32nd Electric Vehicle Symposium (EVS32)
Lyon, France, May 19-22, 2019

Project SmartLoad - Increased Reliability for Highly Automated Electric Vehicles

Dr.-Ing. Christian Schyr[1]

[1]*AVL Deutschland GmbH, Karlsruhe, Germany, christian.schyr@avl.com*

Summary

The requirements for autonomous electric vehicles are high: Safety and reliability are top priority. Even though the complexity of vehicle systems increases due to automation, the failure probability is not allowed to increase in any case. Analogous to automated airplanes, this has to be ensured through redundant and therefore cost intensive components. But how much redundancy and cost increase is truly necessary? How can potential failures and problems be detected as early as possible and mastered by the automation and control functions? The research project SmartLoad pursues these queries within the context of a new development process for highly automated electric vehicles.

Keywords: automated, control system, component, standardization, testing processes

1 Motivation and Goals

Highly automated electric vehicles (EV) have the potential to create safer, more efficient and environmentally friendly transport. This could reshape entire sectors of the economy and improve the lives of millions of people, notably those unable to drive or with limited access to mobility. However, many questions relating to safety standards, traffic rules, insurance regimes, cybersecurity and data protection are open. They must be addressed within new development, testing and homologation processes before the mass introduction of these vehicles to the market.

With this in mind, UNECE's Global Forum on Road Traffic Safety (WP.1), has adopted a non-binding legal resolution serving as a guide for the countries which are Contracting Parties to the 1949 and 1968 Conventions on Road Traffic in relation to the safe deployment of highly and fully automated vehicles in road traffic in September 2018 [1].

The resolution provides the following definitions:

- "Automated driving system" refers to a vehicle system that uses both hardware and software to exercise dynamic control of a vehicle on a sustained basis.
- "Dynamic control" refers to carrying out all the real-time operational and tactical functions required to move the vehicle. This includes controlling the vehicle's lateral and longitudinal motion, monitoring the road environment, responding to events in the road traffic environment, and planning and signalling for manoeuvres.
- "Operational design domain" (ODD) refers to the environmental, geographic, time-of-day, traffic, infrastructure, weather and other conditions under which an automated driving system is specifically designed to function.

- “Highly automated vehicle” refers to a vehicle equipped with an automated driving system. This automated driving system operates within a specific operational design domain for some or all of the journey, without the need for human intervention as a fall-back to ensure road safety.
- “Fully automated vehicle” refers to a vehicle equipped with an automated driving system. This automated driving system operates without any operational design domain limitations for some or all of the journey, without the need for human intervention as a fall-back to ensure road safety.

The following recommendations in the resolution are now most relevant for the development process of highly automated electric vehicles:

- Monitor and safely interact with the surrounding traffic environment.
- Only operate within their operational design domain.
- Clearly and effectively provide appropriate notice, if the vehicle leaves its ODD.
- Be capable of achieving a state that maximizes road safety when a given trip cannot or should not be completed. For example, in case of a failure in the automated driving system or other vehicle system.
- React to unforeseen situations in a way that minimizes danger to the vehicle’s users and other road users.

In order to cope with this resolution and the upcoming legislation, a new development process for highly and fully automated electric vehicles has to be introduced. The main reason is that all functions for automated vehicle guidance will define and induce the loads onto the highly integrated electric and electronic components. The requirements on the verification of safety and reliability will rise significantly for single components but also for the complete vehicle, interacting with its environment or an external operator.

For verification of system reliability those manifold and in its complexity new interactions have to be considered to a much larger extent as in conventional vehicles. The required high reliability has to be ensured also after any update of hardware components or software functions during the lifetime of the automated electric vehicle as shown in Figure 1. In such future vehicle concepts, however, these loads are mainly determined by the highly automated functions of the integrated longitudinal and transverse guidance during driving. In doing so, the probability of default must decrease analogously to aircraft, e.g. through the use of redundant and thus cost-intensive electrical and electronic subsystems. When using the established development methods, the number of test scenarios will increase and thus the necessary test effort in the real world driving tests will increase enormously.

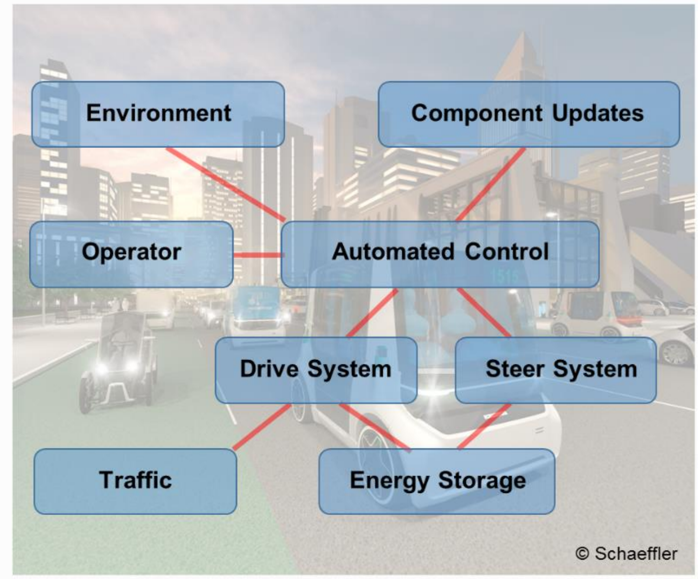

Figure 1: Influencing factors for reliable highly automated EV

From this facts the following goals of the research project SmartLoad have been derived:

- Research into a robust software and system architecture to ensure the reliability of control functions for automated and highly stressed electric components during vehicle operations.
- New concepts for a functional safe design by optimal and cost efficient usage of redundant components and functions, with simultaneous intelligent onboard condition monitoring and prediction.
- New modular and standardizable development methodology to prove the influence of interactions between control applications and damage mechanisms onto the reliability of the vehicle and its components in highly automated operations.
- Demonstration of the new methods and processes with a highly automated prototype vehicle and with several industrial use-cases and reference applications.

The project SmartLoad is executed with an iterative and agile approach in two phases with associated milestones for project control. Achievement of the project goals will be demonstrated in the first phase by a demonstrator (figure 2) and in the second phase by industrial reference applications (figure 3). Through appropriate review processes, in cooperation with the associated partners from the areas of interurban individual mobility, commercial vehicles and public transport, a user-friendly assessment of project progress and the feasibility of the developed technical solutions is ensured.

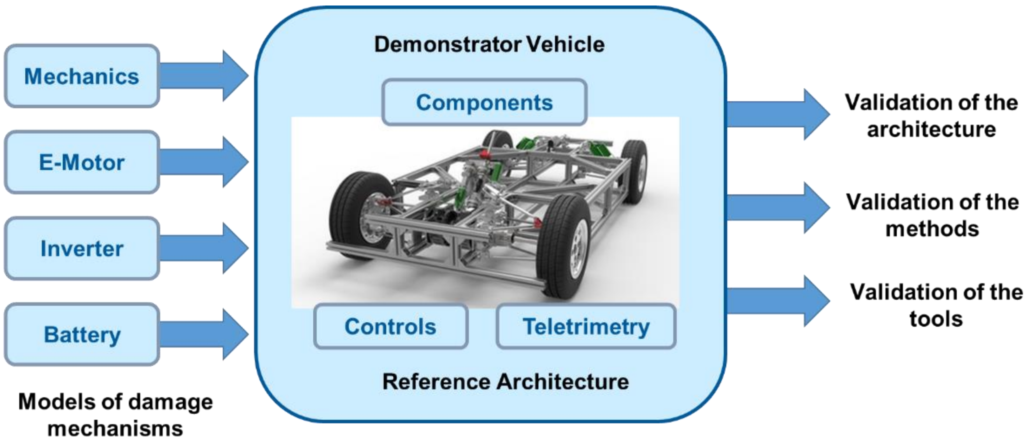

Figure 2: Demonstration in the first project phase

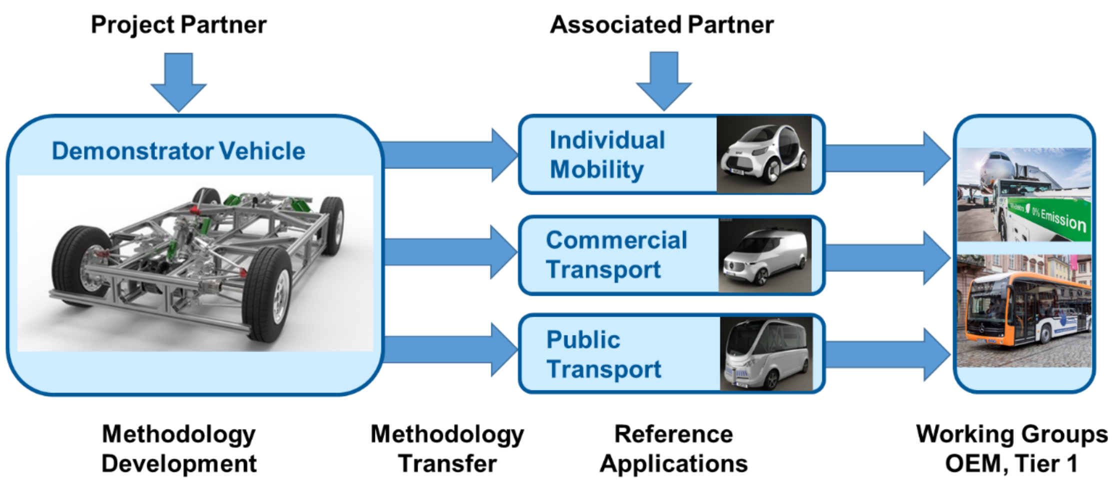

Figure 3: Application in the second project phase

2 Reference Architecture

In Project SmartLoad a reference architecture is developed, which ensures an efficient and safe "fail-operational" design for example by integration of de-rating and condition monitoring and prediction functions. The architecture is based on the robust and reliable sensor and perception platform developed in project RobustSENSE [2].

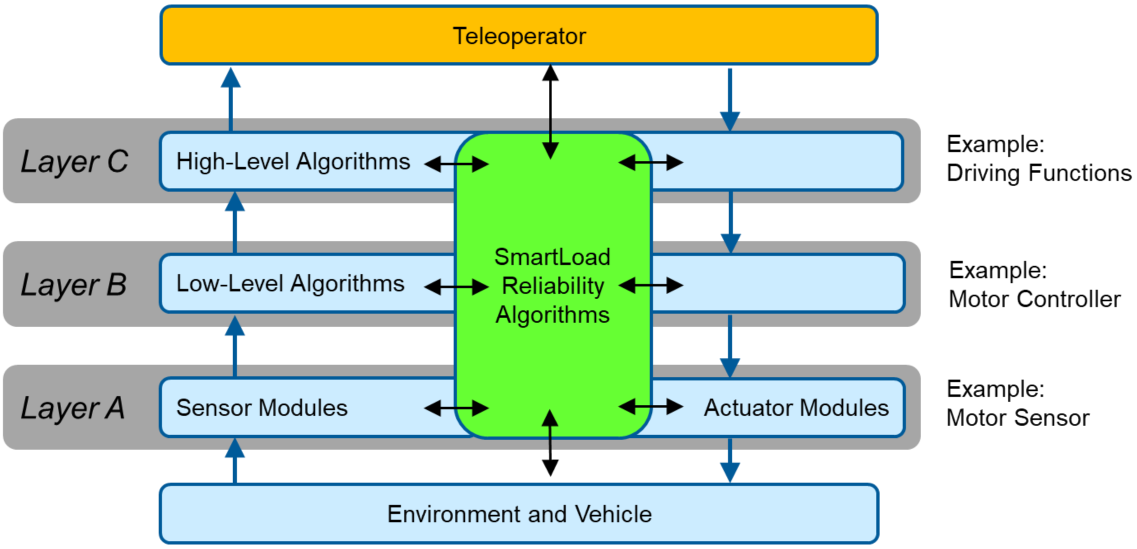

Figure 4: Reference architecture for reliable highly automated EV

The system architecture for highly automated driving functions can be roughly divided into sensors for detecting the environment, software components for their processing and actuators for executing the driving decisions as shown in Figure 4. Unlike mechanical systems, the software architecture of such a system is not subject to material fatigue and wear. Sources of error therefore arise for the software architecture from avoidable errors in the development process of the the individual processing components and the failure and degradation of sensors and actuators at run time. The following categories of failure causes of automated driving systems are identified in [3]. This classification correlates with layers A to C of the SmartLoad reference architecture:

- Component errors and hardware deficits.
- Deficits in the detection of road, traffic and environmental conditions.
- Deficits of the control algorithms (in complex and difficult situations).
- Behavioral accidents (adequate behavior and compliance to rules and regulations).
- Faulty operator - vehicle interaction (confusion of operating modes and wrong commands).

Component errors and hardware deficits primarily affect the sensors and actuator components of the vehicle. Control computers and infrastructure hardware (network components, energy storage components) are also included in this category.

The realization of a reliable highly automated driving function thus requires an efficient combination of redundancy on hardware, software and functional level as well as degradation potentials of the individual components. As long as the component is able to maintain its own functionality despite degraded quality of service of a dependent component, it propagates the effects on its own quality of service to dependent components. If the quality falls below a required minimum, the necessity of functionality is the decisive criterion. If the function is safety-critical, the component failure must be compensated by a replacement mechanism. This replacement mechanism realizes a redundant design of the functionality by adapting the system configuration.

3 Functional Safe Design

The planned approach in the SmartLoad project is the close and efficient integration of methods from Systems Engineering, Functional Safety according to ISO 26261 and the new SOTIF (Safety Of The Intended Functionality) standard, applied to highly automated driving functions.

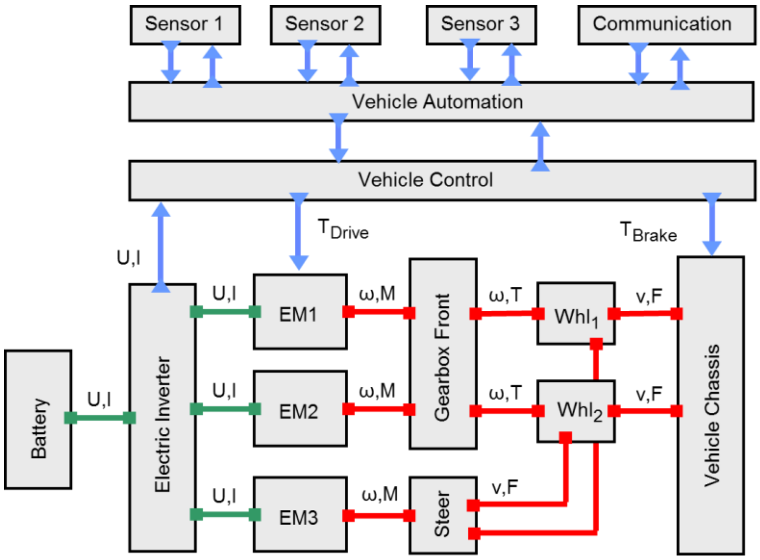

Figure 5: High-level system boundaries for an automated EV

The basis for any efficient and agile development process is the systematic definition of the system boundaries of the highly automated vehicle, its subsystems and the environment in operational use. For this the method of the "Contact and Channel Model" is applied [4]. The element model combines the concrete design-oriented level of description of technical systems with the associated abstract function-oriented level. Working Surface Pairs (WSP) and Channel and Support Structures (CSS) are the basic elements of the model and define the interface between the two levels of description.

WSP are two arbitrarily shaped generalized surfaces of a technical system, which are in contact, either wholly or temporarily, between which energy, matter and information are transmitted. The CSS connects exactly two pairs of working surfaces in space and directs energy, matter and information from one WSP to another. CSS can be partial volumes of solids, liquids, gases and fields. However, CSS can also save these items and forward them later to one of the two WFPs. Figure 5 shows the system analysis of a highly automated electric vehicle with a steered and driven axle as an example for the application of the “Contact and Channel Model”.

Based on the analysis of the system boundaries, a Failure Mode and Effects Analysis (FMEA) with subsequent hazard and risk analysis is performed, as shown in the example for the steering motor EM3:

System Component / Function	Potential Cause of Failure				Actual State					Hazard and Risk Analysis			
	Type of Failure	Consequences	Reasons	Harmful operating conditions	Detection actions	Occurance	Severity	Detection	RPZ	Severity -S-	Exposure -E-	Controllability -C-	ASIL
EM3 / Steering motor torque inverter	Solder connection to transistor defective	Steering Torque = 0 Nm	Thermal aging of the solder joint	Large temperature strokes	Temperature cycling test	4	10	5	200	S3	E2	C3	B

The failure of the power electronics of the steering motor due to thermal aging of the solder joint should be predicted safely. As a measure, a temperature monitoring of the power electronics is possible. For this purpose, a temperature sensor for the correct detection of the thermal condition is applied to the "hot spot" of the power electronics and a precise damage and lifetime model for predicting of the degradation as well as end of life is formulated, calibrated and integrated into the vehicle architecture. This will reduce the rating in the hazard and risk analysis to a lower ASIL level.

The operational design domain of an highly automated electric vehicle can be divided into the following four fields: Safe – Known, Safe – Unknown, Unsafe – Known, Unsafe – Unknown. Today's development methods in the automotive environment are concerned with the known area and have the goal of minimizing the unsafe area. With the new SOTIF standard evolutionary consideration and minimization of the unknown range is added. e.g. are also the system not known restrictions in the environmental detection of the sensors as potential error cases considered (figure 6 left).

If such systems are operational in the field, the environment of highly automated vehicles continues to develop rapidly. Influences such as urban planning, new means of transport, new technologies etc. provide for new Unsafe and / or Unknown situations. A wider variation of the applications of such vehicles will also result in a shift of the areas (figure 6 center).

By combining the methods of Systems Engineering, Functional Safety and SOTIF, as well as their implementation in an agile method, it shall be possible to react quickly to unknown or non-design developments of the environment. The consideration of events in the field with fast and efficient functional updates of the hard- and software should minimize the size of the critical areas of unsafe - known and unsafe – unknown (figure 6 right).

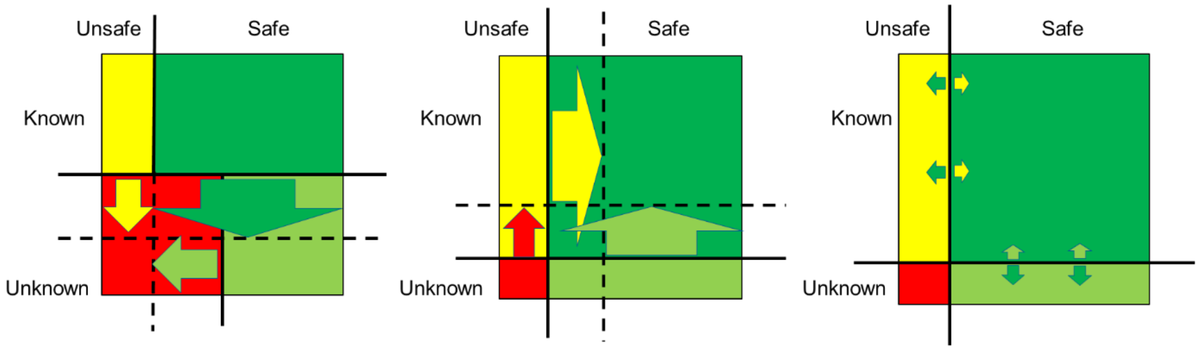

Figure 6: Application of the SOTIF standard for highly automated EV

4 Development Methodology

In conventional vehicles with a low level of automation, established design methods are applied, which are typically based on comprehensive measurement series in field operation or by accompanying numerical simulations. From this data the relevant time-based driving or operating profiles are determined and load collectives are derived. With knowledge of the relevant damage mechanisms the loads on component level are calculated and test plans are created [5]. With this input the required reliability is proven on component test beds for example on e-motor, inverter or battery test beds. Afterwards extensive durability tests on vehicle level ensure that all interactions relevant to damage have been considered and the vehicle is released to production.

In future highly automated electric vehicles the following facts are relevant for product design and validation:

- Increase of overall vehicle power and component power density in short development cycles.
- Highly dynamic and cross-domain functions for vehicle guidance and control.
- Expanded range of applications and changes of operating conditions during the lifetime.
- Adaptive learning or software updates of damage relevant functions during operation.

Therefore the immediate application of results from vehicle measurements to determine the required reliability on component and system level is not possible anymore. The new development process proposed in project SmartLoad takes now those facts into account as shown in Figure 7.

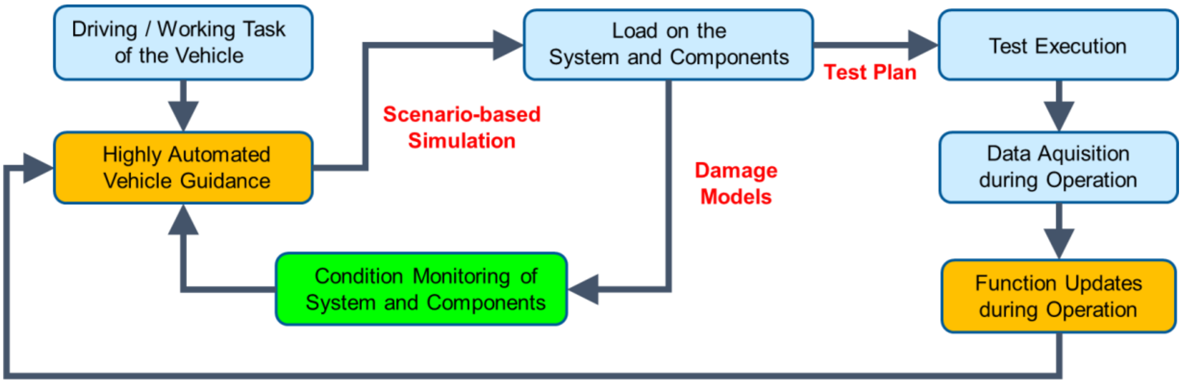

Figure 7: Development process for reliable highly automated EV

The core elements of the proposed development process in project SmartLoad centered around the scenario-based simulation of the driving respectively working task of the automated EV in its operational environment [6], [7]. This will produce a detailed data basis to implement advanced onboard calculation of damage models for a reliable condition monitoring of the system and its components while the vehicle is in highly automated operation. A comprehensive and efficient onboard data acquisition with reliable and secure functions updates will be available during operation. For verification and validation of the overall system during development and also during operation an efficient test execution is performed on connected component test beds [8], [9] and on vehicle test beds including sensor and environment simulation [10] as shown in Figure 8. For this purpose a real-time internet connection between the test beds of the partners will be established to run scenario-based tests with distributed components, for example the steering motor a test bed in Karlsruhe, the drive inverter in Wangen and the drive motor in Stuttgart.

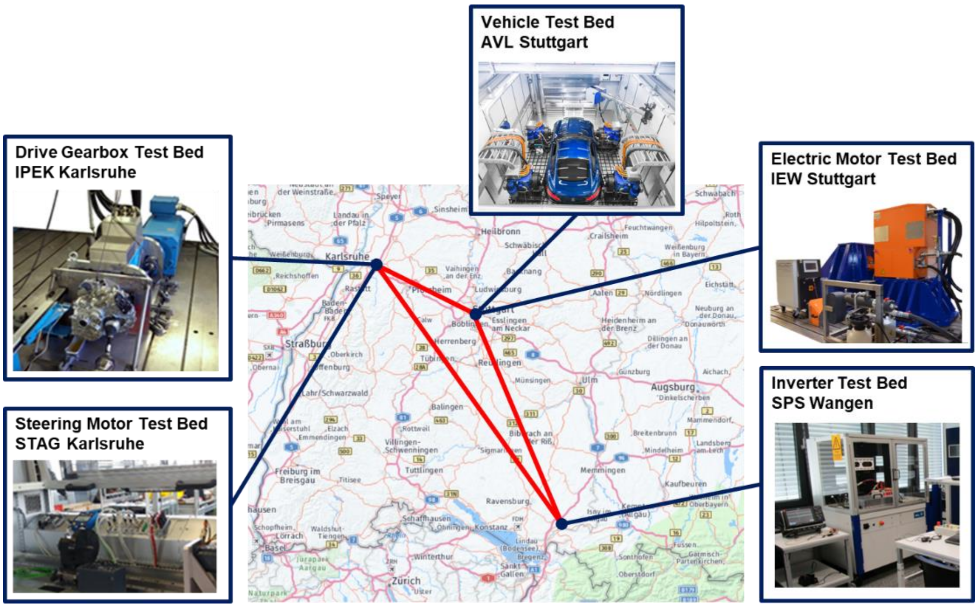

Figure 8: Test execution on connected test beds of the partners in project SmartLoad

The development process will be based on standardized test procedures to increase synergy effects and interoperability. In the project it is examined whether the required scenario-based tests can be specified precisely enough in the standards OpenDRIVE, OpenCRG, OpenSCENARIO, as well as OTX (Open Testsequence eXchange).

The aim is to standardize the test cases in such a way that they can be used in a combination of test drives, test bench tests and simulations across different platforms and thus they could be used as single source across the different simulation tool and test bed suppliers on the market.

5 Demonstration

The reference architecture and the application of the proposed development process are demonstrated on a prototype vehicle in the first phase of project as shown in Figure 9. The modules are provided from the research partners within the defined SmartLoad reference architecture.

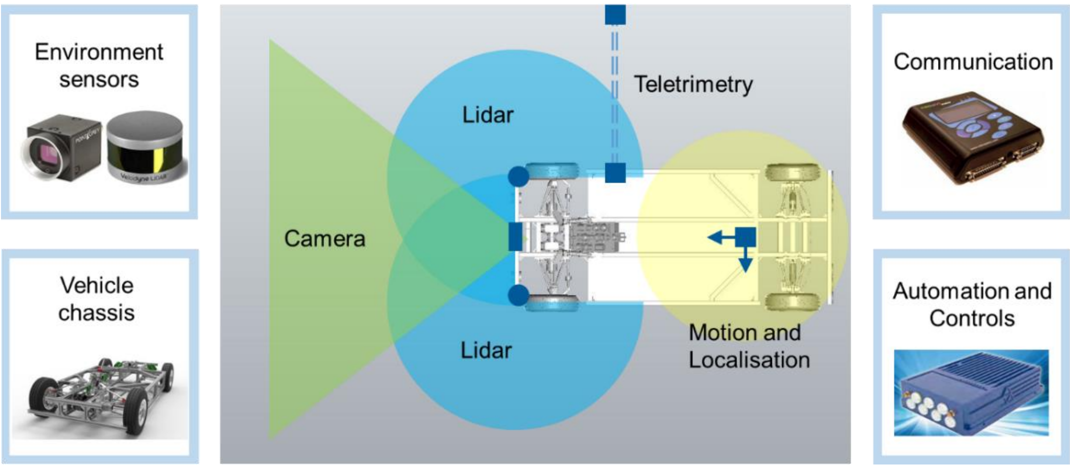

Figure 9: Demonstrator vehicle in project SmartLoad

The demonstrator vehicle in scale 1:1.5 with Ackermann steering and wheel-selective electric drives on the steered axle can be driven at a speed of max. 30 km/h and has a turning radius of about 10 m. The vehicle will be able to operate autonomously with its environment, motion and localization sensors and is included in the network of connected test benches. A connection to a remote control room is to be made possible via a communication interface for teletrimetry. This is an advanced telematics system for the asynchronous and synchronous transmission of data of various data formats with high data rates and an integrated MCD functionality (measurement, calibration and diagnostics) with read and write access to all automation and control components in the vehicle. The individual modules of the demonstrator system are explained in more detail below.

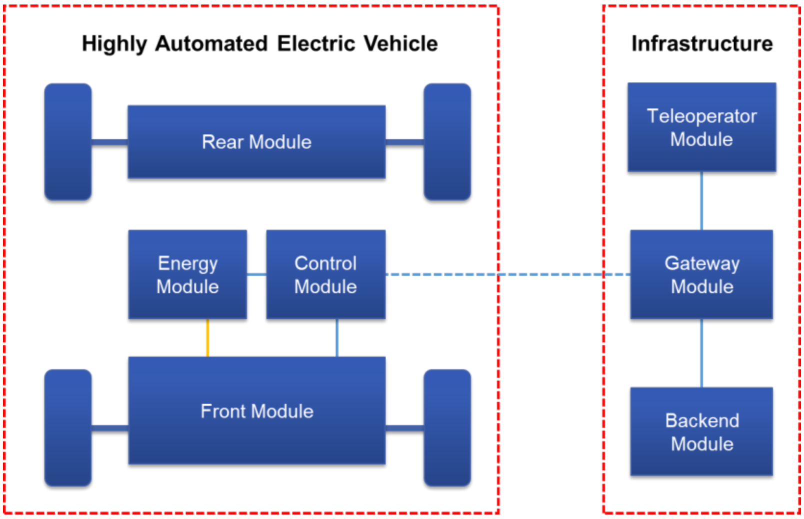

Figure 10: Layout of the overall demonstrator system

As can be seen in Figure 10, the vehicle has a data connection via mobile radio to a gateway module. The so-called backend module communicates with a gateway module via the Internet and allows access to the modules in the vehicle. The backend module is connected to a teleoperator module, which provides the user interfaces for intervention of human personal during development and operation.

The vehicle consists of the front and rear modules, the energy module and the control module. The rear module is designed as a non-driven axle in the planned design. The structure of the front module is shown in Figure 11 as described in [13].

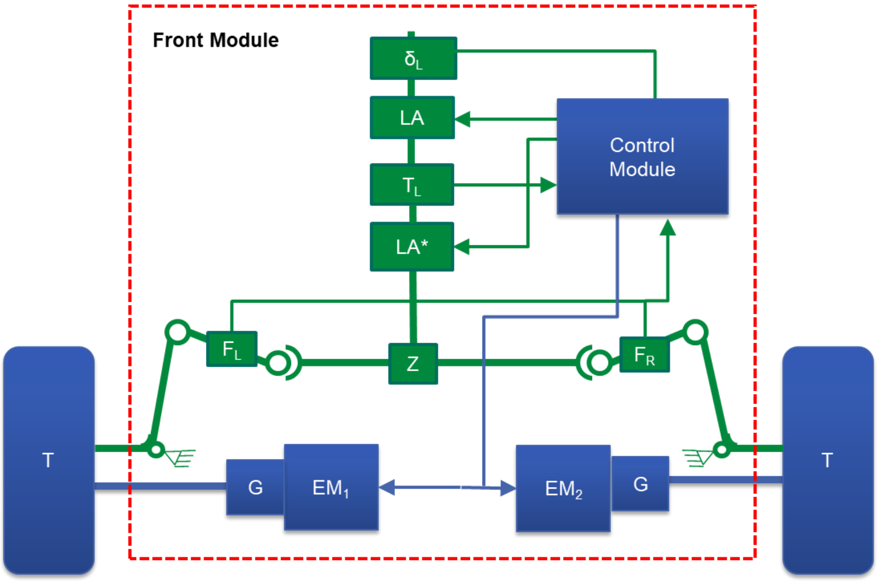

Figure 11: Front module in the demonstrator vehicle

The two wheels of the steered axle are individually driven by electric motors ($EM_{1/2}$). The steering system consists of a steering column, a steering gear (Z) with rack and the tie rods (including force sensors $F_{L,R}$). To control the steering angle two steering actuators available, which are placed on the steering column. The first steering actuator (LA) contains the angle sensor of the steering column (δ_L). The torque sensor (T_L) is installed on the steering column between the steering actuator (LA) and the redundant steering actuator (LA*). As mechanical components the steering gear (Z), traction gearbox (G) and the half-shafts to the tires (T) are integrated.

The control module takes over the function for managing the redundancies of the front module. If a failure of a sensor or actuator is detected, the module implements the vehicle movement by means of an alternative redundant function. Likewise, any sensor degradation or actuator restriction is communicated to the control module, so that the trajectory planning can be carried out depending on the currently functioning sub-systems.

The project defines three use cases (UC) for the demonstrator system. From the use cases, exemplary test scenarios are implemented and examined. All use cases are based on the same autonomous electric vehicle platform. This includes a use case for passenger transport, another for the transport of small goods like parcels and one for large and heavy loads to be transported in a trailer.

The characteristic parameters of the demonstrator vehicle in the different use cases are compared in the following table.

Use-Case	Velocity	Acceleration	Torque	Steer Angle	Payload
UC1 - People Transport	high	medium	medium	low	low
UC2 - Parcel Transport	medium	high	medium	medium	medium
UC3 - Trailer Transport	low	low	high	high	high

The use cases are mainly used to study the influence and interaction of the control and automation functions onto the reliability and lifetime of the mechanical and electrical components. For example the demonstrator is operated as a People Transport in Use Case 1. It is in a driving scenario at medium speed (50 km/h) downhill on a wet and curvy road. During this autonomous vehicle operation due to thermal aging of the solder joint of a transistor a fault in the power electronics of the steering actuator occurs. The controller automatically detects the faulty mode of operation and switches off the steering actuator due to a lack of alternative operating mode. The vehicle can no longer be steered via the steering actuator. The damage incurred has no negative feedback on the other vehicle systems, so they are fully operational. Depending on the system configuration a redundant steering actuator or the wheel-individual drive system takes over the steering function to safely complete the driving scenario at reduced speed. At the same time the teleoperator is informed about the situation over the gateway module and can prepare the necessary steps to update the faulty component at the next maintenance stop.

6 Application

In the second project phase the results from the demonstrator system are taken over to reference applications from the areas of interurban individual mobility, commercial vehicles and public transport. Working groups with vehicle manufacturers and their supplier will ensure the dissemination of the project results into future vehicle development programs. Thus, the presented project will contribute to the validation of new products and processes and the value chain of future electric vehicles in Europe.

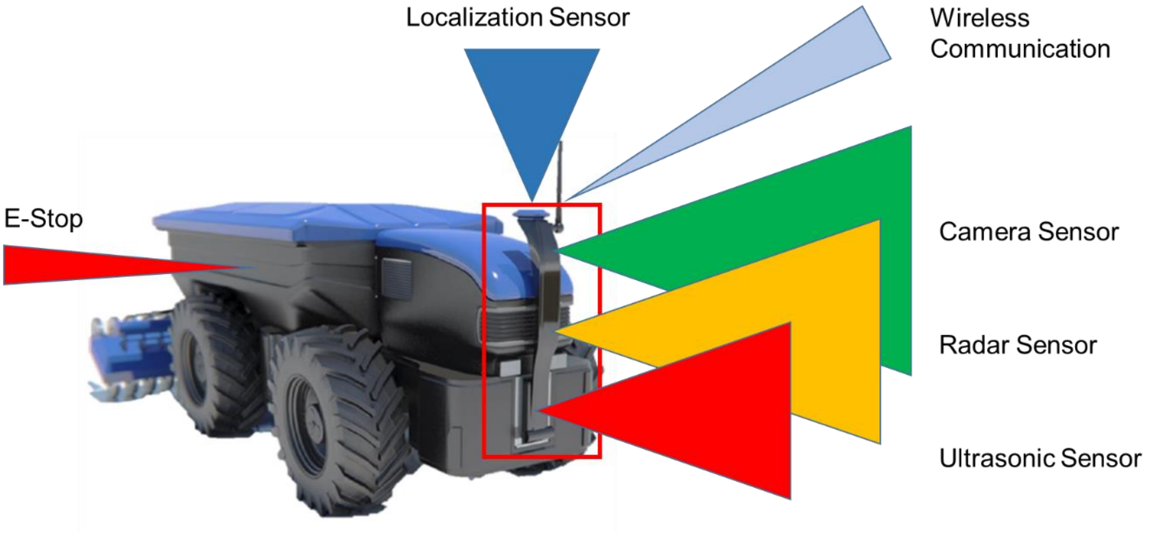

Figure 12: Reference application “Automated E-Tractor” from AVL

A strong focus in the reference applications is given to identify critical driving scenarios in urban environments. This serves as a basis to apply a simulation based validation methodology for development and even homologation of the given highly automated EV within a teleoperated system. Such critical scenarios as shown in figure 13 are for example a “People Mover” as public shuttle between parking garage and hotel or an “Automated E-Tractor” as municipal maintenance vehicle for road cleaning and repair.

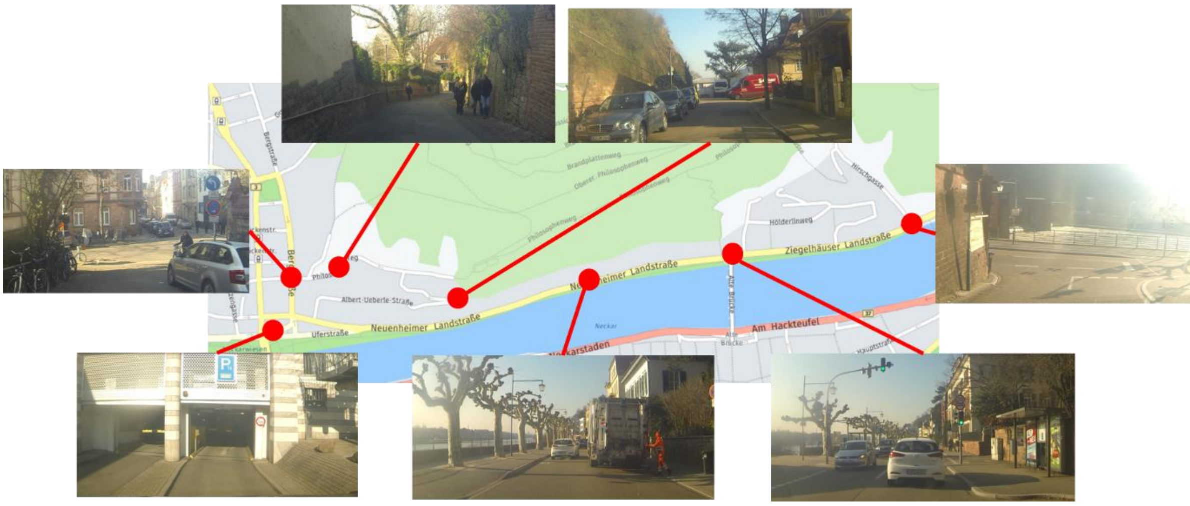

Figure 13: Scenario-based validation of highly automated EV in urban environments

A future test catalog for highly automated EVs in urban environments will be composed for example with the following critical situations:

- Automated parking and charging of the EV in public garages or private depots.
- Exit from a depot or garage to a busy road while giving right of way.
- Reliable operation on steep hills.
- Safe driving through pedestrian areas or through school areas.
- Safe stops when encountering pedestrian crossing
- Evasive maneuvering when encountering slow traffic or pedestrians on the driving lane
- Safe driving through roads with multi-modal traffic lanes for bikes, cars, truck, bus and electric tram.
- Handling of complex intersections with operational and defect traffic lights.
- Safe driving in adverse weather situations like heavy rain, storm or snow.

7 Summary

The SmartLoad project contributes to the upcoming industrial usage of highly automated electric vehicles by demonstrating new development methods and tools for different levels of automation and vehicle types in the selected reference applications. This proves the possible reduction in complexity, number of components, weight and cost while increasing the level of reliability.

The key to this lies in resolving the trade-off between highest reliability and costly physical redundancy through the use of new system architectures, new development methods and testing tools for highly automated electric vehicles.

Acknowledgments

Federal Ministry of Education and Research

The inital project idea has been developed by e-mobil BW, the state agency for new mobility solutions and automotive Baden-Württemberg. The presented work is done cooperatively by the partners of the SmartLoad consortium, receiving funding from the German Ministry for Education and Research under the Elektronom program:

- AVL Deutschland GmbH
- FZI Research Center for Information Technology
- KIT Karlsruhe Institute of Technology:
  Institute of Product Engineering, Institute of Vehicle System Technology
- RA Consulting GmbH
- Schaeffler Technologies AG & Co. KG
- SET Power Systems GmbH
- University of Stuttgart: Institute of Electrical Energy Conversion

References

[1] *UNECE Global Forum on Road Traffic Safety*, www.unece.org/trans/roadsafe/wp1rep.html, accessed on 2019-03-15

[2] *Robust and reliable platform for automated driving,* www.robustsense.eu, accessed on 2019-03-15

[3] H.-P. Schöner, *Simulation in development and testing of autonomous vehicles*. 18. Internationales Stuttgarter Symposium. Springer Vieweg, Wiesbaden 2018

[4] A. Albers, C. Schyr, *Modellbasierte Produktvalidierung mittels Integration von funktionalen und physikalischen Beschreibungen*. Tagungsband 4. Paderborner Workshop Entwurf mechatronischer Systeme, Paderborn 2006 (HNI-Verlagsschriftenreihe Band 189)

[5] H. Hick, K. Denkmayr, *The Load Matrix — a method for optimising powertrain durability and reliability test programmes.* Probabilistic Safety Assessment and Management. Springer, London

[6] H. Abdellatif et.Al., *Facing the Challenges of Development and Homologation of Autonomous Driving Using Virtual Approaches*. NVIDIA GPU Technology Conference, Munich 2018

[7] *European Initiative to Enable Validation for Highly Automated Safe and Secure Systems,* www.enable-s3.eu, accessed on 2019-03-15

[8] A. Albers et. Al., *XiL-BW-e – Laboratory Network Baden-Württemberg for Electric Mobility*, EVS30 Symposium, Stuttgart 2017

[9] D. Nickel et. Al., *Innovative Testing Process for Electric Powertrains*, EVS30 Symposium, Stuttgart 2017

[10] C. Schyr, A. Brissard, *DrivingCube - A novel concept for validation of powertrain and steering systems with automated driving*. 13th International Symposium on Advanced Vehicle Control, Munich 2016

[11] P. Kautzmann et. Al., *A Novel Chassis Concept For Power Steering Systems Driven By Wheel Individual Torque At The Front Axle*. 25th Aachener Kolloquium, Aachen 2016

Author

Christian Schyr studied mechanical engineering at Vienna University of Technology and aerospace engineering at the University of Texas at Austin. He received a Ph.D. from Karlsruhe Institute of Technology.

Currently he is project manager at AVL Deutschland GmbH in Karlsruhe and works in research projects to develop new testing methods and tools for autonomous and electric vehicles in the automotive and maritime domain. From October 2018 he coordinates the research project SmartLoad.