UNICAR*agil* - Disruptive Modular Architectures for Agile, Automated Vehicle Concepts

Timo **Woopen***, M.Sc., Bastian **Lampe***, M.Sc., Torben **Böddeker***, M.Sc.,
Prof. Dr.-Ing. Lutz **Eckstein**
Institute for Automotive Engineering, RWTH Aachen University, Aachen, Germany

Alexandru **Kampmann***, M.Sc., Dr.-Ing. Bassam **Alrifaee***,
Prof. Dr.-Ing. Stefan **Kowalewski**
Informatik 11 – Embedded Software, RWTH Aachen University, Aachen, Germany

Univ.-Prof. Dr.-Ing. Dieter **Moormann**
Institute for Flight System Dynamics, RWTH Aachen University, Aachen, Germany

Dipl.-Ing. (FH) Torben **Stolte***, M.Sc., Inga **Jatzkowski***, M.Sc.,
Prof. Dr.-Ing. Markus **Maurer**
Institute of Control Engineering, Technische Universität Braunschweig, Braunschweig, Germany

Mischa **Möstl***, M.Sc., Prof. Dr.-Ing. Rolf **Ernst**
Institute of Computer and Network Engineering, Technische Universität Braunschweig, Braunschweig, Germany

Stefan **Ackermann***, M.Sc., Christian **Amersbach***, M.Sc.,
Prof. Dr. rer. nat. Hermann **Winner**
Institute of Automotive Engineering, Technische Universität Darmstadt, Darmstadt, Germany

Dominik **Püllen***, M.Sc., Prof. Dr. Stefan **Katzenbeisser**
Security Engineering Group, Computer Science Department, Technische Universität Darmstadt, Darmstadt, Germany

Dr.-Ing. Stefan **Leinen***, Prof. Dr.-Ing. Matthias **Becker**
Chair of Physical and Satellite Geodesy, Institute of Geodesy, Technische Universität Darmstadt, Darmstadt, Germany

Prof. Dr.-Ing. Christoph **Stiller**
Institute for Measurement and Control, Karlsruhe Institute of Technology, Karlsruhe, Germany

Prof. Dr.-Ing. Kai **Furmans**
Institute for Material Handling and Logistics, Karlsruhe Institute of Technology, Karlsruhe, Germany

Prof. Dr. Klaus **Bengler**
Chair of Ergonomics, Technical University of Munich, Munich, Germany

Dr.-Ing. Frank **Diermeyer***, Prof. Dr.-Ing. Markus **Lienkamp**
Chair of Automotive Technology, Technical University of Munich, Munich, Germany

Dr.-Ing. Dan **Keilhoff*,** Prof. Dr.-Ing. Hans-Christian **Reuss**
Chair in Automotive Mechatronics, University of Stuttgart, Stuttgart, Germany

Dr.-Ing. Michael **Buchholz***, Prof. Dr.-Ing. Klaus **Dietmayer**
Institute of Measurement, Control and Microtechnology, Ulm University, Ulm, Germany

Dr.-Ing. Henning **Lategahn**
Atlatec GmbH, Karlsruhe, Germany

Dr.-Ing. Norbert **Siepenkötter**
flyXdrive GmbH, Aachen, Germany

Martin **Elbs**
IPG Automotive GmbH, Karlsruhe, Germany

Dr.-Ing. Edgar **v. Hinüber**
iMar Navigation GmbH, St. Ingbert, Germany

Marius **Dupuis**
VIRES Simulationstechnologie GmbH, Bad Aibling, Germany

Christian **Hecker**
Schaeffler Technologies AG & Co. KG, Herzogenaurach, Germany

* The marked authors are first authors with equal contribution.

Summary

This paper introduces UNICAR*agil*, a collaborative project carried out by a consortium of seven German universities and six industrial partners, with funding provided by the Federal Ministry of Education and Research of Germany. In the scope of this project, disruptive modular structures for agile, automated vehicle concepts are researched and developed. Four prototype vehicles of different characteristics based on the same modular platform are going to be build up over a period of four years. The four fully automated and driverless vehicles demonstrate disruptive architectures in hardware and software, as well as disruptive concepts in safety, security, verification and validation. This paper outlines the most important research questions underlying the project.

1 Introduction

Forty years ago, in 1978, a consortium of four German universities started the UNI-CAR project [1]. With this large, demanding and complex project, the university consortium was able to enrich its original teaching and research tasks and significantly enhance its reputation in the automotive industry. In 1981, a prototype was presented at the International Motor Show in Frankfurt. It featured innovations such as tire pressure control, pedestrian safety systems and a direct injection diesel engine. All of them became state of the art in modern vehicles.

Since then, traffic as well as the automotive industry have changed in many ways. Automated driving, connected vehicles, shared mobility and electrification are the megatrends of today [2]. Many new research questions arise. Due to their complexity, only an interdisciplinary approach is capable of providing adequate solutions.

For this reason, UNICARagil brings together a consortium of seven universities (with 14 chairs involved) and six industrial partners. Under the leadership of the RWTH Aachen University, the universities TU Braunschweig, TU Darmstadt, Karlsruhe Institute of Technology, TU München, University of Stuttgart and Ulm University work together with the industrial partners Atlatec GmbH, flyXdrive GmbH, iMAR Navigation GmbH, IPG Automotive GmbH, Schaeffler Technologies AG & Co. KG and Vires Simulationstechnologie GmbH. This consortium combines comprehensive expertise and several hundred person-years of experience in the development of automated vehicles.

Various emerging technologies allow for a new mobility experience in combination with higher traffic efficiency and safety. However, suitable vehicle concepts that allow to keep up with short innovation cycles of the aforementioned technologies have to be envisioned. The prevailing evolutionary development methods in the automotive industry have been successful for the last 130 years but will be unsuitable for facing the emerging future trends. Thus, UNICAR*agil* focuses on new disruptive modular architectures for agile and automated vehicle concepts. The development avoids inherited liabilities in order to provide solutions for challenges imposed by emerging mobility trends and to set impulses for the future.

2 Overall Concept

With a disruptive modular approach, UNICAR*agil* paves new ways for the development of agile automated and electrified urban vehicles. Disruptive approaches are those that completely rethink previous procedures and thus reveal previously unseen solutions. The project focuses on scientific questions from various areas of automotive engineering, electrical engineering and computer science. The focus areas of the project are **automation**, **safety, security, verification & validation,** and **modularization**.

Fig. 1 shows a schematic overview of the overall concept. At its center, a scalable **platform** provides the basis for various new vehicle concepts. It is equipped with four **dynamic modules** that are responsible for steering, accelerating and braking the vehicle. Each module has a 48 volt wheel hub motor and can reach steering angles of up to 90 degrees. New agile maneuvers become possible, since each module is independently steerable. The platform can be equipped with various **add-on modules** and thus be used for different purposes. The goal is to develop **fully automated** and **driverless** vehicles. The interior design is deliberately conceptualized in consideration of a driverless operation. The sensors required for environment perception are integrated into the vehicles in the form of disruptive **sensor modules** that combine various sensor technologies, with safety-relevant redundancies in mind.

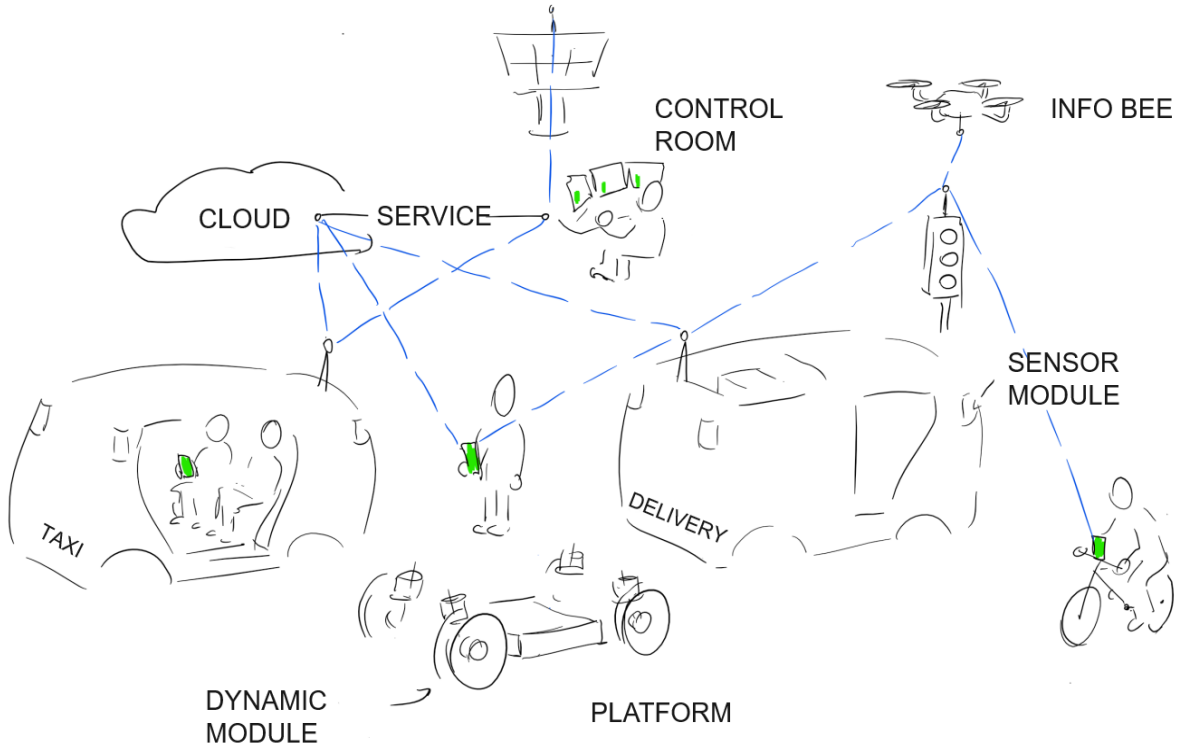

Fig. 1: Sketch of the Overall System.

Communication between vehicles and **cloud services** are used to share and evaluate data, which helps planning a safer and more efficient behavior. So-called **Info Bees** that add to the environmental perception of the vehicles support this process. A control room allows remote human intervention in case of exceptional conditions such as an inability of the platform to maneuver safely. In such situations, the vehicle will slow down and eventually stop. Afterwards, the control room can take over driving via teleoperation.

A new functional and a new electrical and electronic (E/E) architecture become necessary in order to implement the described functionalities. A large number of electronic control units, decentralized data storage and limited high-performance data communication characterizes the currently established E/E architectures. Even small changes to a system cause enormous effort in the re-execution of the verification and validation processes. Expandability and the assurance of failure safety are therefore aggravated. Consequently, a new E/E architecture is proposed. It borrows its terminology from biological nervous systems. Fig. 2 shows a simplified sketch of the disruptive E/E architecture.

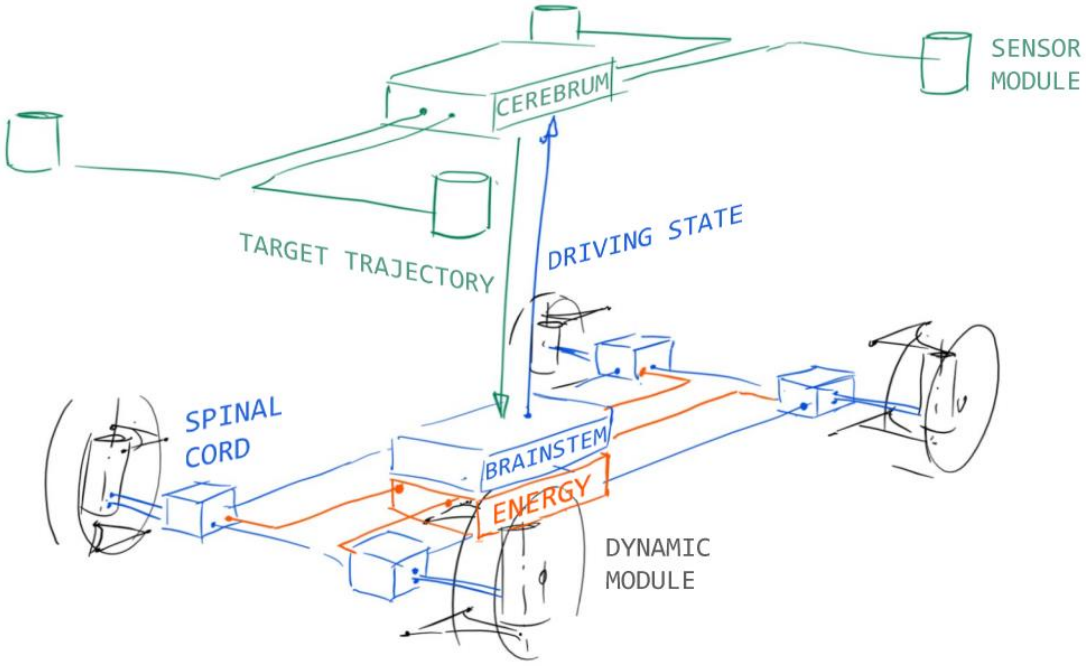

Fig. 2: Disruptive Control-Units Architecture Based on Human Brain Structure.

The perception of the environment is realized by the sensor modules, which resemble the sensory organs. The collected data is preprocessed in the sensor modules and then handed over to the **cerebrum**, which is responsible for high-level data processing, such as behavioral and trajectory planning. On the **brainstem** level, the planned trajectory is tracked**.** The **spinal cord** provides the necessary steering angles and braking or acceleration torques to the dynamic modules. An integrated 48 volt wheel hub motor drives each dynamic module. This allows individual wheel acceleration, brake and steering torques to be communicated to the modules. In addition, the spinal cord is able to react to defects or failures of the brainstem reflexively and thus contributes a further part to failure safety. A redundant electrical system enables this approach.

Fig. 3 shows the **functional architecture** representing the necessary functionalities for the execution of subtasks on an abstract level. In addition to these subtasks, external elements (shown left) may support the vehicle in the driving task. The so-called "A-model" combines the classic levels of the driving task according to Donges [3] with the increased demands by the perception and information processing of automated vehicles. Disruptive core elements of this model are the spinal cord-like linkage of sensors and actuators on a low level for a reflexive reaction to sudden events. Another core element is the trajectory evaluation ex-post, which provides valuable information for the equally disruptive **Collective Memory**, from which all connected vehicles may benefit, also with various degrees of automation.

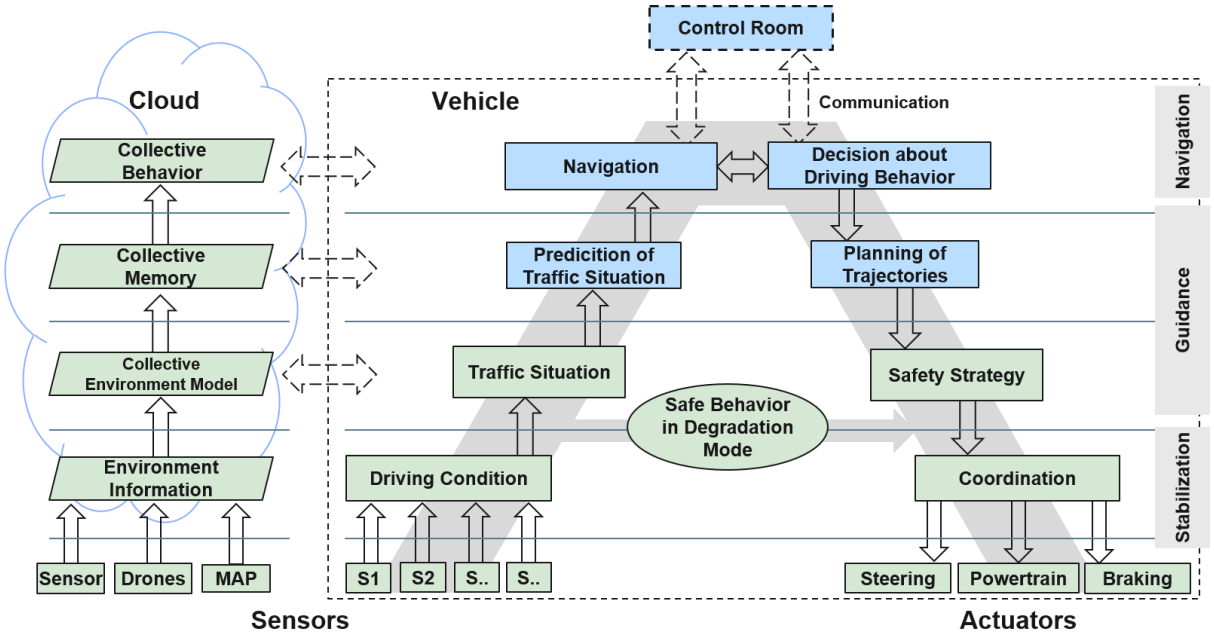

Fig. 3: A-Model for the Functional Architecture.

An automotive service-oriented software architecture (ASOA) will lay the foundation for all software functionalities. Among other things, ASOA will allow for flexible integration of components at runtime, thereby contributing to the modularity concept pursued throughout the project. Modules and subsystems can select and use the required functionalities at runtime in the form of services. These can be offered and requested. This disruptive approach aims at an agile **updateability and extensibility** of the system.

These proposed architectural approaches and the lack of a human fallback level in vehicles developed for automated operation pose new challenges in the field of **safety**. In this project, a safety concept is developed that goes beyond the previous approaches of the ISO 26262 [4]. One part of this safety concept is the so-called self-perception, which always observes and evaluates the current system status regarding the vehicle's current capabilities. Due to increasing interconnectedness and digitization, **security** also plays an important role and is ensured by the developed hardware and software concepts. Furthermore, it will be investigated how security and safety can be combined. The modularization in hardware and software makes it possible to consider the verification and validation challenges of automated vehicles in a modular way. Hence, one goal is to develop a concept for modular verification and validation, wherein each module may be verified and validated separately. Consequently, the effort for complete system verification and validation can be minimized. The described modular architectures promote **versatility and scalability**. The vehicles are supposed to transport both people and goods. They are scalable in size as a result of the modular platform. Cooperative behavior increases **efficiency, comfort and safety**. The vehicles cooperate not only with each other, but also with other traffic participants. In the event of a failure of the vehicle, it shall always be able to transition into in a safe state, the **Safe Halt**, i.e. to stop at the next safe opportunity. The control room may then take over the vehicle operation from this safe state.

The dynamic modules allow the platform to move in a completely new and disruptive way. Trajectories perpendicular to the vehicle's longitudinal axis will be possible and help with the parking process. This new **maneuverability** offers the potential to positively change traffic in steadily growing cities. The cloud-based optimization of the dynamically varying transport task and its distribution to a vehicle fleet may further increase the **efficiency** of traffic. **Cooperation** not only happens between individual automated vehicles, but also between the vehicles and other road users. They will be able to interact with the vehicle, so suitable exterior elements need to be developed. The interfaces between human and machines play a decisive role for automated vehicles. In the interior, the focus is no longer put on the driving experience, but on the experience of being driven. For this reason, innovative interior concepts and interfaces are developed that make automated driving comfortable and trustworthy.

On this basis, the following four UNICAR*agil* vehicle prototypes are realized. They aim at exemplarily demonstrating the potential of the disruptive, modular and scalable concept.

1. **AUTO*taxi***: A "classic" application for automated vehicles. A fully automated and driverless taxi that is called by a smartphone and comfortably transports passengers to the desired destination.
2. **AUTO*elfe***: This automated vehicle is privately owned and is considered part of a family to do shopping or to take the children to school.
3. **AUTO*liefer***: A "mobile packing station" with efficient and intelligent conveyor technology that can pick up and deliver parcels independently.
4. **AUTO*shuttle***: Passengers can travel as if on a train, as several electronically coupled vehicles behave like one rail vehicle. The AUTOshuttle transports small groups and is used in local public transport.

In summary, the overall concept can be presented in various design and architectural views. These in turn subdivide further. Fig. 4 shows an overview of these viewpoints.

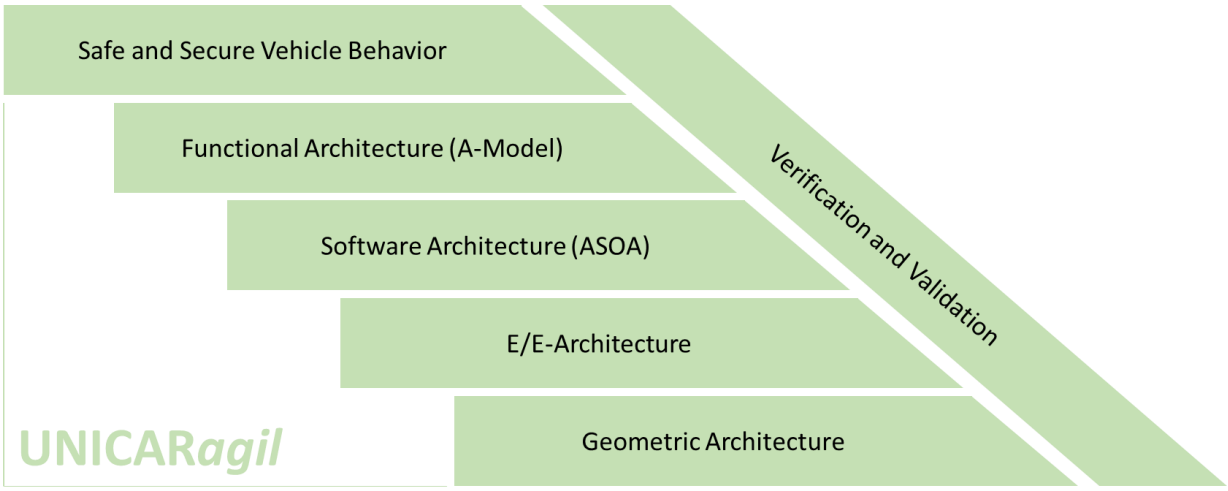

Fig. 4: Different architectural viewpoints in the project UNICAR*agil* referring to [5].

These different architectural viewpoints form the basis for the development and research work in the project. They address numerous scientific questions, which are presented in the following sections.

3 Geometric Design

In UNICAR*agil*, the geometric design deals with various different aspects, such as the geometrical main load-bearing structures, the exterior and interior design as well as Human Factors. This section outlines the change to the overall vehicle and interior design regarding new boundary conditions set by the disruptive modular concepts envisioned in the UNICAR*agil* project.

3.1 Disruptive Changes in Vehicle Structures

Most current vehicle structures are built around an ergonomic driver's workplace and a conventional drive train powered by a combustion engine. Today´s vehicles are made to be driven by a human operator. The design process as well as the vehicle's geometry are highly influenced by regulations and standards. Electrification leads to a simplification of the drive train and a high degree of freedom in the package design. Within the project, a combination of by-wire systems and wheel hub motors will be developed and prototyped. The wheel hub motors, the brakes, the steering and the suspension are combined into dynamic modules. These modules have a defined interface but no further restriction with respect to their position, thus the package of the vehicle is no longer ruled by the mechanical architecture but will be adapted according to the vehicle's purpose. Dynamic modules can be placed freely within the design space and changed in number depending on weight and size of the vehicle. Further research is carried out with respect to the structural design. In today´s vehicles, the size and position of the main load carrying structures is highly dependent on the driver's field of view and on well-established door concepts that are made for a standard two row seating arrangement. In case of driverless vehicles, the driver's field of view is no longer a safety critical requirement. Thus, the load-bearing structure can be developed following the most weight efficient path. The structural design space will be defined by the exterior design concept, ingress and egress as well as the required interior space, which emerges from the developed ergonomic seating concepts. Within this space, optimization methods are used to define the main load carrying structures, solely limited by the manufacturing concept, the material choice and the vehicle design. To design the four prototyped concepts (cf. Section 2), current legislation for structural safety is analyzed and evaluated with respect to its validity for fully automated and driverless vehicles in an urban environment. Loads, accelerations, and intrusion targets are derived from relevant accident scenarios.

3.2 Scalable and Modularized Vehicle Structures

When looking at mobility as a service instead of personal mobility enabled through the ownership of a vehicle, a huge variety of automated purpose design vehicles is conceivable. In this project, the focus lies on delivery services, on on-demand mobility

and on tailored public transportation. This results in the four introduced concepts: AUTO*taxi*, AUTO*elfe*, AUTO*liefer* and AUTO*shuttle*. The given design freedom is used to create a modular and scalable structure that can be adapted to a variety of urban mobility concepts represented by the four vehicle concepts. The vehicle structure is divided into a driving platform and an add-on transport module. The former is scalable in its length and the latter in its length and height. A maximum amount of carry-over parts is targeted and scalable interfaces are defined to ensure the maximum amount of flexibility. The number of different parts shall remain small. In combination with modularized crash management systems and dynamic modules, the use case specific vehicle concepts are designed on one common toolbox with little drawbacks in weight and design freedom.

3.3 User Experience Based Interior Development

Since a fully automated and driverless vehicle – as envisioned in UNICAR*agil* – lacks the necessity of a manually operated interface to the chassis actuators, one formerly main requirement for the interior design becomes obsolete. A transformation from a "driver's workspace" to a "living room" is possible. This allows shifting the focus from operational safety to better user experience. Currently, there exists no fully automated vehicle in series production. Hence, only a small amount of data on customer expectations regarding an automated vehicle's interior design is available. Starting from a customer survey, followed by user benchmarked mockup tests up to the final interiors, a user-centered design approach is followed. In addition, scenario-based methods are used to capture the users' perspective on the developed vehicles. The resulting main requirements are transformed into first interior concepts. These are evaluated by product clinics and further adapted to the users' needs.

4 Mechatronic Design

The mechatronic design described in this section comprises electrics and electronics needed to provide electric and computing power as well as to enable communication. Furthermore, this section presents the concept of a Safe Halt and that of the control of vehicle dynamics.

4.1 Hardware Design

Verification and validation of automated driving functions are fundamental challenges of today's research and development activities. The presented structure of different levels – in this project called cerebrum, brainstem and spinal cord (c.f. Section2) – aims at verifying and validating a system by the verification and validation of its modules. Well-defined interfaces ensure the separation of tasks between the different levels.

The task of the sensor modules is to perceive the environment of the vehicle. Based on the collected data, each sensor module creates an individual environment model. In a first step, a control-unit (cerebrum) computes a single environment model based on those provided by the individual sensor modules and extrapolates the current traffic

scenario. In a second step, both the main and the fallback trajectory are calculated in accordance with the desired tactical behavior. The trajectories are handed over to another control-unit (brainstem), where the main trajectory is tracked. Four individual control signals, e.g. drive or brake torques and steering angles, are computed and sent to each dynamic modules' actuators. The four dynamic modules' control-units (spinal cord) are responsible for providing the required forces by the control of voltages and currents. Fig. 5 shows the mechatronic design from a task's point of view.

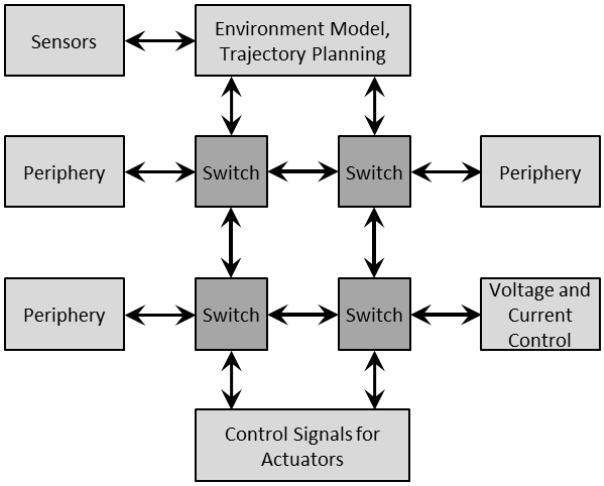

Fig. 5: The Mechatronic Design from a E/E-Hardware's Point of View.

The mechatronic architecture provides multiple interfaces in order to enable control over either the behavior level, the trajectory level or the control level. This is the fundament of the coadjutant safeguarding. In case of a degradation of the cerebrum's functionality, the trajectory planning might be unavailable. Due to the fallback trajectory from the last time step, the brainstem is still able to send desired forces and torques to the dynamic modules. Thus, permanent maneuverability is ensured. In case of unavailable functions of the brainstem, there still is a communication channel available between the environment model and the dynamic modules and their spinal cord. Since the control of the voltage and the current is located in each dynamic module, this function is equipped with sufficient redundancy as well.

In addition to the approach of coadjutant safeguarding, the brainstem will have a failsafe design. This demonstrates an alternative approach of maintaining essential functions and features in automated vehicles.

Beside the described tasks' viewpoint, there is a perspective regarding the different communication partners as well. The mentioned modularity and the demanded expandability raise new questions. All communication partners, including those components, which are mounted later on, have to support the service orientation of the software as well as the partially encoded communication. However, since different E/E components might be used, the communication in between needs to be realized and handled by the mechatronic design. Fig. 6 shows the mechatronic design from a communication partner's point of view.

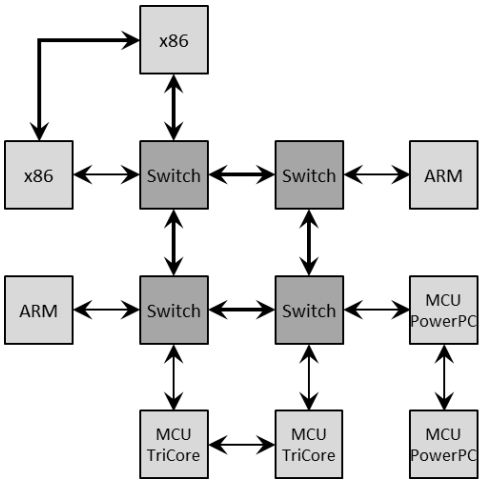

Fig. 6: The Mechatronic Design from a Communication Partner's Point of View.

The power supply is realized with a maximum of 48 volts. The concept therefore offers a purely electric vehicle platform that even people without high voltage training are allowed to work with. However, the 48 volts lead to a rather high current level, especially for the dynamic modules. Thus, the power grid topology strives for short connections between the battery pack and the electric motors.

All UNICAR*agil* vehicles can be charged via cable. Additionally, one vehicle will be equipped with a fully automated inductive charging system. The vehicle localizes the primary coil and then parks itself perfectly aligned for an efficient energy transfer.

4.2 Safe Halt of Highly Automated Vehicles

In a vehicle with a SAE level 3 [8] or higher, the human driver does no longer serve as a fallback solution for the dynamic driving task. Instead of this, a new fallback level is introduced. It is capable of transitioning the highly automated vehicle into a safe state at all times: the Safe Halt [6]. It serves as a fallback level for the automated operation in case of a final degradation mode. An occurrence of the latter may be detected with the help of the self-perception. If the driving mission cannot be pursued further, e.g. in case of a failure of an essential component, the Safe Halt will be initiated. Since this function is not fully active in normal operation mode resulting in a partially cold redundancy, a reliable self-perception is of great importance for the monitoring of the vehicle's current abilities.

For the implementation of the Safe Halt, the following challenges need to be mastered:

- Definition of conditions under which the Safe Halt is to be initiated [7].
- Development of strategies that enable the safe transition of a vehicle into a risk-minimal state at all times, especially if it is in final degradation mode.
- Definitions of functional requirements for the Safe Halt. These include the requirements for the desired control functionality, but also the availability of a reliable self-perception for monitoring the functions' operational reliability.

After performing the Safe Halt, not all functions of the vehicle may be unavailable. Remaining abilities of the vehicle can be used through teleoperated driving. Especially

during a final degradation mode that is only temporary, a remote human driver may be able to handle the situation. As soon as information from the self-perception indicates the possibility to pursue the driving mission again, the human operator can return the vehicle guidance to the automated system.

4.3 Motion Control of Highly Agile and Automated Vehicles

In the UNICAR*agil* project, the vehicles are not driven by a human driver, but are fully automated. Based on the desired trajectory computed by the cerebrum, the motion of the vehicle is controlled by comparison of the desired with the actual vehicle dynamics state. Due to the high number of actuator degrees of freedom (4 x 2) the trajectory control is able to serve as an independent 3-DoF motion provider. Therefore, strategies will be developed that distribute the demand for vehicle motion to the four dynamic modules by individually assigning necessary driving and steering torques.

4.3.1 Vehicle Dynamics State Estimation

The lack of a human fallback level in vehicles with SAE level 3 [8] or higher results in high demands concerning the availability of the estimator, the accuracy of the estimated dynamic driving state and the reliable self-perception of the estimator's current capabilities.

For the development of a highly available, precise and accurate state estimation of the vehicle dynamics, the focus will be put on the following challenges:

- The state estimator of the vehicle dynamics has to be highly available during operation, as it is essential for estimating the current vehicle dynamics. An appropriate set of sensors is to be selected and a fusion strategy fulfilling the above-mentioned requirements is to be developed.
- An important characteristic of the estimation is high accuracy of the driving dynamics states, since they serve as measured input to the subsequent motion controller. The accuracy of the estimated states has a major impact on the performance of the motion control: a strategy is developed that provides precisely and accurately estimated states in order to keep the motion controller well within its operational range.
- Besides dynamics states, the estimator provides related quality metrics in terms of estimated accuracy and integrity. Especially integrity information serves for the assessment of the estimator's output and must cover sensor integrity as well as integrity of the sensor fusion operation. Proven integrity techniques for navigation systems will be adapted to the project-specific requirements within the framework of UNICAR*agil*.

4.3.2 Vehicle Dynamics Control

A vehicle dynamics controller performs the tracking of the automated vehicle along a target trajectory. Its task is to move the vehicle precisely and accurately along the target trajectory by comparing the actual driving dynamics state with the target driving dynamics state. In UNICAR*agil*, vehicles are developed with the option of wheel-

specific steering angles and drive torques. These vehicle characteristics enable the side slip angle to be used as an additional degree of freedom in driving dynamics. A vehicle with four independently steered and driven wheels is over-actuated, which offers new options for the design of a vehicle's driving dynamics.

In order to fully explore possibilities of the driving dynamics provided by the higher degree of freedom, the following steps are systematically carried out:

- Analysis of the effects caused by an over-actuated two-track vehicle on driving dynamics. In this context, ways to optimize properties of driving dynamics are examined, e.g. driving comfort and safety.
- Based on the results of the analyses above, the requirements for a robust vehicle dynamics and trajectory controller are specified. This includes the definition of evaluation criteria for the multivariable control.
- Subsequently, the developed control concept is implemented into the UNICAR*agil* prototypes. The system is then verified and validated.
- Derived from the actual motion state and the estimated road friction, criteria for the calculation of the desired trajectory have to be computed and sent to the trajectory planner.

5 Service-oriented Software Architecture

This section outlines the service-oriented software architecture envisioned in the UNICAR*agil* project. First, the motivation behind using a service-oriented software architecture is elaborated in the automotive context. Second, a brief overview of the software architecture proposed for UNICAR*agil* is provided and resulting research issues are addressed.

5.1 Background and Motivation

With a steadily increasing amount of complex software components running on an ever-growing number of Electronic Control Units (ECU), often with tight real-time constraints, system and variant complexity in modern vehicles is continuing to grow [9]. Development standards, such as the AUTOSAR platform, have been established to tackle the challenges arising from the increasing system complexity by means of defining standardized software interfaces and runtime environments for ECUs. Although AUTOSAR has become the de facto standard since its introduction in 2003, the static integration of resulting systems makes it hard to quickly integrate new components and to adapt the system configuration, especially after vehicles have already been sold. The resulting E/E architectures are function oriented, where each element from the functional system architecture is implemented by a single software component with well-defined interfaces. In a subsequent system-integration step, these components are statically integrated, resulting in a rigid coupling between software components. Knowledge about the component coupling becomes a static part of software components and subsequently of the ECU software image. Thus, adapting the system configuration beyond the system-integration phase becomes a painstaking

process. Statically integrated systems, as described above, lack flexibility with respect to adapting the system configuration or integrating new components. Consequentially, it becomes increasingly hard to face the shorter and shorter development and lifetime cycles for disruptive future automotive trends such as connected and highly automated vehicles.

A service-oriented software architecture for the UNICAR*agil* vehicles is proposed, which will allow for dynamic system reconfiguration and which provides mechanisms for seamless integration of new components. The application of service-oriented software architectures for automotive applications has been proposed and also partially implemented in various efforts [10] [11] [12], none of them go to the radical extend of implementing the complete vehicle software architecture in a service-oriented manner. The following section will briefly outline the essential components involved in the proposed service-oriented architecture.

5.2 Concept Overview

In contrast to systems with an inflexible runtime-integration, software components in service-oriented architectures are implemented as loosely coupled services, which are not integrated at design time, but at runtime [13]. One consequence of this paradigm is that a service, which requires data that it does not produce internally, will only be connected at runtime to another service producing the required data. This allows for interchangeability and reusability of software components, as system-integration decisions are decoupled from the individual software components. Instead, the integration and coupling of services at runtime is guided by an orchestrator, which is a designated and privileged software component that establishes situation-depended connections between services. The connections established between services for a concrete system instantiation induces a connection graph, which will further be referred to as a service composition. The concept is illustrated in Fig. 7, where the same services are connected in varying constellations at runtime, based on the mode of operation or intended vehicle behavior. In the example below, the entirety of services in the vehicle is composed and repurposed in a different way for the automated driving mode compared with the remote operation mode, with the connection being guided by the orchestrator and not by the services themselves. Through the common Ethernet connection between the various ECUs in the UNICAR*agil* vehicles, services will be able to transparently interact with each other across compute platform boundaries. Among other things, the graphs will serve as a basis for a formal analysis of the software system. Please note that the displayed modes of operation serve as an example.

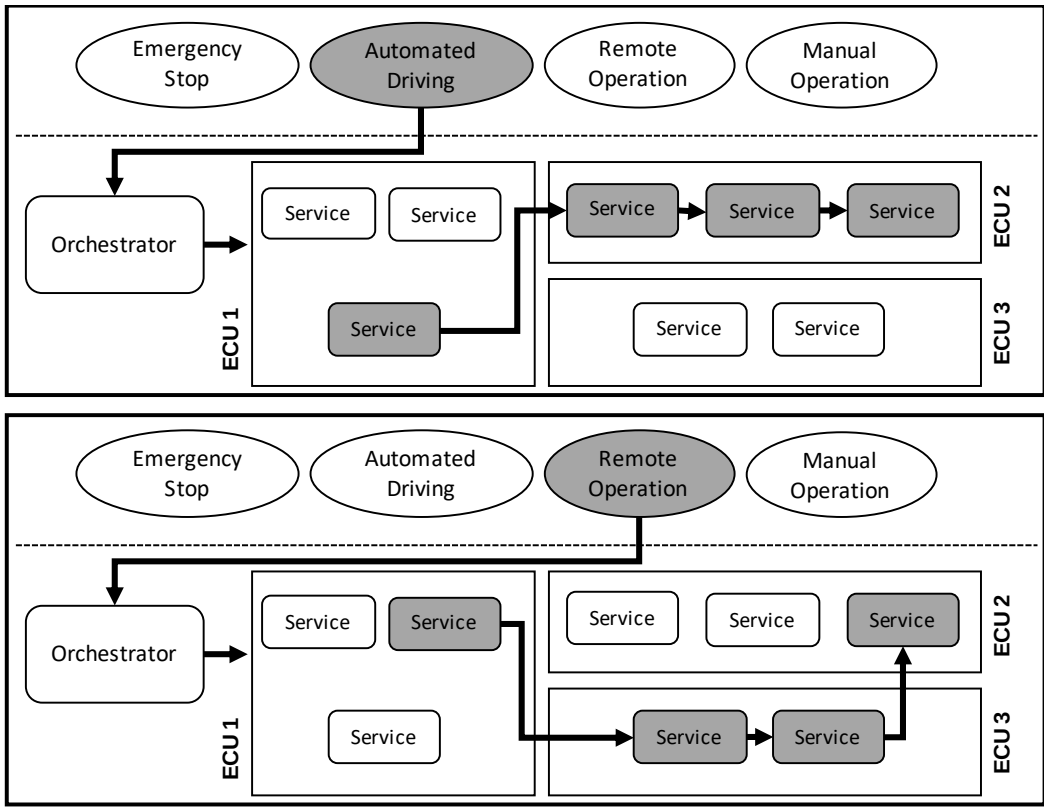

Fig. 7: State-dependent Service Composition at Runtime.

A key concept in service-oriented architectures is that all services are characterized in a machine readable and interpretable format, similar to an electronic datasheet, which is queryable at runtime. This crucial aspect enables the orchestrator to determine the set of services and their characteristics in the vehicle, thus forming the information basis required for service integration. Finding suitable ways of characterizing a service, which has to capture the needs and capabilities of a service, is part of the research effort. In the following, service capabilities are defined as software functionalities that are made available by a particular service to the system and that, in principle, can be accessed by any other service. In turn, the needs of a service are abstract functionalities that are provided by other services (i.e. their capabilities), and which will be made available to the consuming service. Note that the concrete service providing a particular functionality is not relevant to the consuming service and will be determined by the orchestrator.

For example, a service that implements multi-object tracking for automated driving may require the current vehicle acceleration with a specific frequency. In order for the orchestrator to be able to match the aforementioned need for vehicle acceleration with a service capable of providing that information, the respective needs and capabilities have to be formulated in an appropriate, machine understandable framework. Expressing needs and capabilities requires descriptions on various abstraction levels. The coarsest description level is a meta level, which describes "what" functionality is required. In the example above, the demanded "vehicle acceleration" is the meta information. As the meta information is conveyed in bits and bytes, another description level is necessary, which is the datatype-based representation of the meta information. The resulting description accompanying the service binary will be referred to as a

service specification. In statically integrated architectures, the information characterizing the needs and capabilities is often captured in design documents that rarely become an explicit, software addressable part of the resulting software component.

Another essential aspect of the proposed software architecture is the explicit modeling of data quality. Any service that produces information with varying quality will have to measure and attach the information about data quality to each data point issued to other services, wherever possible and reasonable. For example, the information about the vehicle position may include the measurement uncertainty. Data quality information will not only serve as input to the self-perception module, which is an essential part in the safety concept and detailed in the following chapter, but could also enable the software architecture to dynamically select the currently best data source for a specific service need.

A fundamental element for formulating needs and capabilities will be a database of functionality types. The concept is illustrated in Fig. 8. Each entry in the database should be suitable for describing both a service capability as well as a service need, based on the idea that one service's capabilities may be another service's need. Functionality types, depicted as arrows, consist of a meta information description, the data type representation of the actual payload as well as the data type for quality information characterizing the payload. Services are thereby enabled to unambiguously formulate their needs (depicted as arrows entering a service) and capabilities (depicted as arrows leaving a service) in their service specification. At the same time, compatibility between services can automatically be validated at runtime by the orchestrator. The interface database for UNICAR*agil* is envisioned to evolve as a joint effort among all project members that provide software components.

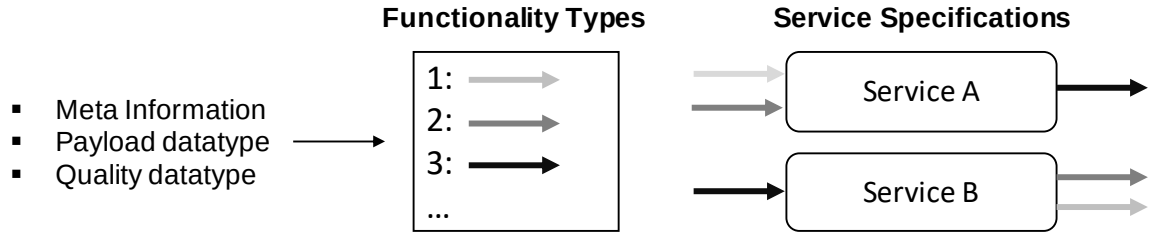

Fig. 8: Unambiguous Formulation of Services Needs and Capabilities Based on a Databased of Interface Types.

A challenge in this project stems from the broad range of computing platforms that need to be integrated into the UNICAR*agil* vehicles. On the one hand, there are full-fledged x86/64 computers running Linux, and, on the other hand, resource constrained ASIL-D safety microcontrollers, lacking any mainstream operating system, with Ethernet being the only commonality linking these vastly different architectures. It is intended to implement the proposed software architecture transparently across all these computing platforms. This means that, ideally, any service can transparently communicate and interact with any other service, regardless of the computing platform they are running on. At the same time, the orchestrator is enabled to detect services and connect them with one another. This cross-device compatibility is aimed to be

achieved through a suitable middleware that builds on top of platform independent communication protocols and careful, lightweight hardware abstraction layers. Although much of the complexity is a result of the seamless integration effort, the overhead induced by the service-orientation has to be restricted to a level that does not violate demanding, automotive real-time requirements. Finally, suitable mechanisms for switching between different service compositions at runtime will have to be carefully designed, especially with respect to safety considerations and real-time constraints.

5.3 Impact on Development Process and Safety

The service-oriented concept outlined above has various implications for the development process. By forcing all services to formalize their needs and capabilities in a model-based process, gaps in the system design were discovered already early on in the project. Additionally, it is intended to make extensive use of code generation for the service implementation and to generate most of the interfaces for handling needs and capabilities. This process allows to preserve as much information as possible from the system design into the actual implementation, thereby enabling clear traceability. Furthermore, the approach will also enable to integrate runtime validation mechanisms to ensure that the actual software architecture matches the intended system design, as service specifications from the design phase can be compared to the actual services present at runtime. Additionally, the runtime integration approach provides a flexible mechanism to handle the different vehicle variants and modes of operation in the UNICAR*agil* project. The various modes of operation can be modeled as different service compositions, allowing to reuse most of the services, and only dynamically adapt the connections established between them. Finally, this service-oriented approach aims for making services more easily exchangeable, as long as a service is replaced with one that provides the same formal capabilities.

This approach is expected to enable automatically performed safety related analysis. Impact analyses on a service composition graph should be able to automatically determine the components affected by a service failure. As identifying all services that are able to fulfill a specific need could be automated, the system will be able to automatically detect redundancies. These redundancies may be used to create fallback strategies for service failures, which in turn can be implemented through the service composition mechanism of the orchestrator.

6 Safety, Security, Verification and Validation

The use cases developed in UNICAR*agil* necessitate an in-depth consideration of safety, security, as well as of verification and validation. One key aspect of the automated driving functionality developed in UNICAR*agil* is – as in any other SAE level 3 or higher functionality [8] – the absence of a human driver and any other supervisor during the automated operation of the vehicle. Consequently, the technical system must implement all tasks which are a human's responsibility in conventional vehicles (e.g. environment perception, decision making, braking, etc.). This implies – in

contrast to already available automation functionalities – significantly new and increased safety requirements of all subsystems that contribute to the vehicle automation functionality. Moreover, the use cases developed in UNICAR*agil* require a high degree of vehicle-internal communication and communication to external infrastructure. This results in substantial security requirements throughout the vehicle's system components. Simultaneously, adequate methods must be furnished that prove that the implemented safety and security concepts are correctly implemented (verification) and – most importantly – suffice for the automated operation (validation). In UNICAR*agil*, safety, security, as well as verification and validation are considered as core challenges and are addressed as outlined in the following subsections.

6.1 Safety

Safety is a key property of vehicles in general, even more of automated vehicles without a human driver as fallback for the technical system. Over the course of the project UNICAR*agil*, the research activities concentrate on three fields of research in order to reach a safe operation of automated vehicles: the concept phase of a development process, the need for self-perception, as well as the proof of timing and safety guarantees of the interconnected services as a foundation for fulfilling fail-operational requirements.

The first focus lies on the concept phase of a development process. The development of a safety concept is a mandatory prerequisite before starting the series development of a vehicle’s automated driving functionality. However, experiences in the project "Automatisch fahrerlos fahrendes Absicherungsfahrzeug für Autobahnen" (aFAS, German for Unmanned Protective Vehicle for Highway Hard Shoulder Road Works) demonstrate that even the development of a comparably simple automated driving functionality – limited to highway hard shoulders and low speeds of 12km/h – pushes the state of the art of safety conception to its limits [14][15][16][17]. Conventional approaches towards safety, as for instance outlined in the ISO 26262 standard [4], do not scale for the driverless and unsupervised operation of vehicles with a more comprehensive functionality. The scope of the ISO 26262 standard only partially considers uncertainties of the automated vehicle operation, namely uncertainties resulting from environment perception, from the prediction of other traffic participants' behavior, from incomplete requirements, as well as from the limited validation depth (see below) [18]. Consequently, the safety activities in the project UNICAR*agil* target the development of an integrated safety framework which supports the systematic and strict top-down development of automated vehicle systems. This consists of a systematic description of the vehicle automation functionality in terms of the item definition and the subsequent hazard analysis and risk assessment according to the ISO 26262 standard.

Eventually, a safety concept, on the one hand, ensures safe vehicle behavior during the automated operation. For this, functional safety according to the ISO 26262 standard is a necessary yet insufficient criterion. Following the standard ensures appropriate handling of system faults. Still, for the more comprehensive category of behavioral safety, it must be ensured that the vehicle provides correct and safe

behavior in manifold scenarios even when no technical fault is present. On the other hand, the safety concept also considers the interconnection of behavioral and functional safety to other safety areas e.g. as presented by Waymo [19]. These are, for instance, crash safety or the safe interaction between the automated system and its users.

In parallel to the safety related activities during a development process' concept phase, it is investigated how safety and security aspects can be considered simultaneously. On the one hand, both faults and attacks lead to unsafe vehicle behavior in the end. On the other hand, safety and security requirements can be contradictory, e.g. an encryption mechanism might increase the latency of safety-relevant messages on vehicular networks beyond acceptable real-time requirements. Thus, resolving these contradictions in an early stage of the development is beneficial.

Another safety feature, which results from the missing human fallback, is self-perception. Human drivers continuously monitor – usually unconsciously – the current performance of the vehicle ("What does the unusual motor noise mean?") and the drivers' own performance ("I am tired.", "It is foggy, I can only oversee the next 50 m."), as well as the situation in the car interior ("Are my fellow passengers feeling okay?") [20]. They adapt their driving behavior, decisions, and mission according to the actual performance and the situation in the car's interior. This task must be taken over by the technical system during the automated operation. Thus, self-perception is a pivotal part of the safety concept, the necessary range of functionality depends on the specific use case. The basic concept requires that each system component provides performance information. This information is accumulated and processed by the self-perception in order to provide performance metrics for each level of a functional system architecture [20].

Self-perception is considered from the beginning of the development as integral system functionality of the use cases developed in UNICAR*agil*. This would enable an automated vehicle operation limited to the specification space and allows an adaption to any degradation. For this, there will be enhancements to works of the ITS community [22][23] as well as of the robotics [24][25] and computer science [26] community. Finally, the self-perception functionality is a potential source of unsafe vehicle behavior itself. Consequently, self-perception is also considered in the safety concept. Moreover, the verification and validation of a self-perception module poses new requirements to the test process.

In parallel to the challenges outlined in the previous paragraphs, new safety challenges arise from the vehicle automation for the hardware and software level. The service-oriented software architecture requires that guarantees for individual services and compositions of services must be provided to facilitate a safety argumentation. This necessitates a detailed investigation of e.g. reliability, availability, or real-time behavior. For these kinds of analyses, it is not sufficient to investigate a service in isolation. Service properties are strongly influenced by software quality, by the hardware services are deployed on, as well as by the properties of the accessed vehicle networks. In UNICAR*agil*, a novel model based approach is developed for timing and

dependency analysis to ensure and plan a reliable error detection corresponding with the functional safety concept for fail-operational guarantees. The foundations of such model-based techniques are the adoption of well-defined mechanisms in the hardware and software architecture of the UNICAR*agil* platform. For instance, the application of Time-Sensitive Networking (TSN) [27][28] techniques in the vehicle network enables planning and enforcement of predictable communication. Analysis and verification for the communication will target non-functional aspects such as message latencies as well as time synchronization throughout the vehicle for measurement timestamping. Again, the challenge of planning and configuring the in-vehicle network is strongly connected to security aspects outlined in the following section.

6.2 Security

Today's road vehicles consist of highly interconnected electronic control units which form a huge computer network. They are probably the most interconnected and complex tools in our daily lives. Many internal components collaborate by exchanging messages over common vehicular buses. While some of them are responsible for non-critical tasks, others are crucial for the passengers' well-being. Attacks on cars have become a hot topic in recent years. It has been shown many times [29][30][31] that adversaries could break into cars to eventually gain partial or even full control. Many attacks target the vehicular bus (CAN bus) which is not cryptographically secured [31], but only physically shielded from the outside world. Once an attacker succeeds in injecting messages, the attacker can take over control. Hence, the use of CAN imposes a security risk on vehicles as Fassak et al. [32] have already shown. This is why road vehicles should face strong requirements when it comes to security, in order to protect passengers and surrounding traffic participants.

Traditionally, communication infrastructure such as the CAN bus is physically hidden such that no unauthorized party is able to access it with a malicious intention. Cars are usually closed and mainly proprietary systems without interfaces to the outside world. Thus, most car manufacturers apply the design principle "security through obscurity" to decrease the attack surface. As mentioned in Section 2, a modular and service-orientated vehicular architecture for the UNICAR*agil* vehicles is proposed. The latter will not only provide new driving experiences with its disruptive geometric and mechatronic design but assumes all vehicles to be digitally embedded into the environment, i.e. to appear as secured devices in an interconnected world. From the outside perspective, a car appears to be a single device within a large network of other devices. An internet connection to the control room (c.f. Section 2) and the cloud, the possibility to individually update internal components, the communication with other cars, and the Ethernet-based internal network lead to the necessity of new security concepts in order to guarantee secure and safe driving. The UNICAR*agil* vehicles become accessible from the outside and therefore have to be effectively secured to exclude adversaries. The driving competency is not any longer delegated to a human driver, but to the on-board automation or to the remote control room. Especially the latter case creates an interface to a highly critical internal communication infrastructure from the outside. New attack vectors arise from the transition from an opaque and closed vehicle to a transparent architecture. In terms of security, UNICAR*agil* vehicles

are a possibly vulnerable platform that needs to be secured to eventually protect its passengers. It is suggested to replace the "security through obscurity" approach with "security by design". This means that securing the car poses a fundamental problem that has to be addressed from the beginning of the car's development and manufacturing process.

Based on a thorough threat analysis, a set of security precautions is proposed which are mainly based on modern cryptography. Instead of hiding communication, it is attempted to cryptographically secure it. First and foremost, both internal and external messages have to be authenticated, such that malicious message injection can be detected. Furthermore, the integrity of the car's control components is validated periodically (e.g. each time the vehicle starts up). This requirement results from the modular vehicular architecture, because it allows to easily replace or update modules. Modules convince themselves of both their own integrity and the integrity of other devices. A fast and secure encryption scheme protects privacy-sensible data from unauthorized access. At the same time, the passenger's privacy is taken into account by providing protection means. The goal is to adopt a cryptography-based certification system which enables to revoke internal modules or even the entire car. A revoked car cannot be longer used, because it is not considered to be trustworthy. This feature may be necessary to comply with law to allow authorities to block a car in case of misbehavior. A secure and privacy-preserving identity management allows assigning the car a unique address that is derived from its interior system properties. Finally, live precautionary measures are proposed that automatically detect intruders or attacks such as denial of services.

Security is a fundamental building block of all UNICAR*agil* vehicles. However, it is not sufficient to realize a reliable and fast security framework, but there need to be means that deal with possible security flaws. It is necessary to combine safety and security in such a way that possible infringements upon the vehicle’s security are handled by elaborated safety mechanisms. For instance, the above mentioned live precautionary measures may be used to notify the self-perception about the presence and the severity of possible security flaws. The self-perception incorporates this information into its holistic representation of the vehicle's current abilities. Subsequently, the automated driving functionality can react properly to the flaw.

Finally, the impact of the security measures on latency should be as small as possible. This is why fast security schemes are applied by exploiting hardware acceleration. As the UNICAR*agil* vehicles are highly heterogeneous systems in terms of speed and programmability, the security framework needs to cope with small and constrained devices (e.g., sensors) and powerful machinery (e.g., brainstem and cerebrum). A transparent integration of all security mechanisms takes place mainly at the edge of middleware and operating system.

Modern security concepts permit the UNICAR*agil* vehicles to become open and secure devices communicating with the surrounding world.

6.3 Verification and Validation

Wachenfeld and Winner [33] introduce the so-called approval trap, which states that a feasible verification and validation of automated vehicles requires new methods. Current methods, such as distance based, statistical verification and validation, cannot be transferred to SAE level 3 or higher automation without adaption. Simultaneously, the disruptive and modular approach of UNICAR*agil* provides additional challenges regarding the verification and validation as well as regarding the according test concepts.

Modularity and scalability are two of the key aspects in UNICAR*agil*. However, current test concepts strongly rely on vehicle and integration tests. Keeping this approach would require vehicle and integration tests for all variants that can be built with the modular design of UNICAR*agil* and thus increases the required verification and validation effort even more. If it succeeds to shift the verification and validation effort from the vehicle level to the module level, one could verify and validate the modules individually without need of vehicle and integration tests, thus each module could be replaced by another one that fulfills the same safety and security requirements. Moreover, new vehicle variants can be created with minimal verification and validation effort. Additionally, as each single module is less complex than the complete vehicle, the relevant parameter space for the verification and validation can be reduced significantly by particular testing, as deduced by Amersbach and Winner [34].

In order to develop a modular verification and validation approach, the following challenges have to be faced within the project:

- Testability has to be considered during the concept and design of the individual modules and their interfaces.
- The coverage from integration and vehicle tests has to be transferred to particular tests of the individual modules.
- Verification and validation criteria as well as test cases have to be defined on module level.
- The approach of modular verification and validation itself has to be validated.

Approving UNICAR*agil* vehicles with a distance based approach in all urban areas in Germany would require approximately 2 billion test kilometers, based on the calculation approach by Wachenfeld and Winner [33] and statistical data [35][36]. Even if the test effort can be reduced by modular verification and validation as outlined above, a huge parameter space has to be considered. One factor that leads to this huge parameter space and therefore enormous verification and validation effort is the high number of possible scenarios within the specified Operational Design Domain (ODD). Thus, narrowing down the ODD in terms of road categories can reduce the number of possible scenarios and therefore the validation effort. Categorization of road segments based on the required capabilities to drive on them could be used for a limited, stepwise approval of SAE level 3 or higher automation. To approve the UNICAR*agil* vehicles for a specific road category, only the required capabilities for this category have to be validated and the UNICAR*agil* vehicles could be approved for all

allocated road segments. Starting the approval with categories that require few capabilities, the UNICAR*agil* vehicles can be released in a limited ODD that can be expanded when new categories are approved.

To implement this approach, attributes of road segments that influence the required capabilities need to be understood and a method needs to be developed that categorizes the road network. Furthermore, the transferability of the approval of one specific segment to all segments of the same category has to be investigated.

In addition to the new verification and validation methods, as many tests as possible should be carried out in a virtual test environment in order to reduce the overall effort for verification and validation. However, valid simulation models are not available for all components and use cases yet (e.g. there exist no physical simulation models for environment perception sensors). Hence, x-in-the-loop environments and real world testing need to be included in the test concept. Therefore, a test and simulation framework will be developed within the project that includes simulated test drivers for all considered test environments and supports individual tests of single modules. The modules are simulated on the input interfaces and evaluated based on the output interfaces. To validate the simulation framework itself, at least one proving ground – that can be used as ground truth – has to be digitally cloned in order to compare virtual and real world test results.

7 Automated Driving

The disruptive and modular concept developed in UNICAR*agil* aims at fully automated and driverless vehicles. The focus of the prototypes lays on urban and suburban traffic. Within UNICAR*agil*, the automation is one example for the implementation and application of the geometric, mechatronic, and software design concepts as well as safety, security and validation methods described in the previous sections.

This section focuses on the automation tasks of environment perception and modelling, interpretation and prediction of traffic situations, behaviour decision, as well as trajectory planning for the UNICAR*agil* vehicle. The results will be realized on the cerebrum level of information processing within the mechatronic architecture (cf. Section 4). The calculated trajectories are the main interface to the brainstem level, which handles the trajectory control as described in Section 4.3. In order to support the behavior planning of all traffic participants, each vehicle’s model of the environment is shared via a cloud-based Collective Environment Model. Trajectories are evaluated and stored as experience in a cloud-based Collective Memory. Knowledge extracted from this experience is made available as a service. In addition to an automated operation, the UNICAR*agil* vehicles will comprise the possibility of being remotely controlled by a teleoperator from a control room.

7.1 Sensor Modules

The development of generic sensor modules is one example of the modular design, but also of the safety and security concepts in UNICAR*agil*. One sensor module will

comprise of LiDAR, RADAR, as well as monocular and stereo camera sensors together with a sensor data processing unit. The modular hardware and software concept of the module will allow (e.g. for low-cost variants or specific purposes) to omit one or more of the sensors. All different types of UNICAR*agil* vehicles (cf. Section 2) will include equal generic sensor modules.

The sensor module can be considered as a module from the geometric (cf. Section 3) and the mechatronic viewpoint (cf. Section 4). Additionally, due to the service-oriented software architecture, the modular design allows for a replacement with a spare module or with an updated version of the module, e.g. if new or different sensor types are available. Due to the usage of different sensor types and overlapping fields of view of the sensors, each sensor module already contains redundancy for the perception task.

Due to the agility of the vehicle provided by the dynamic modules (cf. Section 2), which allows for arbitrary driving directions, the perception has to cover 360° of the vehicle’s environment. Therefore, four sensor modules per UNICAR*agil* vehicle are used. They will be placed on the corners of the chassis/cabin. Each sensor module then covers a range of up to 270° around the respective vehicle's corner. This adds additional redundancy in perception due to the overlapping coverage of different sensor modules.

In addition to the sensors, each sensor module comprises of its own data processing unit, which firstly performs all required preprocessing of the collected raw data, e.g. disparity calculations of stereo camera images, scene labeling, object detection and classification, etc. Secondly, each sensor module already calculates an internal perception model by information fusion from the preprocessed data and tracks the detected objects. The module's environment model is the interface to the cerebrum, which performs the further tasks of automation. However, if needed for other tasks, data from earlier stages is available from the respective preprocessing steps (e.g. objects from a single sensor for assistance of teleoperation) thanks to the service-oriented software architecture.

7.2 Off-vehicle Environmental Information and Collective Memory

Through wireless information and communication technology (ICT), traffic participants are able to share data that lies beyond the natural barriers of each participants' local perception. When extended with additional aspects such as experience, knowledge and intents, this allows for a new level of cooperative and anticipative behavior of automated vehicles.

Critical situations may not only be handled better by such vehicles but they may also be avoided in the first place. Behavior can be planned in consideration of the behavior of other traffic participants. It may therefore be optimized for safe, efficient and convenient trajectories. In UNICAR*agil*, two cloud-based concepts are developed and implemented for these purposes.

Vehicles may share their individual perception and intended behavior through the Collective Environment Model. It enables traffic participants to obtain a more complete

and reliable model of the current and future state of the world. The Collective Environment Model will also process information provided by a so-called Info Bee, an unmanned aerial vehicle (UAV) or drone, which exploits both its positional advantage and less restricted agility to provide data of larger areas. The Collective Environment Model is made available to all traffic participants as a cloud service.

The second developed cloud service is the Collective Memory. Vehicles often encounter similar situations thousands of times throughout their lifetime. Experiences about these situations are usually lost. In UNICAR*agil*, these experiences are collected in the Collective Memory. Planned behavior is evaluated based on whether it led to desirable trajectories. Machine Learning and Data Mining are used to extract patterns from all experiences and evaluations. Recommendations for desirable behavior based on the respective situation and its predicted chronological development are formed and made available to all traffic participants.

7.3 Cerebrum

The cerebrum itself is a module that in hardware is a sole data processing unit. It performs all further tasks of automation up to trajectory planning, provided as software services on this hardware. In a first step, the environment models from the four sensor modules of the vehicle are combined to one single vehicle environment model. This environment model, the Collective Environment Model and the Collective Memory are the basis for the behavior and trajectory planning tasks. In contrast to conventional vehicles, the trajectory planning has more degrees of freedom or at least less restrictions due to the agility of the UNICAR*agil* vehicle enabled by the dynamic modules.

In addition to the normal trajectory, the cerebrum always provides a fallback safety trajectory which leads to the Safe Halt with pre-defined conditions (e.g. on the side of the road, but not on intersections/railway crossings). This fallback trajectory will be used by the brainstem or the spinal cord controllers in the case the cerebrum level of information processing fails completely, as described in Section 4.2.

A goal of the project is the efficient utilization of the computational power in the sensor modules and the cerebrum as well as the communication channels in between. Therefore, in UNICAR*agil,* research for the automation level will lead towards a tailored processing of data and subsequent algorithms in dependence of the driving state and the vehicle's abilities (e.g. environmental modelling adaption based on driving direction, speed, etc.). Additionally, high-level algorithms for automation like trajectory planning include data from further information sources, e.g. Info Bees. Challenges are the online adaptability of the respective algorithms as well as the handling of initialisation times if services were stopped completely and restarted on demand.

7.4 Self-perception, Verification and Validation

The adaptation of algorithms to the driving state and the vehicle's capabilities, but also the safety and security concepts (cf. Section 6) require the permanent monitoring of each component in the vehicle. In UNICAR*agil*, the automation concept includes self-

perception mechanisms on sensor level to assess the state and performance of each sensor as well as performance monitoring of the subsequent algorithms like the environment modelling and trajectory planning. Thus, the UNICAR*agil* vehicles will be able to detect degradation and the resulting changes in safety limits of the automation system and can therefore adapt its behavior accordingly with respect to the road category up to a stop of the vehicle and handover to a teleoperator in the control room (cf. Section 7.5).

The new verification and validation concepts developed in UNICAR*agil* as described in Section 6.3 will be the basis for verification and validation of the automation system of the UNICAR*agil* vehicles. On module level, these procedures will not only allow for verification and validation of the developed modules independently, but also for the ability to update software services as well as hardware modules even during the operation phase of a vehicle. The automation system will be integrated into an open framework for automated driving, which is to be developed over the course of the project. It will be based on the open-source framework ROS [37] and all interfaces the framework will be publicly available.

7.5 Control Room

The control room is a constituent component of the holistic concept of UNICAR*agil*. The main focus of adding a control room to the concept is to increase the overall reliability and operational readiness of the vehicle fleet. A positive side effect is an additional increase in safety as well.

The UNICAR*agil* control room involves the observation and manipulation of the traffic flow of automated vehicles in a specific area as well as direct control of the motion of an individual vehicle. Possible utilization scenarios for manipulation of the traffic flow are equal distribution of traffic, emergencies or large-scale standstills. A handover of the control over the vehicle to a human operator in the control room can occur in cases of a degraded environment perception, ambiguous situation interpretation or in any other situation, where a safe navigation cannot be guaranteed by the automated functions.

The vehicle and the control room are connected via the commercial mobile network. By concept, an uninterruptible network connection is not obligatory. All approaches and solutions are able to handle connection losses by maintaining vehicle safety. Nevertheless, service quality will benefit from a low latency and high bandwidth connection. To support large scale and high rating functionality, the system is designed for the 5G mobile standard.

Direct control of the vehicle motion is realized through teleoperation [38]. The handover from the automated system to the human operator takes place at vehicle standstill to avoid time critical situations. Video streams as well as additional sensor data are transmitted to the operator in the control room. Depending on the current abilities of the vehicle, the operator will submit a maneuver, a path, a trajectory or low level driving commands to the vehicle.

In case the impairment of the automated system occurs only temporarily, the operator hands back the vehicle guidance to the onboard system as soon as the automated functions of the vehicle are able to fulfill the driving task again.

8 Outlook

In this paper, the project UNICAR*agil*, the underlying research questions and first concepts are presented. Over the course of the project, each of the aforementioned concepts is implemented and the individual as well as the overall impact of the results on the convenience, efficiency and safety of future mobility are evaluated. The four vehicle prototypes will be built up at different university sites and will be presented to the public at the end of the project. The participants of the consortium are in close contact to ensure the best possible project progress. The project partners will generate scientific publications addressing the different research topics regularly.

9 Acknowledgement

This research is accomplished within the project “UNICAR*agil*” (FKZ EM2ADIS002). We acknowledge the financial support for the project by the Federal Ministry of Education and Research of Germany (BMBF).

10 References

[1] BREUER, Bert et. al., 1983
UNI-CAR – Der Forschungspersonenwagen der Hochschularbeitsgemeinschaft – Schlussbericht,
Funding Reference: TV7985, BMBF

[2] PFEIL, Felix, 2018
Megatrends und die dritte Revolution der Automobilindustrie: Eine Analyse der Transformation der automobilen Wertschöpfung auf Basis des Diamantmodells,
Research Papers on Marketing Strategy 13/2018,
ISBN 978-3-00-059102-0

[3] DONGES, Edmund, 1982.
Aspekte der Aktiven Sicherheit bei der Führung von Personenkraftwagen.
In: Automobil-Industrie 27,183–190

[4] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2011.
ISO 26262: Road vehicles – Functional safety: International Organization for Standardization.

[5] BAGSCHIK, Gerrit, NOLTE, Marcus, ERNST, Susanne and MAURER, Markus, 2018
A System's Perspective Towards an Architecture Framework for Safe Automated Vehicles
In: 2018 IEEE International Conference on Intelligent Transportation Systems (ITSC), Maui, Hawaii, USA 2018. Accepted to appear.

[6] NOLTE, Marcus, BAGSCHIK, Gerrit, JATZKOWSKI, Inga, STOLTE, Torben, RESCHKA, Andreas and MAURER, Markus, 2017.
Towards a Skill- And Ability-Based Development Process for Self-Aware Automated Road Vehicles.
In: IEEE Conference on Intelligent Transportation Systems 2017

[7] RESCHKA, Andreas and MAURER, Markus, 2015.
Conditions for a safe state of automated road vehicles.
In: it - Information Technology, 57 (4).

[8] SOCIETY OF AUTOMOTIVE ENGINEERS INTERNATIONAL, 2014
SAE J3016: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems.
http://standards.sae.org/j3016_201401/

[9] BROY, Manfred, KRÜGER, Manfred, PRETSCHNER, Alexander and SALZMANN, Christian, 2007.
Engineering Automotive Software
In: Proceedings of the IEEE
doi 10.1109/JPROC.2006.888386

[10] KÜFEN, Jörg, HUDECEK, Janek, and ECKSTEIN, Lutz, 2014.
Automotive Service Oriented System Architecture - Ein neuartiges Architekturkonzept und sein Potential für zukünftige Fahrzeugsysteme
In: Automotive meets Electronics. Dortmund, 2014.
VDE Verlag
ISBN 978-3-8007-3580-8

[11] WAGNER, Marco, ZÖBEL, Dieter, and MEROTH, Ansgar, 2011.
An adaptive Software and Systems Architecture for Driver Assistance Systems based on service orientation.
In: International Journal of Machine Learning and Computing, 2011
doi 10.7763/IJMLC.2011.V1.53

[12] FÜRST, Simon, BECHTER, Markus, 2016
AUTOSAR for connected and autonomous vehicles: The AUTOSAR adaptive platform.
In: 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop, (pp. 215-217). IEEE.
10.1109/DSN-W.2016.24

[13] MACKENZIE, C. Matthew, LASKEY, Ken, MCCABE, Francis, BROWN, Peter F, METZ, Rebekah, 2006.
Reference Model for Servivce Oriented Architecture 1.0.
OASIS Standard, page 18.

[14] STOLTE, Torben, RESCHKA, Andreas, BAGSCHIK Gerrit, and MAURER, Markus, 2015.
Towards Automated Driving: Unmanned Protective Vehicle for Highway Hard Shoulder Road Works.
In: 18th International Conference on Intelligent Transportation Systems. Las Palmas, Spain, September 2015.
Piscataway, New Jersey: IEEE, pages 672–77.
10.1109/ITSC.2015.115

[15] BAGSCHIK, Gerrit, RESCHKA, Andreas, STOLTE, Torben, and MAURER, Markus, 2016.
Identification of Potential Hazardous Events for an Unmanned Protective Vehicle.
In: IEEE Intelligent Vehicles Symposium (IV), Gothenburg, Sweden, June 2016.
Piscataway, New Jersey: IEEE, pages 691–97.
10.1109/IVS.2016.7535462

[16] BAGSCHIK, Gerrit, STOLTE, Torben, and MAURER, Markus, 2017.
Safety Analysis Based on Systems Theory Applied to an Unmanned Protective Vehicle.
In: Procedia Engineering. Vol. 179, pages 61–71.
10.1016/j.proeng.2017.03.096.

[17] STOLTE, Torben, BAGSCHIK, Gerrit, RESCHKA, Andreas
and MAURER, Markus, 2017.
Hazard Analysis and Risk Assessment for an Automated Unmanned Protective Vehicle.
In: IEEE Intelligent Vehicles Symposium (IV), Redondo Beach, CA, USA, June 2017.
Piscataway, New Jersey: IEEE, pages 1848–55.

[18] MAURER, Markus, 2018.
aFAS - Die Aufgabenstellung.
Presented at the final demonstration of the project aFAS, Frankfurt, Germany, June 20, 2018.

[19] WAYMO, 2017.
Waymo Safety Report - On the Road to Fully Self-Driving
October 2017.

[20] RESCHKA, Andreas, BAGSCHIK, Gerrit, ULBRICH, Simon, NOLTE, Marcus, and MAURER, Markus, 2015.
Ability and Skill Graphs for System Modeling, Online Monitoring, and Decision Support for Vehicle Guidance Systems.
In: IEEE Intelligent Vehicles Symposium (IV), Seoul, Korea, June 2015
Piscataway, New Jersey: IEEE, pages 933–39, 2015.
10.1109/IVS.2015.7225804.

[21] MATTHAEI, Richard, and MAURER, Markus, 2015.
Autonomous Driving – a Top-down-Approach.
In: at - Automatisierungstechnik 63, no. 3, pages 155–167.
10.1515/auto-2014-1136

[22] BERGMILLER, Peter Johannes, 2015.
Towards Functional Safety in Drive-by-Wire Vehicles.
Dissertation, TU Braunschweig, Braunschweig, Germany, 2015.

[23] RESCHKA, Andreas, 2017.
Fertigkeiten- und Fähigkeitengraphen als Grundlage des sicheren Betriebs von automatisierten Fahrzeugen im öffentlichen Straßenverkehr in städtischer Umgebung.
Dissertation, TU Braunschweig, Braunschweig, Germany, 2017.

[24] KRAUSE, Evan A., SCHERMERHORN, Paul, and SCHEUTZ, Matthias, 2012.
Crossing Boundaries: Multi-Level Introspection in a Complex Robotic Architecture for Automatic Performance Improvements.
In: Twenty-Sixth AAAI Conference on Artificial Intelligence, Toronto, Canada, July 2012.
Palo Alto, CA, USA: AAAI, pages 214-220.

[25] KIRCHNER, Dominik, and GEIHS, Kurt, 2014.
Adaptive Model-Based Monitoring for Robots.
In: Intelligent Autonomous Systems 13, pages 43–56.
10.1007/978-3-319-08338-4_4

[26] HERBRICH, Ralf, MINKA, Tom, and GRAEPEL, Thore, 2007.
TrueSkill™: a Bayesian skill rating system.
In: Advances in neural information processing systems. Vancouver, Canada, December 2007.
Cambridge, MA, USA: MIT press, pages 569–576

[27] THIELE Daniel, and ERNST Rolf, 2016.
Formal worst-case performance analysis of time-sensitive Ethernet with frame preemption.
In: 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA). September 2016.

[28] THIELE Daniel, ERNST Rolf, and DIEMER Jonas, 2015.
Formal worst-case timing analysis of Ethernet TSN's time-aware and peristaltic shapers.
In: 2015 IEEE Vehicular Networking Conference (VNC). December, 2015.

[29] SCHIRRMACHER, Dennis, 2018.
Angreifer könnten aktuelle BMW-Modelle über Mobildfunk kapern
Online [Access: 26-06-18]: https://www.heise.de/security/meldung/Angreifer-koennten-aktuelle-BMW-Modelle-ueber-Mobilfunk-kapern-4055235.html.

[30] SCHÄFFER, Florian, 2017.
Macchina M2: Hardware zum Car-Hacking auf Kickstarter
Online [Access: 26-06-18]: https://www.heise.de/make/meldung/Macchina-M2-Hardware-zum-Car-Hacking-auf-Kickstarter-3632247.html.

[31] SCHERSCHEL, Fabian, 2016.
Auto mit bösartigem Lied gekapert
Online [Access: 26-06-18]: https://www.heise.de/security/meldung/Auto-mit-boesartigem-Lied-gekapert-3087160.html .

[32] FASSAK, Samir, EL IDRISSI, Younes El Hajjaji, ZAHID, Noureddine, and JEDRA, Mohamed, 2017.
A secure protocol for session keys establishment between ECUs in the CAN bus.
In: International Conference on Wireless Networks and Mobile Communications (WINCOM), Rabat, Morocco, November 2017.
Piscataway, New Jersey: IEEE, pages 1-6.

[33] WACHENFELD, Walther and WINNER, Hermann, 2016.
The Release of Autonomous Vehicles.
In: WINNER, Hermann, MAURER, Markus, GERDES, J. Christian and LENZ, Barbara, Eds. Autonomous Driving. Technical, Legal and Social Aspects.
Berlin, Heidelberg: Springer, pages 425-449.
ISBN 978-3-662-48847-8.

[34] AMERSBACH, Christian and WINNER, Hermann, 2018.
Funktionale Dekomposition - Ein Beitrag zur Überwindung der Parameterraumexplosion bei der Validation von höher automatisiertem Fahren (als Beitrag angenommen).
In: 12. Workshop Fahrerassistenzsysteme und automatisiertes Fahren, Walting, Germany, September 2018.
Darmstadt: UNIDAS e.V.

[35] STATISTISCHES BUNDESAMT (DESTATIS), 2017.
Verkehrsunfälle Zeitreihen 2016.
Wiesbaden: Statistisches Bundesamt (Destatis).

[36] STATISTISCHES LANDESAMT BADEN-WÜRTTEMBERG, 2018.
Fahrleistungen im Straßenverkehr
Online [Access: 26-06-18]: www.statistik-bw.de/Verkehr/KFZBelastung/v5c01.jsp

[37] ROS: Robot Operating System, 2018
Online [Access: 08-07-18]: http://www.ros.org/

[38] DIERMEYER, Frank, GNATZIG, Sebastian, CHUCHOLOWSKI, Frederic, TANG, Tito and LIENKAMP, Markus, 2011.
Der Mensch als Sensor - Der Weg zum teleoperierten Fahren.
In: AAET - Automatisierungssysteme, Assistenzsysteme und eingebettete Systeme für Transportmittel, Braunschweig, pages 119-135.
ISBN 978-3-937655-25-3