BMW GROUP

SAFETY ASSESSMENT REPORT

SAE LEVEL 3 AUTOMATED DRIVING SYSTEM

Content

Executive Summary 3

A. Introduction to BMW’s SAE Level 3 Automated Driving System 4

1. Human Machine Interface (HMI) 8

2. Object and Event Detection and Response (OEDR) 17

3. Operational Design Domain (ODD) 21

4.Federal, State, and Local Laws and Regulations 23

5. Fallback (Minimal Risk Condition) 25

6. Crashworthiness 28

7. Post-Crash Behavior 33

8. Data Recording and Sharing 35

9. System Safety 39

10. Cybersecurity 45

11. Verification and Validation (V&V) 54

12. Consumer Education and Training 61

Appendix A: List of Abbreviations 66

Executive Summary

The BMW Group is committed to providing a thrilling driving experience for our customers while simultaneously ensuring a safe mobility ecosystem for all road users. Automated driving is the next evolutionary step in mobility that offers drivers the option of handing over some of the less thrilling parts of driving, such as a long commute, to the automated driving system.

In 2018, the BMW Vision iNEXT concept vehicle was debuted at the Los Angeles International Auto Show. BMW's first series vehicle featuring conditional automation – in other words, the first series BMW vehicle that can drive itself without a human driver constantly monitoring the driving task within the design limits – will be based on this iNEXT concept vehicle. The BMW Group believes that drivers should have the choice of driving themselves or of being driven. For this reason, the BMW iNEXT will feature two modes: Boost Mode and Ease Mode. In Boost Mode, the driver can retain the traditional controls and drive the iNEXT in a traditional manner. In Ease Mode, the driver can activate the automated driving system and take their eyes off of the road to focus on other activities.

This type of automation, known as conditional driving automation, represents the first level of automation in which the automated driving system is capable of performing the complete dynamic driving task within a specific set of conditions; however, the driver has to be ready to take back control when the system reaches the design limits. These design limits are collectively referred to as the Operational Design Domain (ODD) and represent the boundaries, both physical and of performance, in which the automated driving system is designed to operate. The design limits of the automated driving system (hereafter referred to as SAE Level 3 BMW ADS) as implemented in the iNEXT include: availability of the feature only on limited access highways up to a maximum speed of 85mph (or up to the permitted speed limit), only when weather and environmental conditions allow the vehicle's sensors to operate without impairment, and the like. The ODD is further detailed in the ODD chapter (Chapter 3).

This Safety Assessment Report will detail in 12 chapters each of the safety aspects of automated driving highlighted in the US Department of Transportation's 2016 Federal Automated Vehicle Policy and its subsequent revisions. *Human Machine Interface* (Chapter 1) explains how the driver interface of the SAE Level 3 BMW ADS is designed to provide intuitive and safe operation. *Object and Event Detection and Response* (Chapter 2) will detail how the system is able to monitor and react to its environment. *Operational Design Domain* (Chapter 3), as mentioned above, will discuss the design limits of the system. *Federal, State, and Local Laws* (Chapter 4) will discuss how the system incorporates the 'rules of the road'. *Fallback* (Chapter 5) will explain in which situations and how the system hands back control of the dynamic driving task to the driver when the system reaches its design limits or how it brings the vehicle to a safe standstill. *Crashworthiness* (Chapter 6) and *Post-Crash Behavior* (Chapter 7) will detail the safety of the vehicle during and immediately after a crash. *Data Recording and Sharing* (Chapter 8) will discuss what information is collected by the system and how that information is used. *System Safety* (Chapter 9) will detail how the vehicle has been designed holistically to ensure safety even in the event of system failures. *Cybersecurity* (Chapter 10) will show how the system has been designed to avoid manipulation that may affect safety. *Verification & Validation* (Chapter 11) will discuss the design process and how the system is confirmed to have met its design targets. And lastly, *Consumer Education and Training* (Chapter 12) will explain how BMW will educate its sales force, its customers and the public regarding its system.

Collectively, each chapter of this Safety Assessment Report will provide a detailed overview of how BMW ensures safety for all road users. We are looking forward to the future of automated mobility and invite you to come along for the ride.

A. Introduction to BMW's SAE Level 3 Automated Driving System

Automated vehicles present a major step forward in technology, with the potential to shape the future of mobility. The main drivers for higher levels of automation are:

- Safety: reducing crashes caused by human error.
- Efficiency and environment: increasing transportation system efficiency and reducing time in congested traffic through new urban mobility solutions.
- Comfort: reducing the cognitive burden on the driver.
- Social inclusion: increasing access for elderly and disabled users.

The topics of driver assistance and automated driving play a pivotal role in the BMW Group's strategy for the future. Building on the BMW Group's experience in developing advanced driver assistance systems (ADAS) with SAE Level 1 and 2 systems over the last few years, we are taking an evolutionary approach towards more advanced levels of automated driving systems (ADS): The BMW iNEXT will be the first model from the BMW Group to offer an SAE Level 3 (conditional driving automation) ADS as optional equipment.

Development of automated vehicle technology is largely carried out at the BMW Group Autonomous Driving Campus in Unterschleißheim near Munich, Germany, which opened in April 2018.

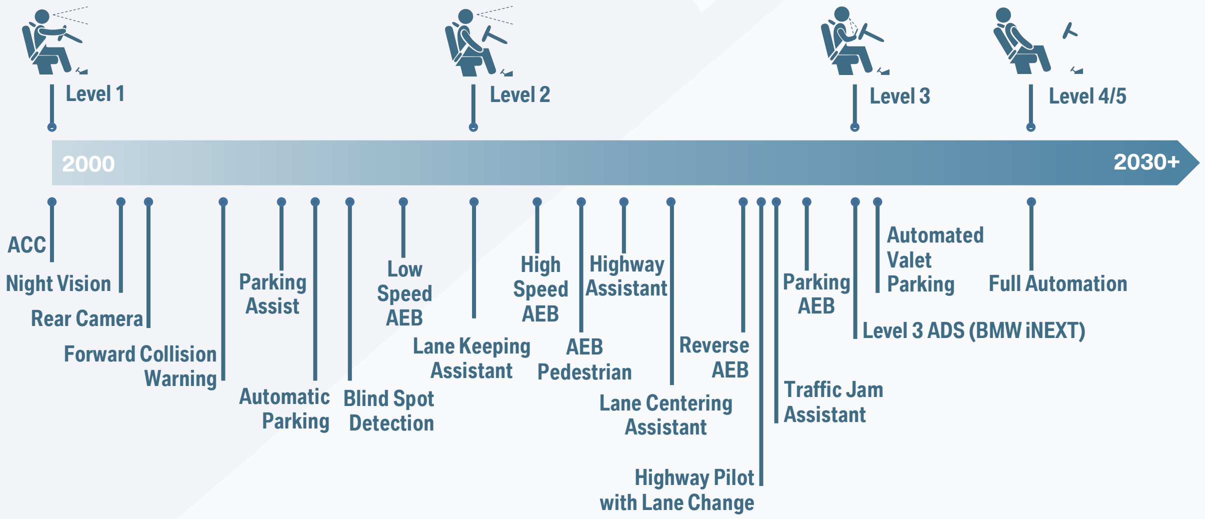


Figure 1. Development of ADAS and ADS at the BMW Group.

The Vision: BMW Vision iNEXT

The BMW Vision iNEXT provides insight into the future of personal mobility. One of the latest Vision Vehicles from the BMW Group, the iNEXT symbolizes the dawn of a new era in driving pleasure, and celebrated its world premiere at the Los Angeles Auto Show in 2018.

The BMW Vision iNEXT combines ground-breaking design with the future areas of activity defined in the company's Strategy NUMBER ONE > NEXT— Autonomous driving, Connectivity, Electrification, and Services (collectively referred to as "ACES") — and answers the question: "What will cars look like when they no longer have to be driven by a person, but still can be?"

Mobility is an intrinsic part of our lives and our experiences. It is, in short, a basic human necessity. Consequently, deliberations about the future of mobility revolve more than ever around people, our emotions and our mobility needs and preferences. The possibilities offered by autonomous driving, electrification and ever-greater connectivity will in the future open the door to completely new experiences and ways of taking a journey by car. At the same time, they also promise to change our desires and lifestyle habits.

BMW Vision iNEXT drivers can choose to either drive themselves (in “Boost” mode) or be driven (in “Ease” mode). “Boost” mode uses the electric drive system to deliver a highly dynamic and virtually silent driving experience with zero emissions. In “Ease” mode, the vehicle offers the driver and passengers a space in which to engage in a wide range of activities.

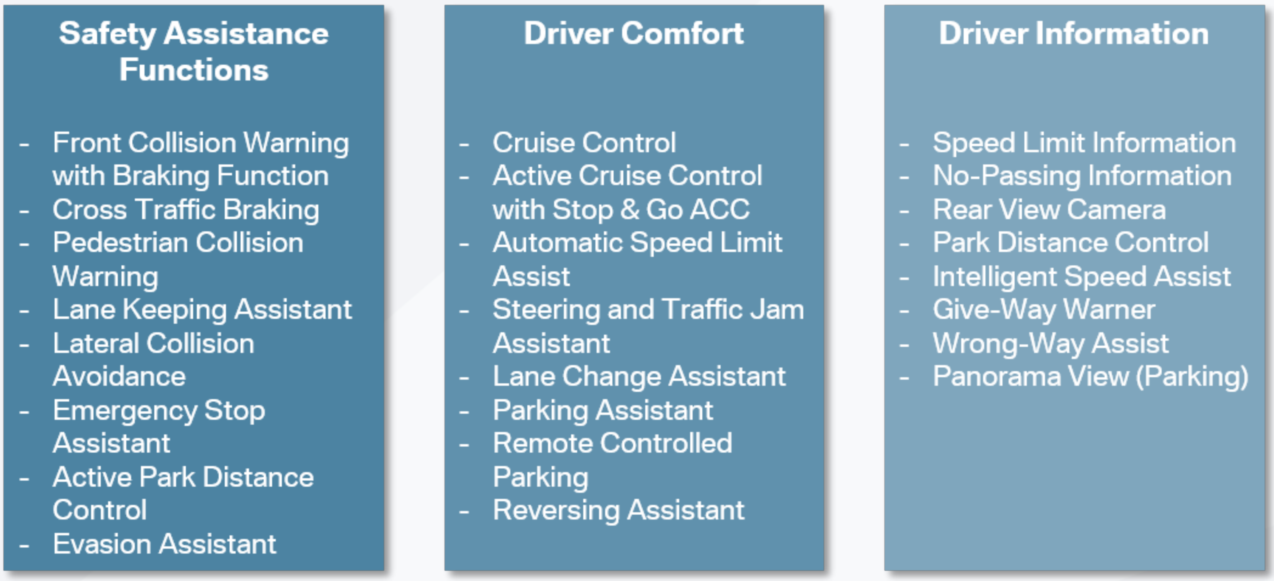
In the future, smart technologies will help people in increasingly subtle and unobtrusive ways. In the BMW Vision iNEXT, these technologies stay in the background and out of sight—hence the name “Shy Tech”—and are only deployed when needed or at the driver’s or passengers’ request.

The Series-Production Vehicle: BMW iNEXT

The series-production model based on the BMW Vision iNEXT – the brand’s new technology flagship – will enter production in the next years.

The BMW iNEXT production model will roll off the assembly line at Plant Dingolfing in Germany. With the launch of the all-electric BMW iNEXT, the BMW Group will take the next step in the development and commercialization of Automated Driving (AD).

The vehicle will offer a number of Advanced Driver Assistance Systems (ADAS, see Figure 2) and the SAE Level 3 BMW ADS as optional equipment. These ADAS functions can be divided into the sub-categories: Safety Assistance Functions, Driver Comfort Functions, and Driver Information.



Safety Assistance Functions

- Front Collision Warning with Braking Function
- Cross Traffic Braking
- Pedestrian Collision Warning
- Lane Keeping Assistant
- Lateral Collision Avoidance
- Emergency Stop Assistant
- Active Park Distance Control
- Evasion Assistant

Driver Comfort

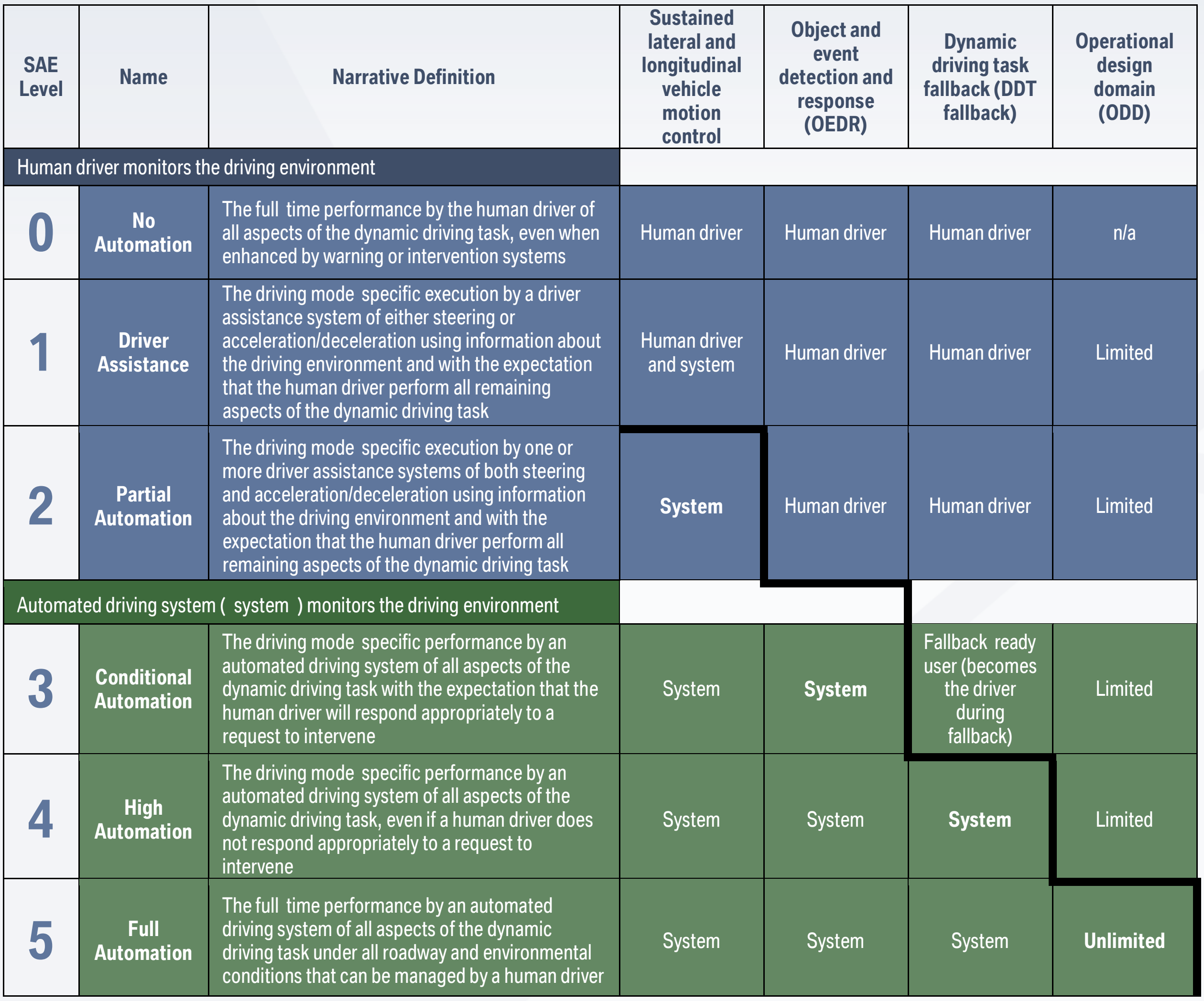
- Cruise Control
- Active Cruise Control with Stop & Go ACC
- Automatic Speed Limit Assist
- Steering and Traffic Jam Assistant
- Lane Change Assistant
- Parking Assistant
- Remote Controlled Parking
- Reversing Assistant

Driver Information

- Speed Limit Information
- No-Passing Information
- Rear View Camera
- Park Distance Control
- Intelligent Speed Assist
- Give-Way Warner
- Wrong-Way Assist
- Panorama View (Parking)

Figure 2. Advanced Driver Assistance Systems in the iNEXT.

The SAE Level 3 BMW ADS function is designed to perform the dynamic driving task on limited access highways including automated lane changes up to a maximum speed of 85mph (see Chapter 2. Object and Event Detection and Response (OEDR)). Because it is an SAE Level 3 function, it allows the driver to relax or even engage in other tasks. As with all SAE Level 3 functions, the driver/user must remain sufficiently alert to fulfill his/her responsibilities as a fallback-ready user (see SAE Level 3 definition in Figure 3). On the other hand, the driver can choose to drive himself or herself (use the iNEXT in “Boost” mode): the vehicle will act like a conventional vehicle and the driver will be assisted by our ADAS.



SAE Level	Name	Narrative Definition	Sustained lateral and longitudinal vehicle motion control	Object and event detection and response (OEDR)	Dynamic driving task fallback (DDT fallback)	Operational design domain (ODD)
Human driver monitors the driving environment						
0	No Automation	The full time performance by the human driver of all aspects of the dynamic driving task, even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a
1	Driver Assistance	The driving mode specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the human driver perform all remaining aspects of the dynamic driving task	Human driver and system	Human driver	Human driver	Limited
2	Partial Automation	The driving mode specific execution by one or more driver assistance systems of both steering and acceleration/deceleration using information about the driving environment and with the expectation that the human driver perform all remaining aspects of the dynamic driving task	**System**	Human driver	Human driver	Limited
Automated driving system (system) monitors the driving environment						
3	Conditional Automation	The driving mode specific performance by an automated driving system of all aspects of the dynamic driving task with the expectation that the human driver will respond appropriately to a request to intervene	System	**System**	Fallback ready user (becomes the driver during fallback)	Limited
4	High Automation	The driving mode specific performance by an automated driving system of all aspects of the dynamic driving task, even if a human driver does not respond appropriately to a request to intervene	System	System	**System**	Limited
5	Full Automation	The full time performance by an automated driving system of all aspects of the dynamic driving task under all roadway and environmental conditions that can be managed by a human driver	System	System	System	**Unlimited**

Figure 3. SAE Level definition according to SAE J3016.

The SAE Level 3 BMW ADS can recognize its performance limits (see Chapter 3. Operational Design Domain (ODD)) and issue a takeover request (TOR) to the driver with sufficient lead time for the driver to perform a takeover (TO) before reaching the system limits. In the unlikely case that the driver does not take over the driving task within this period, the SAE Level 3 BMW ADS performs a risk mitigation maneuver, i.e. it brings the vehicle to a complete stop as safely as possible (see Chapter 5. Fallback (Minimal Risk Condition)).

Nevertheless, there are some driving duties which are not part of the obligations of a SAE Level 3 system and will therefore remain part of the responsibility of the driver. Drivers will be educated with respect to these responsibilities (see Chapter 12. Consumer Education).

These responsibilities include, but are not limited to, the following obligations:

- Licensing and plating.
- Ensuring that no modifications have been made to the vehicle (e.g., tuning).
- Ensuring that the vehicle has the correct tires for the prevailing driving conditions (winter, summer) and that those tires are in good condition.
- Ensuring that the vehicle is in generally good condition for driving (e.g., no cracks in the wiper blades/windshield).
- The driver is fit to operate the vehicle (no drug/alcohol impairment, no risk of drowsy driving).
- The driver is sufficiently alert and in a position to take over the driving task when prompted by the SAE Level 3 BMW ADS.

The BMW Group reserves the right to revise and/or modify the descriptions provided herein prior to the feature’s market introduction.

SAE International. (2018). Taxonomy and Definitions for Terms Related to on-Road Motor Vehicle Automated Driving Systems (J3016_201806). Retrieved from: https://doi.org/10.4271/J3016_201806
Singh, S. (2015, February). Critical reasons for crashes investigated in the national motor vehicle crash causation survey. (Traffic Safety Facts Crash Stats. Report No. DOT HS 812 115). Washington DC: National Highway Traffic Safety Administration. Retrieved from: https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812115
NHTSA. (2016). Accelerating the Next Revolution In Roadway Safety (Federal Automated Vehicles Policy). Retrieved from: https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf
NHTSA. (2017). A Vision for Safety (Automated Driving Systems 2.0). Retrieved from: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf
NHTSA. (2018). 'Preparing for the Future of Transportation (Automated Vehicles 3.0). Retrieved from: https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf

Table 1. Overview of literature used in the Introduction.

1. Human Machine Interface (HMI)

A “Human Machine Interface” can be defined as all parts of an interactive system (software or hardware) that provide information and control necessary for the user to complete a certain task with the interactive system. Applied to ADS, at a minimum the HMI should be capable of informing the user through various indicators that the ADS: is functioning properly, is currently engaged in ADS mode, is currently “unavailable”, is experiencing a malfunction, and/or is requesting a control transition from the ADS to the user. The SAE Level 3 BMW ADS has been designed according to industry best practices and standards. Taken together, the HMI allows the user to safely and comfortably use the SAE Level 3 BMW ADS.

The scope of the following section is to describe how we design, develop, assess, test, and validate our SAE Level 3 BMW ADS’s human machine interface (HMI).

For decades, we have been designing the HMI of our vehicles to deliver a simultaneously customer-oriented and non-distracting driving experience. With the introduction of the SAE Level 3 BMW ADS, the user’s driving experience will be enhanced even further by providing them the opportunity to temporarily hand over the Dynamic Driving Task (DDT) to the ADS when operating within the SAE Level 3 BMW ADS’s Operational Design Domain (ODD). By always keeping the user informed about the SAE Level 3 BMW ADS’s status and his/her responsibilities both as a driver and as a fallback-ready user, the vehicle’s HMI is a key component that enables the safe and comfortable use of the SAE Level 3 BMW ADS. Throughout our complete design and development process, we use state-of-the-art methods to ensure that this vision is met, ranging from driving simulators to driving tests on proving grounds and studies in road traffic.

Voluntary Guidance, Best Practices, Industry Standards, Design Principles, Internal Processes and Company Policies

In addition to the relevant standardization-related documents and the comprehensive inventory of standard development activities given in the U.S. Department of Transportation’s Federal Automated Vehicle Policy guidance, we consider and apply a number of relevant guidance, best practices, industry standards and design principles (see Table 3) during our HMI development process. This internal inventory is constantly updated to take into account state-of-the-art scientific insights.

In parallel, we rely on our own internal processes based on the intended level of automation at hand and the expected level of driver engagement. In accordance with SAE J3016, we expect that the DDT fallback-ready user is receptive to any Level 3 BMW ADS-issued requests to intervene and will respond appropriately. When the driver takes over the driving task, the SAE Level 3 BMW ADS should convey all necessary traffic and environment information in order to facilitate a safe TO. Accordingly, we have implemented a tailor-made process for the HMI development and testing of our Level 3 BMW ADS system.

To develop an SAE L3 ADS HMI that is comprehensible, easy, and safe to use, we rely on an iterative human-centered design process based on ISO 9241 “Ergonomics of human-system interaction” that also guides our evaluation, testing, and validation. At the core of this process are four interdependent human-centered design activities:

1. Understanding and specifying the context of use
2. Specifying the user requirements

3. Producing design solutions to meet these requirements
4. Evaluating the designs against these requirements

We also seek to extend the existing knowledge base by proactively contributing to the method development in human factors research of automated driving and participating in scientific as well public discussion.

HMI design

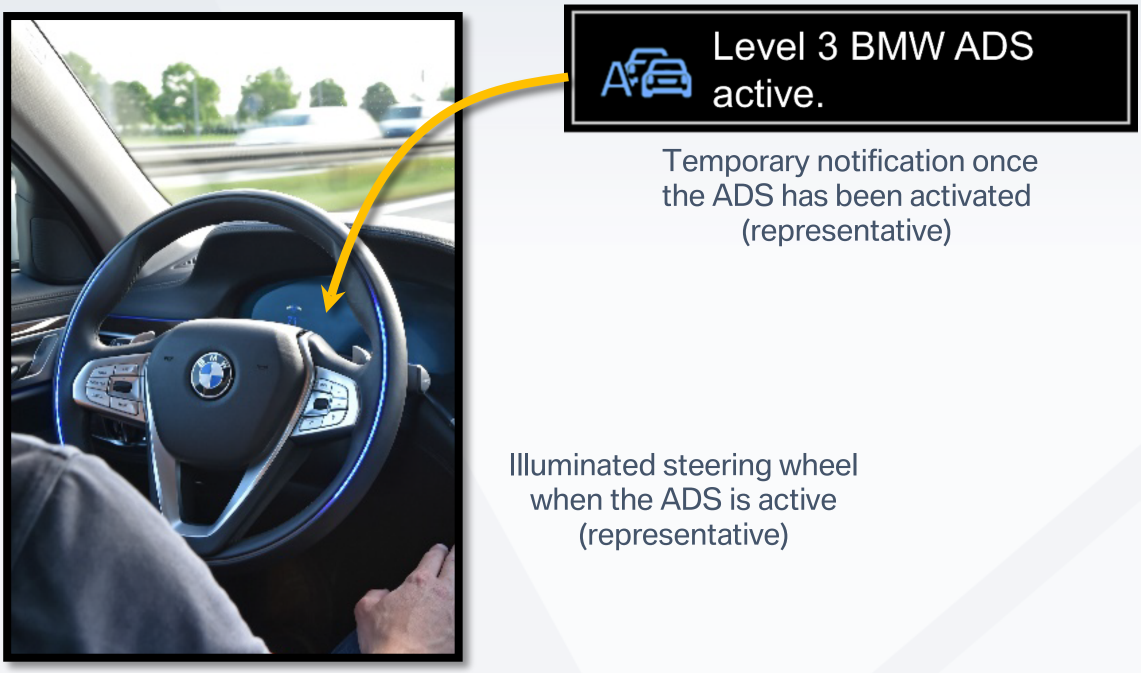
We recognize that for any system that still relies on the human operator as a fallback-ready user (see SAE Level 3 definition), there may be human factor challenges related to driver awareness and engagement. Therefore, the comprehensibility of BMW's HMI is assessed for all states of operation with safety being the primary design goal. This is done through numerous HMI evaluations, empirical as well as non-empirical data, throughout the design and development process. Similarly, the communication with other road users is investigated where and when necessary.

To support the fallback-ready user, our system includes a driver-monitoring system to observe whether the fallback-ready user is awake, is sitting in the driver's seat, and has the seat belt fastened.

To detect if the driver has taken over the driving task after a TOR the driver monitoring system also contains a hands-on-detection-sensor in the steering wheel, a steering-torque-sensor, and pedal-position-sensors. If the driver operates user-interface elements, opens the doors, or tries to shift gears this also will be detected by standard-sensors as used in conventional cars.

We take great care to ensure the HMI is able to communicate every state of operation, as well as all additional information that is relevant to the driver. In this context, information is defined as being relevant if it meets one or more of the following goals:

- Information that aims for a change in user behavior (e.g. the current system status such as "Level 3 BMW ADS active", where the user is no longer responsible for performing the dynamic driving task). In the iNEXT, the activation of the SAE Level 3 BMW ADS will be communicated via different channels: Once the SAE Level 3 BMW ADS is active, a corresponding status message will appear on the instrument cluster (see Figure 4). While the SAE Level 3 BMW ADS is engaged, the steering wheel will be illuminated in blue. **(Please Note: all images, symbols, graphics, HMI elements, and textual driver notifications shown are conceptual and for illustration purpose only herein.)**



Temporary notification once the ADS has been activated (representative)

Illuminated steering wheel when the ADS is active (representative)

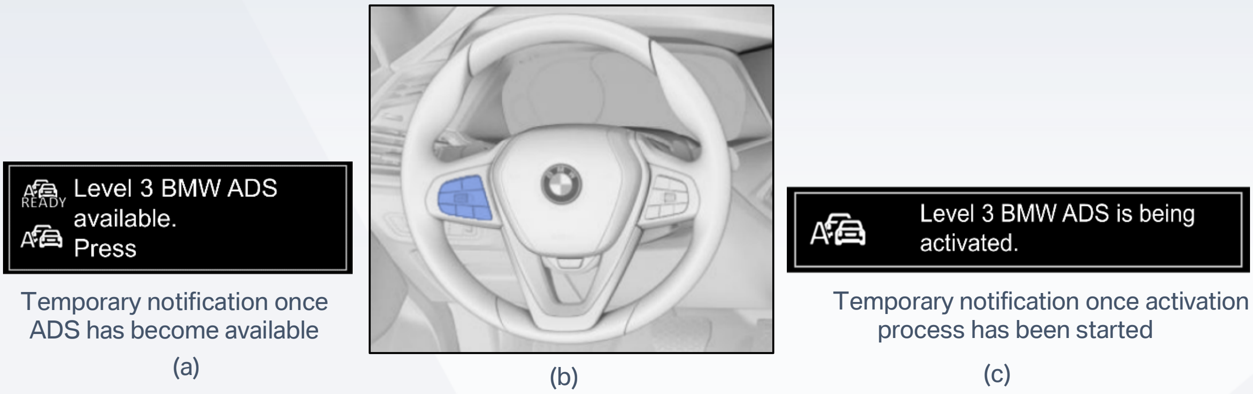
Figure 4. Activation of SAE Level 3 BMW ADS (Exemplary depiction).

- Information that reveals system states and possible limitations (e.g., unavailability of the system and system malfunction) or different possible modes of operation (e.g., SAE Level 1 Driver Assistance or SAE Level 2 ADAS) users might be able to select. Some important states of SAE Level 3 BMW ADS are summarized in Table 2.

Telltale	State of SAE Level 3 BMW ADS
READY	Level 3 BMW ADS is available.
	Level 3 BMW ADS is activated.
	Level 3 BMW ADS is not available.

Table 2. States of the SAE Level 3 BMW ADS.

- Information that makes user interaction more intuitive (e.g., instructions for the activation of the SAE Level 3 BMW ADS, Figure 5 (a), via the buttons on the steering wheel, Figure 5 (b), and the confirmation that the button press was accepted and the system is going to be activated, Figure 5 (c)).



Level 3 BMW ADS available. Press

Temporary notification once ADS has become available

(a)

(b)

Level 3 BMW ADS is being activated.

Temporary notification once activation process has been started

(c)

Figure 5. Activation of SAE Level 3 BMW ADS.

As with every other function we integrate into our system, our development goal is an HMI that is easy to use, intuitive, and with special emphasis placed on the safety of the driver.

In contrast to existing systems (SAE Level 0 up to SAE Level 2), where the driver has to constantly supervise the features, the SAE Level 3 BMW ADS may—temporarily—allow the driver to divert his/her attention from the driving task while still requiring him/her to act as a fallback-ready user. This means that we have to avoid a situation in which a driver assumes the SAE Level 3 BMW ADS is active, when in fact it is not. Therefore, we have implemented the following design solutions:

- Color coded illumination of the steering wheel is used during Level 3 activity (see Figure 6), to make drivers aware of their responsibility in the driving task at first glance at any given time. While the SAE Level 3 BMW ADS is active and operating with full capabilities, the steering wheel is illuminated in blue. When the SAE Level 3 BMW ADS issues a TOR to the fallback-ready user, the steering wheel's illumination turns yellow after first displaying a pre-warning. If the driver does not respond timely to this TOR the next warning stage will be triggered and the steering wheel will be illuminated in red.

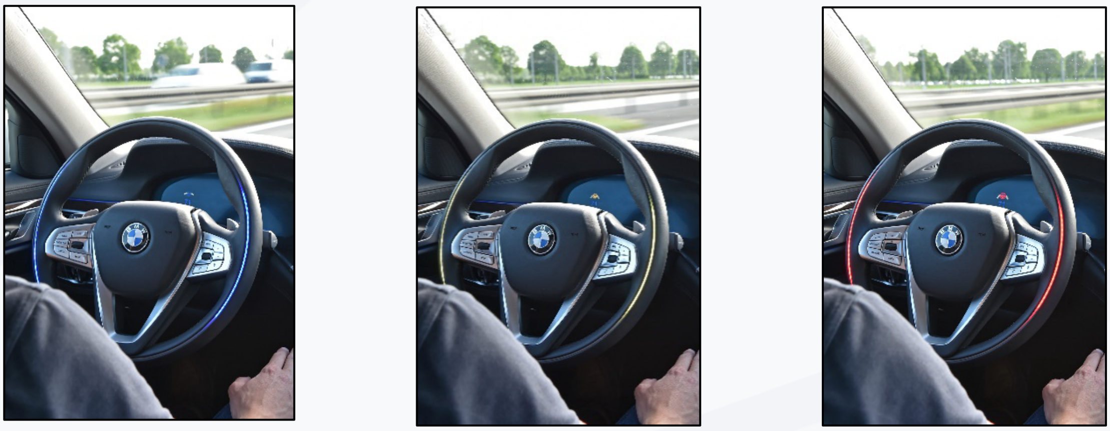
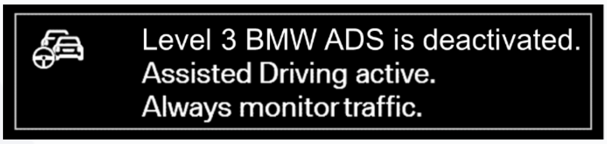


Figure 6. TOR: getting the driver back into the driving task by using the illuminated steering wheel and notifications.

- A successful TO by the user is also communicated via different channels: the blue illumination of the steering wheel is turned off and a message confirming the deactivation and reminding the driver of his/her responsibilities is displayed, see Figure 7.



Level 3 BMW ADS is deactivated.
Assisted Driving active.
Always monitor traffic.

Figure 7. Deactivation: After successful TO the user gets informed about the system state (to remind them about their responsibilities).

- We combine auditory and visual elements (graphical animations on the instrument cluster, as well as strongly apparent illumination patterns on the steering wheel), to ensure that transitions between the active SAE Level 3 BMW ADS and all other levels of automation are as intuitive as possible.
- We optimize the sensory component of the HMI for the specific scenarios the user is confronted with.

Communication and Collaboration with Relevant Stakeholders

We are committed to continuously optimizing our test and validation methods and discussing them transparently with world-leading experts in this domain (see BMW's collaborative effort with industry partners on the White Paper, "Safety First for Automated Driving"). Therefore, we collaborate with independent university and research organizations and publish our methods in conferences and peer-reviewed scientific journals. We also actively engage in nationally- and internationally-funded joint research initiatives to advance and support commonly agreed upon ADS HMI test and evaluation methods, such as the EU-funded project L3 Pilot (https://www.l3pilot.eu/).

Taken together, this approach and our underlying processes enable us to develop a Level 3 BMW ADS that is capable of maintaining safety in relevant operating conditions, while delivering a premium user experience.

Safety in Use for Level 3

Regarding the different levels of automation (SAE Level 0-5), the user's driving tasks and responsibilities change with increasing automation, i.e., each level places different demands on the user (compare the roles of human driver and automated driving system by level of driving automation in SAE J3016, as depicted in Figure 8). There is a paradigm shift with the introduction of an SAE Level 3 automated driving system as this is the first time the vehicle operator does not need to supervise the ADS while it is engaged. As a result, there is a diffusion of responsibility, which introduces the possibility for mode confusion. Above all, L2 and L3 have a high potential for being confused by the driver as both affect longitudinal and lateral control – while one demands continuous supervision, the other does not (see Figure 9). In vehicles with different levels of automation (SAE L1, L2, and L3 or higher), a highly important and challenging goal for a safe function is the user's correct interpretation of the actual driving mode and its affiliated responsibilities and (driving) tasks:

- In the moment of a mode transition.
- While driving with the same automation mode for a certain period of time.

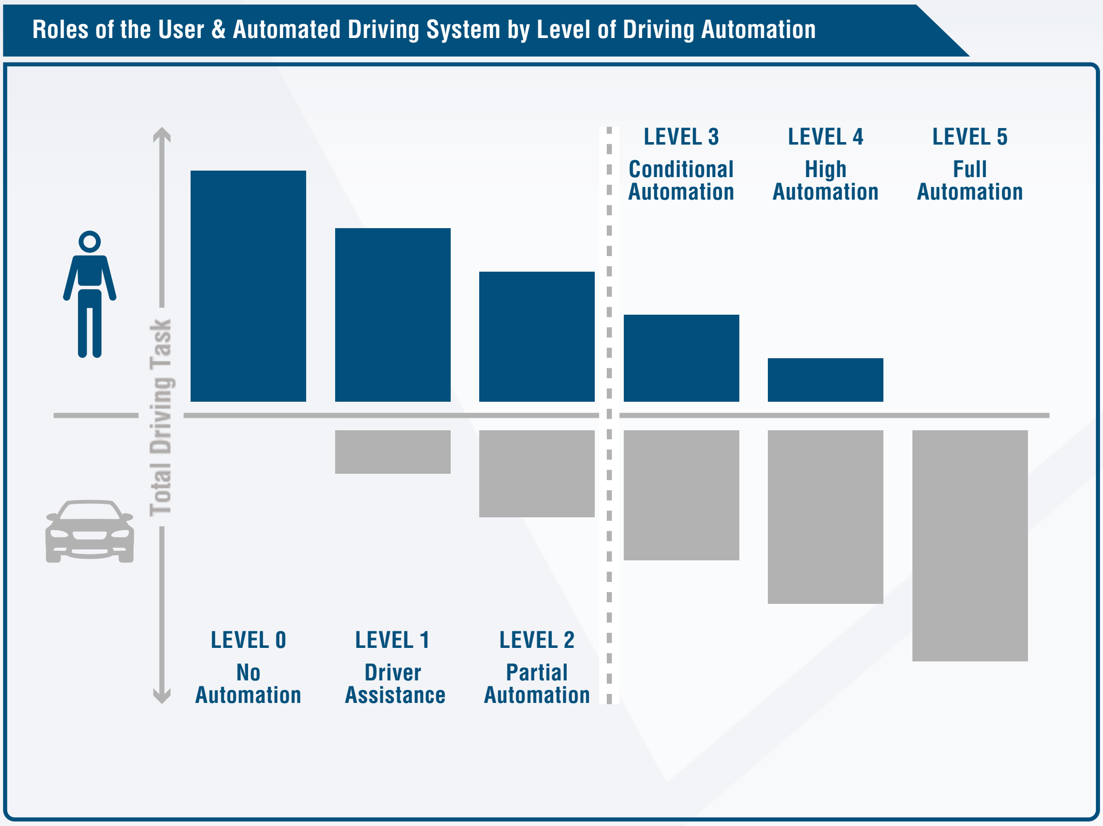


Figure 8. Roles of the User & ADS by Level of Driving Automation as described in the White Paper "Safety First for Automated Driving".

To promote a Level 3 function that is safe in use, the following key requirements for the human-machine interaction should be fulfilled:

- Reliably detect intended driver behavior during activation and, above all, deactivation of a certain driving mode and during (driver-initiated) transitions from L3 to lower levels of automation (minimize false positive and false negative). This requirement refers to all types of HMI operations, including remote control.
- Indicate the actual driving mode and the driver's responsibility in an unambiguous and understandable way.
- Promote appropriate trust in automation for the actual driving mode.
- Issue prominent and easily understandable takeover requests (e.g., combining acoustic and visual signals) that give the vehicle operator enough time to take over manual control and regain situational awareness.
- Monitor the driver's fatigue condition and issue a takeover request early enough where a takeover is not impaired by the driver's condition.

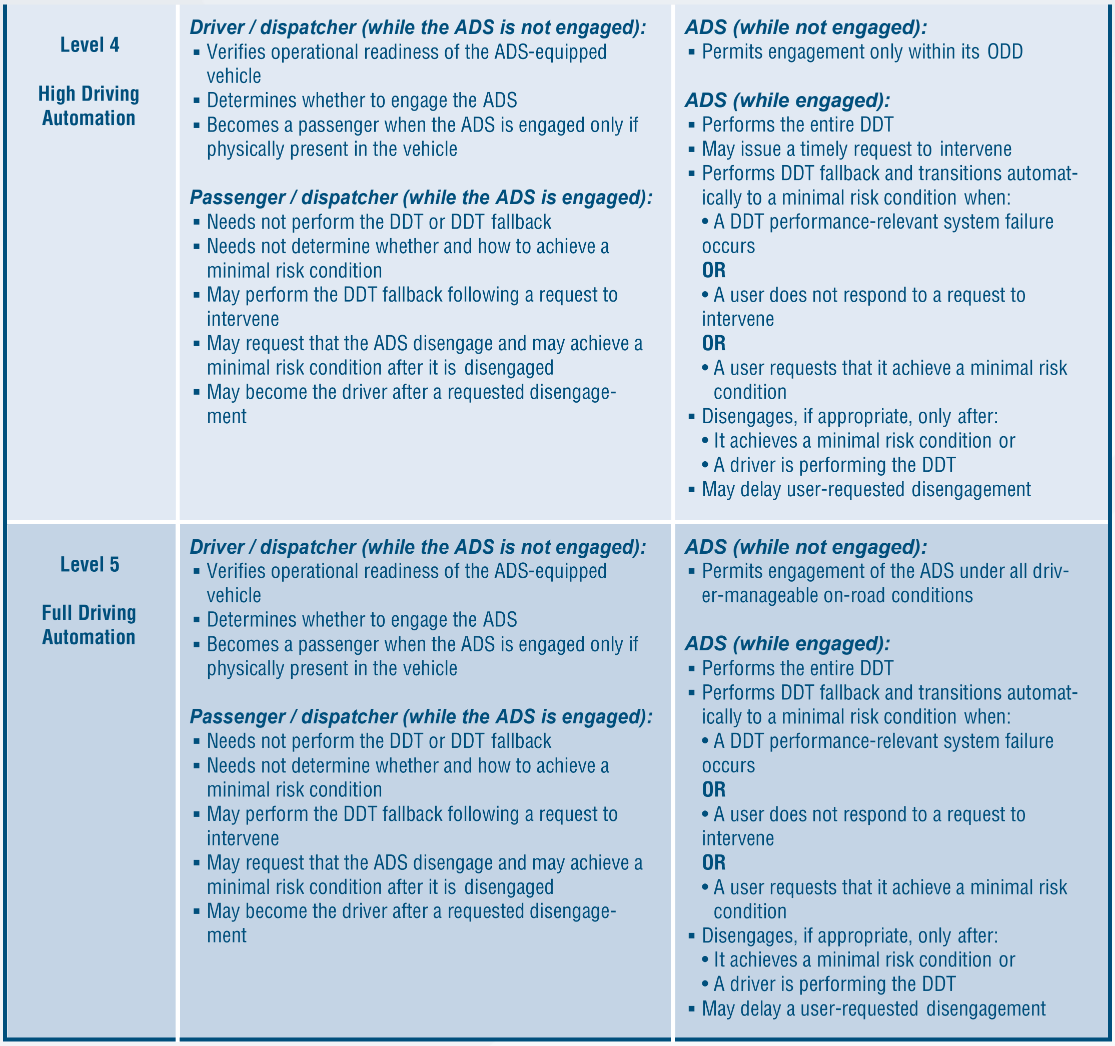
These requirements are taken into account during the functional development and the validation phase. To make sure that the function meets the requirements on a safe human-machine interaction, numerous studies with subjects unfamiliar with automated driving are implemented to test, assess, and validate the concept. This means that the subjects have no experience or prior knowledge of the system in test. Each requirement is operationalized through suitable use cases and measurement criteria that demonstrate how users handle the tasks within the driving environment. Depending on the research question and the relevant use cases, the studies take place in driving simulators or real car settings.

These empirical studies along with a continuous expert evaluation by experienced human factors researchers contribute to a steady improvement and optimization of the concept in the development phase and to a function that is safe in use for the customer.

Role of the Automated Driving System

Level of Driving Automation	Role of the User	Role of the Automated Driving System
DRIVER PERFORMS PART OR ALL OF THE DDT		
Level 0 **No Driving Automation**	**Driver (at all times):** ▪ Performs the entire DDT	***Automated driving system (if any):*** ▪ Does not perform any part of the DDT on a sustained basis (although other vehicle systems may provide warnings or support, such as momentary emergency intervention)
Level 1 **Driver Assistance**	***Driver (at all times):*** ▪ Performs the remainder of the DDT not performed by the driving automation system ▪ Supervises the driving automation system and intervenes as necessary to maintain safe operation of the vehicle ▪ Determines whether/when engagement or disengagement of the driving automation system is appropriate ▪ Immediately performs the entire DDT whenever required or desired	***Automated driving system (while engaged):*** ▪ Performs part of the DDT by executing either the longitudinal or the lateral vehicle motion control subtasks ▪ Disengages immediately upon driver request
Level 2 **Partial Driving Automation**	***Driver (at all times):*** ▪ Performs the remainder of the DDT not performed by the driving automation system ▪ Supervises the driving automation system and intervenes as necessary to maintain safe operation of the vehicle ▪ Determines whether/when engagement and disengagement of the driving automation system is appropriate ▪ Immediately performs the entire DDT whenever required or desired	***Automated driving system (while engaged):*** ▪ Performs part of the DDT by executing both the lateral and the longitudinal vehicle motion control subtasks ▪ Disengages immediately upon driver request
ADS PERFORMS THE ENTIRE DDT WHILE ENGAGED		
Level 3 **Conditional Driving Automation**	***Driver (while the ADS is not engaged):*** ▪ Verifies operational readiness of the ADS-equipped vehicle ▪ Determines when engagement of ADS is appropriate ▪ Becomes the DDT fallback-ready user when the ADS is engaged ***DDT fallback-ready user (while the ADS is engaged):*** ▪ Is receptive to a request to intervene and responds by performing DDT fallback in a timely manner ▪ Is receptive to DDT performance-relevant system failures in vehicle systems and, upon occurrence, performs DDT fallback in a timely manner ▪ Determines whether and how to achieve a minimal risk condition ▪ Becomes the driver upon requesting disengagement of the ADS	***ADS (while not engaged):*** ▪ Permits engagement only within its ODD ***ADS (while engaged):*** ▪ Performs the entire DDT ▪ Determines whether ODD limits are about to be exceeded and, if so, issues a timely request to intervene to the DDT fallback-ready user ▪ Determines whether there is a DDT performance-relevant system failure of the ADS and, if so, issues a timely request to intervene to the DDT fallback-ready user ▪ Disengages at an appropriate time after issuing a request to intervene ▪ Disengages immediately upon driver request

(Continued)



Level 4 **High Driving Automation**	***Driver / dispatcher (while the ADS is not engaged):*** ▪ Verifies operational readiness of the ADS-equipped vehicle ▪ Determines whether to engage the ADS ▪ Becomes a passenger when the ADS is engaged only if physically present in the vehicle ***Passenger / dispatcher (while the ADS is engaged):*** ▪ Needs not perform the DDT or DDT fallback ▪ Needs not determine whether and how to achieve a minimal risk condition ▪ May perform the DDT fallback following a request to intervene ▪ May request that the ADS disengage and may achieve a minimal risk condition after it is disengaged ▪ May become the driver after a requested disengagement	***ADS (while not engaged):*** ▪ Permits engagement only within its ODD ***ADS (while engaged):*** ▪ Performs the entire DDT ▪ May issue a timely request to intervene ▪ Performs DDT fallback and transitions automatically to a minimal risk condition when: • A DDT performance-relevant system failure occurs **OR** • A user does not respond to a request to intervene **OR** • A user requests that it achieve a minimal risk condition ▪ Disengages, if appropriate, only after: • It achieves a minimal risk condition or • A driver is performing the DDT ▪ May delay user-requested disengagement
Level 5 **Full Driving Automation**	***Driver / dispatcher (while the ADS is not engaged):*** ▪ Verifies operational readiness of the ADS-equipped vehicle ▪ Determines whether to engage the ADS ▪ Becomes a passenger when the ADS is engaged only if physically present in the vehicle ***Passenger / dispatcher (while the ADS is engaged):*** ▪ Needs not perform the DDT or DDT fallback ▪ Needs not determine whether and how to achieve a minimal risk condition ▪ May perform the DDT fallback following a request to intervene ▪ May request that the ADS disengage and may achieve a minimal risk condition after it is disengaged ▪ May become the driver after a requested disengagement	***ADS (while not engaged):*** ▪ Permits engagement of the ADS under all driver-manageable on-road conditions ***ADS (while engaged):*** ▪ Performs the entire DDT ▪ Performs DDT fallback and transitions automatically to a minimal risk condition when: • A DDT performance-relevant system failure occurs **OR** • A user does not respond to a request to intervene **OR** • A user requests that it achieve a minimal risk condition ▪ Disengages, if appropriate, only after: • It achieves a minimal risk condition or • A driver is performing the DDT ▪ May delay a user-requested disengagement

Figure 9. Role of the ADS according to SAE J3016.

CAMP. (2016). Automated vehicles research for enhanced safety. Washington, DC: NHTSA.

Campbell, J. L., Brown, J. L., Graving, J. S., Richard, C. M., Lichty, M. G., Bacon, L. P., & Sanquist, T. (2018, August). Human factors design guidance for level 2 and level 3 automated driving concepts (Report No. DOT HS 812 555). Washington, DC: National Highway Traffic Safety Administration.

Department of Defense Design Criteria Standard. (1999). Human Engineering (MIL-STD-1472G).

Driver Focus-Telematics Working Group (2006). Statement of principles, criteria and verification procedures on driver interactions with advanced in-vehicle information and communication systems. Washington, DC: Alliance of Automobile Manufacturers.

Economic and Social Council. (2011). Guidelines on establishing requirements for high-priority warning signals (ECE/TRANS/WP.29/2011/90).

Green, P., Levison, W., Paelke, G., & Serafin, C. (1993). Suggested human factors design guidelines for driver information systems. University of Michigan, Transportation Research Institute.

Hoeger, R., Zeng, H., Hoess, A., Kranz, T., Boverie, S., Strauss, M., & Nilsson, A. (2011). The future of driving–HAVEit (Final Report, Deliverable D61. 1). Regensburg, Germany: Continental Automotive GmbH.

International Organization for Standardization. (2003). Road vehicles -- Ergonomic aspects of transport information and control systems - Specifications and compliance procedures for in-vehicle visual presentation (ISO Standard No. 15008). Retrieved from: https://www.iso.org/standard/34886.html

International Organization for Standardization. (2011). Road vehicles -- Ergonomic aspects of transport information and control systems -- Specifications for in-vehicle auditory presentation (ISO Standard No. 15006). Retrieved from: https://www.iso.org/standard/55322.html

International Organization for Standardization. (2013). Intelligent transport systems -- Forward vehicle collision warning systems -- Performance requirements and test procedures (ISO Standard No. 15623). Retrieved from: https://www.iso.org/standard/56655.html

International Organization for Standardization. (2017). Road vehicles -- Ergonomic aspects of transportation and control systems -- Dialogue management principles and compliance procedures (ISO Standard No. 15005). Retrieved from: https://www.iso.org/standard/69238.html

International Organization for Standardization. (2010). Ergonomics of human-system interaction -- Part 210: Human-centered design for interactive systems (ISO Standard No. 9241-210). Retrieved from: https://www.iso.org/standard/52075.html

JAMA. (2004). Guidelines for In-vehicle Display Systems (Version 3.0).

Naujoks, F., Hergeth, S., Wiedemann, K., Schömig, N., & Keinath, A. (2018, September). Use Cases for Assessing, Testing, and Validating the Human Machine Interface of Automated Driving Systems. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 62, No. 1, pp. 1873-1877). Sage CA: Los Angeles, CA: SAGE Publications.

Naujoks, F., Wiedemann, K., Schömig, N., Hergeth, S., & Keinath, A. (2019). Towards guidelines and verification methods for automated vehicle HMIs. Transportation Research Part F: Traffic Psychology and Behaviour, 60, 121-136.

NASA Technical Standard. (2011). Human Factors, Habitability, and Environmental Health (NASA-STD-3001, VOLUME 2, REVISION A).

NHTSA. (2007). Crash Warning System Interfaces: Human Factors Insights and Lessons learned - Final Report (DOT HS 810 697).

NHTSA. (2016). Accelerating the Next Revolution In Roadway Safety (Federal Automated Vehicles Policy).

NHTSA. (2020). Ensuring American Leadership in Automated Vehicle Technologies Automated Vehicles 4.0.' Retrieved from: https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/360956/ensuringamericanleadershipav4.pdf

Ross, T., Midtland, K., Fuchs, M., Pauzie, A., Engert, A., Duncan, B.,... May, A. (1996). HARDIE design guidelines handbook: Human factors guidelines for information presentation by ATT systems (DRIVE II Project V2008).

SAE International. (2003). Human Factors in Forward Collision Warning Systems: Operating Characteristics and User Interface Requirements (J2400_200308).

Stevens, A., Quimby, A., Board, A., Kersloot, A., Burns, P. (2002). Design Guidelines for safety in-vehicle information systems.

Stevens, A., Cnyk, S. (2011). Checklist for the assessment of in-vehicle information systems. Transport Research Laboratory.

The Commission of the European Communities. (1999). COMMISSION RECOMMENDATION of 21 December 1999 on safe and efficient in-vehicle information and communication systems: A European statement of principles on human machine interface (L 19/69)

The Commission of the European Communities. (2006). COMMISSION RECOMMENDATION of 22 December 2006 on safe and efficient in-vehicle information and communication systems: update of the European Statement of Principles on human machine interface (L 32/200).

Table 3. Overview of HMI specific guidance, best practices, industry standards and design principles applicable to the SAE L3 ADS.

2. Object and Event Detection and Response (OEDR)

As is necessary for human drivers, the SAE Level 3 BMW ADS must continuously monitor and react to the driving environment. On the monitoring side, the vehicle uses a number of integrated sensors to perceive its surroundings, which sensors include cameras, radar, LIDAR, and ultrasonic sensors. These sensors operate in conjunction with one another in order to provide the BMW vehicle with a full 360º view of its surroundings and the perceived environment is then cross referenced to a high definition map to provide certainty of the vehicle's position on the roadway. This perception also includes the identification of other vehicles and potential road hazards, all classified by the BMW vehicle's onboard processing, which can classify people, cars, various objects, and potentially hazardous situations. As the vehicle's environment is sensed and classified, the appropriate next steps are planned using the information from the sensors as input and the BMW vehicle then follows this planned path. All of this sensing, planning, and acting occur in fractions of a second and occur continuously such that a continuous feedback loop is created for a safe, seamless driving experience.

Adapting the classic Sense, Plan, and Act framework from the robotics and automation strategies to automotive ADS, the model including Sensing & Perception (including Localization), Planning & Control, and Actuation & Stability provides a general, implementation-independent view. The following picture illustrates this general chain model:

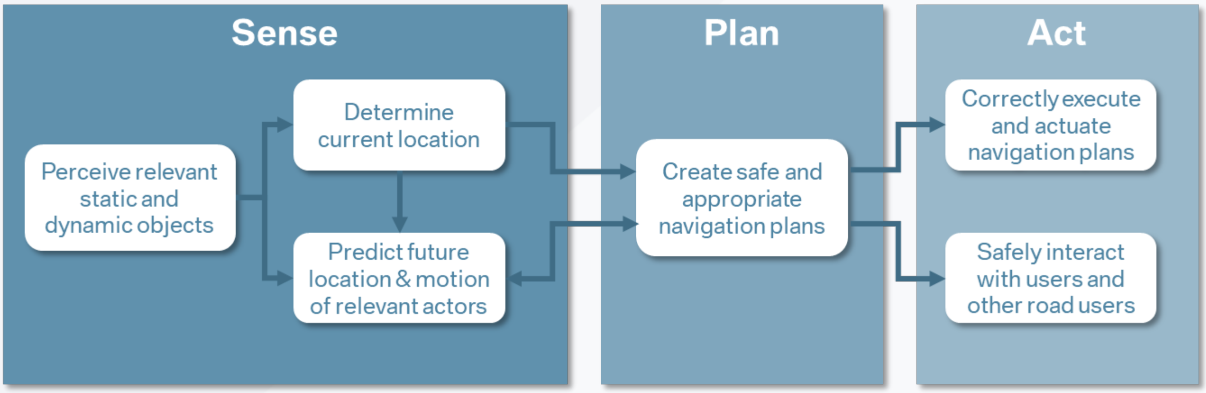

Sense
Plan
Act
Perceive relevant static and dynamic objects
Determine current location
Predict future location & motion of relevant actors
Create safe and appropriate navigation plans
Correctly execute and actuate navigation plans
Safely interact with users and other road users

Figure 10. OEDR Process.

While the SAE Level 3 BMW ADS is operating in its defined ODD, it is responsible for a continuous detection of ODD limits and objects that are relevant to its driving task, deciding upon an appropriate response by taking into account the different relevant entities both within and outside of its travel path and executing the correct driving plan or interaction with its user and other road users.

As of today, a single sensor does not have the capability to simultaneously provide reliable, precise detection, classification, measurement, and robustness to adverse conditions. To ensure a comprehensive detectability, a multimodal approach is required to cover detectability of all relevant entities. These entities include, but are not limited to, infrastructure defining the allowed area of operation, other road users, obstacles, and traffic guiding signs or visible lane markings.

To account for the necessary high level of precision, the SAE Level 3 BMW ADS is using a high-performance setup consisting of several radars, several cameras, a LIDAR, several ultrasonic sensors, and an HD map to capture all external in-situ information and create a reliable 360° model of the world surrounding the vehicle (see Figure 11).

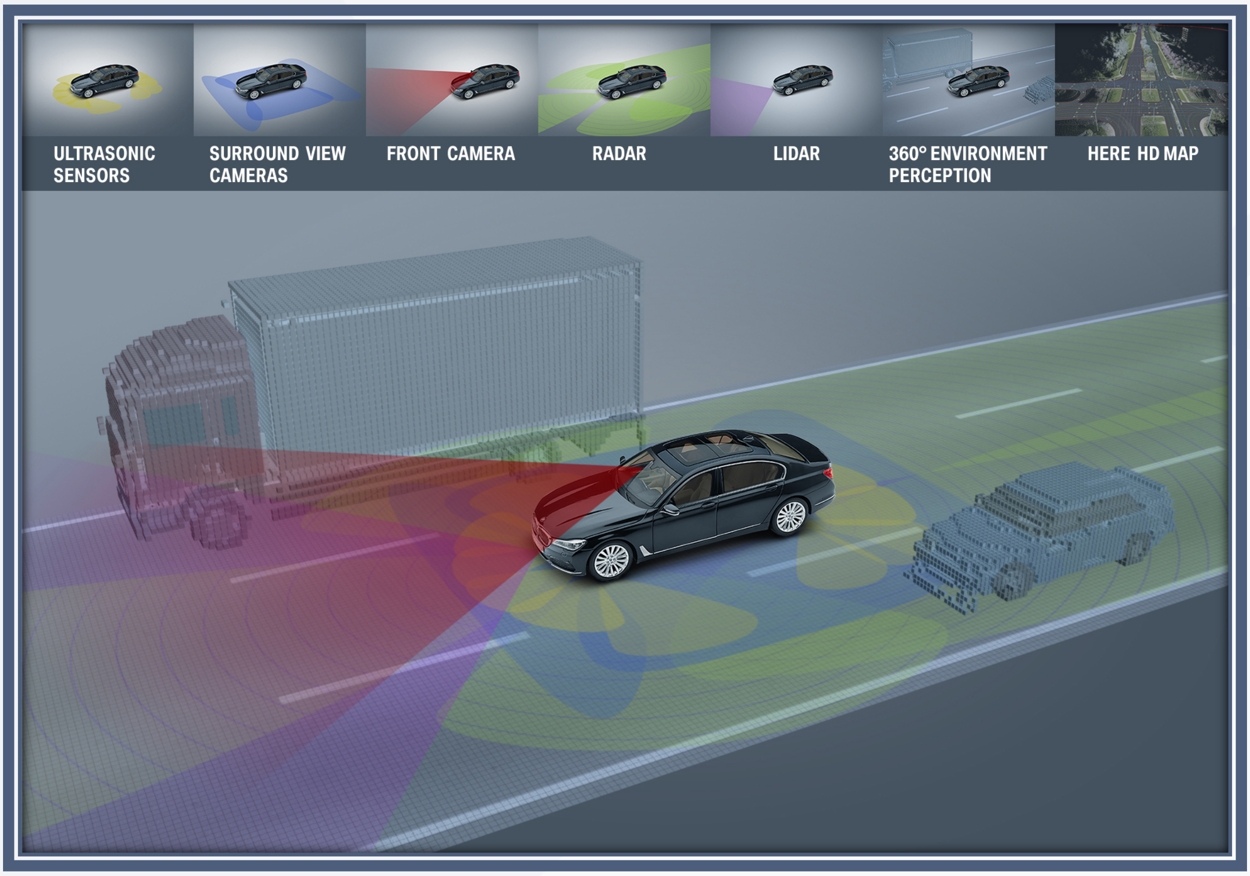


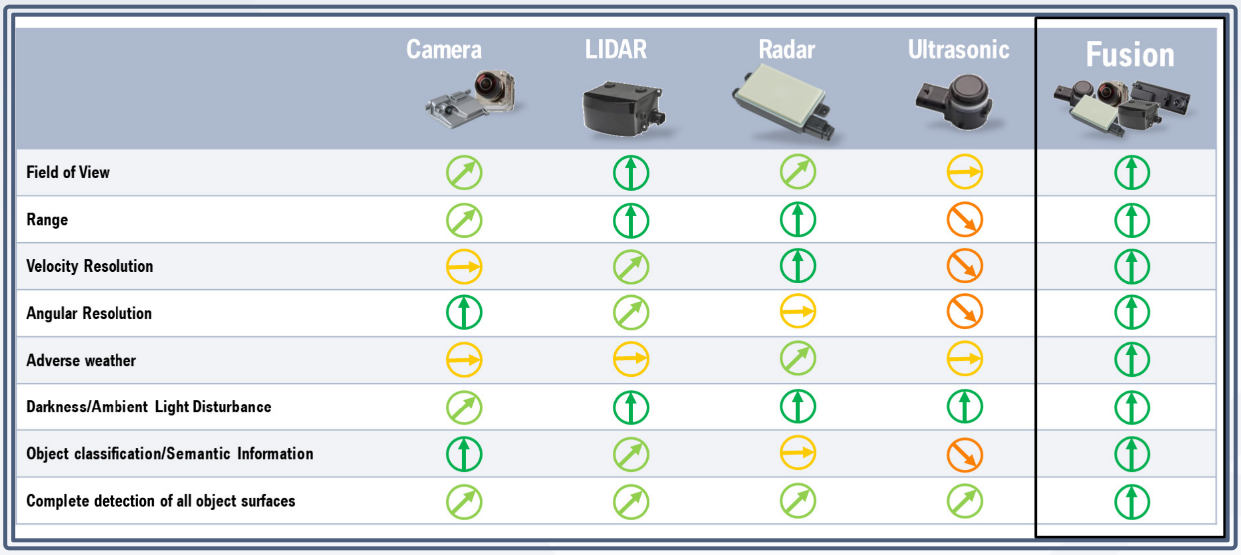
Figure 11. Sensor Fusion - the combination of multiple sensors to ensure a complete perception of the surroundings.

The specifications of the different sensors are described as follows (see also Figure 12):

- Camera: Sensor with highest extractable information content as it is capable of capturing visible cues comparable to human perception. Limited precision in range determination, high sensitivity to adverse conditions.
- LIDAR: High-precision measurement of structured and unstructured elements. Medium sensitivity to environmental conditions.
- Radar: High-precision detection and measurement of moving objects with appropriate reflectivity in radar operation range, high robustness against weather conditions.
- Ultrasonic: Well-established near-field sensor capable of detecting closest distances to reflecting entities.

In addition to the set of on-board sensors, an HD Map is used as an independent source of information. It helps to increase the quality and reliability of the function by precisely calculating where the car is located and providing knowledge about, for example, the end of highways, drivable lanes or areas with increased probability of Vulnerable Road Users (VRU). This is important to ensure that the function is only active on road types as defined in its ODD.

An overview of the advantages and disadvantages of the sensors used is given in Figure 12.



	Camera	LIDAR	Radar	Ultrasonic	Fusion
Field of View	↗	↑	↗	→	↑
Range	↗	↑	↑	↘	↑
Velocity Resolution	→	↗	↑	↘	↑
Angular Resolution	↑	↗	→	↘	↑
Adverse weather	→	→	↗	→	↑
Darkness/Ambient Light Disturbance	↗	↑	↑	↑	↑
Object classification/Semantic Information	↑	↗	→	↘	↑
Complete detection of all object surfaces	↗	↗	↗	↗	↑

Figure 12. Advantages and drawbacks of individual sensors.

The various sensors have different sensitivities towards various adverse weather conditions. By using a combination of sensors that work together, the limitations of any given sensor are potentially supplemented by the strengths of another, thereby allowing enhanced functionality even in conditions that may be challenging for any given sensor. A fusion of different sensors will therefore lead to an overall excellent result for a large range of adverse weather conditions.

Sensors are in some cases able to enrich the raw data with additional information by using a computer vision algorithm before routing the data to the next processing unit. Figure 13 shows, for example, processed camera data including object detection and classification as well as the identified traffic signs and the detected lanes.

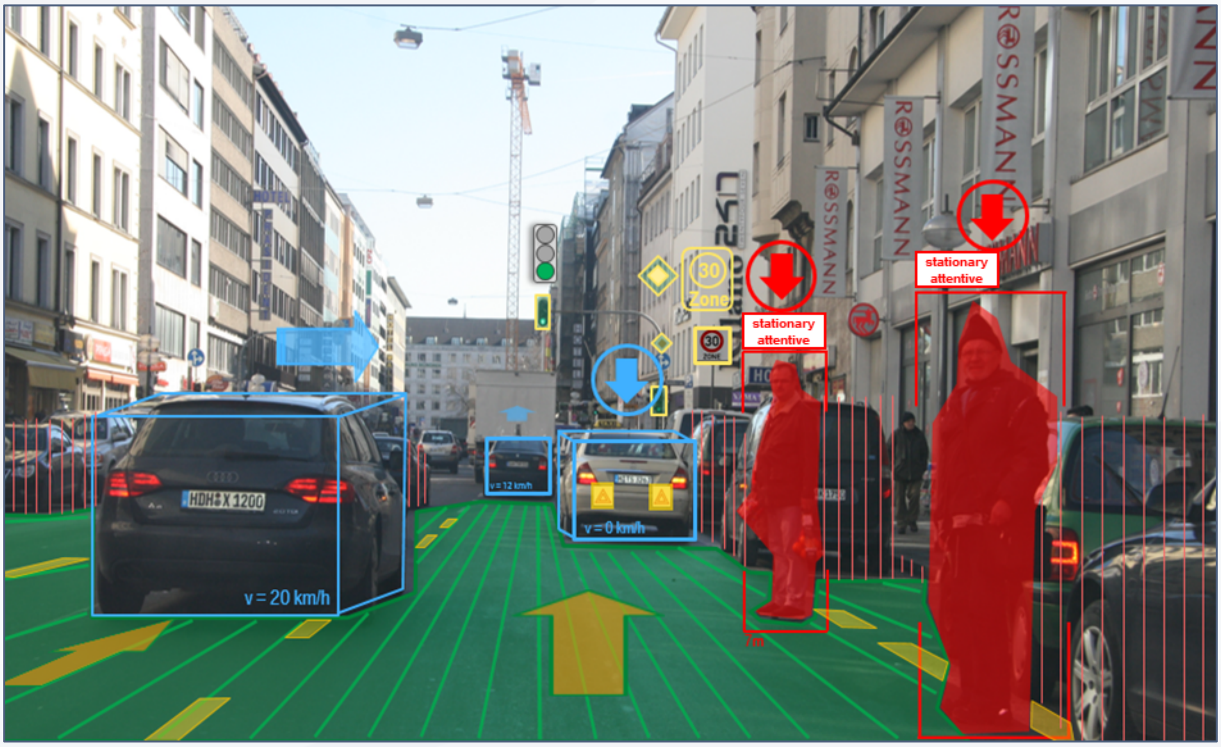


Figure 13. Object detection and classification from camera sensor data.

By fusing all these sensor inputs and the information of the HD Map in a processing unit, the ADS is capable of creating a reliable impression of the surrounding world that is far beyond the range of the individual sensors.

This interpretation of the current environment enables predictions of other road users' imminent behavior. This is important, since the planning of the BMW subject vehicle's movement is impossible without assuming/predicting the future locations of the other traffic participants.

Based on the present environment model and its predicted progression, the function selects a driving strategy according to the dynamically changing road and traffic conditions, for example, by adapting the speed or trajectory of the vehicle. This enables the system to make an appropriate decision for the current situation taking into account driver safety as well as other road users.

For example:

- Objects: The function avoids contact with objects that can introduce a safety hazard, as long as no other road user is harmed (i.e., swerving to avoid an obstacle as long as doing so does not endanger other road users).
- Vulnerable Road Users (VRU) → Pedestrians: Even though we do not expect that we will regularly encounter persons on a highway, the possibility always exists, therefore, we still implement an appropriate response. If a person is located in the lane of the BMW subject vehicle, the SAE Level 3 BMW ADS avoids a collision by steering and/or braking, as possible within the given system limits. If the function is passing a person standing next to the lane of the BMW subject vehicle, the function enlarges the lateral distance to the person as much as possible and reduces the speed depending on the achievable lateral distance to the person.
- Vulnerable Road Users (VRU) →Motorcycles: Aside from pedestrian VRUs mentioned above, other categories of vulnerable road users who may be expected within the ODD include motorcycles. As BMW Group is also a manufacturer of motorcycles, we are keenly aware of the special needs of our SAE Level 3 BMW ADS to detect and react appropriately to such road users. Our sensors are designed and validated to account for motorcycles, including in circumstances unique to motorcycles, such as lane splitting.
- Cars: The SAE Level 3 BMW ADS has a cooperative driving strategy. For example, the function reduces its speed in order to make it easier for other cars to join the traffic flow on highway entry or exit. The SAE Level 3 BMW ADS also observes the vehicles on the other lanes to avoid lateral collisions. The rear of the vehicle is monitored by radars and cameras in order to facilitate a safe lane change.

If there are insufficient conditions detected within the ODD, for example poor visibility or wind, the function will in general reduce speed and increase the distance to other cars, as described in Section 3. Operational Design Domain (ODD). Furthermore, if a situation occurs where the system boundaries are reached, the ADS triggers a TOR to the fallback-ready user with sufficient time allotted for a safe transition to manual driving.

3. Operational Design Domain (ODD)

The Operational Design Domain is the set of design parameters in which the SAE Level 3 BMW ADS is programmed to operate within. The ODD includes all conditions that must be met in order for the SAE Level 3 BMW ADS to be operable. These conditions include but are not limited to: geographical limitations, for example, the SAE Level 3 BMW ADS is only available on limited access highways; environmental limitations, for example, if the BMW vehicle's sensors detect severe weather that would impede the ability to accurately sense the environment; and human driver limitations, for example, the driver must be seated with their seat belt fastened and remain awake, among others. When all of the conditions of the ODD are met, the SAE Level 3 BMW ADS is capable of managing the driving task in lieu of the human driver. Once the BMW vehicle reaches the limits of its ODD, the vehicle will issue a takeover request to the human driver to signal that they should resume control of the driving task. Otherwise, the vehicle will revert to a minimal risk condition, which will bring the vehicle to a stop (discussed in more detail in Section 5. Fallback).

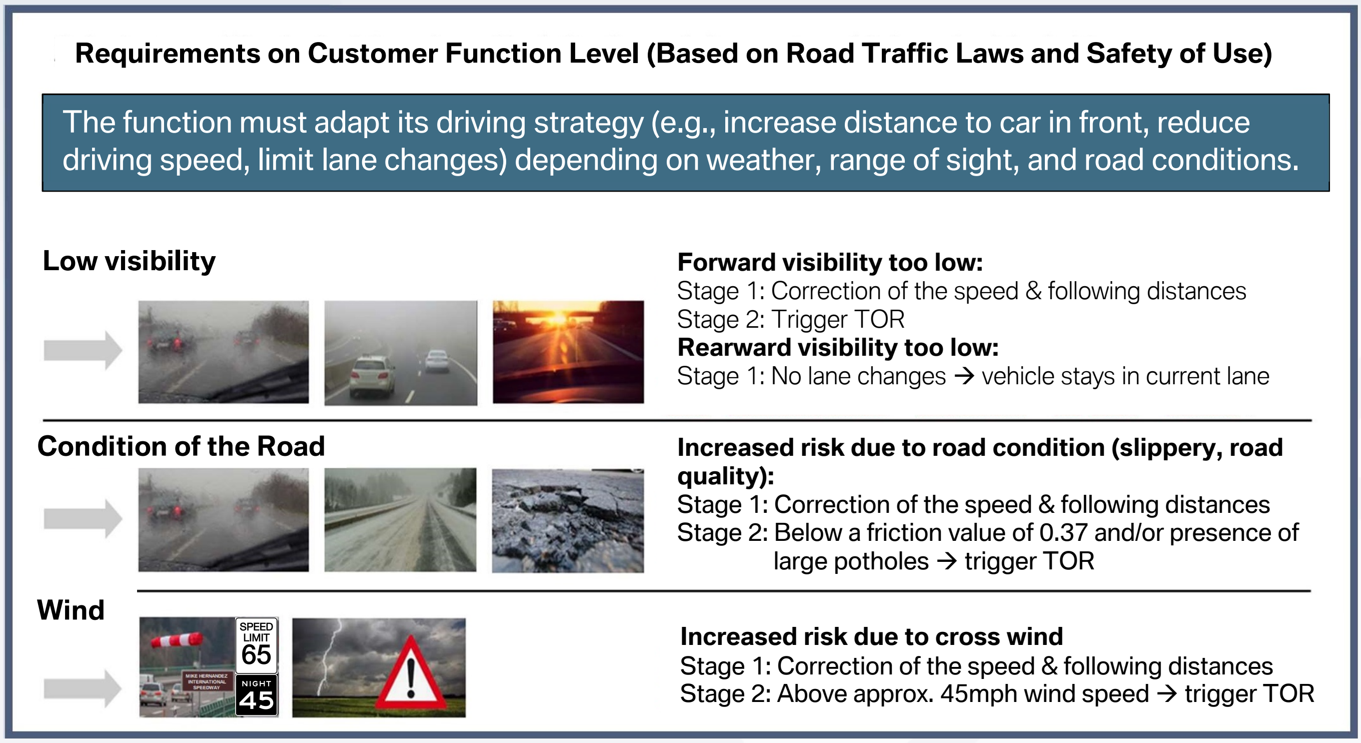
The ODD refers to the conditions under which the SAE Level 3 BMW ADS operates. These conditions include, but are not limited to, environmental conditions like weather and time of day, geographical conditions such as road type and speed range, and legal requirements.

Within its geographical ODD, the SAE Level 3 BMW ADS can only be activated and operate on limited access highways with continuous structural separation from oncoming traffic, no direct crossing traffic or roundabouts. This road type is characterized by a small probability of pedestrians and bicyclists being present. The compliance with these activation conditions will be detected by on-board sensors, for example, the camera system, which is monitoring traffic signs like "highway end", and will also be ensured through information provided by the HD map. The geographical ODD includes geo-fenced boundaries and all applicable traffic rules for the area within these boundaries. Given a variety of factors such as legal requirements, for example, the SAE Level 3 BMW ADS is designed to function at speeds between 0 and 85mph.

Furthermore, the automated vehicle continuously monitors the environmental conditions (environmental ODD) to ensure safe operation under all conditions. For example, the speed of the vehicle will be adapted according to time of day, light conditions, if the roadway coefficient of friction is too small (e.g., if there is snow or ice on the road) or the wind is too strong (see Figure 14).

In the event that the prescribed conditions change in a way that safe driving can no longer be achieved, the system will automatically issue a TOR to the driver if appropriate and initiate a risk mitigation maneuver if no TO by the driver takes place. As an SAE Level 3 system still requires the driver to be available as a fallback-ready user, the system provides a means to detect if the driver is present in the driver's seat with their seat belt fastened and if he/she is able to take over the driving task within a defined time budget (e.g., that he/she is not asleep), see driver readiness monitoring as described in Chapter 1. Human Machine Interface (HMI). If these conditions are not met, the ADS will automatically issue a TOR to the driver and transfer to a minimal risk condition if no TO takes place.

Additionally, a request to take over the control of the vehicle will be sent to the driver if the SAE Level 3 BMW ADS detects any special circumstances on the planned route, such as a wrong way driver or construction zones (details see Chapter 5. Fallback (Minimal Risk Condition)).



Requirements on Customer Function Level (Based on Road Traffic Laws and Safety of Use)

The function must adapt its driving strategy (e.g., increase distance to car in front, reduce driving speed, limit lane changes) depending on weather, range of sight, and road conditions.

Low visibility

Forward visibility too low:
Stage 1: Correction of the speed & following distances
Stage 2: Trigger TOR
Rearward visibility too low:
Stage 1: No lane changes → vehicle stays in current lane

Condition of the Road

Increased risk due to road condition (slippery, road quality):
Stage 1: Correction of the speed & following distances
Stage 2: Below a friction value of 0.37 and/or presence of large potholes → trigger TOR

Wind

Increased risk due to cross wind
Stage 1: Correction of the speed & following distances
Stage 2: Above approx. 45mph wind speed → trigger TOR

Figure 14. Influence of Environmental Conditions on OEDR.

To detect these diverse conditions defining the ODD limits correctly, the input of different on-board sensors is combined with off-board information. Table 4 gives an overview of the sensors and information used during the ODD classification. The functionality of the monitoring systems is ensured via constant self-diagnosis.

Condition	Sensor / Monitoring Principle Example
Driving speed	Wheel speed sensor
Road type	HD map, back end, environment model (fusion of onboard sensors)
Coefficient of friction	Friction map from back end, friction coefficient from environment model (fusion of onboard sensors)
Cross wind	Deviation from planned trajectory, back end
Temperature	Temperature sensor
Road surface and geometry (e.g., inclination, cross slopes, pot holes, etc.)	Environment model (fusion of onboard sensors), HD map
Rain, snow, fog	Environment model (fusion of onboard sensors), rain sensor
Extreme weather conditions	Back end (off-board BMW server)
Driver's status	Interior camera, seat occupancy mat, seat belt buckle, pedal position sensors, hands-on-detection sensor in the steering wheel, steering torque sensor

Table 4. Sensors and off-board information used during ODD classification.

As the BMW Group is constantly improving the quality of its products, it is our goal to expand the boundaries of the ODD over time via "Over the Air" (OTA) updates to enhance safety and the best possible customer experience. Substantial safety-relevant changes to the ODD will trigger an update to this Voluntary Safety Self-Assessment.

4. Federal, State, and Local Laws and Regulations

All BMW vehicles sold in the US are designed to meet applicable federal, state, and local requirements regarding their design, construction, and performance. The production version of the iNEXT will have traditional manual controls, will be capable of being driven like any other BMW, and will be built to meet current requirements. However, since the SAE Level 3 BMW ADS will take over control of the driving task, it will also take into account relevant state and local laws pertaining to vehicle operation, or the "rules of the road" when operating in SAE Level 3 BMW ADS mode. BMW recognizes that regulations for automated driving systems are in the process of being developed. Because of this, we are actively engaging with stakeholders in order to share BMW's approach to ADS and provide input for potential new regulations that will govern the development and deployment of ADS-equipped vehicles into the market. In the interim, BMW is thoughtfully deploying its SAE Level 3 BMW ADS according to the best practices established by relevant industry and governmental organizations. For example, the National Highway Traffic Safety Administration ("NHTSA") has published and updated its guidance for the testing and deployment of ADS in its Federal Automated Vehicle Policy ("FAVP"). BMW submits this Voluntary Safety Self-Assessment pursuant to the recommendation made by NHTSA in the FAVP and subsequent guidance. As regulatory framework conditions may change over time, BMW is equipping its ADS vehicles with Over the Air (OTA) updating capabilities. In this way, the SAE Level 3 BMW ADS are designed to operate in a safe and legally compliant manner well into the future.

Compliance with legal requirements is of the highest importance for the BMW Group. This includes compliance with all homologation requirements as part of the self-certification process and compliance with applicable road traffic laws.

Homologation Requirements

The production vehicle based on the BMW iNEXT is being developed to be driven both as a conventional vehicle and in the conditionally automated SAE L3 driving mode offered by the SAE Level 3 BMW ADS. Since the vehicle will still feature a conventional steering wheel and tradtional controls, all applicable Federal Motor Vehicle Safety Standards (FMVSS) will be met.

The rapid development of ADS is currently outpacing the development of the corresponding regulations. The BMW Group actively works with relevant authorities and stakeholders worldwide to support the development of regulations for ADS. We are also working with industry groups and NHTSA to advance the development of new FMVSS that will (a) streamline innovation for new safety technologies, and (b) advance the safety of highly automated vehicle technology. In the future, new FMVSS and/or changes to existing FMVSS may account for vehicles without conventional controls or conventional seating positions. We welcome these revisions and new standards and will continue to engage with the U.S. Department of Transportation (USDOT) and NHTSA as they seek to prioritize, develop, and implement these standards.

The BMW Group strongly supports the development of federal AV legislation. A national technology-neutral regulatory framework for AVs will help strengthen the existing safety oversight by NHTSA and will complement the iterative work of the USDOT with respect to their AV policy guidance. Furthermore, federal AV legislation will advance these groundbreaking technologies while supporting research and investment in the U.S.

In the meantime, the BMW Group highly appreciates that USDOT and NHTSA have issued guidance for ADS-equipped vehicles in the 2016 Federal Automated Vehicle Policy; the updated 2017 Automated Driving Systems: A Vision for Safety 2.0; the 2018 Automated Vehicles 3.0: Preparing for the Future of Transportation; and the 2020 Ensuring American Leadership in Automated Vehicle Technologies: Automated Vehicles 4.0. These documents provide a framework for the development of safe ADS-equipped vehicles and delineate appropriate federal and state roles in ushering in this new era of personal transportation.

Rules of the Road

Rules of the road are usually set by state and local municipalities. The safe deployment of the BMW Group's conditionally automated SAE Level 3 ADS requires compliance with these rules to facilitate the interaction with conventional road users.

In Level 3, the ADS will perform all operational driving tasks once the SAE Level 3 BMW ADS is engaged, i.e., the SAE Level 3 feature will also be responsible for complying with all applicable rules of the road with respect to the operation of the vehicle while engaged. For traffic laws that are not specifically related to the operation of a vehicle in traffic (e.g., ensuring that cargo is properly secured and child restraints are properly used when required), the driver/fallback-ready user will still be responsible. Compliance with applicable road traffic laws is an important part of the OEDR.

As with other requirements on the behavior of the self-driving system, we program boundaries within the self-driving system to promote compliance with the applicable rules of the road. Which rules of the road are applicable also depends on the ADS' ODD: since our SAE Level 3 BMW ADS is designed to only operate on limited-access highways, special attention was paid to road traffic laws that are applicable in highway situations. As such, our SAE Level 3 BMW ADS is designed to react appropriately to street signs, following distances, and speed limits.

Like any human, an ADS will under certain external conditions need to prioritize the rules of the road in order to maintain traffic safety. One example is having to cross a solid lane marking (e.g., when two highways merge) in order to avoid a crash.

During our product development process we will check every route that the SAE Level 3 BMW ADS system is designed to operate on (see Chapter 11: Validation & Verification) in advance of the launch of the SAE Level 3 BMW ADS. To that end, the BMW Group will deploy test vehicles equipped with sensors and cameras to collect data that will be used to validate and refine the vehicle software that will operate its ADS platform. Part of the validation process will be to ensure that all vehicle systems and software working together will be able to operate the vehicle within its ODD in accordance with the relevant road traffic laws.

Additionally, our HD maps are enriched with additional information, such as region-specific traffic signs and speed limits. To account for regional differences in road traffic laws, the ADS accesses a database with all applicable road traffic laws based on its current position (geo-fencing).The traffic signs and signals detected by our onboard sensors will continuously be cross-checked against the map data. Inconsistencies will be investigated and, if needed, the map data will be updated accordingly.

We also recognize that the "rules of the road" often change over time. Therefore, the BMW Group will design its automated vehicles to accommodate software updates (both in the dealership and via OTA) to its ADAS and ADS when required due to changes in legal requirements. We will have an assessment team responsible for ongoing monitoring of potential changes in the laws and will participate in timely regulatory engagement and advance planning with an implementation team to ensure that applicable deadlines are met.

5. Fallback (Minimal Risk Condition)

For SAE Level 3 systems, a receptive "fallback-ready user" should be ready to take over the driving task when approaching an ODD exit or if there is an ADS failure. In the case of the SAE Level 3 BMW ADS, the production version of the BMW iNEXT vehicle will transition control of the vehicle to the human driver when either the vehicle determines that the conditions detailed in Chapter 3. Operational Design Domain are no longer met or if there is a failure in the ADS system that prevents the SAE Level 3 BMW ADS from fully maintaining control of the driving task. Upon system fallback, the SAE Level 3 BMW ADS will send a cascade of warnings to the human driver in the form of visual, auditory, and haptic alerts with increasing levels of urgency. This warning cascade comprises the SAE Level 3 BMW ADS takeover request and utilizes the HMI as detailed in Chapter 1. Human Machine Interface (HMI). In the event that the fallback-ready user (i.e., the human driver) is not receptive to the warning cascade of the takeover request, the SAE Level 3 BMW ADS will perform a risk mitigation maneuver. This simply means that the vehicle will take an action up to and including bringing the vehicle to a safe stop on the hard shoulder or in the traffic lane if reaching the shoulder is not feasible, for example during heavy traffic.

Due to the system and ODD limitations (geographical and/or environmental), situations might occur where the continued safe operation of the ADS may no longer be possible.

This can be caused by:

- Approach of the ODD limits (Chapter 3. Operational Design Domain (ODD));
- Malfunction within the ADS detected by continuously monitoring relevant vehicle data;
- Operation in a degraded state detected by sensor self-diagnosis.

The user of an SAE Level 3 system always remains the fallback-ready user. Under the conditions described above, the SAE Level 3 BMW ADS will request that the fallback-ready user achieves a minimal risk condition or take over the driving task. If the driver does not respond to this request within a defined time period the system will perform a risk mitigation maneuver.

During the TO process, the ADS will continue to perform the driving task, possibly with a limited function range (e.g., without performing lane-changes in the case of a failure of a rear view sensor).

To support the user during the TO process and ensure continued safe driving, the ADS continuously monitors the fallback-ready user and assesses his/her TO readiness at all times. The characteristic of the warning cascade adapts to the urgency of the situation. The warning cascade was developed using different modalities and various human factor studies with diverse methods to ensure appropriate driver reaction and support for the driver (see Figure 15).

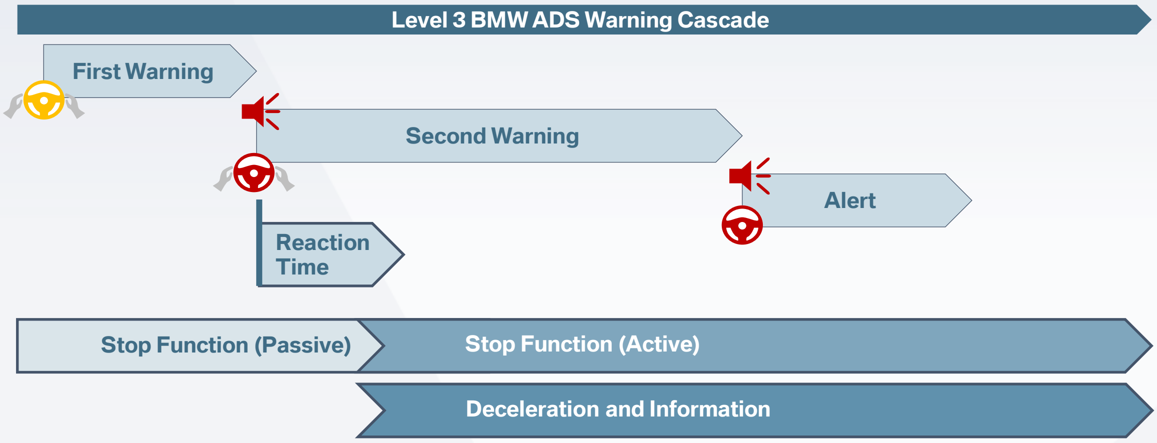
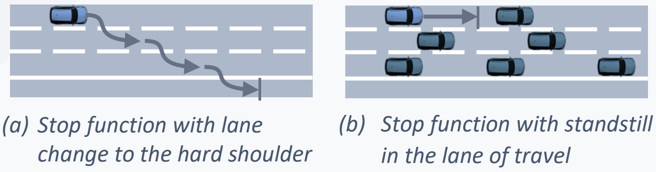


Figure 15. Process for Risk Mitigation Maneuver.

While approaching the ODD limits, the warning cascade consists of a preliminary/cautionary TOR (first warning) and, after a defined reaction time has elapsed, an imminent TOR (second warning). With the issuance of the first warning the SAE Level 3 BMW ADS symbol switches from green to yellow. Additionally, the HMI shows hands that grab the steering wheel. If the driver does not follow the request, the second warning appears and the color of the steering wheel changes to red. This visual warning is accompanied by an acoustic signal. In a third stage, an alert is given by displaying a blinking red steering wheel and an acoustic signal.

In the unlikely event that the fallback-ready user does not comply with the TOR, a risk mitigation function has been implemented. In this case, the vehicle tries to get to a minimal risk condition under consideration of the current traffic situation, the remaining functional capabilities of the system and the criticality of the situation. The risk mitigation strategy may vary depending on these conditions, and depending on the situation may consist of stopping on the shoulder of the road or of stopping within the current lane (e.g. in a traffic jam or if failed sensors do not allow a safe lane-change). The BMW vehicle will find a situationally adequate solution that minimizes the risk for other road users. Once the vehicle has reached a safe position, the hazard lights are turned on and an emergency call (eCall) is triggered.


(a) Stop function with lane change to the hard shoulder

(b) Stop function with standstill in the lane of travel

Figure 16. Different Implementations of the Risk Mitigation Maneuver.

If the activated Level 3 BMW ADS has detected that the vehicle is in imminent danger of colliding with another road user or obstacle with insufficient lead time to give the control back to the driver, the ADS decelerates up to a full standstill if necessary and/or performs an automatic evasive maneuver on its own without additional input from the driver.

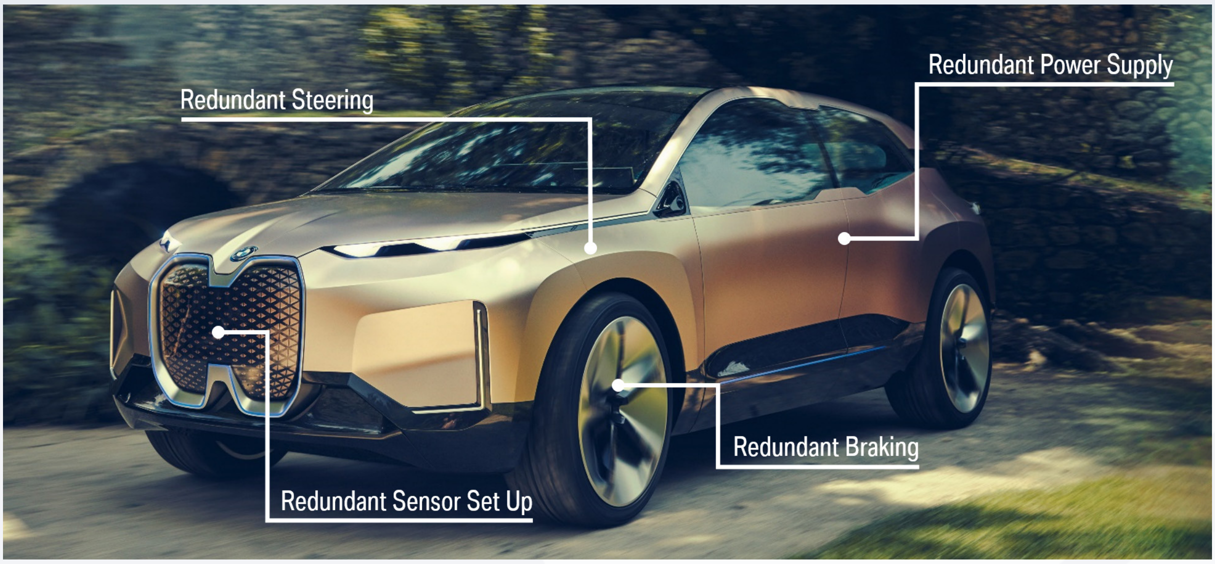


Figure 17. Redundancies in the BMW iNEXT concept vehicle.

Furthermore, the frequency of triggering the fallback is essential when evaluating risks. The BMW Group has implemented diverse sets of safety measures to reduce this frequency as much as possible. Amongst others, this includes measures to keep the driver ready for a TO (see Chapter 1. Human Machine Interface (HMI)), to manage the time budget for a safe TO, and to implement a high level of functional safety and redundancy (see Chapter 9. System Safety). All safety systems that are necessary to safely operate the vehicle have backup systems (see Figure 17).

Just as any other function, the SAE Level 3 BMW ADS fallback will be developed according to the high standards of product development at the BMW Group, including functional safety, safety-in-use, as well as verification and validation.

6. Crashworthiness

Passive safety remains important to any vehicle design whether automated or not. Additionally, the production vehicle based on the BMW iNEXT will be introduced as a “dual use” vehicle capable of being driven using traditional manual controls as well as automated in SAE Level 3 BMW ADS mode. As such, the passive safety development of the iNEXT does not differ from the traditional passive safety development process for any other BMW vehicle and holds the same high level of crashworthiness found throughout the BMW lineup. Specifically, BMW takes into account the design requirements set forth in the Federal Motor Vehicle Safety Standards (FMVSS) as well as considering crashworthiness assessment tests such as the USDOT’s New Car Assessment Program (NCAP) and the Insurance Institute for Highway Safety (IIHS) Top Safety Pick award. Because the SAE Level 3 BMW ADS requires the fallback-ready user to be receptive to taking back control of the driving task, the production version of the BMW iNEXT concept vehicle maintains conventional seating positions (i.e., no swiveling seats). Likewise, the vehicle maintains the same traditional safety mechanisms (seat belts, airbags, etc.) for all other passengers such that the protection is afforded regardless of the mode in which the vehicle is being driven. Lastly, the production vehicle will incorporate pedestrian protection measures within the vehicle, both active (automatic emergency braking) and passive (energy absorbing bumpers/hood).

The safety of our customers is of utmost importance to the BMW Group. Therefore, the topic of “Crashworthiness” is a top priority during the product development process of any new vehicle.

Based on the V-model (see Figure 18), at the beginning of the development process the crashworthiness requirements for the new vehicle are defined. During the definition of the requirements we consider state of the art research results, common standard tests, internal crash scenarios based on accident research, and internal experience, not to mention compliance-based testing and tests suggested by world-wide consumer interest organizations.

These requirements on the vehicle level are translated into requirements for the sub-system and in a next step into requirements for the individual components. In the second half of the process the components, the sub-systems, and the complete vehicle requirements are validated.

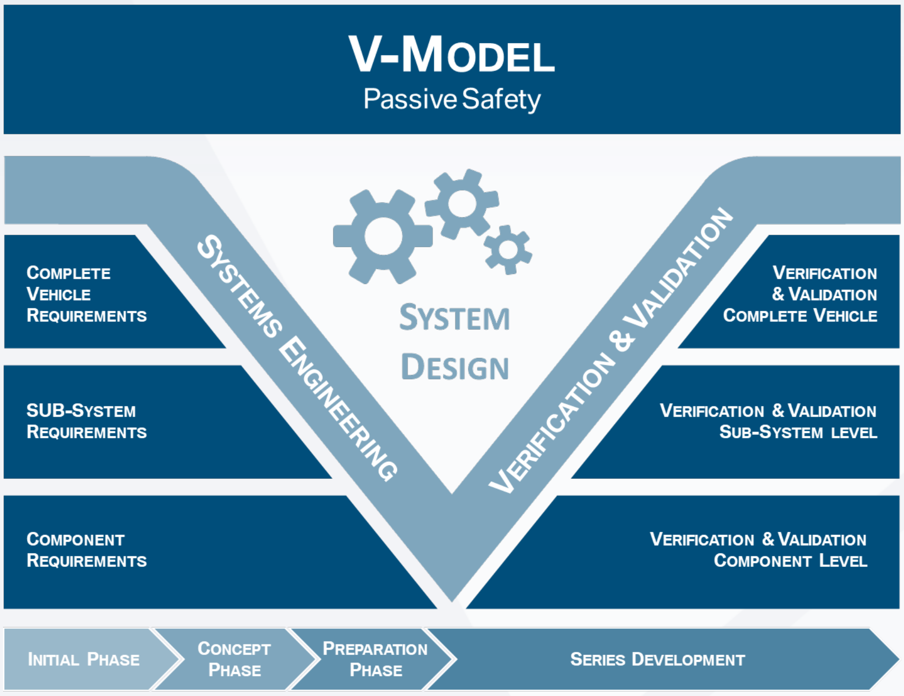

V-Model
Passive Safety
Complete Vehicle Requirements
Sub-System Requirements
Component Requirements
Systems Engineering
System Design
Verification & Validation
Verification & Validation Complete Vehicle
Verification & Validation Sub-System level
Verification & Validation Component Level
Initial Phase
Concept Phase
Preparation Phase
Series Development

Figure 18. Crash Validation.

Occupant Protection

The series production version of the BMW iNEXT can be optionally equipped with the SAE Level 3 BMW ADS. Since all BMW vehicles are tested to fulfill or exceed their market's safety regulations including the FMVSS, as well as take into account consumer tests (NCAP) and the BMW Group's internal standards, both the ADS and non-ADS vehicle will protect occupants in the same way. Since the SAE Level 3 vehicles are per definition "dual use" vehicles, the occupant protection will fulfill the same regulatory requirements that all conventional passenger cars are required to fulfill.

The BMW Group has decades of experience developing vehicles to meet the requirements of FMVSS, and the production version of the BMW iNEXT concept vehicle will take advantage of that experience.

To provide the same level of occupant protection in ADS and non-ADS vehicles, both variants of vehicles are equipped with the same standard crash sensing system.

Additionally, the SAE Level 3 BMW ADS system is equipped with further sensors used for the OEDR. These additional sensors are concentrated on observing what happens outside of the vehicle. The increased sensing capabilities contribute to a primary advantage of ADS-equipped vehicles– the ability to reduce the number of critical situations that lead to accidents. The BMW Group will continue to investigate the potential benefits of these new sensors regarding occupant protection improvements and potential enhancement of pre-crash algorithms.

While using the SAE Level 3 BMW ADS, the user must always be prepared to fulfill their role as a fallback-ready user within a short transition period and therefore the changes to standard seating positions and interior configurations are designed to allow the driver to quickly take back control when necessary. Therefore, conditional automation precludes offering revolutionary seating positions. Before they are implemented, even minor adaptations to the seat or steering wheel position to provide mode awareness are evaluated as to their effect on the occupant loads in the case of a crash.

One of the activation requirements of the SAE Level 3 BMW ADS is that the driver's seat belt be fastened. The production version of the BMW iNEXT concept vehicle will be equipped with rollover sensors as well as inertial and pressure sensors to trigger restraint systems and to shut down the high voltage electric system. These mechanisms are discussed in more detail in Chapter 7. Post-Crash Behavior.

Regarding the safety of children, the production BMW iNEXT vehicle will meet or exceed requirements of U.S. safety regulations and take into account NCAPs worldwide. This includes child restraint tether locations on the outboard positions of the rear seat, as well as installing child seats for evaluation in some full vehicle crash tests. Child seat detection is also integrated into the front passenger seating position as per the FMVSS 208 standard.

Structural Integrity

Structural Integrity is an internal requirement applied to all crash tests in the development of a BMW Group vehicle. These crash tests include official regulations from the U.S., ECE, Japan, Korea, China, consumer organization tests worldwide, as well as the BMW Group's own internal tests. Given the number and variety of these tests, the resulting vehicle structure is designed to balance the energy distribution resulting from a crash and the load paths of the vehicle, which work to distribute forces from many different directions and angles. As a vehicle developed for the worldwide market and therefore subject to a large number of regulatory crash tests, the production BMW iNEXT vehicle will have a robust structural layout.

Before the first crash test is performed in the BMW Group's facilities, a virtual version of the production BMW iNEXT vehicle will have already experienced countless front, side, and rear crashes.

Whether from the FMVSS 200 or 300 series standards or from consumer organization tests, multiple phases of prototype development serve to verify and validate the simulations (see Figure 18). Although the virtual testing offers valuable insights, we also rely on physical crash tests: before the vehicle has reached its first customer, over 100 full vehicle crash tests have been performed. Destructive component testing delivers some of the answers to improve the accuracy of the virtual world.

FMVSS 208: Occupant Crash Protection (Front Crash)

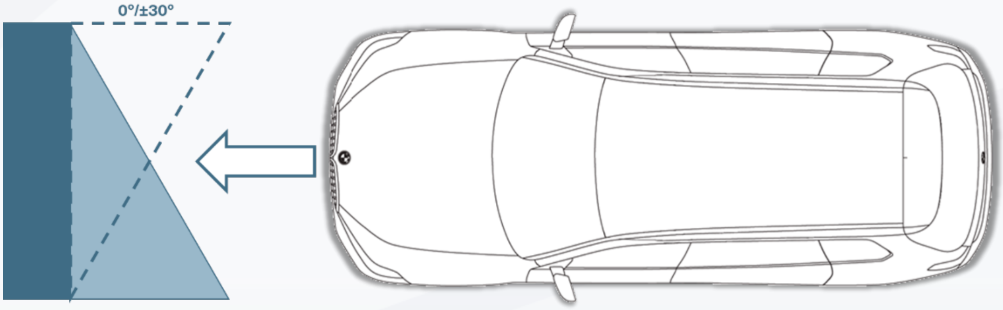


Figure 19. Frontal Crash.

FMVSS 301/305: Fuel System Integrity and Electrolyte Spillage and Electrical Shock Protection (Rear Crash)

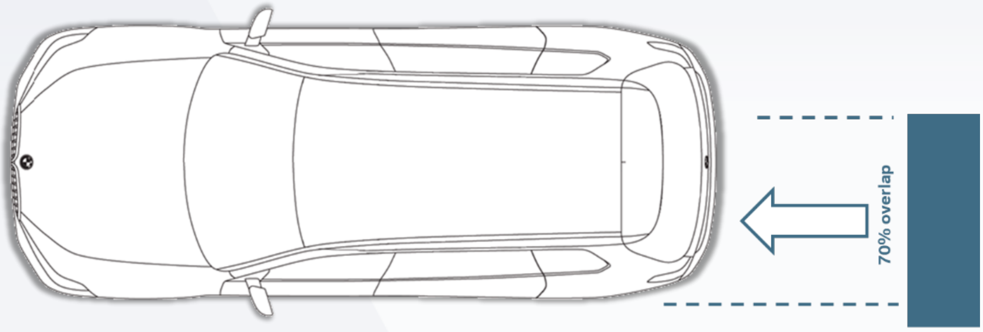


Figure 20. Rear Crash.

FMVSS 214: Side Impact Protection (Side Crash)

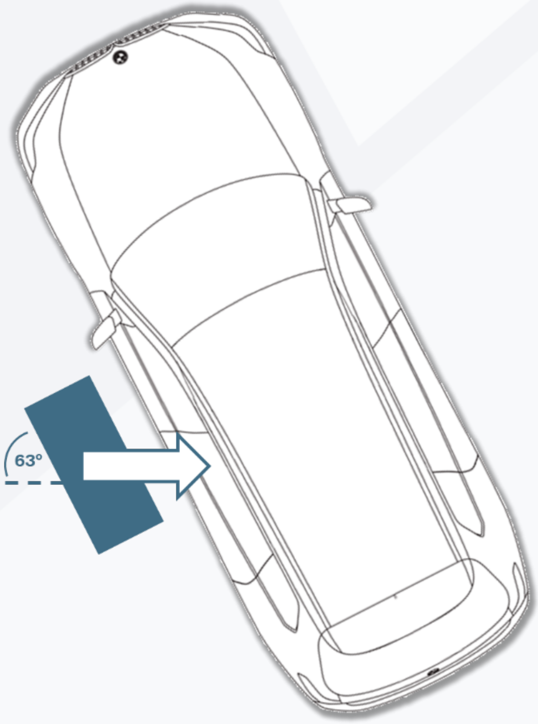


Figure 21. Side Crash.

Protection of Other Road Users

The production BMW iNEXT vehicle is being developed with measures to protect pedestrians and other vulnerable road users as well as other road vehicles. Automatic Emergency Braking (AEB) and Pedestrian AEB will be standard on the iNEXT in the U.S. market and is designed to detect and react to pedestrians, which has been shown to be effective in reducing the overall number accidents. These systems are active even when the ADS is not.

Active Safety

Safety assistance functions play an important role with regard to crashworthiness: they are the first line of defense by helping to avoid crashes and/or mitigating the crash severity. Fig. 2 lists the active safety functions currently available in BMW series vehicles.

Through a field effectiveness evaluation, the effectiveness of BMW's active safety functions currently in the market has been quantified. Evaluating BMW vehicles produced between 2014 and 2017, vehicles equipped with both autonomous emergency braking and lane departure warning were 23% less likely to be involved in a crash with the deployment of at least one restraint system than those not equipped. Similarly, other ADAS safety assistance functions that were previously listed in Figure 2 (Introduction) present additional opportunities to avoid or mitigate crashes in the BMW iNEXT.

In 2016, the BMW Group signed a Memorandum of Understanding (MoU) for the implementation of AEB, which offers a combination of forward collision warning and crash imminent braking. In the MoU, the BMW Group commits to equip at least 95% of all light duty vehicles manufactured for sale in the United States with AEB. The system can help to prevent accidents with stationary vehicles or vehicles driving ahead, as well as with crossing pedestrians. In many cases, if a crash cannot be prevented, the system helps to reduce the impact speed.

In many critical situations, the driver is alerted by a two-stage warning (early warning and acute warning) regarding a possible collision, see Figure 22. Coordinated with the acute warning, the vehicle can be decelerated by the system to a maximum of full deceleration. Depending on the situation, the vehicle can brake to a complete standstill.

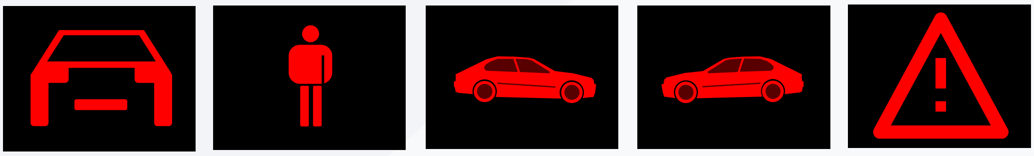


Figure 22. AEB Warning Signals.

Additionally, the different stages of the warning phase are communicated to the driver:

- Red Illuminated Vehicle: Advance warning—first level warning, e.g., in the case of an anticipated danger of collision or a critically short distance to a vehicle driving ahead.
- Red Flashing Vehicle with Acoustic Signal: Acute warning—warning in the event of imminent collision danger if the vehicle approaches another object at a relatively high differential speed.

Spicer, R. et al (2018, December). Field effectiveness evaluation of advanced driver assistance systems. Traffic Injury Prevention, 19:sup2. Retrieved from: https://doi.org/10.1080/15389588.2018.1527030

Table 5. ADAS effectiveness study document.

7. Post-Crash Behavior

The production version of the BMW iNEXT concept vehicle will be capable of performing a self-diagnosis, including after a crash. If the vehicle determines that the functionality of the SAE Level 3 BMW ADS cannot be maintained in a safe manner, a takeover request will be issued to the human driver and reactivation of SAE Level 3 BMW ADS will no longer be possible. For more severe crashes, the production iNEXT vehicle will follow a similar procedure as other BMW vehicles. More specifically, in crashes where airbags have been deployed, mechanisms are in place to unlock the doors, disconnect the high voltage battery, activate the hazard lights, engage the brakes to help reduce the potential of being engaged in a secondary collision, and to initiate an emergency call to the BMW call center.

One major goal of the SAE Level 3 BMW ADS while active is to reduce the likelihood of severe crashes compared to manual driving through a reliable and defensive driving strategy. If the system predicts an imminent crash that cannot be avoided by an evasive maneuver (e.g., because of other traffic participants), active protection systems are preconditioned to reduce crash severity.

The crash detection system employed in both ADS equipped as well as conventional BMW vehicles is the same, for example, inertial movement/acceleration, pressure, and roll-over sensors. This means the detection of crashes with a high probability for occupant injury have been given priority. Though the system may also detect lower severity crashes, the detection of, and response to these crashes falls to the responsibility of the fallback-ready user of an SAE Level 3 ADS. As the appropriate system response depends on the severity of the impact, the production BMW iNEXT vehicle employs complementary and overlapping strategies depending on the severity.

Self-Diagnosis

As a matter of principle the ADS system is constantly performing self-checks and validations to ensure safe operation. This includes (but is not limited to):

- Sensor performance (e.g., misalignment, dirt)
- Availability and integrity of E/E-components (e.g., power supply)
- Mechanical integrity (e.g., tire pressure, chassis alignment)

If vehicle components are damaged such as during an impact, the system will attempt to perform the specified post-crash behavior by means of the redundant fallback components described in Chapter 9. System Safety. This self-diagnosis also takes effect if the impact is too low for the inertial sensors.

Reactivation of the function

A reactivation is only possible if all checks are passed. These checks occur independently of a low or high severity impact, after a repair, or simply while driving. These checks are not limited to being performed only after a crash.

If a crash has impaired any component (e.g., damaged or misaligned sensor) the fault will be detected by the system itself and a reactivation of the SAE Level 3 BMW ADS will not be possible. In any case, after a detected crash a restart of the vehicle will be necessary to perform all checks and re-enable the SAE Level 3 BMW ADS if there is no relevant damage and the checks deliver positive results.

As for any conventionally driven vehicle, the driver of a SAE Level 3 vehicle still has the obligation to ensure roadworthiness of the vehicle after a crash.

After maintenance or repair activities, no specific activities have to be performed. Safe activation and operation are ensured by the self-diagnostics discussed above. Any repair or maintenance activities that have not been performed according to the BMW Group's repair specifications can lead to failed self-diagnostics.

Post-Crash (Including Airbag Deployment)

In addition to the above process, after a crash is detected by the inertial sensors, the ADS will execute the following steps:

1) The driver is alerted and a TOR is issued (see Chapter 5. Fallback (Minimal Risk Condition)).
2) If the driver does not or is unable to resume driving, a risk mitigation maneuver is performed taking into account damage to the system, see Chapter 5. Fallback (Minimal Risk Condition))
3) The post-crash mechanisms in place for conventional (non-ADS) driving are executed.

Example Post-Crash mechanisms

1. Automatic unlocking of the doors.
2. High voltage battery disconnection.
3. Activation of the hazard warning lights.
4. Triggering/Initiation of post-crash AEB.
5. eCall (see below).

ADS onboard power system

A further post-crash measure of the SAE Level 3 BMW ADS is the disconnection of its onboard power system. As discussed in Chapter 9. System Safety, the BMW Group sees the necessity for a certain level of redundancy of the SAE Level 3 BMW ADS onboard system. In case of a fault in both onboard power systems a third rudimentary channel takes over to allow for reaching a minimal risk condition.

The deactivation of the SAE Level 3 BMW ADS system is executed via the vehicle communication buses. The crash notification opens a semiconductor switch in the ADS battery and disables/switches off the ADS onboard power system.

Emergency call (eCall)

Under certain conditions, for instance if the airbags are triggered, an emergency request for the automatic emergency call is initiated immediately after a crash of corresponding severity. The automatic collision notification is not affected by pressing the SOS button.

The eCall LED flashes green when the connection to the BMW Response Center has been established. The BMW Response Center then makes contact with the occupants and takes further steps to help them.

Even if the occupants are unable to respond, the BMW Response Center can take further steps to help them under certain circumstances. For this, data such as the current position of the vehicle (if available) is transmitted to the BMW Response Center which serves to determine the necessary rescue measures.

8. Data Recording and Sharing

All BMW vehicles come equipped with Event Data Recorders (EDRs), which, as regulated by NHTSA, record relevant information in a crash much like a “black box” used in aviation. In addition to the traditional EDR, the production version of the BMW iNEXT concept vehicle will be equipped with extended EDR features as well as additional data collecting equipment to record various data points that can be securely sent to a BMW back end to be used for future product improvements. Data privacy of our customers is of utmost importance. Accordingly, BMW follows all applicable data privacy laws and guidelines, including the California Consumer Privacy Act and the Alliance of Automobile Manufacturers Privacy Guidelines. In alignment with these standards, BMW offers its customers the opportunity to opt out of the data collection used for product improvement. In the event of a crash, some data points will be stored by the vehicle to potentially be used for crash reconstruction and analysis. Data stored on the EDR is encrypted and is only accessible with the express permission of the vehicle owner or by court order as applicable. Data that is shared to the BMW back end for product improvement purposes will not be personally identifiable.

Motivation and overview

All BMW vehicles equipped with highly automated driving technology such as the SAE Level 3 BMW ADS have a number of data recording capabilities to allow for an accurate reconstruction of crash-related events. These events can be divided into two categories:

- Direct involvement (e.g., crash, near-crash, or avoided crash situations);
- Indirect involvement (e.g., a secondary collision caused by a maneuver of the vehicle while driving in automated mode, especially if the driver was not in “the loop”, i.e., the driver did not notice the secondary collision since he/she was engaged in other allowed tasks while the SAE Level 3 BMW ADS was engaged).

For this purpose the conventional Event Data Recorders (EDR) compliant with the regulatory standards for data recording during crash events will be complemented by an additional robust data storage device for logging information from onboard systems, the driving model, and environmental data. This data logging system has self-diagnostics, and stores data securely, protecting it against loss, manipulation and unauthorized access and keeps the data intact even in the event of a crash. The data logging system stores a predefined data set from the vehicle including sensor data (this may include camera data as well), vehicle actions (OEDR), any degraded behavior, and malfunctions (e.g., any fault triggering a TOR and/or a transition into a minimal risk condition and other information needed for any crash-related event reconstruction).

Secure data storage on- and off-board the production BMW iNEXT vehicle is maintained in compliance with applicable privacy laws and regulations, e.g., federal legislation such as the Privacy Act and state laws such as the California Consumer Privacy Act. Additionally, as a member of the Alliance of Automobile Manufacturers (now Alliance for Automotive Innovation), the BMW Group follows the “Automotive Consumer Privacy Protection Principles,” first developed in 2014 and updated in 2018.

In addition to the vehicle data that is recorded for legal/liability reasons, data collection is part of the continuous improvement of the SAE Level 3 BMW ADS, for example to increase map quality, identify changes on the road, inform other cars about critical situations, etc. This data is used during product development to improve quality of all kinds of features for the customer. To this end, relevant data is sent to a secure back end and provided to the development department for further analysis. Customers are informed about these data collection activities and can decide to switch off the logging functions if they choose not to support the development of these features. The data helps, amongst other things, to understand the usage of the functions and to develop improvements which are shared with the whole fleet after being thoroughly validated.

Data Recording

(a) Levels of data recording

Data storage in the Event Data Recorder is divided into several segments depending on the level of automation:

- Basic EDR: Basic information on the crash-related event for reconstruction of the crash algorithm,
- DAS EDR: Influence of the Driver Assistance Systems (DAS) on the crash-related event, and
- HAD EDR: Influence of the Highly Automated Driving (HAD) SAE Level 3+ System on the crash-related event.

The legal/liability-relevant crash data are stored in these EDR segments as safely as possible in crash-resistant, long-term memory storage.

(b) Recorded data

In the case of a crash, only data that is required by law and data that is necessary for crash reconstruction are stored in the vehicle.
This includes the following data:

- Vehicle and passengers status: indicators, warning lamps, occupant status (seat occupancy, belt status, seat position), VIN, etc.
- Restraint system status: deployed airbags, seat belt tensioners, etc.
- Crash dynamic data (from t = -100ms to t = 300ms): acceleration values (along x-, y-, z-axes), delta-v (longitudinal and lateral, vector difference between pre-impact vehicle, velocity and post-impact vehicle velocity), yaw rate, yaw angle, etc.
- Pre-crash phase data is stored in the Basic EDR (from t = -5s to t = 0s): vehicle velocity, accelerator pedal position and brake pedal activation, steering angle, rpm, ABS, GPS position and time, mileage, turn signal, hazard warning lights activation, DSC interventions/ status, etc.
- Pre-crash phase data is stored in the DAS EDR (from t = -12s to t = 0s): Advanced Driver Assistance Systems (ADAS) functional status, warnings, Hands On Request (HOR) / Take Over Request (TOR), Hands On (HO) / Take Over (TO), Minimal Risk Maneuver, vehicle intervention in longitudinal and/or lateral guidance, etc.
- For SAE Level 3 ADS and above, the HAD EDR stores pre-crash data up to 30s prior to the crash.

Without activation of the SAE Level 3 BMW ADS by the driver, no data regarding the SAE Level 3 BMW ADS will be stored. Select driving data with regard to the ADS (SAE Level 3 and above) is recorded and stored in the vehicle for up to 3 months and then automatically overwritten (ring buffer).

Data recording in long-term memory occurs when the vehicle reaches the following trigger threshold conditions:

- Avoided crash: avoidance of an impact caused by an intervention of an AEB (without damage to the vehicle).
- Near crash: change in vehicle velocity in the X-axis or Y-axis direction that is not less than 5mph within a 150ms interval (without deployment of a restraint system device).
- Crash: deployment of an airbag or other restraint system device (e.g., belt tensioner).

The recorded data in long-term memory will be locked from further overwriting only in the case of a crash with deployment of an airbag or another restraint system device. Otherwise the recorded data can be overwritten.

(c) Data retrieval

Data is stored in the vehicle and can be retrieved exclusively by court order or by request of the vehicle owner (during the period of ownership) over the OBD port and/or directly from the event data recorder component (airbag control unit). Remote data retrieval has not been implemented. Legally mandated data can be retrieved with available readout tools. All stored data is encrypted in each of the EDR systems.

Data Collection

(a) Basic principles

In the addition to the EDR systems, the vehicles are equipped with an infrastructure to collect data on demand, for example, when a function is used. Some functions, like emergency call or autonomous driving functions, need a back end connection to send and receive data as part of their functional concept. A very well-known feature used by this communication channel is traffic information on the map and the map itself. For the safety of AD, it is helpful when cars involved in critical situations inform other cars close by so that they are able to react swiftly. This is currently implemented in BMW vehicles to inform other BMW drivers of hazardous traffic conditions for example.

Additionally, data from the vehicle is needed to improve the quality of functions, especially in unusual driving situations. If such an event should occur, a set of data needed for analysis is sent to the back end. Trigger conditions and related data are defined during development but can be modified during the data collection process in order to obtain relevant information.

(b) Data protection and security

Data collected and sent to the back end is treated with care to fulfill all legal requirements for data protection. This includes encrypted transfer between vehicles and the back end as well as regular assessments of the whole data chain through final storage. The BMW Group has established an internal data protection assessment process to ensure data protection and security of all data recording and processing activities of vehicle specific data. Changes in data processing will lead to an updated data protection assessment.

(c) Pseudonymization

Pseudonymization of data is an important step between receiving data from the vehicle and storing the data. In general, no personal data are needed. Therefore, we only record greyscale image data and reduce the resolution to a required minimum. BMW will not use any data collected in the SAE Level 3 scenario to identify any persons. Any person that is, for example, captured on video is simply classified as a “moving object in traffic”.

U.S. Department of Justice. (1974). Privacy Act.
California State Legislature. (2018) California Consumer Privacy Act of 2018.
Alliance of Automobile Manufacturers, Inc. and Association of Global Automakers, Inc. (2018). Automotive Consumer Privacy Protection Principles.

Table 6. Relevant Data Recording and Sharing Documents.

9. System Safety

The production version of the BMW iNEXT concept vehicle will be, in general, no different with regards to the development of its systems to any other BMW vehicle. In other words, BMW follows the same processes to ensure system safety for all its vehicles equally. These processes include the international ISO standards for functional safety (ISO 26262) and safety of the intended function (ISO/PAS 21448) as well as other robust internal BMW processes. The functional safety process requires a hazard analysis and safety risk assessment, which assigns an attribute known as the Automotive Safety Integrity Level (ASIL). For highly safety relevant functions, specific redundancies have been built in so that failures of these systems do not create an unreasonable safety risk. This scenario can be broken up into three categories: “fail operational” where one sensor may fail but the redundant sensors can continue safe operation of the system; “fail degraded” when a failure occurs, the system is still operational but may not have full capabilities; and, “fail safe” in which the system is no longer operational but the failure does not create an unsafe condition. An example of the fail safe operation in the SAE Level 3 BMW ADS is the risk mitigation maneuver discussed in Chapter 5. Fallback (Minimal Risk Condition)). As improvements to the SAE Level 3 BMW ADS are developed, a robust update process becomes critical. The iNEXT production vehicle will be deployed with Over the Air (OTA) update capabilities. These software updates follow industry best practices in their development, validation, and deployment strategies to allow for timely delivery to vehicles in the field.

The BMW Group has a long history of safety innovation through its development processes, which are based on a systematic approach for achieving System Safety.

Design and Validation Process

Over the past years, an increasing number of advanced functionalities have been introduced in vehicles. These advanced systems heavily depend on sensing capabilities, the processing of complex algorithms, and their actuation via electrical and/or electronic (E/E) systems.

BMW vehicles are built to have a high level of robustness and reliability. This is only possible because robust design is an integral part of the BMW Group’s design verification and validation processes. For safety-relevant systems this is of the utmost importance.

To ensure the highest possible robustness of our processes and thus the safety of our products, we have incorporated both external and internal safety standards. The BMW Group’s design process consists of the application of ISO 26262 Functional Safety, ISO/PAS 21448 Safety of the Intended Function (SOTIF) and a number of in-house processes including, but not limited to the development procedures framework “idea to offer” and the whole vehicle electric/electronic integration processes.

Vehicle safety is “the absence of unreasonable risks that arise from malfunctions of the E/E system” (ISO 26262). ISO 26262 further describes a Hazard Analysis and Risk Assessment: the Hazard Analysis and Risk Assessment focuses on potential risks that arise from a component malfunctioning. Based on this assessment, high-level safety goals to mitigate these risks can be defined. Furthermore, ISO 26262 contains requirements and recommendations to prevent and mitigate systematic failures and random hardware failures that could have an impact on the realization of the safety goals.

Even if a system relying on sensors to identify its surroundings is free from any faults addressed in ISO 26262, the intended functionality or the system's performance limitations can cause potentially hazardous behavior. This leads to the definition of SOTIF as the absence of unreasonable risk due to these potentially hazardous behaviors related to such limitations. One key safety element is to ensure the correct understanding of the ADS by its user, which is discussed in more detail in Chapter 12. Consumer Education.

All of these safety standards rely on a basic safety concept: their goal is to eliminate non-acceptable risks. ISO 26262 provides helpful guidelines for the initial design of a safe ADS to meet this goal. The BMW Group therefore incorporates the "risk based approach" as defined by ISO 26262 consistently throughout the product development process.

Figure 23 shows how the definition of risk reduction methods (Automotive Safety Integrity Level (ASIL) according to ISO 26262) can be employed.

The standard distinguishes five different classifications: QM, ASIL A, ASIL B, ASIL C and ASIL D. QM signifies that ISO 26262 does not need to be applied in addition to the necessary standard quality measures. The highest integrity requirements are classified as ASIL D: this level signifies that in case of a malfunction the potential for severely life-threatening or fatal injury is likely. ASIL D therefore sets the highest threshold to make sure that the dependent safety goals are appropriate and have been implemented adequately.

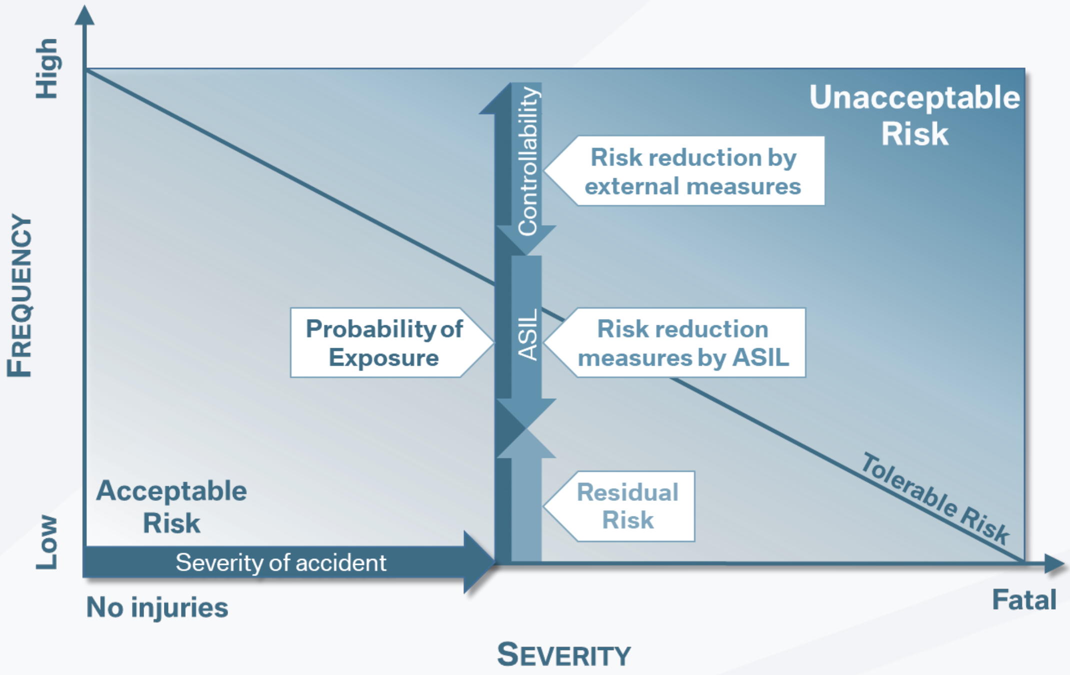


Figure 23. Reduction of the Tolerable Residual Risk based on ASIL.

The complexity of automated driving functions in combination with the possibility of driver intervention even at high levels of automation (SAE Level 3+) increases the necessity to ensure the safety of a function (without system defects) and to derive appropriate safety measures. Therefore, the BMW Group implements the ISO/PAS 21448 SOTIF standard also for SAE Level 3+ functions. The necessary "evidence" is created through field testing and validation as described in Chapter 11. Verification and Validation (V&V).

If certain system safety aspects cannot be covered by the application of the safety standards described above, the BMW Group incorporates elements from other safety standards and best practices from other industrial sectors, namely IEC 61508. IEC 61508, the general basis of ISO 26262, can help to address availability topics and the corresponding architecture models.

Part of the safety evaluation of automated driving systems based on ISO 26262 is also the safety evaluation of non-vehicle elements such as the high definition (HD) map. The HD map used in the SAE Level 3 BMW ADS delivers a mechanism to provide the SAE Level 3 BMW ADS with information on the upcoming road segment. This information is compared with the geographical ODD requirements of the SAE Level 3 BMW ADS and is a necessary prerequisite for the activation of the SAE Level 3 BMW ADS, making the map input safety-relevant. Therefore, the HD map is also validated as part of the full vehicle's validation approach.

Hazard Analysis and Safety Risk Assessment

The hazard analysis and safety risk assessment is rigorously implemented according to ISO 26262 System Safety. For ISO/PAS 21448 SOTIF as discussed above this analysis is used in a similar way to define a safe function for use.

The SOTIF assessment usually leads to adjustments of the functionality, e.g., limitations of the performance to allow for a safe function under non-fault conditions. In the Functional Architecture, the BMW Group differentiates between Technical SOTIF and Human Factors SOTIF, as the measures validation can be shown either by technical design decisions (safety-by-design) or by validation of human behavior with the system to show the safe operation (design decisions linked to the assessed risks). In additional regard to Functional Safety, the safety goals for the driving function are defined and functional and technical safety concepts are derived according to ISO 26262.

Design Redundancies

Under fault conditions, the safe function can be achieved via a "fail operational" strategy (redundancy), a "fail degraded" strategy (operating with degradation), or a "fail safe" strategy (bringing the vehicle to a safe stop). Which approach is chosen always depends on the nature of the design element under fault condition and the remaining capabilities of the system.

Design safety considerations taken into account include:

- design architecture
- sensors
- actuators
- communication failure
- potential software errors
- reliability
- potential inadequate control
- undesirable control actions
- potential collisions with environmental objects and other road users
- potential collisions that could be caused by actions of an ADS
- leaving the roadway
- loss of traction or stability
- violation of traffic laws
- deviations from normal/expected driving practices

After consideration of the requirements stated in ISO 26262 and IEC 61508 and choosing a safety concept, requirements for the design are identified and the architecture of the automated driving system can then be derived.

The BMW Group sees the necessity of a diverse redundancy (diversity): both the primary and the secondary channel are themselves redundant, and have their own diagnostic units. This allows the detection of the channel under fault and lets the other channel take over. In the case a fault affects both channels, a third rudimentary channel takes over to allow for reaching a minimal risk condition.

Figure 24 shows an overview of the implemented redundancy concept.

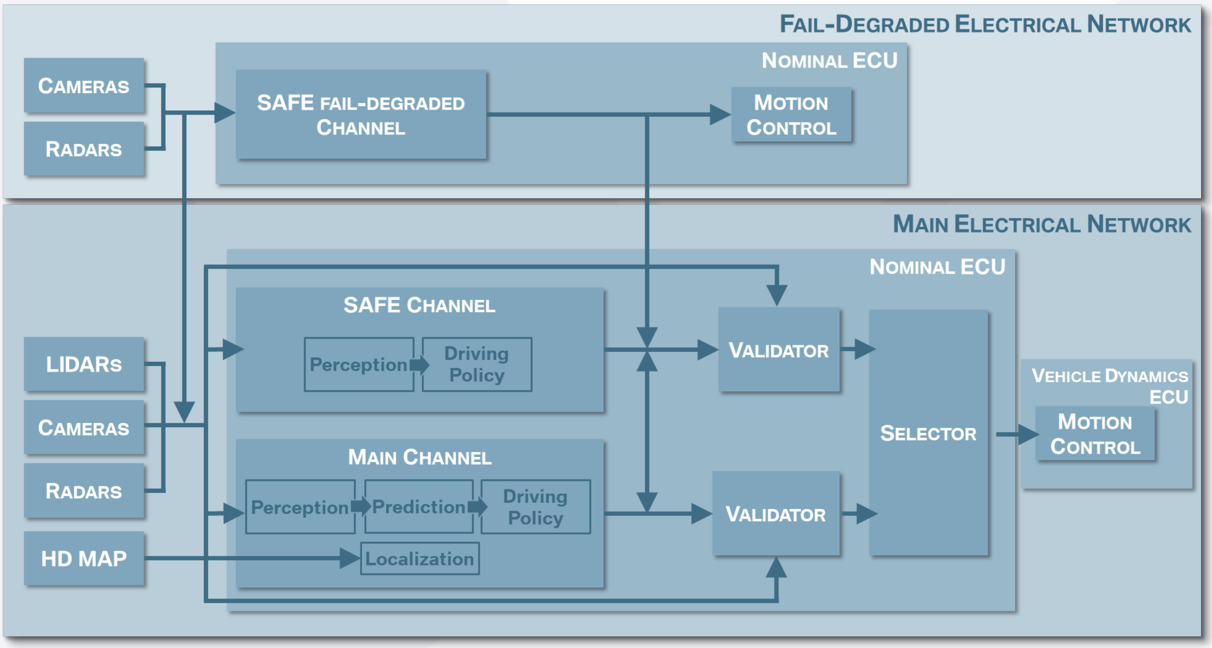


Figure 24. Implemented Redundancy Concept in the BMW ADS.

Safety Strategies (ADS Malfunctions)

The goal of the implemented redundancies is to allow the driver, as a fallback-ready user, to take over the driving task. If the fallback-ready user does not take over the driving task, a risk mitigation maneuver is triggered (see Chapter 5. Fallback (Minimal Risk Condition)).

The risk mitigation maneuver ensures safe operation until a fail-safe state is reached (i.e., driver takes over the driving task or vehicle comes to a complete stop). It will be executed when safe continuous operation of the SAE Level 3 BMW ADS cannot be ensured, for instance:

- if the standard TOR was ignored by the driver;
- due to a hazard in the environmental conditions leading to reduced sensor or actuator performance (sensor blinding, low friction value, etc.); and,
- due to a failure of vehicle components (mechanical, E/E).

The fail-operational strategy is illustrated in Figure 25.

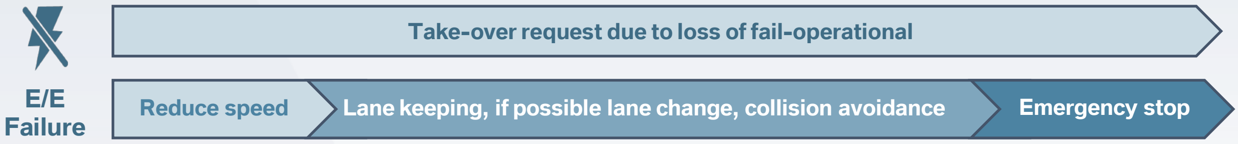

Take-over request due to loss of fail-operational
E/E Failure
Reduce speed
Lane keeping, if possible lane change, collision avoidance
Emergency stop

Figure 25. Fail-operational Strategy.

Software Development Processes

The influence of software on vehicle functionality is steadily increasing. To account for this growing influence, the BMW Group has developed a number of processes to control the development of all complex electronic vehicle control systems on all levels (software, hardware, subsystems, systems, and the complete vehicle).

The software development process is based on the applicable parts of ISO 26262. This includes a breakdown of the safety goals, as discussed above, into software requirements and architecture. Through change control management, this gets assigned throughout all development departments (including the supply chain) and is part of the overall series development process. The documentation and change management process is a regular part of the UNECE type approval of complex electronic vehicle control systems (UNECE R79 Annex 6, UNECE R13H Annex 8). A similar process is implemented for self-certification in the US.

The BMW Group's strategy for the safety of artificial intelligence (AI) is to develop automated driving functions based on a fail-degraded concept. That means that the performance layer, which includes the AI algorithms, is always safeguarded by a deterministically-developed safety layer, which is responsible for all safety functions. These safety functions are always active during automated driving and control the behavior of the vehicle. The safety functions are completely independent from the performance layer.

Software Update Processes

To update the software of a vehicle—after certification and even after the first registration—is increasingly important, for example, for addressing safety issues, performing software corrections and supporting recalls. In accordance with the concepts of the future UN regulations on cybersecurity and over the air updates (see UN Task Force on Cyber security and OTA issues (CS/OTA)), software in BMW vehicles is always developed and validated at corresponding vehicle levels.

The developed and validated software update can still be delivered to the car in the traditional, well-established system for updating software via the retail organization, however OTA software updates have become an important option.

Whether an update is performed via a physical connection in a dealership or remotely over the air, it will not be released before the validation process (see Chapter 11. Verification and Validation (V&V)) has been completed. To ensure compliance with the applicable safety standards, the software is tested in BMW test vehicles operated by professionally trained safety drivers before its release to customer vehicles. Before testing the new software on proving grounds and public roads, a risk analysis taking into account the role of the safety driver is performed to ensure that road traffic safety is not affected.

The key processes and procedures that have been established for administrating software updates are as follows:

- Relevant information concerning safety-relevant software updates is documented and securely stored at the BMW Group;
- Information regarding initial and updated software versions, including integrity validation data, and relevant hardware components of a safety-relevant system are identified;
- Interdependencies of the updated system with other systems are identified;
- Specific target vehicles applicable to a software update are identified;
- Compatibility of possible software/hardware configurations for the last known configuration of target vehicles with the software update prior to deployment is verified;
- Assessment, identification, and recording of whether a software update will affect other safety-relevant systems required for the safe and continued operation of the vehicle or if the update will add or alter functionality of the vehicle compared to when it was registered;
- The vehicle user is informed about updates;
- Information is made available to relevant authorities or technical services.

Update Procedure

When a safety-relevant software update occurs after vehicle registration, including OTA updates, the following steps will be employed:

1. Before implementation of the update, the BMW Group will ensure that the update processes allow updates to be conducted safely and securely. If the update process is changed a new validation is required.
2. The BMW Group will assess whether a software update will directly or indirectly impact the compliance of the approvals of a vehicle's self-certified systems and document the result.
3. If the update does not have an impact on the compliance of any self-certified systems (e.g., updates to fix software bugs), the BMW Group will still ensure the update process employed is safe and secure.
4. The update may then be conducted and the BMW Group will ensure the update process employed is safe and secure.

The BMW Group will periodically validate the processes used.

International Organization for Standardization. (2011). Road vehicles - Functional safety (ISO 26262:2018). Retrieved from https://www.iso.org/standard/43464.html
International Organization for Standardization. (2019). Safety of The Intended Functionality (ISO/PAS 21448). Retrieved from: https://www.iso.org/standard/70939.html
International Organization for Standardization. (2019). Road Vehicles – Cybersecurity Engineering (Draft. ISO/SAE CD 21434). Retrieved from: https://www.iso.org/standard/70918.html
National Highway Traffic Safety Administration. (2016). Assessment of Safety Standards for Automotive Electronic Control Systems (DOT HS 812 285). Retrieved from: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/812285_electronicsreliabilityreport.pdf
International Electrotechnical Commission. (2010). Functional Safety (IEC Standard No. 61508:2010). Retrieved from: https://webstore.iec.ch/publication/22273
UN Task Force on Cyber Security and Over-the-Air issues. (2018). Draft Recommendation on Software Updates (Informal document GRVA-01-18). Retrieved from: http://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29grva/GRVA-01-18.pdf

Table 7. Overview of System Safety Relevant Standards and Guidelines.

10. Cybersecurity

As the number of electronic systems on the vehicle increases, so does the number of attack vectors with which an adversary may attempt to access a vehicle's data or even manipulate its systems. In order to reduce cybersecurity risks, the BMW Group develops vehicles based on a security development lifecycle, which includes the design, production, and monitoring of the hardware and software throughout the vehicle's lifecycle. To this end, BMW has implemented numerous processes to handle cybersecurity incidents, analyze threat intelligence and exchange it with external entities, and to develop and roll-out security updates to the vehicle. BMW is an active participant in the Automotive Information Sharing and Analysis Center (Auto-ISAC), which is an industry platform to share cybersecurity threat and intelligence information relevant to the automotive sector. For all on-board and off-board vehicle systems, including connected devices and the BMW back end, BMW has implemented a security architecture that utilizes the security-by-design approach and is based on the latest industry best practices. For all cyber-physical systems, basic protection levels have been implemented, which may include encryption and authentication. Furthermore, for the vehicle's most critical systems and data, additional safeguards have been implemented to achieve an even higher protection level for BMW customers and all road-users in general.

To cope with an emerging threat landscape in the cyber realm (e.g., safe driving-relevant interferences, manipulation, theft), the BMW Group has established a comprehensive cybersecurity program. First of all, it is crucial to understand the main differences between vehicle safety and cybersecurity.

Vehicle safety (see Chapter 9. System Safety) focuses heavily on integrity, which generally means vehicle signals are only acted upon if they are genuine, transmitted, and received properly. Safety's main goal is also the availability of the safe operation of a vehicle and often requires a system to be reliable and fail-safe (i.e., redundant). Cybersecurity therefore requires a focus on integrity, confidentiality, and availability of a system or information. Thus, cybersecurity assesses if a system can be manipulated in a way that may compromise these aspects.

Automated Driving (AD) is forcing the automotive industry to face new challenges caused by the growing connectivity within automated vehicles, between multiple vehicles, as well as the environment they operate in. These challenges range from fulfilling safety regulatory requirements up to protecting fleets and customers from cybersecurity attacks. In order to enable vehicles for automated driving, more features and thus more interfaces are being added leading to a growing vehicle ecosystem, as shown in Figure 26.

While some of these interfaces process information from external sources like the IT-back end systems, other interfaces are capable of controlling a vehicle's driving functionality. Adding new interfaces not only enhances the vehicle's features, but also increases the technical complexity leading to bigger cyber-attack surfaces for malicious actors.

In short, technology has advanced to a level where vehicles cannot maintain a safe state unless they also operate securely. Ultimately, cybersecurity principles and practices must be applied to the product development processes to ensure malicious actors or attackers cannot gain arbitrary control of a vehicle's driving systems.

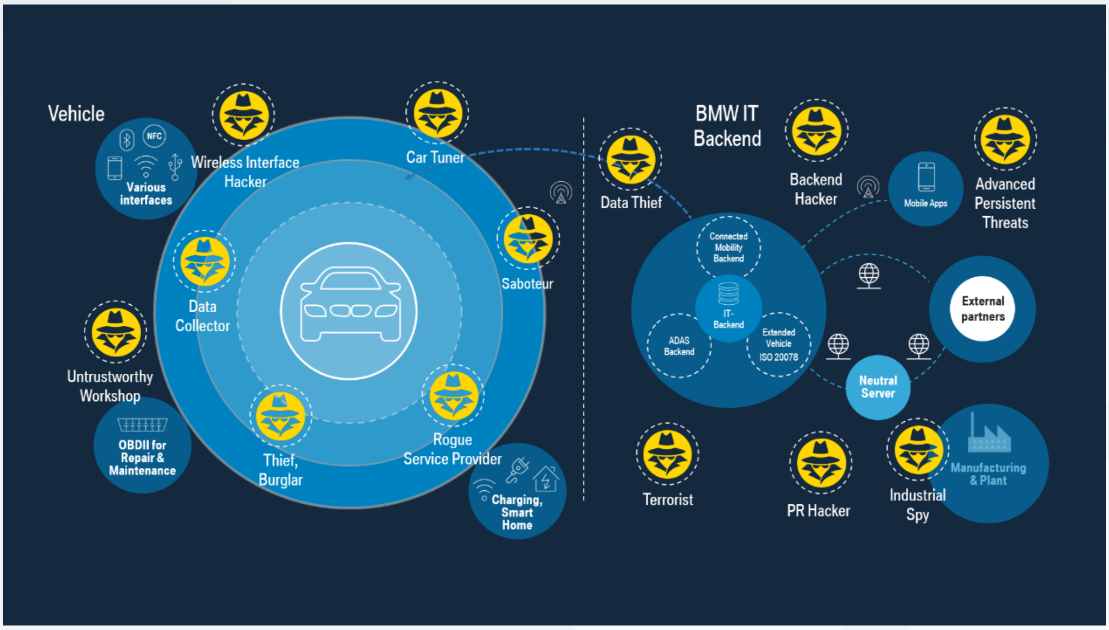


Figure 26. The vehicle ecosystem is growing and becoming more complex resulting in higher attack surfaces for threat actors.

As the complexity of an ADS rises, so does the likelihood for potential cybersecurity risks and the need for the right level of cybersecurity protection. Road-users' and driver's safety relies on the systems' integrity. Therefore, ADS must offer sufficient protection against manipulation and unauthorized access at all operation modes, especially for driving functionality. It is the BMW Group's priority to ensure the highest safety standards for its products and to protect their safety and security in the best possible way.

The challenge for cybersecurity in extending from SAE Level 2 to SAE Level 3+ vehicles lies in the fact that the ADS becomes increasingly more reliant on external data sources, such as sensor information, HD maps, or positioning data. If the integrity or authenticity of this data was compromised, the building blocks of the ADS would use incorrect data to maneuver the vehicle along its route. This could ultimately result in positioning the vehicle in incorrect or non-existent lanes, failing to recognize obstacles, or misinterpreting traffic situations. Therefore it is BMW Group's responsibility to create sufficient cybersecurity safeguards and controls to appropriately protect automated vehicles from malicious intent.

BMW Group's Cybersecurity Program

In this section, the BMW Group's approach to address the different threats to its products will be further described. Additionally, this section gives an overview of the product development process the BMW Group uses to design and build automated driving systems that resist cyber-attacks. Security has to be designed into a system to achieve comprehensive coverage. A rigid and fully integrated security engineering process is the basis for creating secure, and therefore safe systems.

The process helps to tightly integrate various security controls and safeguards, which will be described in a later section. Traditional IT cybersecurity focuses on different security principles, one of the most essential of which is known as "defense-in-depth". The BMW Group adopts defense-in-depth among many other cybersecurity principles to ensure that different controls on different system layers are in place, so the vehicle is not reliant on its perimeter alone to withstand cyber-attacks. Effective utilization of cybersecurity technology and functions in the BMW Group's products is the outcome of the defense-in-depth paradigm.

BMW Group's Secure Development Lifecycle Approach

The key elements of the program are Security Engineering, Security Technology & Functions, and Security Operations as shown in Figure 27. While this section provides an overview of the key elements, more details can be found in the deep-dive sections of this chapter.

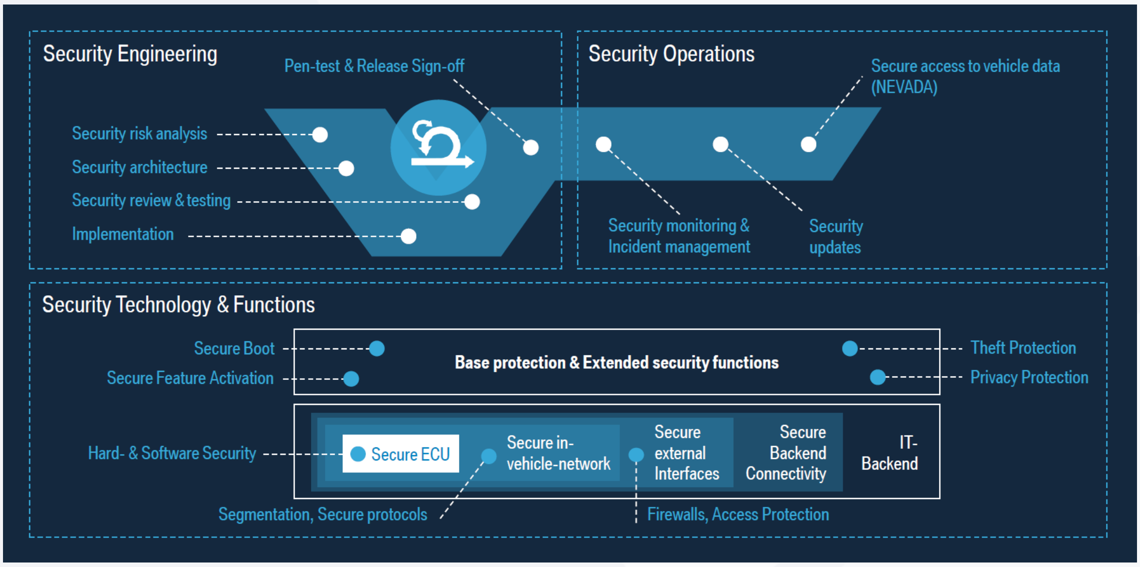

Security Engineering
Pen-test & Release Sign-off
Security risk analysis
Security architecture
Security review & testing
Implementation
Security Operations
Secure access to vehicle data (NEVADA)
Security monitoring & Incident management
Security updates
Security Technology & Functions
Secure Boot
Secure Feature Activation
Base protection & Extended security functions
Theft Protection
Privacy Protection
Hard- & Software Security
Secure ECU
Secure in-vehicle-network
Secure external Interfaces
Secure Backend Connectivity
IT-Backend
Segmentation, Secure protocols
Firewalls, Access Protection

Figure 27. Overview of BMW Group's Secure Development Lifecycle Approach.

In the Security Engineering phase, we have developed and implemented a risk-based methodology for vehicle development based on the security-by-design principles.

As a result of the security engineering process, appropriate Security Technology & Functions are designed to fulfill different protection needs for both our customers and other road users. During the engineering process, each control unit, functionality or back end system is designed with a basic protection level and further assessed by our security experts. In case the assessment identifies higher protection needs, extended safeguards will be designed to close the gap.

The third element—Security Operations—kicks in when the BMW Group's products have been released to the market. It leverages modern technology as well as industry collaborations to identify new vehicle threats, analyzes their impact to products and depending on the identified risks triggers follow-up processes, such as vehicle software updates. The Auto-ISAC is the automotive industry's main platform to exchange valuable information on emerging threats, incident handling and automotive cybersecurity best practices.

In general, all automotive cybersecurity activities strive to meet four protection goals: Safety, Financial, Privacy & Data Security, and Customer Satisfaction. The importance of Safety as a protection goal has been discussed in Chapter 9. System Safety. Privacy and data security aim to protect both customer and vehicle data. The protection goal of finance addresses all risks concerning monetary losses for both customers and the BMW Group caused, for example, by theft or manipulation. Last but not least, the protection goal of customer satisfaction deals with manipulations and security incidents, strengthening the public's trust in the BMW Group's products.

At BMW Group, cybersecurity is taken very seriously and thus corporate management is responsible for achieving automotive cybersecurity goals and establishing processes incorporating cybersecurity principles as security-by-design throughout the whole company. Implementation of these principles is tracked by our associates that participate in a network consisting of cybersecurity experts from all relevant business units across the company.

The approach incorporates several cybersecurity best-practices publications that have been released by various organizations, particularly NHTSA's guidance on "Automated Driving Systems (ADS): A Vision for Safety 2.0", "Preparing for the Future of Transportation: Automated Vehicles 3.0 (AV 3.0)" and "Cybersecurity Best Practices for Modern Vehicles", all of the Auto-ISAC Best Practice Guides, SAE's "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems J3061", and ISO/SAE CD 21434 "Road vehicles—Cybersecurity Engineering," which is still under development.

In the following sections, more details can be found on the key elements of the BMW Group's cybersecurity program.

Deep-Dive: Security Engineering

The BMW Group follows a clearly structured product development process. In order to achieve an appropriate level of security for each of the protection goals, it is crucial to integrate automotive security concepts into the early stage of the product development process. The BMW Group's security-by-design-oriented development process can be divided into five basic stages:

1. Design stage: setup of vehicle security architecture and definition of requirements for an efficient basic protection level, which goes along with automotive cybersecurity risk monitoring followed by threat modelling.
2. Concept stage: risk limitation performed based on new concepts for efficient safeguards, which lead to additional security requirements. All of these are based on defense-in-depth and other common security principles.
3. ECU and software development stage: integrated planning and measuring of security maturity levels, e.g. through implementation concepts and milestones, in particular for highly connected components and AD features.
4. Integration and validation stage: comprehensive security testing and verification for the initially determined risks as well as newly identified threats during the development lifecycle, including penetration tests to incorporate hackers' perspectives and source code reviews.
5. Optimization stage: ongoing improvement and updating of security-by-design and the general development process.

The BMW Group not only carries out all of these steps for control units and vehicle functions, they are also incorporated in the design of the on-board network, the external vehicle connectivity via radio interfaces (e.g., mobile radio, Bluetooth), as well as all physical access points (e.g., OBD interface).The BMW Group's product development process uses a hybrid form of the waterfall model, or V-model as previously mentioned, paired with agile methods. On one hand, the overall vehicle development follows the waterfall model, while on the other hand agile methods are applied when developing distinct ECU software parts, e.g., AD functionality. This hybrid approach enables the BMW Group to combine the best of both worlds resulting in high flexibility for feature development and fixed milestones for security testing.

The BMW Group recognizes penetration testing as an essential element of the integration and validation stage of its development process: only the attacker's perspective can offer valid information about the existence of flaws in system design and implementation. To benefit from hackers' genuine input for verification and validation purposes, we commission both in-house and external cybersecurity consultants. The findings and subsequent actions are fed back into the development workflow before the market launch. Penetration tests are repeated as part of the security operations, both scheduled periodically and as needed.

Another important element of our product cybersecurity strategy are manual source code reviews and automated code scans to check critical points in software on control units and our servers, apps, and 3rd party services.

Deep-Dive: Security Technology & Functions

BMW Group's automotive security approach with regard to Security Technology & Functions as shown in the bottom part of Figure 27 comprises three components:

- Security architecture - following a security-by-design approach, especially defense-in-depth;
- Basic protection level - defined by a default set of safeguards for all control units, functions and system components; and,
- Extended protection level - an individual set of premium safeguards applied to highly sensitive control units, functions, and system components (e.g., AD functionality or telematics).

BMW Group's security engineers assess the overarching protection goals, relevant attack scenarios, and attacker profiles for each customer function and vehicle control unit to define the necessary individual protection level and identify appropriate technology solutions.

The basic protection level will be applied to all control units of the on-board systems of future vehicle generations. It contains elements such as means for secured on- and off-board communication, authentication mechanisms for ECUs, vehicles, and IT back end, as well as key management features (key and certification management), secure OTA updates and more. Industry standards and best practices are being constantly monitored by our engineers to keep the basic protection level up-to-date.

In addition to the basic protection, extended security protection is developed and implemented following an assessment of the necessary protection level of each individual control unit, function or system component of the vehicle and its ecosystem. With regard to the vehicle architecture, security functions have been designed as a multi-layer defense-in-depth approach. The basic idea behind defense-in-depth is to establish a system with several levels of protection, thus allowing the vehicle to maintain a general protection level, withstand attacks, and not be entirely compromised even in the event that an individual protection level fails or is penetrated.

Based on this approach, the BMW Group has created a layer model (see Figure 28) consisting of six security-relevant layers:

- Third parties
- IT back end
- Car2Backend connectivity
- Vehicle interfaces
- On-board network
- Electronic control units

The layer model covers the vehicle and its touchpoints with the vehicle ecosystem. Both the basic and extended protection levels impact both individual layers and multiple layers of the above mentioned layers. The proper implementation of all safeguards in these different security layers ensures that a successful attack on an individual safeguard will not compromise the integrity of the overall system. To further outline the layer model, Figure 28 shows an example of how the different layers affect the automated driving features as part of both a vehicle and a back end system:

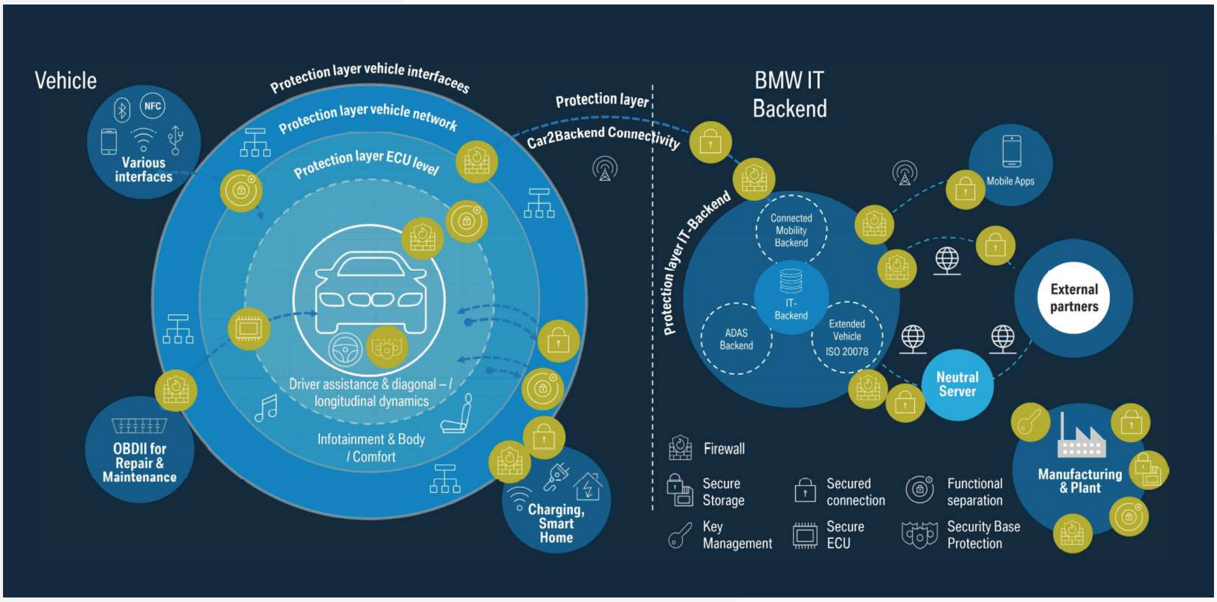


Figure 28. Layer model of the BMW Group's vehicle security architecture.

As far as AD is concerned, the core functionalities, namely sensor fusion, driving strategy, and vehicle motion control are located in the innermost circle of the multi-layer-architecture. In this case, these are the layers of the on-board network and ECU.

External data is also an essential part of AD functions. For example, HD map data is used during AD operation. This data requires regular updates. Nevertheless, the AD core functions never communicate directly with any off-board entities and vice versa. Instead, external communication is proxied and firewalled through other ECUs and dedicated interfaces following the least privilege principle.

In this example, an AD map update from a third-party map provider will first be authenticated at its source and forwarded to the BMW Group's IT back end layer. There, first quality checks as well as data fusion take place. Then, via a mutually authenticated and encrypted vehicle-back end link, the vehicle will download necessary map updates over the air. Then the map data is decrypted locally on an ECU, e.g., in the infotainment domain where it is managed in a dedicated storage space.

Eventually, AD functions may import the data via a dedicated on-board network interface through a firewalling gateway as part of the vehicle on-board network. In the end, the ECU will locally check the authenticity information from the IT back end in order to ensure the end-to-end integrity of the data before relying on it for AD purposes.

The combination of all safeguards on each of the five layers ensures that at no point adversarial data might be injected, no data alteration remains undetected, and an external attacker is not able to directly access any of the vehicle motion control interfaces that could impact the safe and secure operation of the vehicle's AD functions.

Deep-Dive: Security Operations

After completion of the security engineering phase the vehicle goes into production and is delivered to the customer. The systematic automotive security approach covers the design phase to market launch when the vehicle can be handed over to the customer. Nevertheless, the continuously changing threat landscape requires the BMW Group's full attention after customer delivery to keep pace with technological progress and the activities of potentially malicious actors.

Security Monitoring / Threat Intelligence

The BMW Group monitors global security incidents to stay on top of new developments and attack scenarios concerning its vehicles and IT systems. Information is discussed both via the official OEM channels and with cybersecurity experts at cybersecurity and hacking conferences. New threats are evaluated regarding their relevance to the company's products. In addition, the BMW Group takes supply chain security seriously and has entered into agreements with hardware and software manufacturers to be alerted about potential vulnerabilities early on. More details about collaboration on threat intelligence exchange are explained in subsequent sections.

Incident Management

As in the IT industry, a regulated software lifecycle throughout a product's life is essential for closing potential security gaps quickly and efficiently. Furthermore, it is necessary to take aging cryptography, certificate revocation, as well as rapid progress in new offensive technologies into account. Therefore, the BMW Group established clear processes for handling automotive security incidents. The ability to handle incidents strongly relies on the support of the BMW Group's suppliers. The traditional model of control unit suppliers, who consider software as an integral part of the overall system without the need for extensive updating after the series launch, is no longer feasible. The BMW Group is well aware of this issue and has addressed it in its automotive value chain.

Active vehicle software support is becoming an essential part of vehicle development, allowing us to respond quickly in case of potential security vulnerabilities. This is why the BMW Group requires all suppliers of components for future vehicle generations to remain capable to act on short notice, also beyond the active development phase.

Cybersecurity Collaborations and Partnerships (Auto-ISAC)

The BMW Group is aware that a high cybersecurity level is only achievable with the right partners and thus appreciates partnerships, actively participates in various collaborations, and promotes exchange of threat information. The BMW Group actively seeks support of the cybersecurity expert community through collaboration with other automotive companies about cyber attacks and sharing threat intelligence, while still maintaining competition on technical solutions.

An important non-profit organization in the field of automotive cybersecurity that encourages collaboration is the Auto-ISAC, founded in August 2015 by the automotive industry. The Auto-ISAC strives for a higher automotive industry security level by sharing information on new threats and real incidents as well as providing best practices on how to improve cybersecurity processes within an automotive organization. The BMW Group is a founding member of the Auto-ISAC and since then has been an active participant by working on various best practice guides on cybersecurity processes, by attending industry meetings on current cybersecurity topics, and sharing relevant threat and vulnerability information. BMW Group's security experts process the threat intelligence provided by the Auto-ISAC intelligence platform and forward it to engineers or the incident response team as necessary.

As far as best-practices are concerned, the BMW Group is not only working actively together with the industry on their development but has also fully internalized the following Auto-ISAC Best Practice Guides: Security Development Lifecycle, Governance, Incident Response, Third Party Collaboration & Engagement, Training & Awareness, Risk Management, and Threat Detection, Analysis and Monitoring. The overall approach shown in this section is aligned with all Auto-ISAC Best Practice Guides to succeed in securing our products.

Aside from the Auto-ISAC, the BMW Group has partnered up with many IT security companies. If security gaps are identified by our partners, they are treated appropriately by the incident response team when time-critical remediation is required, as well as the security engineering team for long-term security design improvements.

In addition, a regular outreach and exchange with academia and the research community helps the BMW Group to improve the cybersecurity of our products in the long run. Our bug bounty and vulnerability disclosure programs encourage independent security researchers (ethical hackers) to report identified security gaps to us.

It is also important to know, that the BMW Group is actively contributing to the ISO/SAE Joint Working Group 21434 "Road Vehicles—Cybersecurity Engineering" and works together with the global automotive industry to set sound minimum requirements for security engineering efforts each automotive company has to fulfill.

Secure Vehicle Data Access

The BMW Group is aware of increasing data generated by its connected vehicles and the demand to access the data by users and third parties. BMW Group ensures both access to a vehicle's user generated data as well as portability of that date to third parties by offering BMW and MINI CarData.

The BMW Group is one of the first automobile manufacturers to introduce this service and execute it in accordance with the EU General Data Protection Regulation (EU-GDPR). CarData is an implementation of the "Extended Vehicle Approach", which is supported by the German Association of the Automotive Industry (VDA). The "Neutral Server" in Figure 28 is an essential component in that approach and ensures BMW Group's maintenance of a high level of cybersecurity and data privacy for connected vehicles' services and data.

With BMW CarData, BMW Group offers its customers the opportunity to view selected telematics data for their vehicle and, if interested, to actively release it for third parties they trust. In order to be able to offer tailored services, the request for data access clearance is always initiated by the third party and then approved by the user.

VDA. (2018). VDA Position Paper on Automotive Security.

ISO. (2018). ISO 20077 Road Vehicles — Extended vehicle (ExVe) methodology. Retrieved from: https://www.iso.org/standard/67597.html

Auto-ISAC. (2018). Auto-ISAC Best Practice Guide on Incident Response v1.2.

Auto-ISAC. (2018). Auto-ISAC Best Practice Guide on Collaboration and Engagement with Appropriate Third Parties v1.2

Auto-ISAC. (2018). Auto-ISAC Best Practice Guide on Awareness and Training v1.0

Auto-ISAC. (2018). Auto-ISAC Best Practice Guide on Governance v1.2

Auto-ISAC. (2018). Auto-ISAC Best Practice Guide on Risk Assessment and Management v2.0

Auto-ISAC. (2018). Auto-ISAC Best Practice Guide on Threat Detection, Monitoring & Analysis v1.0
Auto-ISAC. (2019), Auto-ISAC Best Practice Guide on Security Development Lifecycle v1.2
SAE. (2016). Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. (J3061_201601). Retrieved from: https://www.sae.org/standards/content/j3061_201601/
NHTSA. (2016). Cybersecurity Best Practices for Modern Vehicles. Retrieved from: https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf

Table 8. Relevant Cybersecurity Best Practices.

11. Verification and Validation (V&V)

Verification and Validation represents the right half of the V-model referenced in previous sections. For the SAE Level 3 BMW ADS, this covers the V&V at each level including: SW level (e.g., code coverage); component level (e.g., sensors); subsystem level (e.g., automated steering control); system level (e.g., function logic of the SAE Level 3 BMW ADS) and vehicle level (e.g., interaction of the SAE Level 3 BMW ADS with its environment). For verification, each level is tested against the referenced specific design requirements in the left half of the V-model which fulfill various standards, such as those previously listed in Chapter 9 System Safety. For validation, the SAE Level 3 BMW ADS is additionally tested at various levels against a variety of pre-defined realistic scenarios and in real-world traffic. Several tools are used in this context including: Hardware/Software (HW/SW) open-loop reprocessing, HW/SW-in-the-loop simulation (e.g., driving strategy including minimum-risk condition); customer studies in driving simulator (e.g., driver-vehicle interaction); real-world test drive open-loop (e.g., sensor performance) and closed-loop (e.g., driving dynamics). Lastly, the closed-loop test drive in the target vehicle is also used for full-vehicle validation to ensure that the systems operate appropriately on the road. At this full vehicle level, rigorous testing is conducted for the SAE Level 3 BMW ADS similarly to the testing that is conducted for traditional BMW vehicles. By combining simulation in the above mentioned context with the testing at the vehicle level, the SAE Level 3 BMW ADS is being developed to provide statistical confidence in its operational safety. After the initial deployment of the SAE Level 3 BMW ADS, the safety of the system is continuously monitored by gathering and analyzing anonymous data from in-use vehicles. If necessary, required safety updates are provided accordingly.

Introduction to Verification & Validation

The verification and validation of the system safety are of the highest priority for the BMW Group. Therefore, the BMW Group is actively working on international standards (e.g., ISO 26262, ISO/PAS 21448) to further establish safety architecture, concepts, and validation for automated driving. One key project for validation is PEGASUS, a German research project to establish suitable validation methods with focus on SAE Level 3 highway driving, with follow-up projects planned (e.g., SetLevel4to5 and VV-Methoden). The BMW Group also cooperates within the industry to define safety standards along with adequate tools and techniques, which are documented in the White Paper “Safety First for Automated Driving”. The ideas and concepts established in this White Paper act as a guideline for the BMW Group’s verification and validation activities for the SAE Level 3 BMW ADS.

Based on the years of experience we gained from developing advanced driver assistance systems (up to SAE Level 2) for series production vehicles, we have developed verification and validation processes and organizational structures to address all relevant safety aspects of our functions and expand these processes, structures, and methods where meaningful for automated driving systems.

The terms “verification” and “validation” are defined as follows:

- Verification: “Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled” [ISO 15288].
- Validation: “Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled” [ISO 15288].

Test Goal Categories

The safety-relevant test goal categories for the SAE Level 3 BMW ADS are derived from the 12 principles established in the safety vision chapter of the White Paper "Safety First for Automated Driving".

The safety-relevant test goal categories are:

- Functional Safety (ISO 26262)
- Technical Safety-Of-The-Intended-Function (SOTIF)
- Human Factor Safety-Of-The-Intended-Function (SOTIF)
- Security
- Validation of the simulation

These categories also cover the safety goals described in Chapter 9. System Safety.

Compliant with ISO 26262, all functional requirements are traced from system level to software level and linked to corresponding test cases for verification and validation.

General Approach

In general, a multi-step approach has been defined to ensure the safe deployment and continued operation of the SAE Level 3 BMW ADS (see Figure 29):

1. Analysis – safety by design.
2. Verification – verification of the safety by design requirements.
3. Validation – statistical demonstration by focused testing.
4. Field Operation – field observation after deployment.

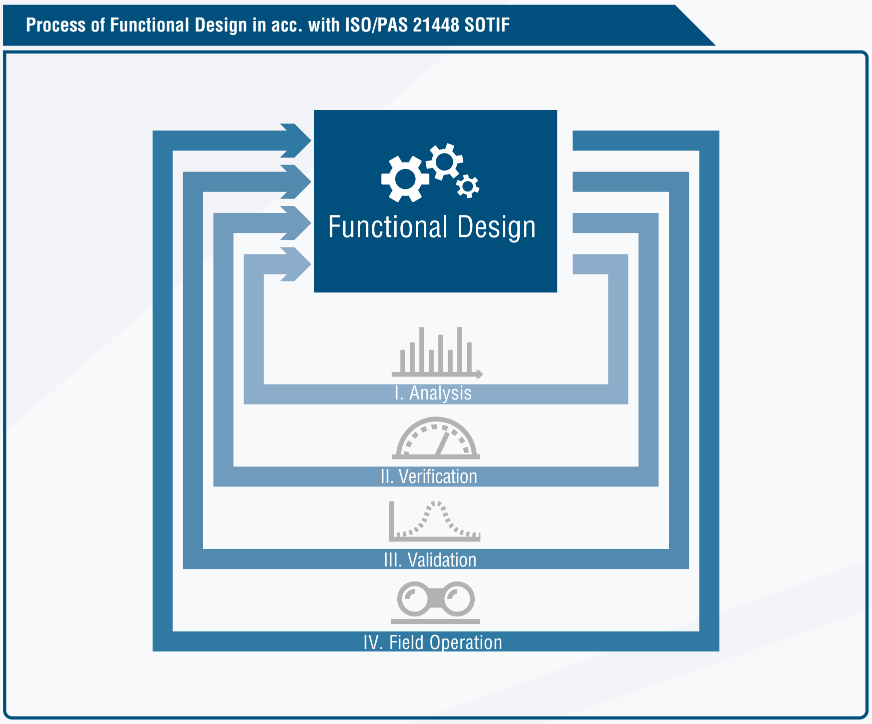


Figure 29. Verification and Validation Process (Reference: White Paper "Safety First for Automated Driving".).

During development, requirements are derived from the safety-by-design approach (Analysis), which includes the hazard and risk analysis for functional safety, the technical SOTIF, the human factor SOTIF, and security aspects. Apart from requirements, quality audits of the development process or the implementation of a robust system design through analysis techniques are done in the analysis phase.

The verification step ensures that requirements derived through the safety-by-design strategy are met. This step ensures that known scenarios are covered and that the system behaves as specified. The principle of safety-by-design is fundamental to the safety approach. However, basing the system safety only on safety-by-design would be insufficient as some unsafe scenarios might be unknown during the development phase.

Therefore, we use statistical approaches to demonstrate the safety, including previously unknown scenarios during development, with enough confidence to build an appropriate statistical argument (Validation). Validation puts the verified system to the test in scenarios or situations that the system would likely encounter in everyday driving after its release. To this end, we build up a database with highly representative scenarios with regard to their occurrence in the real world and with regards to criticality. Also corner cases, which test the system behavior at the boundary of the ODD, in combination with extreme / challenging test parameters, are taken into account (Koopman et al., 2019).

Additionally, we implement a post-deployment observation processes (Field Operation). This includes both field monitoring of the safety performance of the ADS and any updates needed to address weaknesses discovered after deployment. In this step, the ODD is also continuously monitored and validated against the a priori assumptions.

Findings from all steps are iteratively fed back into the ADS design, as well as the development and test processes to ensure a continuous improvement of all aspects of the system safety. When changes to the system are necessary we follow a strict change management process to ensure that changes in the system do not introduce new risks, as described in Chapter 9. System Safety.

Different Test Platforms and Simulation

In order to test relevant aspects of the system itself and the system components, we use different test platforms as listed in Table 9. These vary in the application of virtual and real stimuli as described in the Test Platforms chapter of the White Paper "Safety First for Automated Driving".

Test Platform	Abb.	Description	Example
Software-in-the-Closed-Loop	**SiL**	Partial Target SW is executed on prototypical hardware, whereas the SW decisions influence the virtually generated stimulus	E.g. MATLAB, Simulink model AUTOSAR Stack, C++ DLL
Software reprocessing (open loop)	**SW Repro**	Target SW is executed on prototypical hardware, whereas the SW decisions have no influence on the stimulus	E.g. replay of synthetic data to stimulate a CEM
Hardware-in-the-Closed-Loop	**HiL**	Target SW is executed on target HW, whereas the HW outputs influence the HW inputs	E.g. AUTOSAR Stack on Radar without frontend
Hardware Reprocessing (Open Loop)	**HW Repro**	Target SW is executed on target HW, whereas the HW outputs do not influence the HW inputs	E.g. monitor HiL
Driver-in-the-Loop	**DiL**	Target software is executed on prototypical or target hardware in the target vehicle or a mockup, and the environment is modified with virtual stimuli, whereas the driver's reaction influences the vehicle's behavior.	E.g. driving simulator or ViL (augmented reality for safety critical maneuvers)

Table 9. Different Test Platforms.

All of these test platforms are used for verification and validation of the OEDR within the ODD of the SAE Level 3 BMW ADS. Within each platform, simulations play an important role, where an entire system (e.g., a full vehicle with tires and AD functions), a sub-system (e.g., an actuator or a hardware controller), or a component (e.g., a sensor or a communication bus) may be simulated. The models used are abstractions of the physical reality and rely on simplifications of the true complexity in the real world. In order to reach the required level of accuracy for a simulation model, we continuously improve our simulation models through validation against real-world corner cases from vehicle testing.

Vehicle Testing and Data Gathering

While virtual testing helps to validate a lot of different scenarios, real-world driving in the target vehicle is also an essential part of the verification and validation process for the following reasons:

- Real world data for vehicle and sensor model validation: vehicle data and data detected by vehicle sensors are important sources to quantify and argue model accuracy (e.g., vehicle dynamics or simulated sensor models).
- Real world data for scenario accumulation: fleet data may be used to determine what relevant (corner) cases to simulate in the first place.
- Real world data for traffic modeling: the generation of novel scenarios in simulation requires realistic traffic participant behavior in order for virtual simulations to remain meaningful and representative.
- Performance evaluation on predefined reference routes and free route testing: by evaluating the system performance regularly on predefined reference routes in diverse areas of the U.S. (different states, specific climate conditions, road conditions, infrastructure and behavior of other road users) we can identify and take into account regional differences.
- Execution of specific test cases: due to potential shortcomings in the simulation environment or model imperfections specific test cases may need to be executed in the target vehicle.

In particular, we are executing world-wide and U.S.-specific vehicle testing during the development phase (e.g., exhaustive testing and endurance runs) of the SAE Level 3 BMW ADS, as well as field monitoring after deployment (e.g., for validation of the assumed ODD during development).

Before releasing the SAE Level 3 BMW ADS to customers, we will have completed studies to demonstrate that the system can be handled safely by the driver (e.g., activation, deactivation, and take over requests).

In addition, the BMW Group’s development fleet is driving millions of miles world-wide gathering petabytes of vehicle data (and reference data) in huge data storage centers which are used for development and validation testing. This activity is also taking place in North America in order to ensure that cases specific to US ODDs are taken into account during development.

The recorded data from world-wide and U.S. specific endurance runs are used to validate the safety of the function logic (e.g., safety relevant performance indices) and to validate the models used in our simulation framework. Also, the encountered real-world scenarios are used to generate realistic simulation scenarios, especially corner cases, which can then be varied by relevant parameters to validate the robustness of our algorithms with regards to system safety.

Test Scenarios

For the selection of relevant test scenarios several input sources are taken into account (e.g., fleet monitoring, endurance runs, free open road testing, and expert knowledge).

The following list gives an overview of driving scenario characteristics we are focusing our validation efforts on with regards to system safety:

- Relevant expected real world incidents, based on the method of equivalency classes (see Test Strategy);
- Corner cases within the ODD;
- Fallback situations when the limits of the ODD are reached or system malfunctions which may lead to a fail-operational or fail-safe state;
- Crash avoidance situations (NHTSA's Framework for ADS Testable Cases – DOT HS 812 623).

The fallback/minimal risk behavior is verified and validated by explicitly generating situations where malfunction within the SAE Level 3 BMW ADS function or degraded states of components are simulated or where the SAE Level 3 BMW ADS is intentionally operated at the ODD limits (see Chapter 5. Fallback (Minimal Risk Condition)). This can be done by simulation or driving on test tracks with error injection or a deliberate approach of the ODD limits.

Additionally, real world data of fallback situations is collected via endurance runs and from field observation and used for the continuous improvement of the fallback strategies and the robustness of the system.

Test Strategy

The figure below shows an example of the above-mentioned test platforms used to verify and validate the tested system elements with regards to corresponding test goal categories.

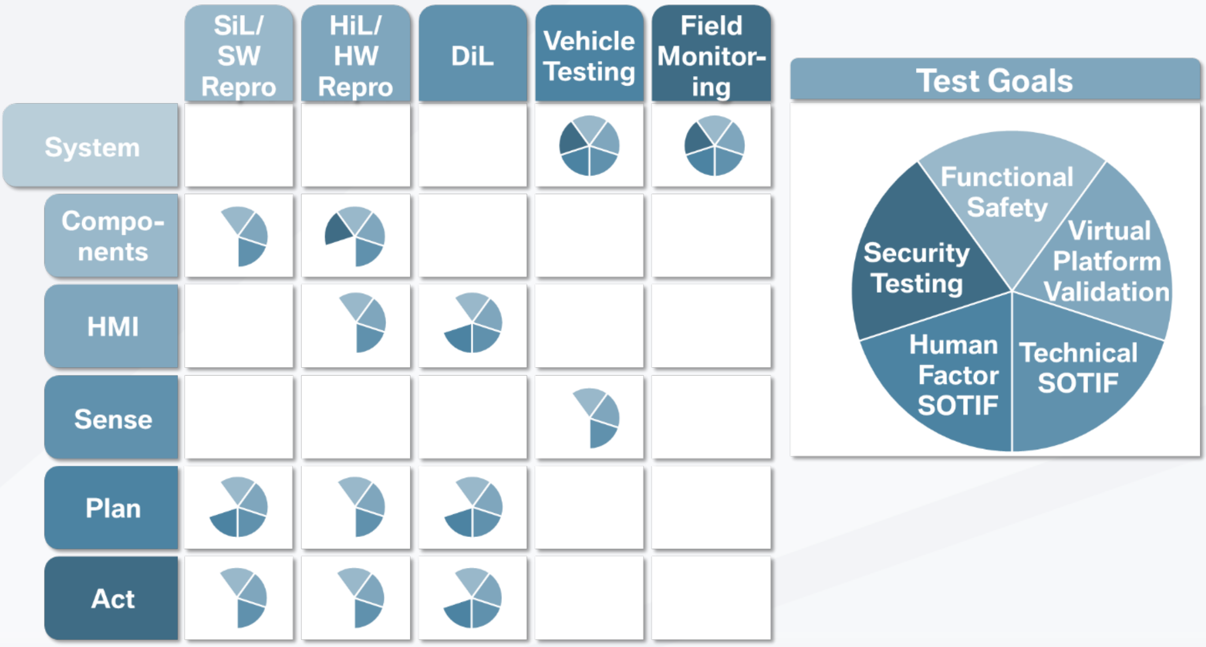


Figure 30. Test Goals with their Corresponding Test Platforms and System Elements.

One of the key challenges within the validation of the SAE Level 3 BMW ADS is the statistical demonstration of system safety and a positive risk balance without driver intervention (see White Paper "Safety First for Automated Driving").

In a purely statistical, black-box approach for validation of the safety of automated driving functions "automated vehicles would have to be driven hundreds of millions of miles and sometimes hundreds of billions of miles to demonstrate their reliability in terms of fatalities and injuries" (Kalra and Paddock, 2016).

In order to address this challenge with a feasible effort, the parameter space of influencing factors to be tested is partitioned into so-called equivalency classes, as proposed in the White Paper "Safety First for Automated Driving".

Equivalency classes are categories of factors in relation to their proportional influence on the presence of unsafe outcomes. The criteria to define equivalency classes are supported by the exposure, severity and controllability levels (as defined in ISO 26262) as a representative sample of operational situations to be grouped in equivalent classes. For a more detailed definition of equivalency classes, please refer to the White Paper "Safety First for Automated Driving".

Using the concept of equivalency classes helps in the most critical scenarios (corner cases). By doing this, a leveraging factor can be generated between the amount of driven and simulated validation miles and the hereby represented real life miles experienced by a regular vehicle. Thus, the specifically selected number of miles used for validation (real world driving and simulation) can represent a much larger number of miles driven by the customers under regular driving conditions.

Combining millions of miles of vehicle real-world testing with many million miles of simulation including scenario variation, in combination with the concept of equivalency classes allows for the management of the challenge stated above and provides a statistical demonstration of system safety and positive risk balance without driver interaction.

Vehicle-Driver Interaction

For validation of the vehicle-driver interaction concepts (HMI, takeover situations, etc.), driver-in-the-loop (DiL), and vehicle-in-the-loop testing are used during development. The level of controllability of the SAE Level 3 BMW ADS for the driver in pre-defined scenarios with an expected driver response time is validated via customer studies. Before going on public roads with customers, the HMI-driver interaction is validated within driving simulator studies with representative customers, with safety drivers and expert drivers on closed proving ground and free road driving. Additionally, real world data of fallback situations is collected via endurance runs and from field observation and used for the continuous improvement of the fallback strategies.

Safety-Relevant HD Map Content

Safety-relevant HD map content is validated by comparing it to a reference data set. System tests are performed to ensure that the AD system is statistically safe in the case of map/real world mismatch. Using safety-by-design methodologies, simulation and end-to-end validation we ensure that the map content is as accurate as possible. Fleet testing and field monitoring is also used for analyzing mapping data that implicate the map as a possible source of error.

International Organization for Standardization. (2011). Road vehicles - Functional safety (ISO 26262:2018). Retrieved from: https://www.iso.org/standard/43464.html

International Organization for Standardization. (2019). Safety of The Intended Functionality (ISO/PAS 21448). Retrieved from: https://www.iso.org/standard/70939.html

International Organization for Standardization. (2015). Systems and software engineering – System life cycle processes (ISO/IEC/IEEE 15288). Retrieved from: https://www.iso.org/standard/63711.html

Kalra, N. and Paddock, S. (2016). Driving to Safety: How Many Miles of Driving Would It Take to Demonstrate Autonomous Vehicle Reliability? Retrieved from: https://www.rand.org/pubs/research_reports/RR1478.html

Koopman, P., Kane, A. & Black, J. (2019, February). Credible Autonomy Safety Argumentation (Safety-Critical Systems Symposium). Bristol UK. Retrieved from https://users.ece.cmu.edu/~koopman/pubs/Koopman19_SSS_CredibleSafetyArgumentation.pdf

NHTSA. (2018). A Framework for Automated Driving System Testable Cases and Scenarios (DOT HS 812 623). Retrieved from: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13882-automateddrivingsystems_092618_v1a_tag.pdf

Table 10. Overview of System Verification and Validation Relevant Standards and Guidelines.

12. Consumer Education and Training

While BMW's SAE Level 3 BMW ADS is intended to be intuitive to the end user, it is still beneficial to both educate the customer on the use of the system as well as communicate to the public at large on BMW's approach to automated vehicles. With regards to the customer, it is important to educate them on the functionality of the system, including their role as the fallback-ready user, as well to educate the customer on the capabilities and limitations of the system. This education is important for the customer to understand their responsibilities when using the system, as well as to avoid over-trust and/or misuse of the system. With dealers being the primary touch point to the customer, it is BMW's responsibility to provide the appropriate resources such as educational tools and training to dealer sales and service that interface with the customer to explain the functionality, responsibilities, and limitations of the system. Lastly, it is important for BMW to communicate to the public at large our approach to automation through tools such as this safety self-assessment.

Consumer education is a key element to building public trust and realizing the full potential of the new HAD systems. The BMW Group will provide its customers with information on the SAE Level 3 BMW ADS before they experience the SAE Level 3 BMW ADS in their vehicle. This will be done through educational materials and via well-informed and trained retail and service staff. However, our direct customers will not be the only users of our SAE Level 3 BMW ADS system — common use cases such as rental cars and other road users who will interact with our SAE Level 3 BMW ADS controlled vehicles come to mind. It is therefore important for us to not only educate our customers, but also provide information to the public.

Training of Dealers

An important first pillar of our consumer education approach is a properly trained retail staff.

Advancing mobility innovation is a core element of our strategic focus. Providing leading-edge technology requires a systematic approach for communicating to, and training of our dealers and customers. To maximize their satisfaction with our portfolio of products and services, we provide numerous channels of education, information and resources with each commercial release. Our history and experience in delivering innovative technologies establishes a foundation for delivering the necessary educational tools in support of launching the SAE Level 3 BMW ADS.

As an important part of the BMW Group's overall educational concept, the BMW Group provides technical training to all service technicians in order to ensure our customers' vehicles are being maintained and repaired to the highest standards. Training comes in many forms, including but not limited to online web-based courses, self-study reference material, technical videos, and instructor-led, hands-on courses.

The automation of our vehicles will require us to not only educate our consumers about the new technology, but also our service technicians. In a first step, we have already begun educating our technicians on driver assistant systems such as Blind Spot Detection (BSD), Advanced Cruise Control and Lane Keeping Assistant, to name a few of the BMW Group's ADAS features. A crucial part of educating our technicians is to inform them how to properly diagnose and repair these systems in the event that such work is needed. The diagnosis and repair of our automated systems will play a crucial part in our continued success as we move towards higher levels of vehicle automation.

Education of the System Users

The important second pillar of our consumer education approach is the education of the user about the SAE Level 3 BMW ADS.

a) Content of user education

Content that will be addressed during the education of the user are:

- The prescribed use/functional intent of the ADS and the remaining responsibilities of the user in his/her role as a “fallback-ready user” (e.g., emergency fallback scenarios);
- The conditions under which the system is designed to operate including the limits of its ODD and of the sensors; and,
- Operational parameters of the ADS, such as the correct use of the system (e.g., activation/deactivation).

The clear communication of the role of the driver while the vehicle is operating in SAE Level 3 BMW ADS mode will be a central element of our user education. We believe appropriate communication will have a large influence on road safety based upon our experience with SAE Level 2 ADAS, as well as based upon lessons learned from other industries.

The responsibilities of a fallback-ready user have to be stated very clearly. The driver will have to be able to resume the driving task within a relatively short time span after the system issues a TOR. That also means that when the vehicle is performing the complete operational driving task while operating in SAE Level 3 BMW ADS mode, the driver should not be, for example, asleep or impaired in any way.

Another important issue is the driver’s mode awareness. This is especially important since the production BMW iNEXT vehicle will be equipped with both the SAE Level 3 BMW ADS feature as well as several other driver assistance systems (e.g., lane keeping assistant and lane change assistant). In order for the driver to correctly understand his/her role while engaging systems with different SAE assisted driving levels, the responsibilities of the driver in each level need to be clearly communicated, see Table 11 and Figure 31.

SAE Level 2	SAE Level 3
ADAS performs parts of OEDR	ADS performs complete OEDR
Driver always fully responsible	Driver as fallback-ready user
Immediate (self-initiated) driver response	TO several seconds after transition demand
Driver monitoring: focus on attentiveness	Driver monitoring: focus on receptivity and basic vigilance
Driver has to follow traffic code	ADS has to follow traffic code

Table 11. Driver’s Responsibilities in SAE Level 2 and SAE Level 3.

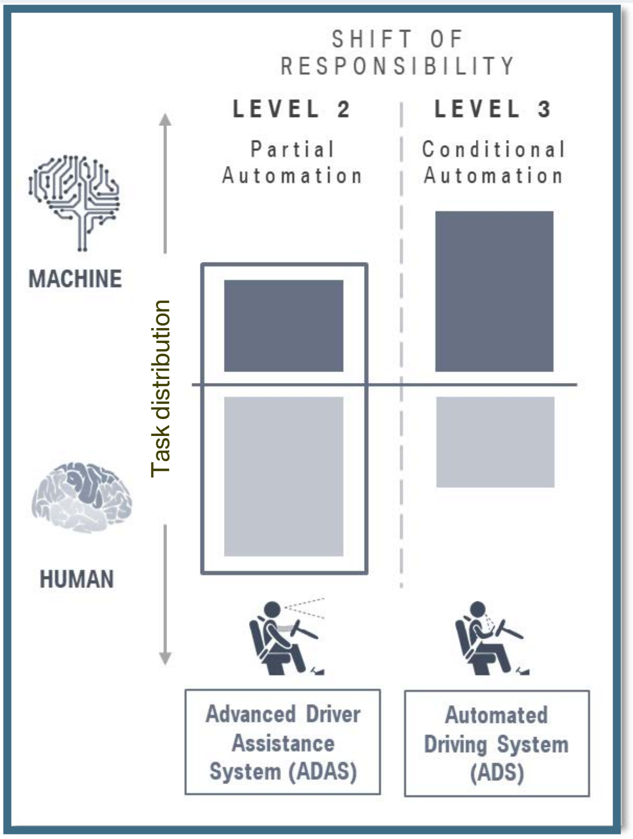


Figure 31. Task distribution and shift of responsibility.

b) How to educate the user

From our experience and through our research, we know that a person's preferred way to learn varies by individual and depends, for example, on factors such as age, gender, or even past experience with the brand (new vs. previous BMW driver). In order to satisfy individual needs, we have created a multi-channel approach to dealer and customer education. This includes channels such as:

- Owner's manuals (print, off-board digital, on-board digital, smartphone app)
- Intelligent personal assistant (IPA) on-board of the vehicle
- Videos (quick how-to, training, marketing)
- Compact "Getting Started Guides" (printed or digital brochure explaining important vehicles features and functions in a brief and easy-to understand format)
- Smartphone apps
- Hands-on demonstrations, tutorials, and clinics
- Experiential driving sessions

Our comprehensive offer of educational tools provides a foundation for the SAE Level 3 BMW ADS rollout. Since launching SAE Level 2 ADAS with our Driving Assistant and Driving Assistant Plus options, we have employed experiential learning events with subject matter experts of these systems.

In 2015, the BMW Group began offering pre-launch demonstration sessions and experiential driving sessions for employees. These sessions were led by subject matter experts to provide associates with real-world experience of our first commercially available SAE Level 2 ADAS.

Beginning in 2018, we launched even more advanced SAE Level 2 ADAS, including our Assisted Driving Plus capability (our first ever steering and traffic jam assistant which can be used in restricted "traffic jam" conditions). Prior to commercial launch, we expanded the demos and experiential learning events to include extra-company stakeholders such as marketing agency partners and events for auto show personnel. These experiential events were then incorporated into vehicle launch events for the first time.

c) BMWGenius^{TM}

Launched in 2013, the BMW Genius program was created to elevate the customer experience in the retail environment. This program created a new role in the dealership whose sole purpose was to serve as a non-commissioned product expert. The main responsibilities of the Genius is to assist customers prior to, during, and after the purchase. The Product Geniuses are intensively trained on both BMW products as well as customer service. Within the sales process, they assist with a needs assessment to best match a consumer with specific BMW models and features. Post-sale, the Genius handles the delivery process and subsequent "deliveries" via the BMW Encore^{TM} program wherein a customer can return to the dealership for more explanation after he or she has had time to experience the vehicle.

Human-Focused Design of the ADS

Conditionally automated SAE Level 3 vehicles are a novel concept for today's public. We firmly believe the best way to enable consumers to safely interact with the SAE Level 3 BMW ADS is to make the user experience as intuitive as possible and to design the product around the customer.

There is no way to guarantee that every driver will receive individual instruction. Use cases such as rental cars, secondary sales or even something as simple as multiple drivers in the same family illustrate why we cannot solely rely on direct customer education. That is why we place so much emphasis on the development of intuitive in-vehicle systems. The HMI of our vehicles—no matter if they are equipped with an ADS or not—is designed to be self-explanatory and thus intuitive, easy and above all safe to use. This is done by providing user orientation, controllability, feedback and, where adequate, help throughout the interaction with our systems. This allows us to provide an efficient, effective and satisfying user experience that is constantly being tested in empirical studies during design and development.

Education of the Public

Lastly, it is important to not only focus on customers of the BMW Group when addressing the topic of consumer education. One aspect of consumer education is also the education of all members of the public that will come into contact with our systems during their everyday commute.

This safety assessment report is one example of how we will communicate the SAE Level 3 BMW ADS's capabilities—and also its limits—to the interested public.

We believe that the voluntary safety self-assessment as envisioned by NHTSA is an important tool for highly automated vehicle systems to communicate information regarding the current status of the development of the systems, and the remaining challenges. This safety assessment report will be the first in a series of regular updates, released upon reaching the next milestones of development of our highly automated driving systems.

Appendix A: List of Abbreviations

ABS	Antilock Brake System
ACES	Automated - Connected - Electrified - Shared
ACSM	Advanced Crash- and Safety Management Control Unit
AD	Automated Driving
ADAS	Advanced Driver Assistance System
ADS	Automated Driving System
AEBS	Advanced Emergency Braking System
AI	Artificial Intelligence
ASIL	Automotive Safety Integrity Level
Auto-ISAC	Automotive Information Sharing and Analysis Center
AUTOSAR	Automotive Open System Architecture
AV	Automated Vehicle
BSD	Blind Spot Detection
BCP	Basic Central Platform
BMW	Bayerische Motoren Werke
CD	Commission Draft
CL	Closed-Loop
CS	Cybersecurity
DC	Direct Current
DiL	Driver-in-the-Loop
DOT	Department of Transportation
DSC	Dynamic Stability Control
E/E	Electrics/Electronics
ECE	Economic Commission for Europe
ECU	Electronic Control Unit
EDR	Event Data Recorder
EDR DAS	Driver Assistance systems Event Data Recorder
EDR HAD	Highly Automated Driving Event Data Recorder
FMVSS:	Federal Motor Vehicle Safety Standard
FuSa	Functional Safety
GB	Gigabyte
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HD	High Definition
HiL	Hardware-in-the-Loop
HMI	Human Machine Interface
HO	Hands-On
HOR	Hands-On Request
HW	Hardware
IEC	International Electrotechnical Commission
IPA	Intelligent Personal Assistant
ISO	International Standardization Organization
ISTQB	International Software Testing Qualifications Board
IT	information technology
L2	SAE Level 2
L3	SAE Level 3
L3+	SAE Level 3-5

LED	Light Emitting Diode
LIDAR	Light Detection and Ranging
MB	Megabyte
MIL-STD	Military Standard
MISRA	Motor Industry Software Reliability Association
MoU	Memorandum of Understanding
MRC	Minimal Risk Condition
NCAP	New Car Assessment Program
NFC	Near Field Communication
NHTSA	National Highway and Traffic Safety Administration
NIST	National Institute of Standards and Technology
OBD	On-Board-Diagnosis
ODD	Operational Design Domain
OEDR	Object and Event Detection and Response
OEM	Original Equipment Manufacturer
OL	Open-Loop
OTA	Over-the-Air
PAS	Publicly Available Specification
PEGASUS	Project for the Establishment of Generally Accepted quality criteria, tools and methods as well as Scenarios and Situations for the release of highly-automated driving functions (German research project)
PR	Public relations
PR Hacker	Hacker, who wants to generate PR with the publication of a hack
SAE	Society of Automotive Engineers
SiL	Software-in-the-Loop
SOTIF	Safety of The Intended Function
SW	Software
TO	Take Over
TOR	Take Over Request
U.S.	United States
UN	United Nations
UNECE	United Nations Economic Commission for Europe
V&V	Verification and Validation
ViL	Vehicle-in-the-Loop
VIN	Vehicle Identification Number