Institute for Software and Systems Engineering

TU Clausthal

VanAssist

VanAssist

Towards Safe Automated Driving

Connected Dependability Cage & Remote Command Control Center

M. Sc. Andreas Vorwald

Gefördert durch:

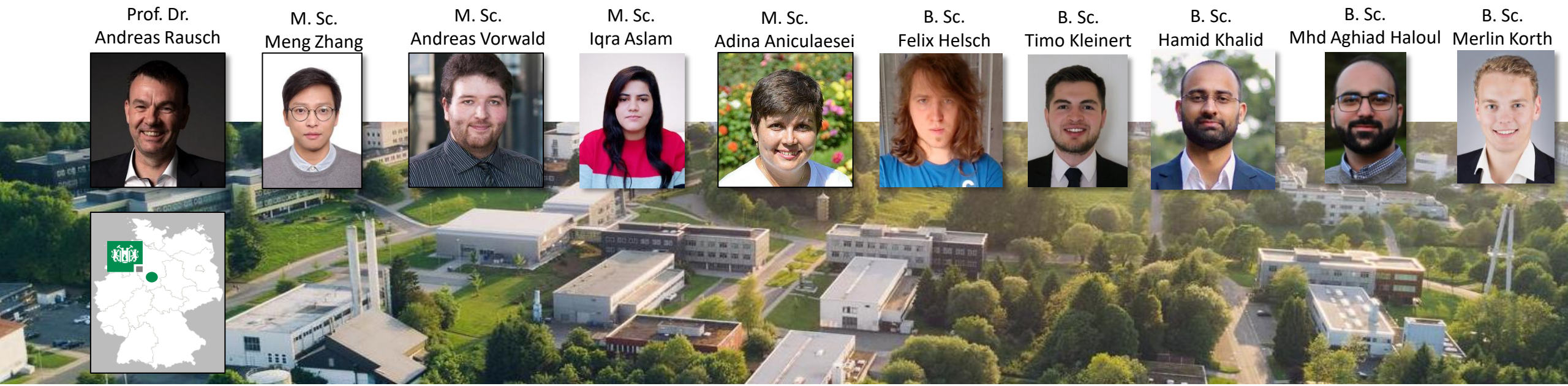
Bundesministerium für Verkehr und digitale Infrastruktur

aufgrund eines Beschlusses des Deutschen Bundestages

Wer sind wir?

VanAssist

- Forschungsgruppe: Dependable and Autonomous Cyber-Physical Systems
- https://www.isse.tu-clausthal.de/forschung/forschungsgruppen/dependable-and-autonomous-cyber-physical-systems



Agenda

- Motivation
  - SAE Stufen des automatisierten Fahrens
  - VanAssist
- Lösungsansatz
  - Dependability Cage
  - Connected Dependability Cage
  - Beispielhafter Ablauf
- Zusammenfassung und Ausblick

Agenda

- Motivation
  - SAE Stufen des automatisierten Fahrens
  - VanAssist
- Lösungsansatz
  - Dependability Cage
  - Connected Dependability Cage
  - Beispielhafter Ablauf
- Zusammenfassung und Ausblick

SAE Stufen des automatisierten Fahrens: Zusammenhang zwischen Absicherung und der Operational Design Domain (ODD)

VanAssist

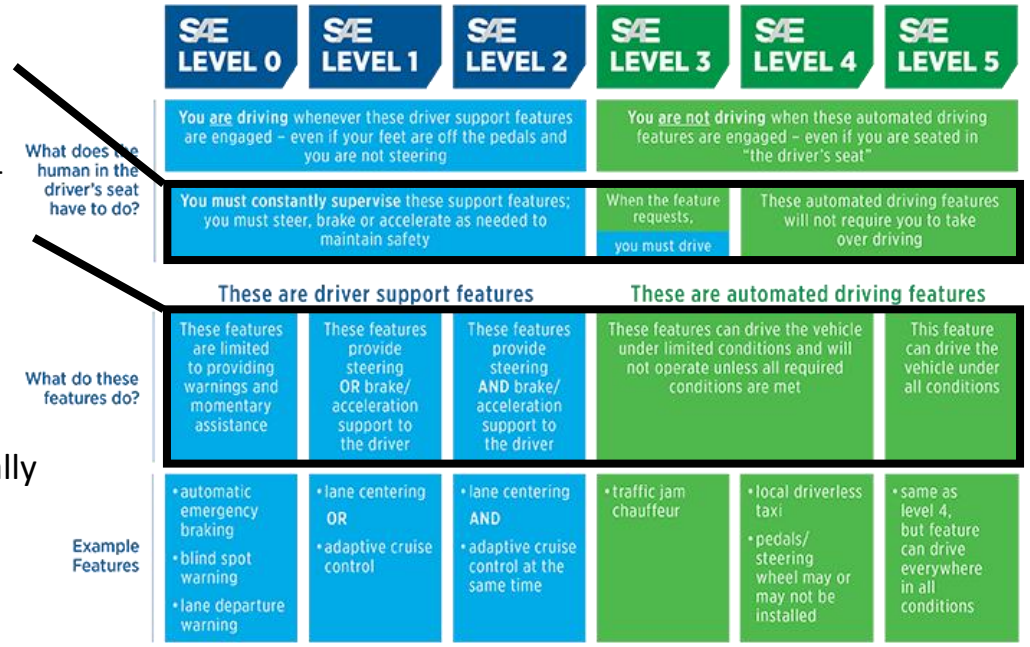
Safety (False-Positive) Anforderungen
→Das System muss **korrekt** reagieren, **falls es reagiert**.
→Fail-Safe

Safety (False-Positive) + Lifeness (False-Negative) Anforderungen
→Das System **muss in allen Situationen korrekt** reagieren.
→Fail-Operational

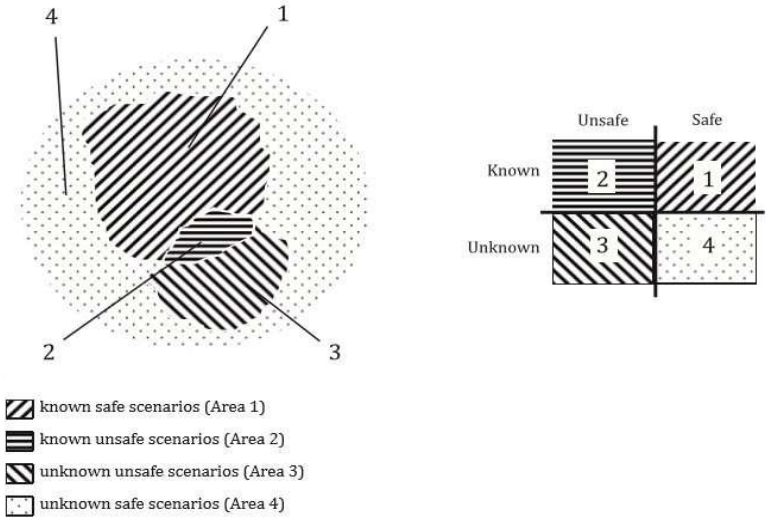
Die **Verantwortlichkeit** über die **funktionale Sicherheit** spielt hier eine entscheidende Rolle.

SOTIF: Die **Domäne**, für die das Fahrsystem ausgelegt ist spielt hier eine entscheidende Rolle. →**Operational Design Domain (ODD)**

ODD: „Operation conditions under which a given driving automation system or feature thereof is specifically designed to function, including, but not limited to, environmental, geografical, and time-of-day, and/or the requisite presence or absense of certain traffic or roadway characteristics.“ [3]



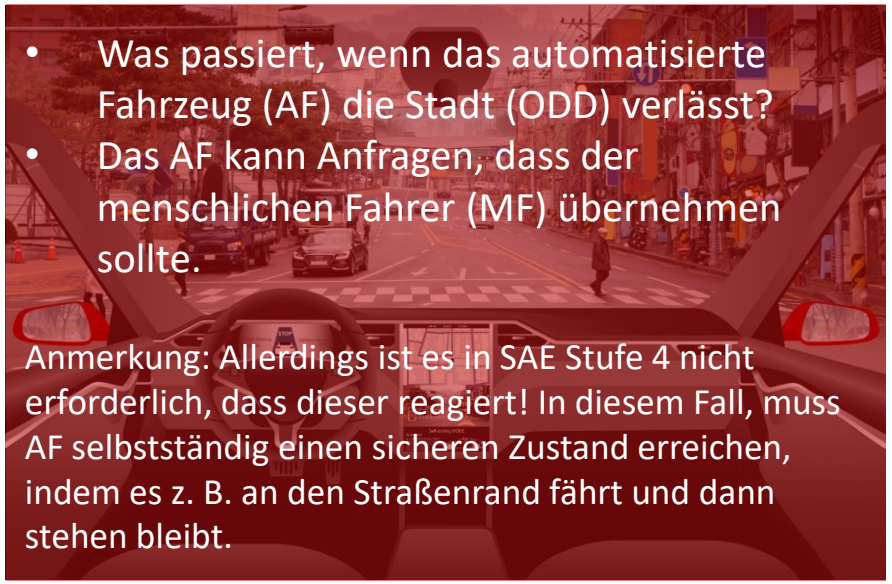
Society of Automotive Engineers Stufen der Fahrautomatisierung [2]



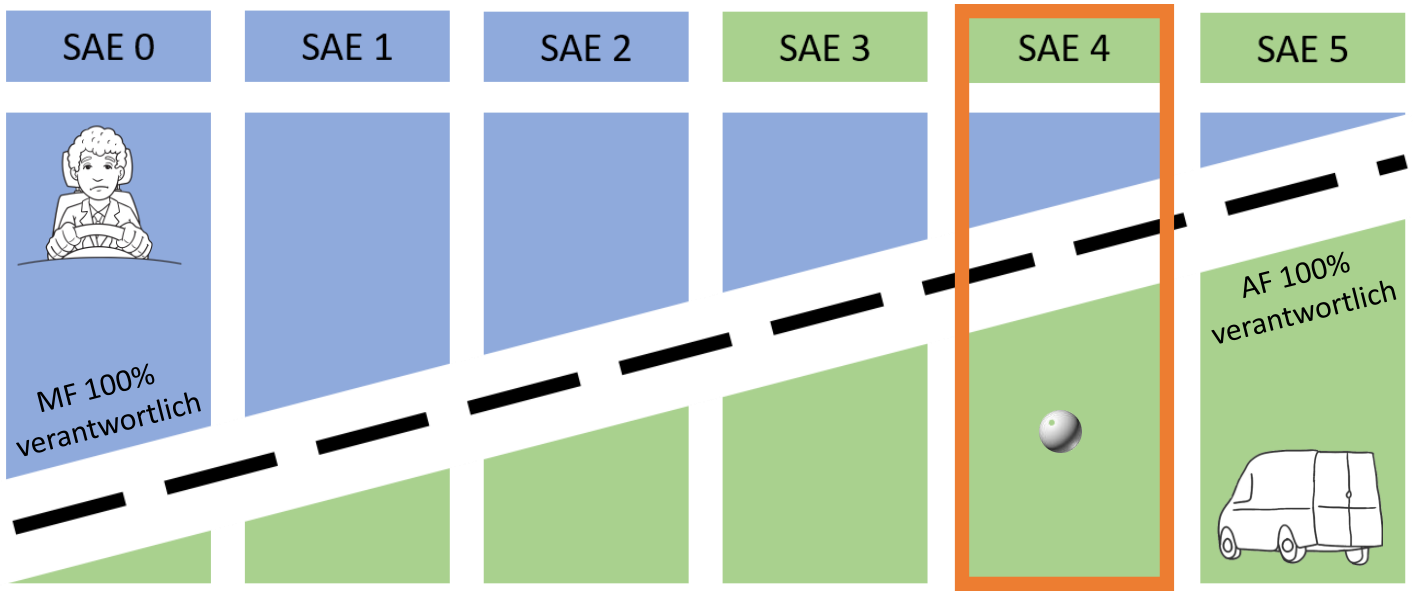
Safety of Intented Functionality Scenarios [1]

[1] ISO/PAS 21448, Road vehicles – Safety of intended functionality, Januar 2019
[2] SAE International Releases Updated Visual Chart for Its “Levels of Driving Automation” Standard for Self-Driving Vehicles, SAE online verfügbar unter: https://www.sae.org/news/press-room/2018/12/sae-international-releases-updated-visual-chart-for-its-%E2%80%9Clevels-of-driving-automation%E2%80%9D-standard-for-self-driving-vehicles
[3] SAE J3016, Surface Vehicle Recommened Practise - Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, Juni 2018

SAE Stufen des automatisierten Fahrens: Zusammenhang zwischen Absicherung und der Operational Design Domain (ODD)



City Pilot @ SAE 4



Grafische Veranschaulichung der Verantwortlichkeitsverteilung zwischen automatisierten Fahrzeug (AF) und menschlichen Fahrer (MF)

Forschungsfrage 1: Wie kann die ODD des automatisierten Fahrzeugs zur Laufzeit überwacht werden?
Forschungsfrage 2: Wie kann ein zuverlässiger Transfer der Verantwortlichkeit zwischen automatisiertem Fahrzeug und menschlichen Fahrer realisiert werden?

Agenda

- Motivation
  - SAE Stufen des automatisierten Fahrens
  - VanAssist
- Lösungsansatz
  - Dependability Cage
  - Connected Dependability Cage
  - Beispielhafter Ablauf
- Zusammenfassung und Ausblick

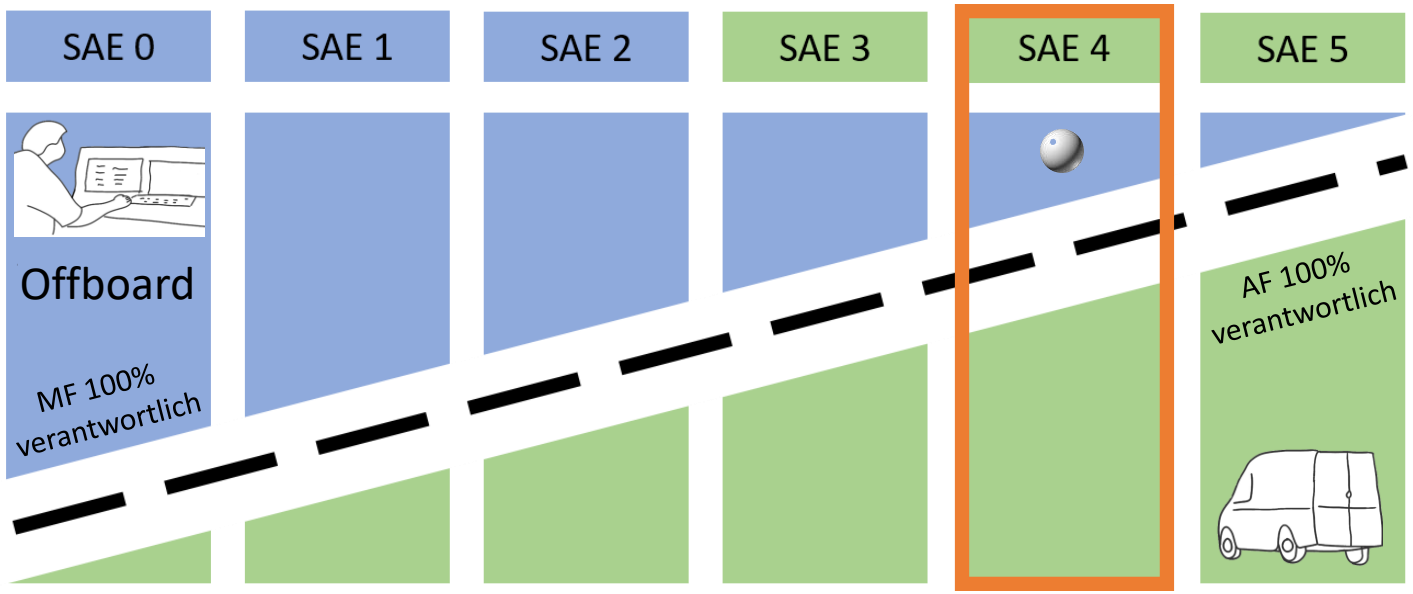
VanAssist Motivation und Ziel

VanAssist

VanAssist
zielt auf die Entwicklung einer integrierten Fahrzeug- und Systemtechnologie, die eine weitgehend emissionsfreie und automatisierte Zustellung von Gütern in urbanen Zentren ermöglicht.

VanAssist Ziel: Entlastung des Paketzustellers

Remote Command Control Center



Grafische Veranschaulichung der Verantwortlichkeitsverteilung zwischen automatisierten Fahrzeug (AF) und menschlichen Fahrer (MF)

Forschungsfrage 3: Wie kann ein zuverlässiger Transfer der Verantwortlichkeit zwischen automatisiertem Fahrzeug und einem entfernten Offboard-Sicherheitsfahrer realisiert werden?
Forschungsfrage 4: Wie können Verantwortlichkeiten insb. bei asymmetrischen Verhältnissen zwischen automatisierten Fahrzeugen und Offboard-Sicherheitsfahrern adäquat koordiniert werden?

Agenda

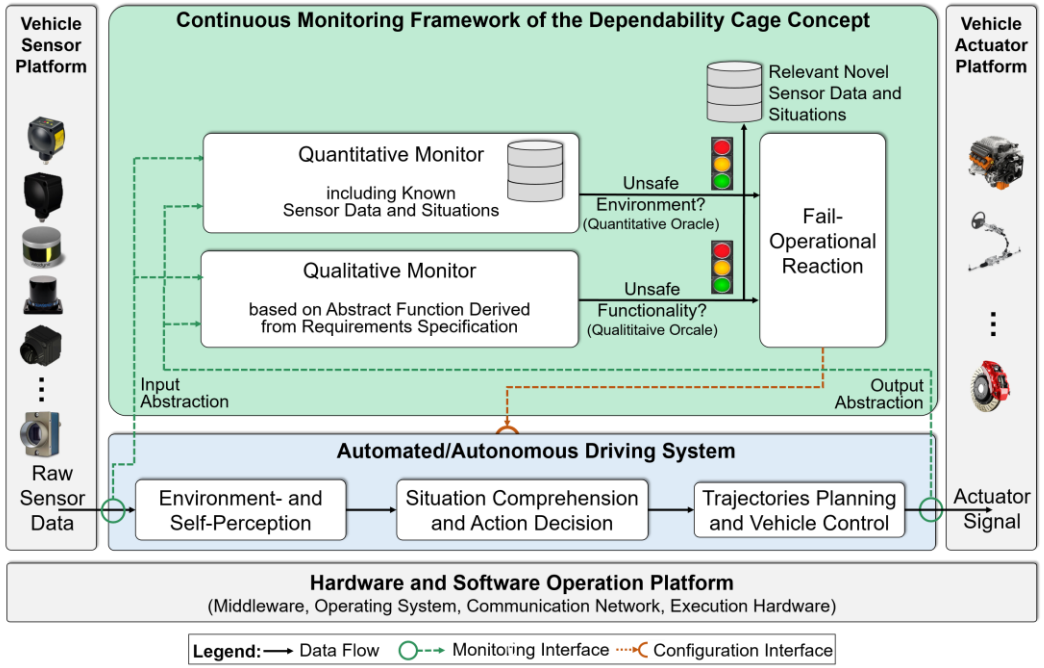
- Motivation
  - SAE Stufen des automatisierten Fahrens
  - VanAssist
- Lösungsansatz
  - Dependability Cage
  - Connected Dependability Cage
  - Beispielhafter Ablauf
- Zusammenfassung und Ausblick

Ausgangspunkt: Unser Dependability Cage Ansatz…

Unser Dependability Cage Ansatz ist ein Laufzeit-Safety-Überwachungssystem für automatisierte/ autonome Fahrzeuge, bestehend aus [1] [2]:

- ***Qualitative Monitor***: Absicherung der Korrektheit des Systemverhaltens hinsichtlich Sicherheitsanforderungen.
- ***Quantitative Monitor***: Absicherung des Systems hinsichtlich der zur Entwicklungszeit berücksichtigten und getesteten Situationen und Systemumgebungen.
- ***Fail-Operational Reaktion***: Überführung des gestörten Systems in einen sicheren Zustand, z. B. durch Gracefull Degradation wie in [3].

…zur Lösung der Forschungsfragen: **Erweiterung zum Connected Dependabilty Cage Ansatz**



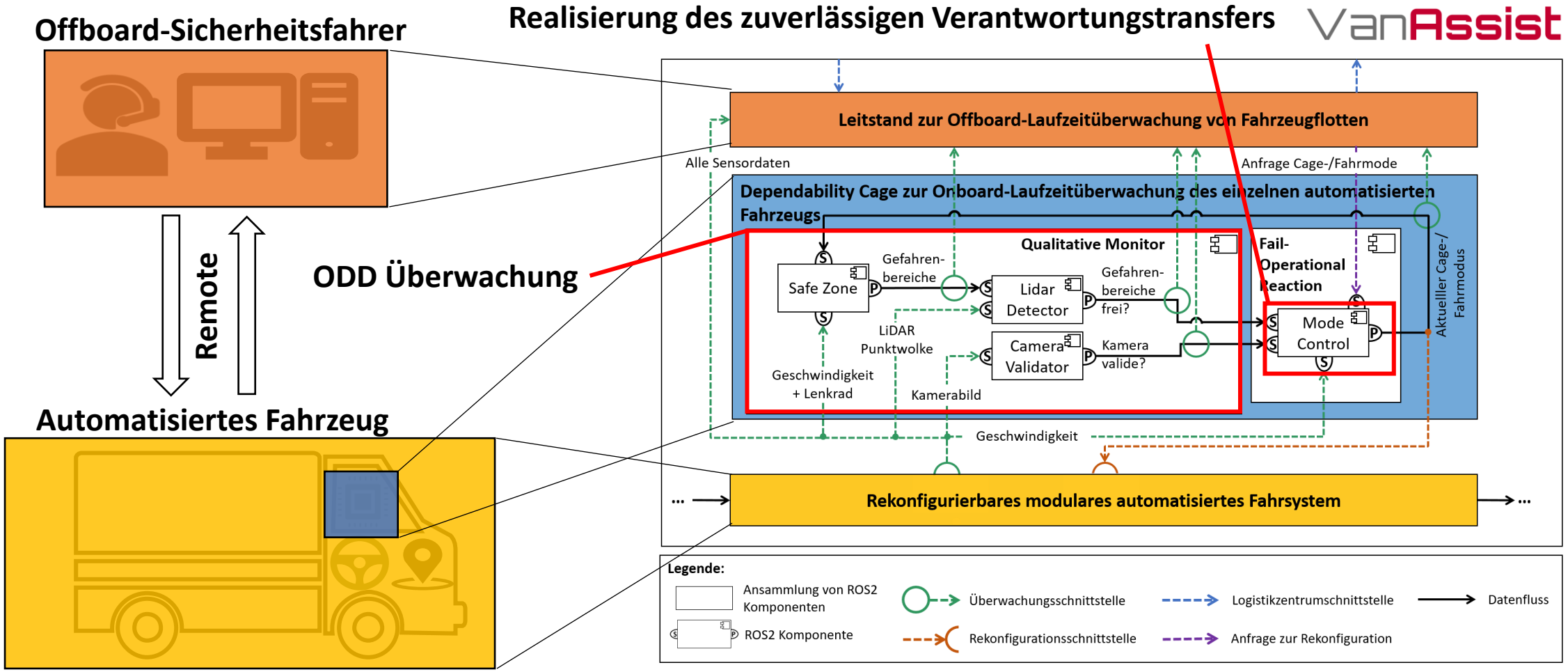
Dependability Cage Architektur nach [2]

[1] A. Aniculaesei, J. Grieser, A. Rausch, K. Rehfeld, T. Warnecke : Towards A Holistic Software Systems Engineering Approach for Dependable Autonomous Systems, 1st International Workshop on Software Engineering for AI in Autonomous Systems, Gothenburg, Schweden, 2018.
[2] J. Grieser, M. Zhang, T. Warnecke, A. Rausch .: Assuring the Safety of End-to-End Learning-Based Autonomous Driving through Runtime Monitoring, 23rd Euromicro Conference on Digital System Design (DSD), Kranj, Slovenien, 2020.
[3] A. Aniculaesei, J. Grieser, A. Rausch, K. Rehfeld, T. Warnecke: Graceful Degradation of Decision and Control Responsibility for Autonomous Systems based on Dependability Cages, 5th International Symposium on Future Active Safety Technology toward Zero, Blacksburg, Virginia, USA, 2019.

Agenda

- Motivation
  - SAE Stufen des automatisierten Fahrens
  - VanAssist
- Lösungsansatz
  - Dependability Cage
  - Connected Dependability Cage
  - Beispielhafter Ablauf
- Zusammenfassung und Ausblick

Lösungsansatz: Connected Dependability Cage



Connected Dependability Cage Architektur in VanAssist

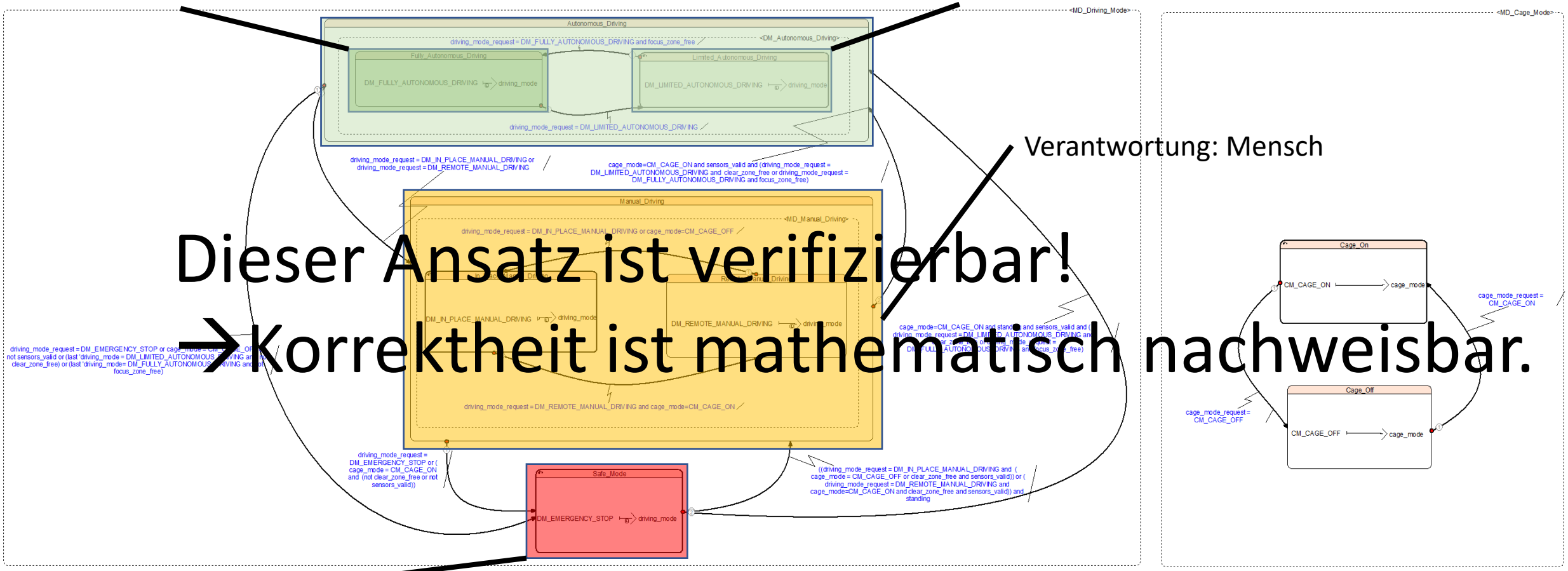
Connected Dependability Cage: Mode Control

VanAssist

Verantwortung: Fahrsystem

Verantwortung: Mensch + Fahrzeug (Kooperativ)

Verantwortung: Mensch



Dieser Ansatz ist verifizierbar!

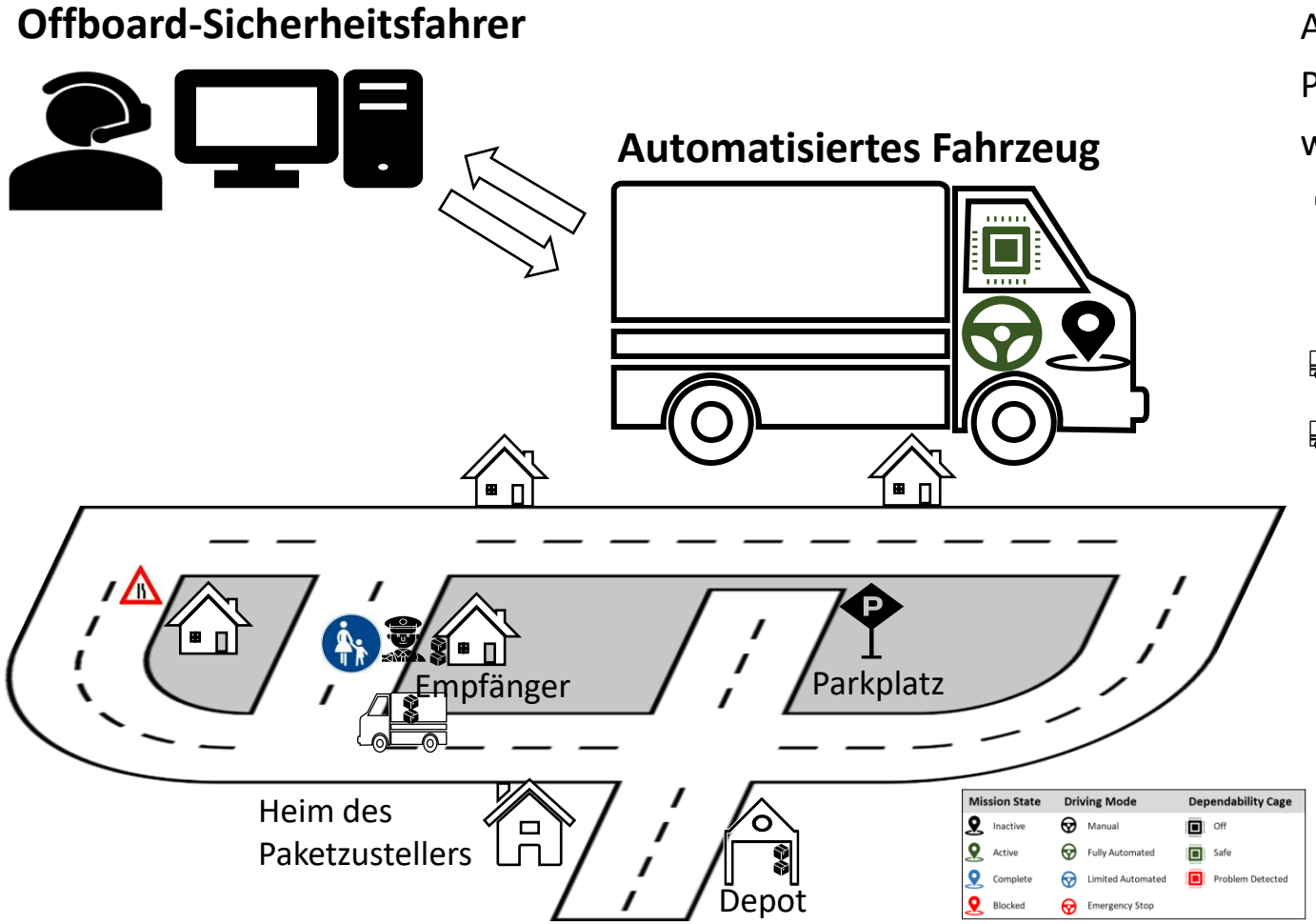
→Korrektheit ist mathematisch nachweisbar.

Verantwortung: Mensch

Agenda

- Motivation
  - SAE Stufen des automatisierten Fahrens
  - VanAssist
- Lösungsansatz
  - Dependability Cage
  - Connected Dependability Cage
  - Beispielhafter Ablauf
- Zusammenfassung und Ausblick

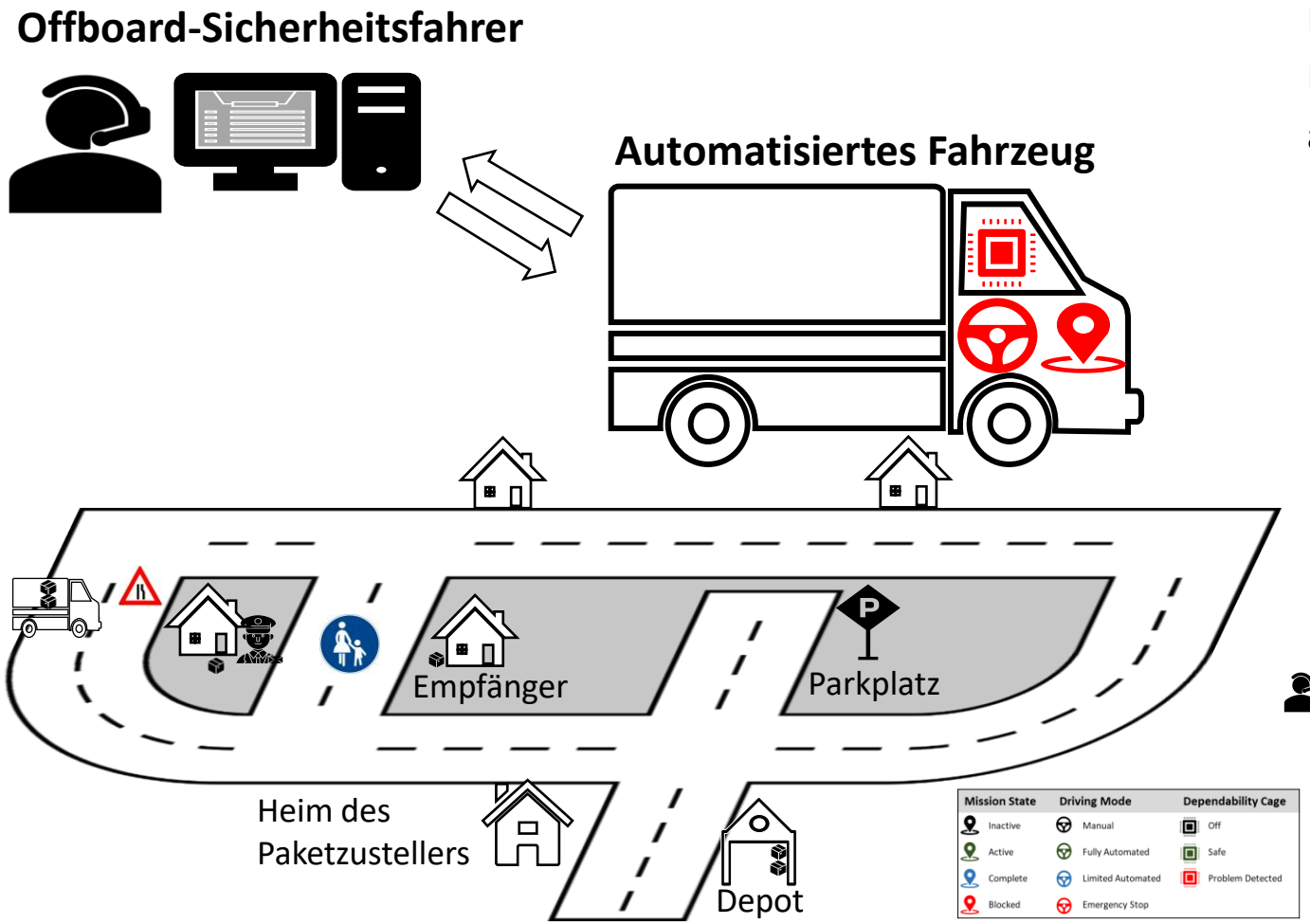
Lösungsansatz: Beispielhafter Ablauf einer Paketzustellung



Aktuelle Mission: Automatisiert zum Treffpunkt mit dem Paketzusteller fahren, damit der Paketzusteller Pakete für weitere Zustellungen entnehmen kann.

- Aktiviert die aktuelle Mission. Das automatisierte Fahrzeug darf dabei nicht durch die Fußgängerzone fahren.
  → **Mission State: Active**
  → **Driving Mode: Fully Automated**
- Fährt automatisiert zum Treffpunkt mit dem Paketzusteller.
- **Ungeplante Aktion:** Eine unvorhergesehene Fahrbahnverengung wird erkannt, wodurch das automatisierte Fahrzeug einen Notstop auslöst.
  → **Mission State: Blocked**
  → **Driving Mode: Emergency Stop/ Driving Blocked**

Lösungsansatz: Beispielhafter Ablauf einer Paketzustellung



Folgeschritt: Der Offboard-Sicherheitsfahrer analysiert das Problem und löst das Problem aus der Ferne, sodass das automatisierte Fahrzeug die Mission fortsetzen kann.

Wird informiert, dass sich das automatisierte Fahrzeug im Mode Emergency Stop/ Driving Blocked befindet, wodurch die Fahraufgabe nicht mehr abgeschlossen werden kann.

Analysiert die Situation aus der Ferne und löst das Problem, indem das automatisierte Fahrzeug auf Limited Automated konfiguriert wird. Das reduziert den Sicherheitsbereich (Safe Zone), begrenzt jedoch die zugelassene Maximalgeschwindigkeit. In diesem Mode überwacht der Offboard-Sicherheitsfahrer kontinuierlich die Aktionen des automatisierten Fahrzeugs, sodass dieser bei einem Sicherheitsrisiko einen emergency stop auslösen kann.
→ **Driving mode: Limited Automated**
→ **Mission state: Active**

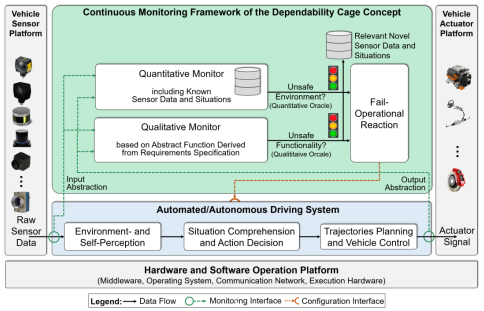
Führen die aktuelle Mission zusammen (kooperativ) fort.

Erreicht den Treffpunkt. Der Paketzusteller nimmt die Pakete für die zweite Lieferung aus dem automatisierten Fahrzeug.
→ **Mission state: Complete**

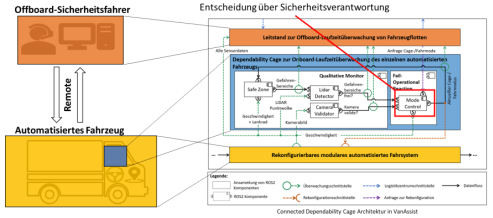
Agenda

- Motivation
  - SAE Stufen des automatisierten Fahrens
  - VanAssist
- Lösungsansatz
  - Dependability Cage
  - Connected Dependability Cage
  - Beispielhafter Ablauf
- Zusammenfassung und Ausblick

Zusammenfassung

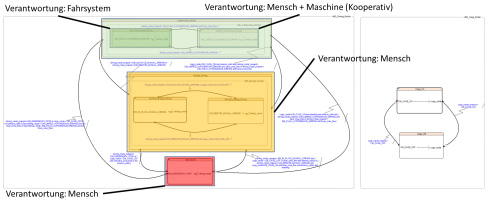


Dependability Cage Ansatz als Ausgangspunkt zur Lösung unserer Fragestellungen



Erweiterung zum Connected Dependability Cage Ansatz zur ODD Überwachung und zuverlässigen Verantwortungstransfer.

Remote Command Control Center, um Offboard-Sicherheitsfahrern die entfernte Überwachung und den menschlichen Eingriff zu ermöglichen.

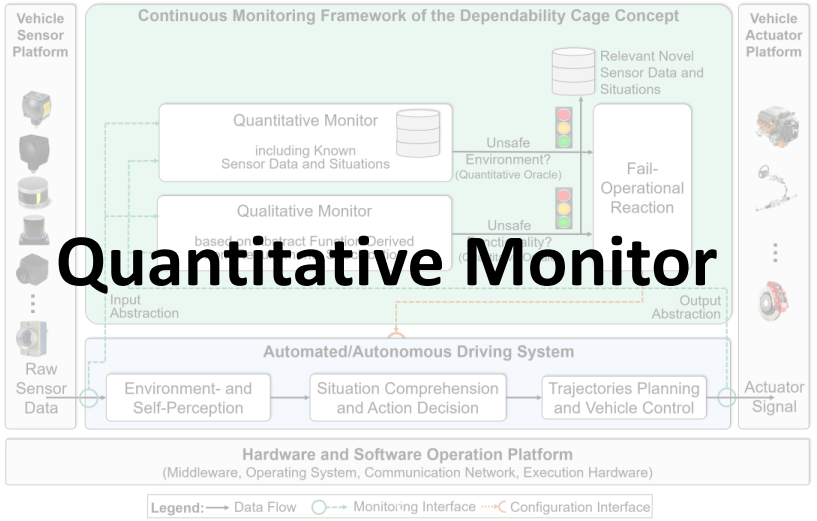


Eine zentrale Komponente des Connected Dependability Cages legt die Verantwortung fest. Dieser Ansatz ist verifizierbar!

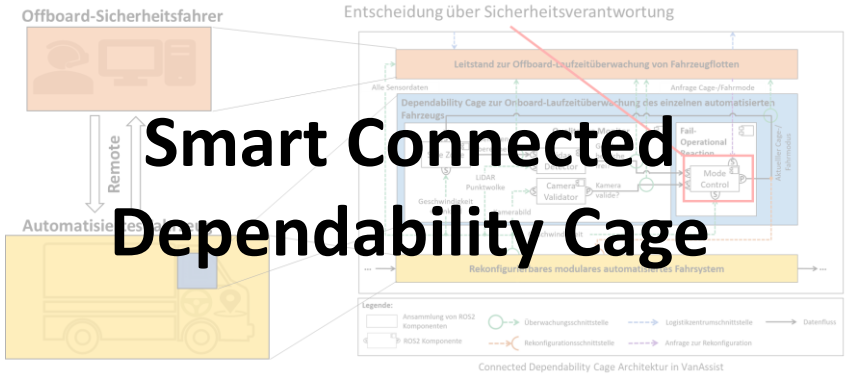
Ausblick

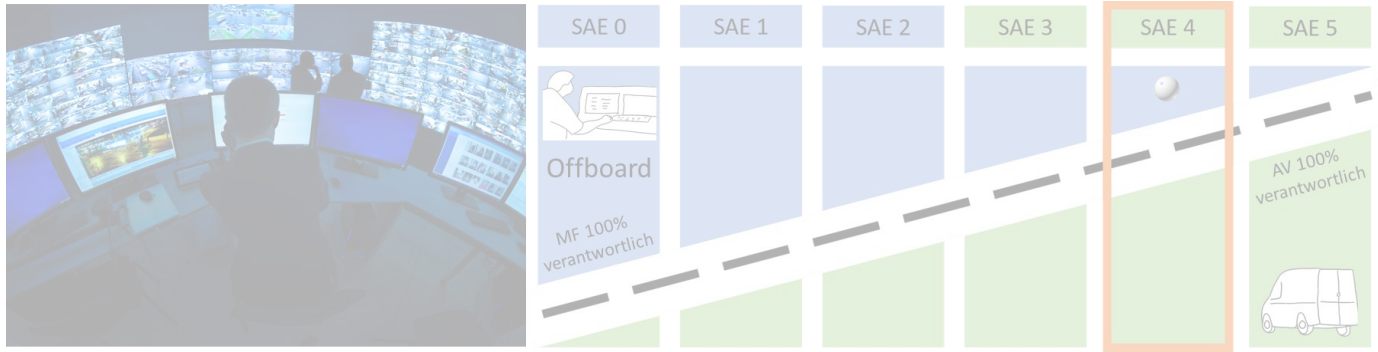
VanAssist

Quantitative Monitor

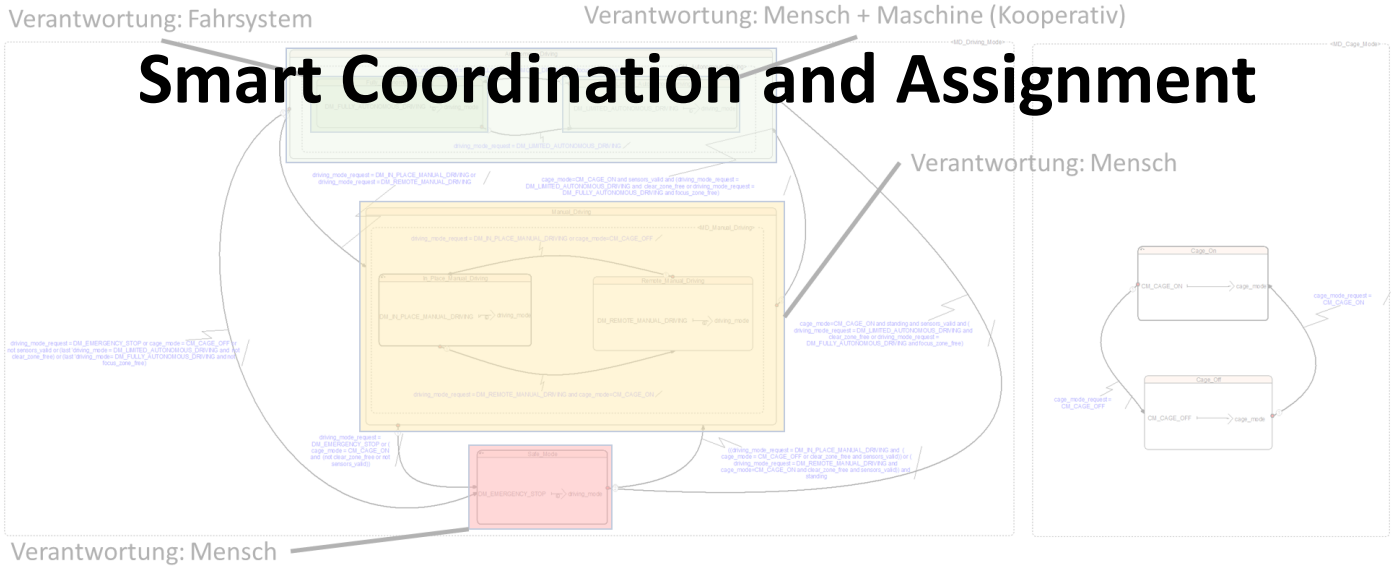


Smart Connected Dependability Cage





Smart Coordination and Assignment



Institute for Software and Systems Engineering

TU Clausthal

VanAssist

VanAssist

Vielen Dank für Ihre Aufmerksamkeit

M. Sc. Andreas Vorwald

Gefördert durch:

Bundesministerium für Verkehr und digitale Infrastruktur

aufgrund eines Beschlusses des Deutschen Bundestages