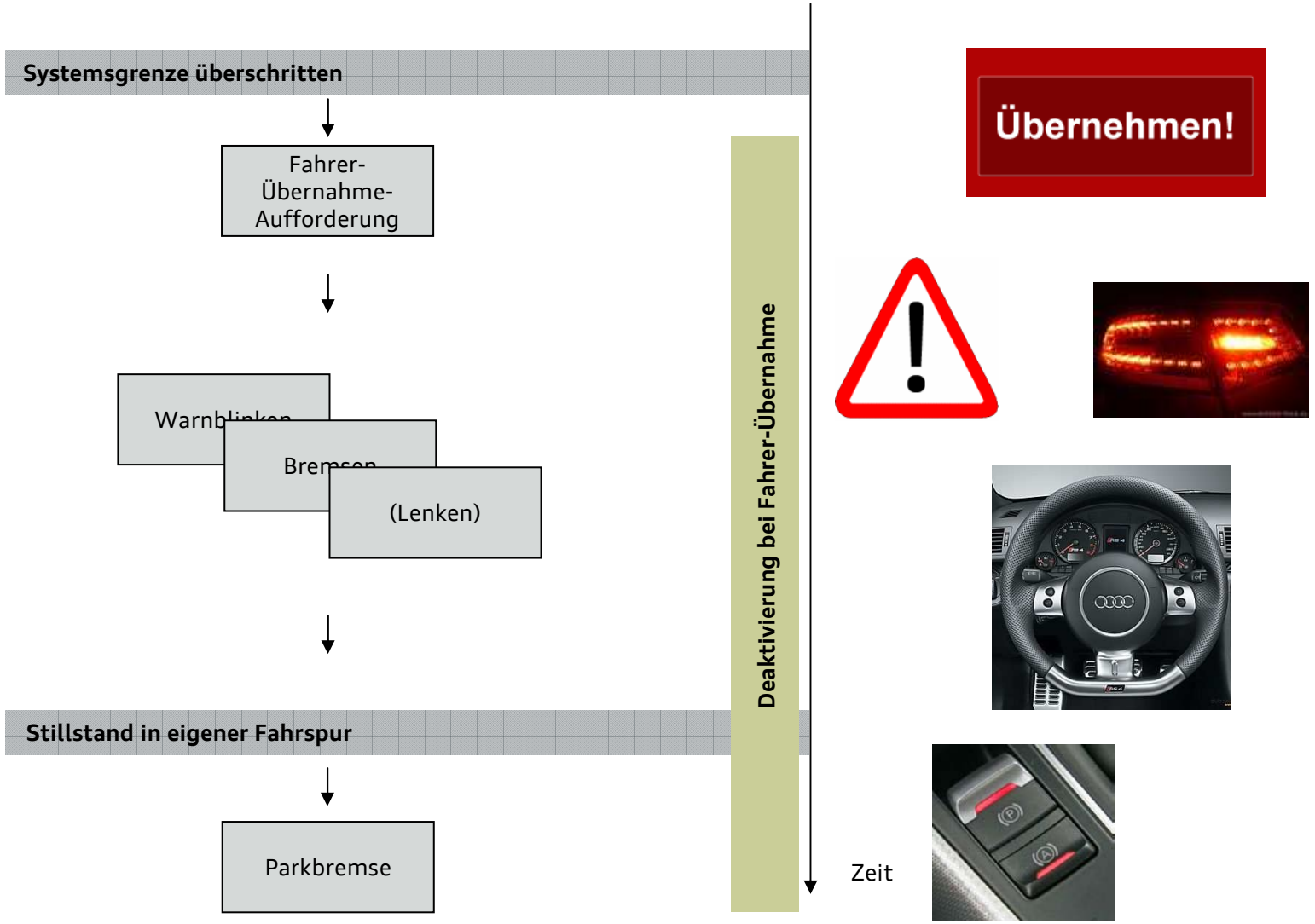
    Hintermann mit geringer Relativgeschwindigkeit (Fahren auf Sicht)

    Zwischenzeitliches Anhalten ist kein ungewöhnliches Verhalten

    Ansteuerung des Standstreifens ist im Fehlerfall ein zu komplexes Manöver



Aktionspläne zur Erlangung eines sicheren Zustandes bei einem autonomen Stauassistenten



Aktionspläne zur Erlangung eines sicheren Zustandes bei einem autonomen Stauassistenten

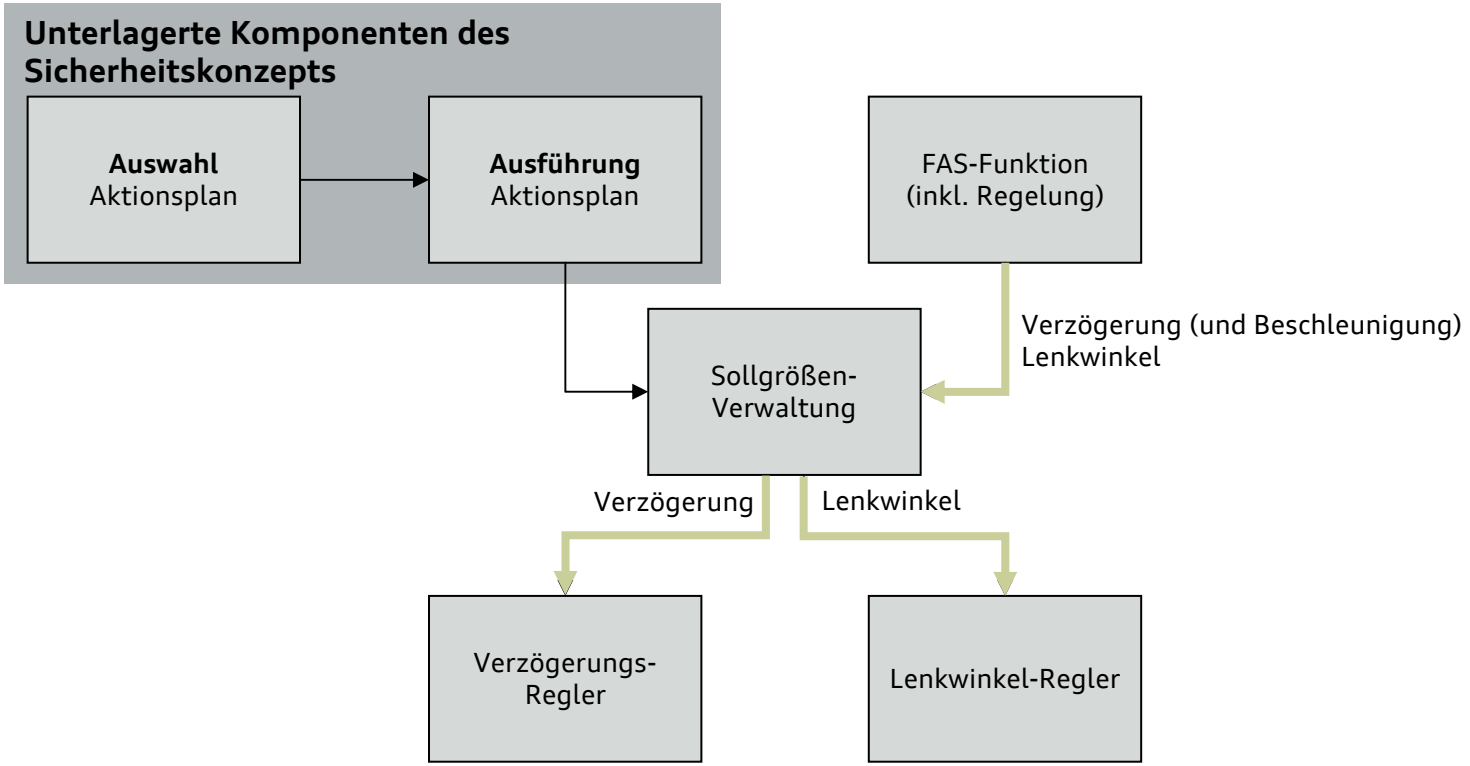
- 2 Aktionspläne zur Beeinflussung der Längsführung
  - „Bremsung“
  - „Bremsung auf Ziel“
  - Gleichzeitiges Ablaufen von Aktionspläne möglich

- 1 Aktionsplan zur Beeinflussung der Querführung
  - „Notlenken“
  - Ausführung nur gemeinsam mit Aktionsplan zur Längsführung

- Mit diesen Aktionsplänen kann (bei entsprechender Parametrierung) auf alle möglichen Systemgrenzenüberschreitungen reagiert werden!

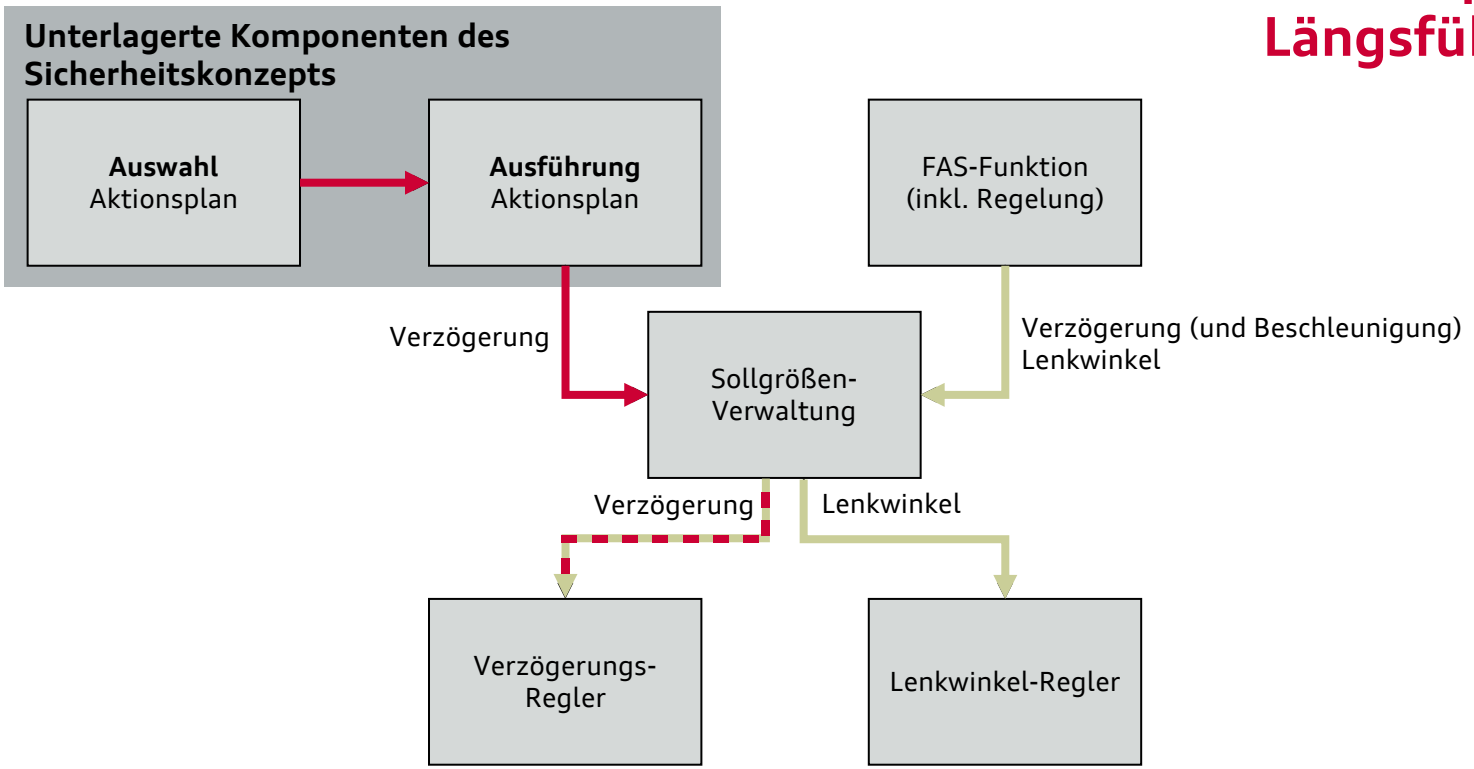
Aktionspläne zur Erlangung eines sicheren Zustandes bei einem autonomen Stauassistenten

Normalbetrieb



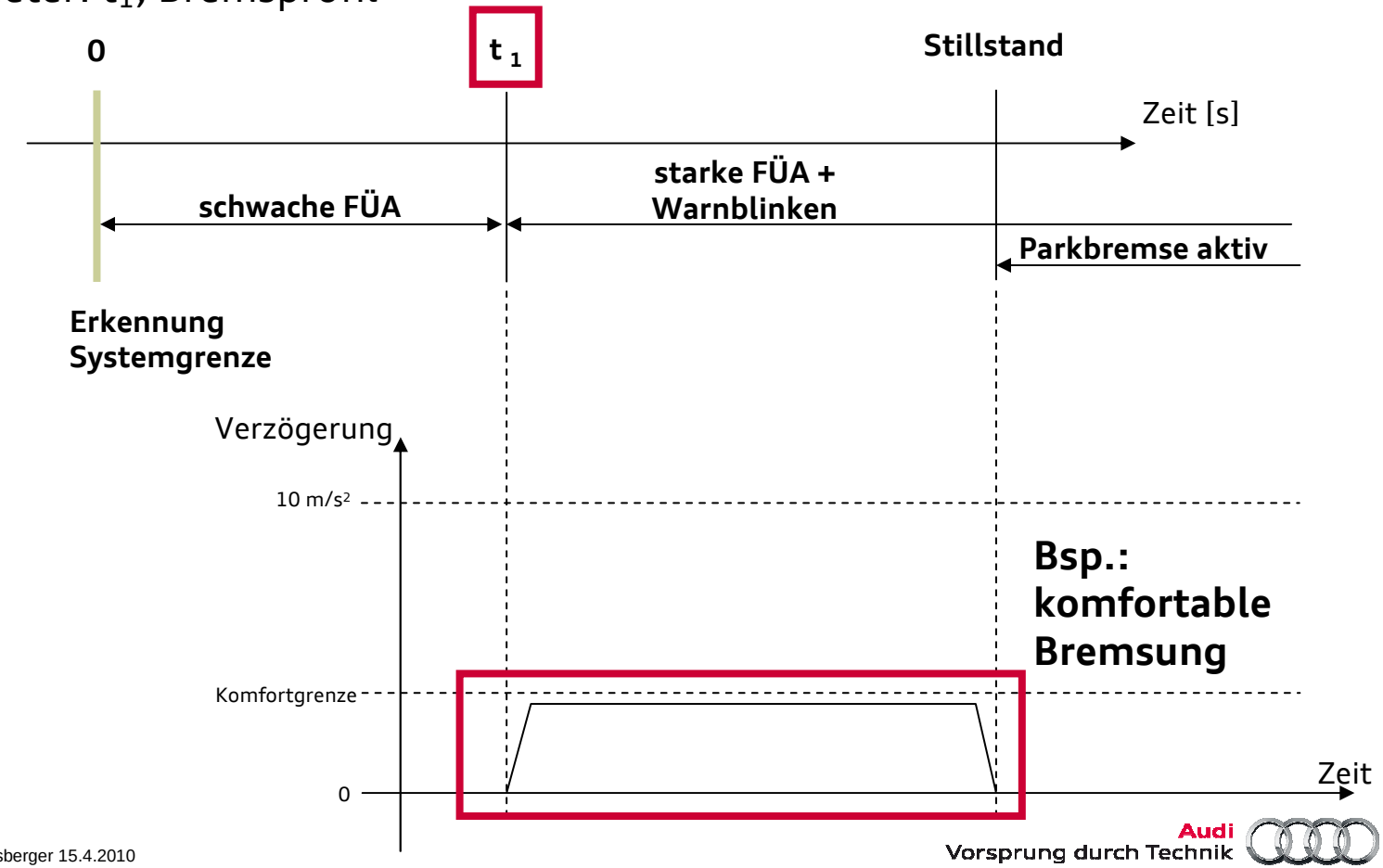
Aktionspläne zur Erlangung eines sicheren Zustandes bei einem autonomen Stauassistenten

Aktionsplan für Längsführung



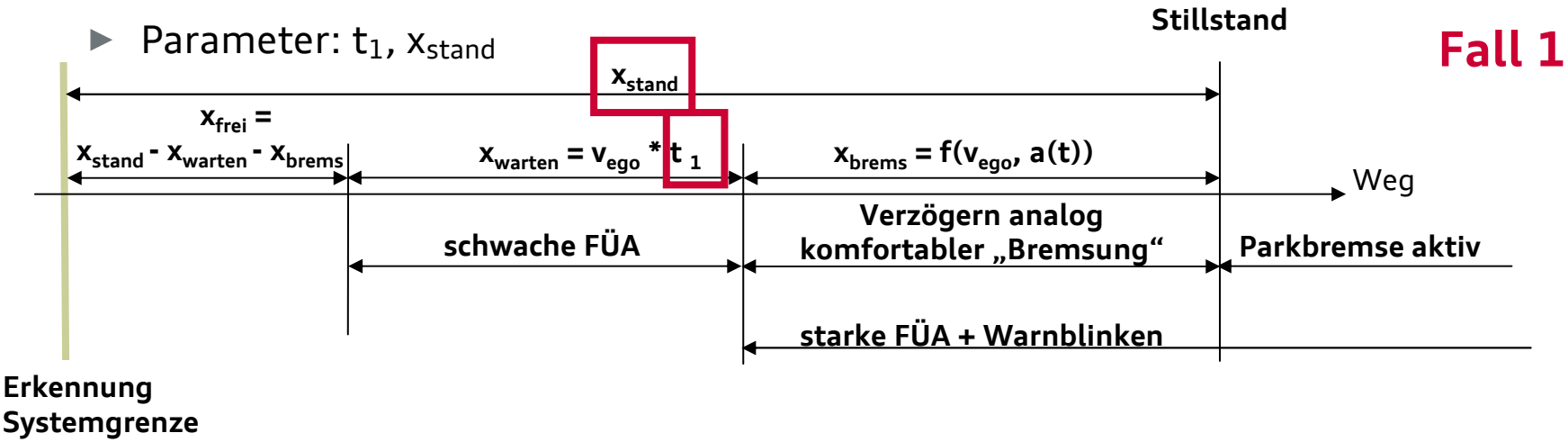
Aktionspläne zur Erlangung eines sicheren Zustandes bei einem autonomen Stauassistenten

- „Bremsung“: Stehen innerhalb t [sec]
  - Bsp.: Stauauflösung
  - Parameter: t_1, Bremsprofil



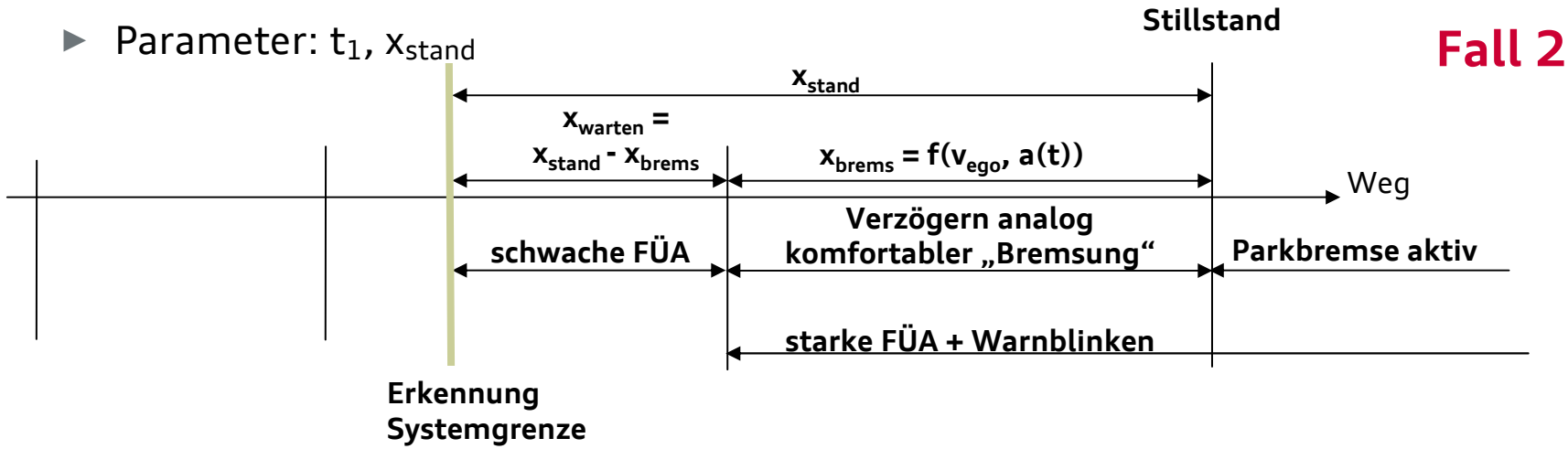
Aktionspläne zur Erlangung eines sicheren Zustandes bei einem autonomen Stauassistenten

- „Bremsung auf Ziel“: Stehen innerhalb x [m]
  - Bsp.: Autobahnende
  - Parameter: t_1, x_{stand}



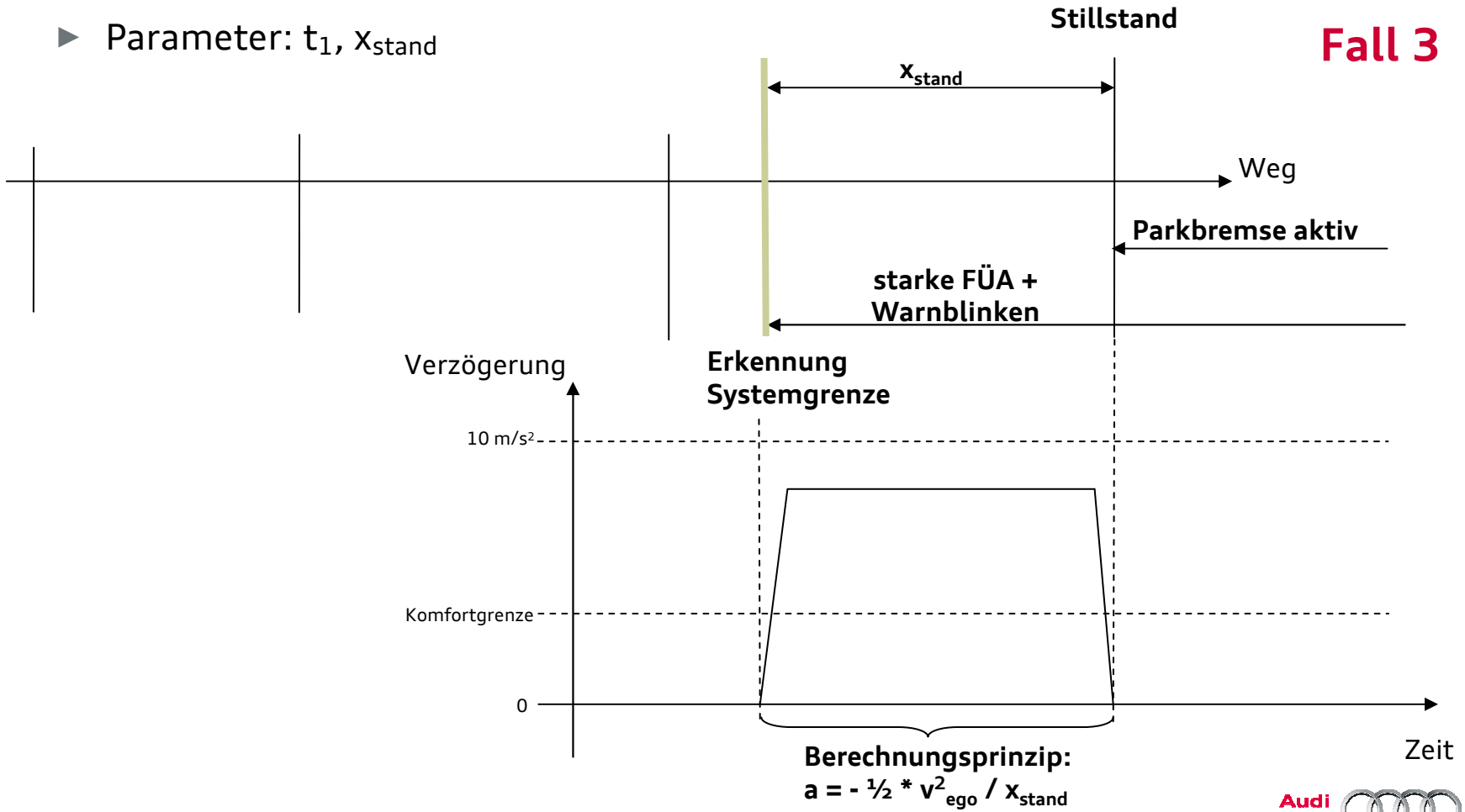
Aktionspläne zur Erlangung eines sicheren Zustandes bei einem autonomen Stauassistenten

- „Bremsung auf Ziel“: Stehen innerhalb x [m]
  - Bsp.: Autobahnende
  - Parameter: t_1, x_{stand}

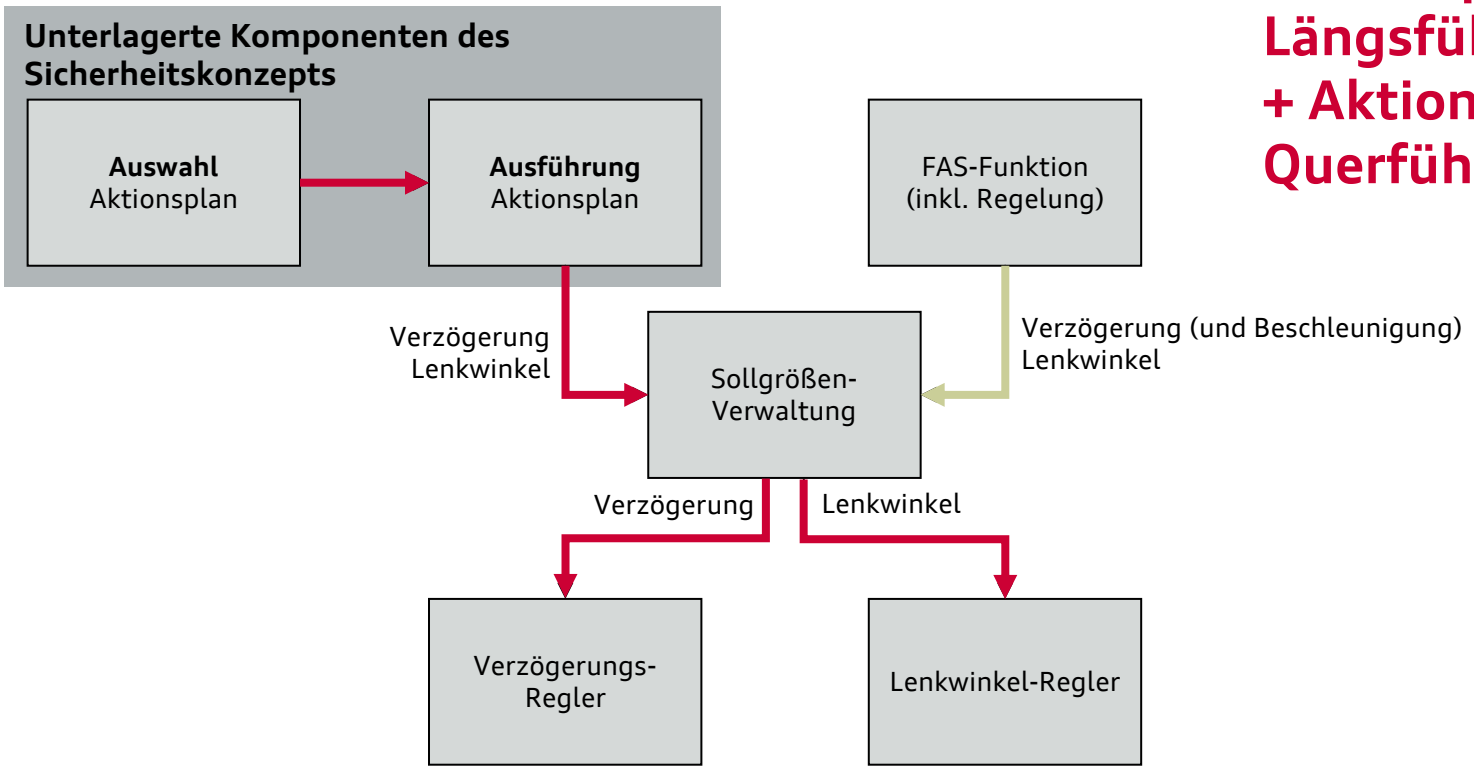


Aktionspläne zur Erlangung eines sicheren Zustandes bei einem autonomen Stauassistenten

- „Bremsung auf Ziel“: Stehen innerhalb x [m]
  - Bsp.: Autobahnende
  - Parameter: t_1, x_{stand}



Aktionspläne zur Erlangung eines sicheren Zustandes bei einem autonomen Stauassistenten



Aktionsplan für Längsführung + Aktionsplan für Querführung

Aktionspläne zur Erlangung eines sicheren Zustandes bei einem autonomen Stauassistenten

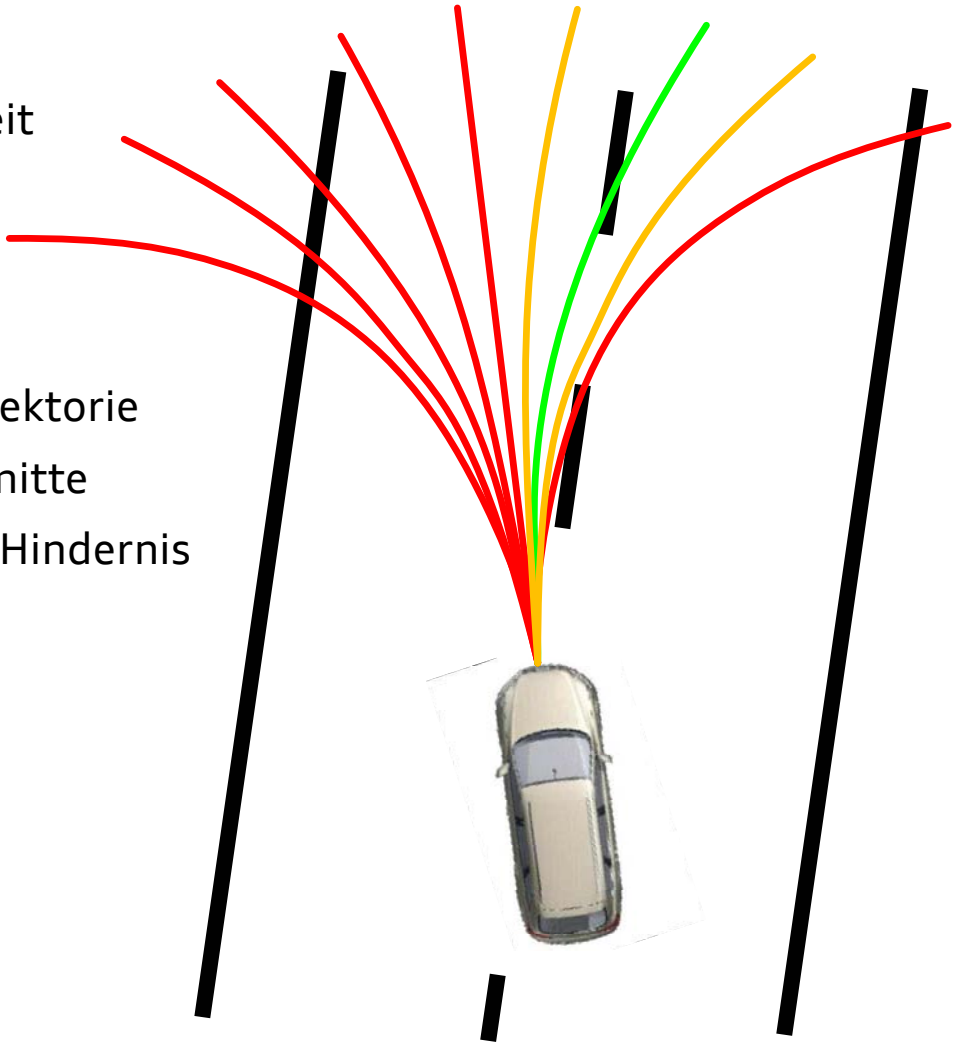
- „Notlenken“: Lenken mit Fokus Sicherheit
  - Bsp.: Unplausibles Spurverlassen
  - Reaktiver DAMN-Algorithmus [10]
  - Hierarchisches Bewertungsschema

    Abstand zu Hindernis entlang Trajektorie

    Abweichung Trajektorie von Spurmitte

    Lateraler Abstand Trajektorie von Hindernis

    Trajektorienkrümmung



[10] J. Rosenblatt, „DAMN: A Distributed Architecture for Mobile Navigation,” Technischer Bericht, Robotics Institute, Carnegie Mellon University, Pittsburgh, 1997.

Zusammenfassung

- Vollautomatische Fahrfunktionen: Fahrer zieht sich von Überwachungsaufgabe zurück
- Um Nebenbeschäftigungen tolerieren zu können: aktive Fail-Safe-Mechanismen notwendig, die Fahrzeug auch ohne Fahrereingriff in sicheren Zustand übergehen lassen
- Sichere Zustand STA: Stillstand in eigener Fahrspur
- Aktionspläne
  - Abfolge von Aktionen zum Übergang in einen sicheren Zustand
  - 2 Aktionspläne zur Beeinflussung der Längsführung
  - 1 Aktionsplan zur Beeinflussung der Querführung
  - Überlagerung von Brems- und Lenkanforderungen durch unterlagerte Komponente
  - Abfangen sämtlicher Fehlerfälle

Audi
Vorsprung durch Technik

Vielen Dank.

Kontakt: extern.markus.hoerwick@audi.de