
CHALMERS
UNIVERSITY OF TECHNOLOGY

# Improving Safety of Autonomous Vehicles: A Verifiable Method for Graceful Degradation of Decision and Control Responsibilities

SAE INTERNATIONAL

ARTICLE INFO
Article ID: 12-08-02-0021

doi:10.4271/12-08-02-0021

# Improving Safety of Autonomous Vehicles: A Verifiable Method for Graceful Degradation of Decision and Control Responsibilities

***Adina Aniculaesei,[1] Iqra Aslam,[1] Meng Zhang,[1] Abhishek Buragohain,[1] Andreas Vorwald,[1] and Andreas Rausch[1]***

*[1]Clausthal University of Technology, Institute for Software and Systems Engineering, Germany*

## Abstract

Developing safe and reliable autonomous vehicles is crucial for addressing contemporary mobility challenges. While the goal of autonomous vehicle development is full autonomy, up to SAE Level 4 and beyond, human intervention remains necessary in critical or unfamiliar driving scenarios. This article introduces a method for gracefully degrading system functionality and seamlessly transferring decision-making and control between the autonomous system and a remote safety operator when needed. This transfer is enabled by an onboard dependability cage, which continuously monitors the vehicle's performance during its operation. The cage communicates with a remote command control center, allowing for remote supervision and intervention by a safety driver. We assess this methodology in both lab and test field settings in a case study of last-mile parcel delivery logistics and discuss the insights and results obtained from these evaluations.

### History

Received: 07 Aug 2024
Revised: 31 Dec 2024
Accepted: 26 Feb 2025
e-Available: 24 Mar 2025

### Keywords

Runtime monitoring, Safety assurance, Graceful degradation of functionality, Connected dependability cages, Safety-critical systems, Autonomous driving systems, Connected automated vehicles

### Citation

Aniculaesei, A., Aslam, I., Zhang, M., Buragohain, A. et al., "Improving Safety of Autonomous Vehicles: A Verifiable Method for Graceful Degradation of Decision and Control Responsibilities," *SAE Int. J. of CAV* 8(2):297–315, 2025, doi:10.4271/12-08-02-0021.

ISSN: 2574-0741
e-ISSN: 2574-075X

This article is part of a focus issue on the Safety, Reliability, and Trustworthiness of Intelligent Transportation Systems.





# 1. Introduction

Advancements in autonomous driving systems are transforming transportation technology. Market leaders such as Waymo [1] aim to revolutionize personal transportation by implementing self-driving systems in vehicles. Autonomous vehicles (AVs) have the potential to enhance traffic safety by reducing human error and driver fatigue through advanced driving assistance systems (ADAS) and autonomous driving systems (ADS) [2].

Features pertaining to ADAS include electronic stability control (ESC), anti-lock braking systems (ABS), and collision avoidance systems (CAS), all designed to assist drivers with the execution of the dynamic driving task (DDT). Some of these systems, e.g., ABS, ESC, and CAS, are part of the more general category of active safety measures, with the main goal of ensuring the safe and predictable behavior of the vehicle, regardless of the driver's involvement [3].

Throughout this article, we use the concept of *ego-vehicle* to refer to the vehicle, which is partially or completely controlled by ADAS or by ADS [4]. Its components and subsystems are subject to development and testing during the different phases of the system development process and the vehicle as a whole is subject to monitoring during its operation.

Abdel-Aty and Ding [2] analyzed accidents involving AVs and human-driven vehicles using a matched case–control logistic regression model. Their research indicates that ADS is less likely to cause accidents in rainy conditions compared to human drivers, due to high-performance sensors such as RADAR, which can detect obstacles over 150 m away in adverse weather, e.g., fog or rain [5], while human perception is limited to about 10 m [6].

Moreover, the integration of various sensors, including cameras, LiDAR, GNSS, and RADAR [7, 8], enables AVs to detect pedestrians and vehicles in diverse weather conditions such as cloudy, snow, rain, and darkness [9, 10]. However, the study in [2] noted that AVs have a 5.25 times higher accident rate during dawn and dusk compared to human drivers, likely due to changing lighting conditions affecting obstacle detection accuracy, leading to potential errors in recognition, e.g., false positives or false negatives. Additionally, AVs have a lower risk of causing rear-end and sideswipe accidents, i.e., accidents in which the front of one vehicle hits the side of another vehicle [2]. This is because AVs, equipped with sensors that monitor the vehicle's surrounding environment, may detect and react much faster to potential rear-end or sideswipe conditions [2]. An example of such a system is an adaptive cruise control (ACC) system, which may use LiDAR sensor data to keep track and regulate the distance between the ego-vehicle, i.e., the vehicle on which the ADS or the ADAS operates, and the vehicles in front of it [11]. The ACC system alerts the driver if the distance becomes smaller than the safety distance [12], in this way reducing the risk of rear-end accidents. Compared to the accident data of ADS, the accident data pertaining to accidents caused by human drivers exhibit a tendency of the latter to have larger velocity differences at larger spacing ranges between the ego-vehicle and the vehicles in front of it [13]. This contributes significantly to the higher frequency of occurrence of rear-end and sideswipe accidents [14], e.g., in case the vehicle in front applies the brakes and the driver of the ego-vehicle has no time to adjust its speed and avoid a rear-end collision. The likelihood of an accident is influenced by the movements made by the ego-vehicle prior to the incident [2]. Accidents involving ADSs are less common than those involving human-driven vehicles when the ego-vehicle is proceeding straight, running off the road, or entering a traffic lane [2]. This is likely due to the faster and more precise reactions of AVs, which can quickly detect hazardous situations and implement corrective measures, such as adjusting speed and steering angle, more effectively than human drivers [2].

The standard SAE J2016 [15] defines six levels of automation.[1] for driving systems, ranging from SAE Level 0, where no automation is implemented and the driver is solely responsible for the DDT and the vehicle safety, up to SAE Level 5, where the ADS manages all aspects of the DDT in all kinds of operating environments and initiates necessary safety measures to bring the vehicle to a safe state when required. Starting at SAE Level 3, the ADS is responsible for executing all aspects of the DDT, including monitoring of the vehicle's environment. For ADSs at SAE Level 3 and above, it is crucial that the system operates correctly within its predefined conditions, maintaining both safety and operational requirements to ensure fail-operational performance.

Various verification and validation (V&V) methods are necessary to ensure that ADSs of SAE Level 3 and above can safely operate in real-world environments. During their development, these systems undergo extensive assessment to demonstrate compliance with international safety standards, specifically for functional safety (FuSa) and the safety of the intended functionality (SOTIF), outlined in ISO 26262 [16] and ISO 21448 [17], respectively.

[1] *Automated driving features at SAE Level* 1: ACC and lane keep assistance system (LKAS) controlling either the longitudinal or the lateral vehicle motion [15]. *Automated driving features at SAE Level* 2: an ADS incorporating both ACC and LKAS features, with the driver remaining in overall control of the vehicle [15], e.g., Autopilot from Tesla and Ditronic+ of the steering assistant in the Mercedes S-Class. *Automated driving features at SAE Level* 3: a highway pilot with ACC and LKAS functionalities, in low-speed, stop-and-go freeway traffic [15], e.g., the drive pilot from Mercedes S-Class and EQS. *Automated driving features at SAE Level* 4: valet parking system performing the entire DDT (curb-to-door or vice versa) without the driver's supervision [15]. *Automated driving features at SAE Level* 5: an ADS that, once programmed with a concrete destination, is capable of operating the vehicle throughout complete trips on public roads, regardless of starting and end points, intervening road traffic, or weather conditions [15], e.g., shuttle buses for passenger transport on company premises or at trade fairs.

Notice that, in the V&V processes for ADSs, many verification tasks are carried out through different testing methods, i.e., unit testing, integration testing, or field tests, depending on which level in the system hierarchy the V&V process is applied. For example, unit tests are used for checking the functionality of individual software components, whereas integration tests are carried out as the software components are integrated gradually with one another in order to create the whole software system. The target vehicle platform on which the software system is deployed is then subject to extensive field tests, in order to check if the final product fulfills the lawful regulations as well as the customers' requirements.

ISO 21448 complements ISO 26262 by presenting measures to achieve SOTIF in ADSs, which is defined as the absence of unreasonable risk due to hazards arising from functional insufficiencies of the ADS. Such insufficiencies may occur when the ADS operates in environments that do not comply with the system's operational design domain (ODD)[2] specifications. One approach to complying with SOTIF for ADSs of SAE Level 3 and above is to monitor the system and its environment during operation to check that both the operating conditions and safety requirements are being met. On one hand, the current operating conditions must align with the system's operating conditions as defined in the ODD specification. This involves verifying whether the current environment falls within the predefined ODD. The ego-vehicle's sensors continuously monitor its surroundings, and the collected sensor data is analyzed to determine if the ADS operates within its predefined ODD or if the ODD constraints are no longer satisfied. On the other hand, the system's behavior must meet the safety requirements established during the requirements elicitation and safety analysis phases. For example, consider the lane-changing assistance (LCA) system analyzed by Mauritz in [18]. The ODD constraints specify an operational environment limited to German highways. A key safety requirement for this system states: "The system shall be able to consider fast objects on the neighbor lane approaching the ego-vehicle from behind with at least 5 m/s relative velocity for a lane change to the left neighbor lane." This safety requirement requires that the LCA system must not initiate a lane change to the left lane if a vehicle in that lane is approaching from behind the ego-vehicle at a relative velocity exceeding 5 m/s.

If the ODD specification or safety requirements become invalid during operation, a fallback mechanism must take over responsibility for the AV control and safety. Notice that, despite the advantages brought on by ADS and ADAS, the study in [2] discovered that there are some driving scenarios that seem to be challenging for AVs, i.e., execution of lane changes and turning into heavy traffic, such as turning at intersections [19, 20]. One reason may be that AVs have difficulties in gaining situational awareness, which consists of perceiving elements in the vehicle's environment, assessing the importance of these elements, and anticipating future changes in their state [21]. One challenge an AV faces when trying to gain situational awareness is the generation of sufficient information about and the comprehensive detection of its surrounding environment from a single independent source due to limited sensor ranges and limited coverage of the environment by the AV sensors [11, 22]. Since some AVs may be programmed to follow specific rules, not all driving scenarios are necessarily considered when the vehicle is built [23–25]. Complex driving scenarios may become a challenge for the AV, e.g., unprotected left turn at intersections [26], and this complexity can be enhanced by further factors, e.g., limited priority and variations in trajectories of the oncoming traffic in intersections [27]. There is a tendency for AVs to be overcautious at intersections [27], i.e., they exhibit longer startup delays in intersection scenarios, which can lead to rear-end or sideswipe accidents with human-driven vehicles [28]. In comparison to AVs, human drivers seem to react and adapt their behavior more seamlessly when faced with a complex driving scenario [28]. Additionally, due to their limited understanding of social cues and psychological insights [29–31], AVs may face challenges in performing lane changes, merging into heavy traffic [32], or accurately interpreting pedestrian intentions [33].

Since there is no requirement that a safety driver be present in a vehicle controlled by an SAE Level 4+ ADS, the fallback mechanism involves a human safety operator who can remote intervene when necessary. Indeed, European regulations now require technical oversight for ADS at SAE Level 4 and above. In May 2021, the German parliament enacted a law allowing AVs in Germany to operate on public roads without a physical driver. This is initially limited to designated areas, approved in advance, e.g., such as shuttle services on company premises or at trade fairs. The law mandates that a technical supervisor must continuously monitor the vehicle's operation. The human operator is responsible for remotely intervening when necessary, either by stopping the vehicle or authorizing specific driving maneuvers [34].

The human safety operator, located in a remote command control center (CCC), monitors the AV's operation using live sensor data and intervenes when necessary. Additionally, a system for the gradual degradation of the ADS is required to ensure a smooth transfer of responsibility for the DDT and the vehicle's safety to the operator.

Consider an example where an ADS is controlling a vehicle on a German highway. The vehicle's sensors detect another car with its hazard lights on, partially obstructing the lane of the ego-vehicle. While there is no general

[2] The *ODD* consists of operating conditions under which a given ADS is specifically designed to function, including, but not limited to, environmental, geographical, and time-of-day restrictions, and/or the requisite presence or absence of certain traffic or roadway characteristics [15], e.g., weather conditions, road surface, urban area, or highway.

minimum speed limit on German highways, vehicles are prohibited from driving at unnecessarily low speeds to avoid disrupting traffic flow and reducing collision risks. In this situation, after evaluating the live sensor data from both the AV and roadside sensors, a human safety operator may decide to intervene and temporarily reduce the ego-vehicle's speed as it passes the stationary car. Once the ego-vehicle has successfully overtaken the stationary car, the safety operator restores full autonomy to the ego-vehicle, allowing it to return to its maximum allowed speed on the highway.

*Research Focus*. Although the idea of graceful degradation of the ADS functionality was posited in [35], the actual concept of graceful degradation and its development has never been fully discussed. This article presents a formally verifiable method for implementing graceful degradation of decision-making and control responsibilities in ADS. The proposed method ensures that the ADS always meets its safety requirements by clearly defining and separating responsibilities between the ADS and the human safety operator in the CCC.

The graceful degradation concept is supported by an integrated system safety architecture for ADS, consisting of several distributed subsystems. This integrated safety architecture includes a dependability cage (DC) responsible for onboard monitoring of safety requirements for a single AV, and a remote CCC that allows a human safety operator to supervise and intervene in a fleet of AVs at various levels, depending on the AV's current driving situation. The safety requirements subject to monitoring through the DC are defined and refined during the requirements elicitation and safety analysis phase of the system development process. These safety requirements are formulated at the system level, where the AV is considered to be the system under analysis.

The concept of the DC was first introduced in [36] and has been continuously developed since then [37–40]. The DC establishes a safe zone around the AV, which must be obstacle-free for vehicle-safe operation. Further technical details on how the safe zone is computed can be found in [37, 38]. The integrated safety concept consisting of onboard monitoring via the DC and offboard monitoring through the remote CCC is presented in [39].

The concept of graceful degradation, supported by human intervention through the remote CCC, is scalable. The CCC operates similarly to an aviation control tower, overseeing only the aircraft within its designated jurisdiction. Similarly, CCCs can be strategically placed at various points along the road network, each responsible for a specific area. When an AV enters the jurisdiction of a particular CCC, it begins communicating with the center, transmitting sensor data. Upon exiting that area, the AV disconnects from the current CCC and establishes communication with the next one as it enters its jurisdiction. Furthermore, the jurisdiction area of a remote CCC can be divided into smaller areas, with each of the smaller areas falling under the supervision of one human safety operator. Naturally, the design and implementation of a distributed system consisting of multiple remote CCCs is a challenge for the future.

Effective communication between the remote CCC and the AV requires a high-speed, low-latency network for the real-time transmission of large sensor data volumes. The concept presented in this article assumes the existence of such infrastructure. In fact, a communication network is already operational in Lower Saxony, Germany, covering 280 km along the A2, A7, A39, and A391 motorways, as well as the B3, B6, B243, and L295 federal and regional roads [41]. As an example, 71 masts equipped with camera and communication technologies have been installed on the A39 motorway to anonymously track road users and other objects in the traffic area. This system provides valuable data on the requirements for future ADSs. Masts can communicate with each other and with vehicles equipped with the necessary technology. In addition to the permanent masts, mobile masts are also used for testing outside the motorway, enabling analysis of automated driving maneuvers on various road types and locations. This network integrates with the Intelligent Mobility Application Platform (AIM), which has been fully functional in Brunswick's city center since 2014 [42]. We envision in future work the integration of a remote CCC, which supports the concept of graceful degradation with this infrastructure and, therefore, do not address this topic any further in this article.

*Contributions*: The contributions of this article are three-fold:

1. A formally verifiable method for the graceful degradation of decision-making in ADS,
2. A case study in parcel delivery logistics on which the method for graceful degradation is evaluated, and
3. Scenario-based evaluation of the graceful degradation in a controlled lab setting and on a test field track.

Notice that previous work in [36–39] describe parts of DC, e.g., the concept of the safe zone in [37, 38] and the remote CCC in [39]. None of these papers provide details on the concept of graceful degradation and its concrete implementation.

*Paper Structure*. The rest of the article is structured as follows. Section 2 presents related work in human–robot collaboration (HRC) and teleoperation of AVs. Section 3 introduces the concept of graceful degradation of system functionality. Section 4 introduces a case study in the application area of last-mile delivery logistics, which is being used in Section 5 as a basis to evaluate the graceful degradation concept both in a controlled lab setup and on a test field track. Section 6 concludes this article with a summary of its contributions and an overview of potential future work.

## 2. Related Work

HRC has emerged as a promising area of research due to the increasing need for communication between humans and complex robotic systems. This indicates that, in addition to effective interactions demonstrated in the field of human–machine interaction, strong collaboration between humans and robots is essential for success [43].

Although AVs strive for full autonomy by reaching SAE Level 4 and beyond, human operators are still required to take control of the vehicle in critical and novel situations when needed. Even companies such as Waymo, which operates at SAE Level 5, acknowledge the limitations of fully AVs in handling all system failures, emphasizing the necessity of human involvement [44].

In 2006, Cooke highlighted a common misconception: the assumption that the absence of a human's physical presence in a vehicle equates to no human involvement [45]. Instead, the challenges that require human intervention will persist. To effectively assess situations and ensure autonomy, it is essential to keep humans in the loop [46]. Companies engaged in autonomous taxi or shuttle services often integrate remote operations into their business models, incorporating interfaces that support remote management, monitoring, and assistance modes [47]. Consequently, collaboration between remote operators and AVs is often considered a prerequisite for deploying AVs on public roads [47], enabling real-time monitoring.

In 2020, Swedish project HAVOC [47] developed a simulator platform and prototype to explore the remote control and monitoring of heavy vehicles for safety assurance. The user tests were carried out with 15 participants and the input obtained from these tests was used to develop guidelines for remote control and monitoring. Mutzenich [46] and Stayton [44] proposed an extension of the taxonomy of ADS introduced in the standard SAE J3016 [15] with an additional level, which involves remote intervention from a separate location, emphasizing in this way the necessity of control centers for remote monitoring and teleoperation.

In 2021, a study introduced a design prototype for the human–machine interface (HMI) used in teleoperating highly automated vehicles in public transport, highlighting the importance of usability, situational awareness, and user acceptance [48]. Another study by Fabris et al. [49] addressed the challenges of maintaining high situational awareness and navigational efficiency during teleoperation by proposing a remote-control center for unmanned ground vehicles. Kalinov et al. [50] proposed an application interface to provide remote control for human interaction with autonomic robotic systems for performing safety tasks such as assessing, monitoring, and teleoperation, limited to virtual reality (VR).

Teleoperation of AVs becomes crucial in safety-critical scenarios. Neumeier et al. [51] presented a possible architecture for a teleoperated system and teleoperation station. Additionally, an approach was developed that allows the visualization of the real-time environment surrounding the teleoperated system via a video stream. Shen et al. [52] demonstrated immersive teleoperation possibilities for a physical test vehicle using 3G, 4G, and WiFi technologies. Hosseini [53] introduced an HMI-based interface to visualize in real-time the 360° field of view around a remote vehicle using LiDAR and camera sensors, thereby improving vehicle performance in driving scenarios that require precise control. However, their approach was limited to mixed reality and low additional data transmission. With ongoing exploration of teleoperation, Graf [54] provided a comprehensive framework for AVs' teleoperation interfaces focusing on situational awareness requirements and analysis.

Kalamkar [55] assessed scenarios for remotely teleoperating a vehicle for brief durations with the assistance of a human operator, ensuring stability while monitoring other vehicles in a fleet. Although the study involves collaborative teleoperation, the current bottleneck is primarily associated with VR technology.

In addition to human intervention, significant research has been dedicated to developing fail-operational systems that enable AVs to maintain functionality during component or system failures, but with limited functionality. The work in [56] highlights the importance of fail-operational software architecture as critical to sustaining vehicle operation during faults, avoiding full system disengagement or dangerous stops. In addition to that, some more studies focused on minimal risk maneuvers (MRMs), which are actions that a vehicle can execute to achieve minimal risk conditions during system failures, as well as on strategies to handle emergency situations autonomously. In [57], the authors explored the use of MRMs to reduce risk when automated driving transitions to manual control, ensuring a safer fallback mode. Another study presents a fail-operational control architecture incorporating real-time trajectory planning for emergency scenarios, allowing vehicles to continue operating at reduced functionality until reaching a safe stop [58].

In parallel, the use of degraded operational modes has been proposed as a critical approach to managing system failures without relying solely on remote intervention. These modes enable vehicles to continue functioning at reduced capacity, preventing sudden halts or dangerous roadside stops. Reference [59] focused on safety diagnostics and degraded operational strategies emphasizing the need to incorporate autonomous fallback mechanisms that ensure vehicle safety even when components are partially impaired.

The research reviewed in this section illustrates that while significant emphasis is placed on situational awareness and teleoperation, equally important are the systems designed for fail-operational autonomy and degraded emergency responses. This underscores the need for a comprehensive system that combines onboard monitoring of a single vehicle with offboard monitoring of an

entire vehicle fleet. Such a system should also address how responsibility is transferred between the human operator and the vehicle, ensuring effective collaboration in the evolving landscape of AV technology.

# 3. Overall Concept of Graceful Degradation and Integrated Safety Architecture

In this section, we introduce the concept of graceful degradation and provide a brief overview of the integrated system safety architecture designed and implemented in this research to support it. Additionally, we define a safety requirement and an ODD constraint and illustrate how they are monitored during the AV's operation.

## Overall Concept of Graceful Degradation

Figure 1 gives an overview of the concept of graceful degradation of the ADSs' functionality depicted as a state machine. Three types of intervention levels are defined in the concept of graceful degradation:

- $IL_0$—is used when there is no human intervention, and the ADS can complete the driving task on its own.
- $IL_{Intermmediate}$—represents intervention levels in which the responsibility over the DDT is shared and distributed between the ADS and a human safety operator remote CCC.
- $IL_{Max}$—expresses the intervention level at which the ADS is not able to complete its driving task at all and the human safety operator is required to take over full responsibility for the vehicle's safety and control.

Notice that an increase in the intervention level corresponds to a degradation of the ADS's functionality, whereas a decrease in the intervention level means an upgrade of the ADS's functionality.

## Integrated System Safety Architecture

To support the concept of graceful degradation of system functionality and enable practical demonstration, we implemented a cooperative system safety architecture with several distributed subsystems.

Although the integrated safety architecture has already been introduced in [39], we will briefly revisit it in this section for the sake of completeness.

This architecture includes a DC for onboard monitoring of the AV's safety. A remote CCC maintains constant communication with the DC, allowing a human safety operator to interact with the AV remotely. This interaction facilitates the gradual transfer of responsibility from the ADS to the human operator, achieving a graceful degradation of the AV's functionality.

The integrated system safety architecture consists of four layers for deploying various subsystems, as illustrated in Figure 2 (right side). The highest layer represents a logistics center that handles the global logistical planning of an autonomous car fleet. The lowest layer manages the modular ADS, which includes components such as environment and self-perception, situation comprehension and action decision, and trajectory planning and

**FIGURE 1** Overall concept of graceful degradation of the system functionality represented as a state machine with the intervention levels in and the transitions between them. (Adapted with permission from Ref. [60].)

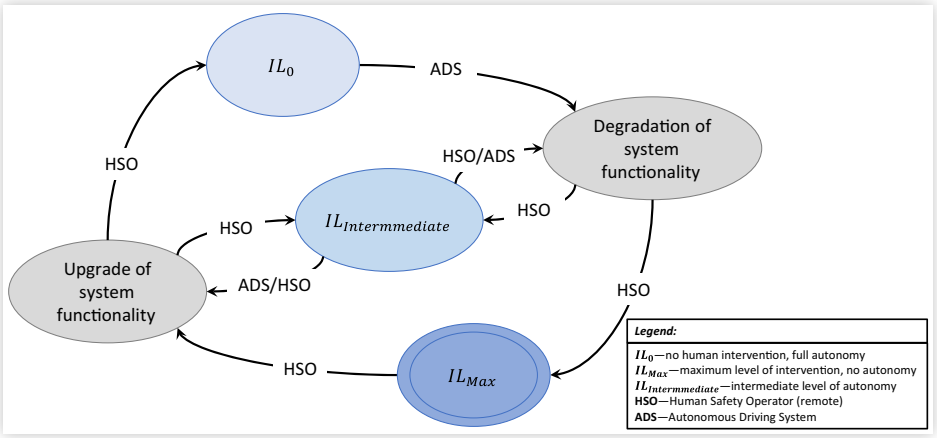
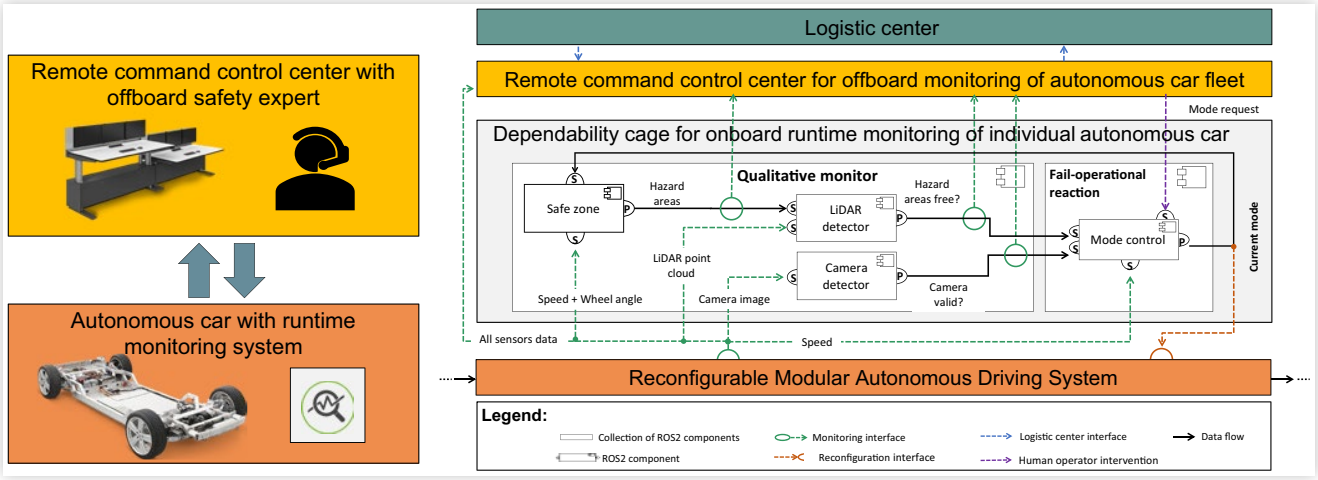


**FIGURE 2** Integrated system safety architecture for autonomous driving systems. (Adapted with permission from Ref. [39].)






vehicle control (see Figure 2). This layer is deployed on each individual autonomous car in the fleet.

The modular ADS within the safety architecture is designed to be reconfigurable. This means that each module implements a specific, self-contained functionality relevant to the DDT in the autonomous system and can be individually switched on or off. In critical situations, such as a functional failure, a module can be replaced by a redundant one. This reconfigurability allows for appropriate fail-safe and fail-operational responses to be realized.

Above the modular ADS layer lies the DC layer, responsible for onboard runtime monitoring of each AV's safety. The DC layer comprises two primary components: a software runtime monitor, referred to as the *qualitative monitor*, and a software component for *Fail-Operational Reaction* (see Figure 2). The qualitative monitor processes sensor data from the vehicle's systems, including speed, wheel angle, LiDAR point clouds, and camera images. It continuously evaluates safety requirements established during the requirements elicitation and safety analysis phases conducted early in the system development process. The qualitative monitor communicates the results of its safety verification to the fail-operational reaction component. This component takes input from the qualitative monitor and the remote CCC's request for a specific driving mode. Based on this input, it computes a new driving mode and sends it to the reconfigurable ADS to ensure continued safe operation.

The remote CCC layer interfaces with the DC layer, providing oversight for the entire fleet of AVs from a remote location. This layer features a centralized remote CCC that performs real-time offboard safety monitoring by analyzing live data streamed from the vehicles' sensors. Functioning as a redundant safety system, it complements the onboard DCs that monitor the AVs. Additionally, the remote CCC, along with the human safety operator supervising the AVs through live sensor data streams, works in parallel with the onboard systems to ensure comprehensive safety oversight.

## System Safety Requirements and ODD Constraints

During operation, the qualitative monitor ensures that the AV complies with both the safety requirement specification SR1 and the ODD constraint specification ODD-C1. These specifications were defined early in the development process during the requirements elicitation and safety analysis phases. The informal specifications, written in structured natural language, are as follows:

- **SR1:** *The ADS shall not cause a collision of the ego-vehicle with static obstacles ego-vehicle's environment.*
- **ODD-C1:** *The ADS shall operate only under appropriate lighting conditions that can be determined from the sensor data provided by the ego-vehicle's camera sensors.*

Before delving into how the safety requirement and the ODD constraint are monitored, it is important to first examine their specifications and understand the distinction between the two. The objective of the safety requirement (SR1) is to define the desired behavior of the ADS that controls the ego-vehicle. In contrast, the ODD constraint specifies requirements imposed on the operational environment of the ego-vehicle.

## Monitoring Safety Requirements and ODD Constraints

Safety requirement SR1 ensures that the AV maintains the required safety distance by focusing on a dynamically calculated safe zone in front of the vehicle, aligned with its direction of travel. This requirement mandates that

the safe zone remains obstacle-free to ensure safe operation. The qualitative monitor calculates the safe zone dynamically based on the vehicle's movement parameters, such as steering and acceleration or deceleration [37, 38]. This calculation is performed by the *safe zone* component and defines two areas: the focus zone, marked in orange, and the clear zone, marked in green, surrounding the ego-vehicle (see Figure 10). The *LiDAR Detector* component uses the defined safe zone to analyze the LiDAR point cloud. If the number of LiDAR points within the safe zone exceeds a specified threshold, an obstacle is considered present. When this occurs, the LiDAR Detector component triggers the *Fail-Operational Reaction* component, which activates a fail-safe driving mode through graceful degradation, thereby maintaining the AV's safety.

The ODD constraint ODD-C1 ensures the accuracy of the camera sensor data. The *Camera Detector* component validates this data by assessing the sharpness of the camera image [39]. If the camera sensor is obstructed by objects, such as falling leaves, or if its performance is compromised by low-light conditions, such as nighttime, then the sharpness of the image falls below a given threshold. The *Camera Detector* triggers then the *Fail-Operational Reaction* component to activate a fail-safe driving mode.

The *Fail-Operational Reaction* system includes a *Mode Control* component, which manages the decision-making process. This component determines when to switch to either fail-safe or fail-operational driving mode and communicates with the ADS to implement the appropriate response.

The graceful degradation of ADS functionality is triggered when either the safety requirement or the ODD constraint becomes invalid during vehicle operation. In this article, both the safety requirement and the ODD constraint are closely associated with safety hazards, such as the risk of collision when obstacles enter the AV's safe zone. If either the safety requirement or the ODD constraint is violated, it indicates a potential hazard, and such a failure to meet these specifications is categorized as a critical failure.

The handling of non-critical failures, as well as the differentiation between critical and non-critical failures, are areas for future research. Furthermore, the recovery from non-critical failures, using the principles of graceful degradation and dependability cages, will also be explored.

# 4. A Case Study in Last-Mile Delivery Logistics

In the previous section, we introduced the high-level concept of graceful degradation in system functionality. This section presents a case study in last-mile delivery logistics, which will later be used to evaluate the concept. We begin by discussing the challenges of the standard parcel delivery logistics process, followed by an overview of the proposed solution. We then present the practical development of graceful degradation. Finally, we focus on key application scenarios that demonstrate the graceful degradation of system functionality.

## Challenges in Standard Last-Mile Delivery Processes

The case study stems from the VanAssist project [60], a research initiative aimed at developing reliable, mostly emission-free, and autonomous parcel delivery logistics for urban areas. A key partner in the project was a German parcel delivery operator. The challenges faced by this operator in their parcel delivery processes reflect broader issues within the entire parcel delivery logistics sector.

The standard last-mile parcel delivery process of the parcel delivery company follows the following pattern. In the morning, parcels are sorted according to the delivery route and loaded into the delivery vehicle by the driver. The journey begins with traveling to the destination area, typically 10 km to 50 km away [60]. For urban centers, multiple vehicles often follow the same route from the company's branch headquarters. At the destination, parcels are distributed based on the stop distribution and density. Commonly, the delivery person parks the vehicle at a suitable location and completes several deliveries on foot from that point. They may carry or transport all items at once or return to the vehicle as needed between deliveries [60].

The delivery driver delivers each consignment individually, traveling from stop to stop. This approach allows the driver to carry only the current consignment but requires frequent starting, stopping, moving, and parking of the vehicle. Often, finding suitable stopping points is challenging, leading to significant traffic disruptions [60]. After completing the delivery route, the driver returns to the branch, often sharing the same return route with multiple vehicles. Upon arrival at the distribution center, undelivered and collected parcels are unloaded at designated gates. Depending on the volume of returning vehicles, drivers may experience waiting times [60].

## Solution for Last-Mile Delivery Logistics

The concrete objectives of the project were to increase the efficiency of delivery by minimizing and automating redundant work steps, as well as relieve the burden on the delivery driver through an intelligent automated vehicle system [60]. In order to achieve this objective, the solution proposed by the project was to develop a prototype for an autonomous driving delivery van, which would be remotely monitored by a control center on company premises, e.g., when the van is autonomously

maneuvering at the gate to unload its cargo, as well as in urban environments [60]. Additionally, the postman is given intelligent assistance in the parcel delivery task through autonomous driving functions of delivery vehicle [60].

The delivery process should become more efficient by integrating intelligent autonomous delivery vehicles into the existing workflow. The envisioned optimized delivery process would follow the following workflow [60]:

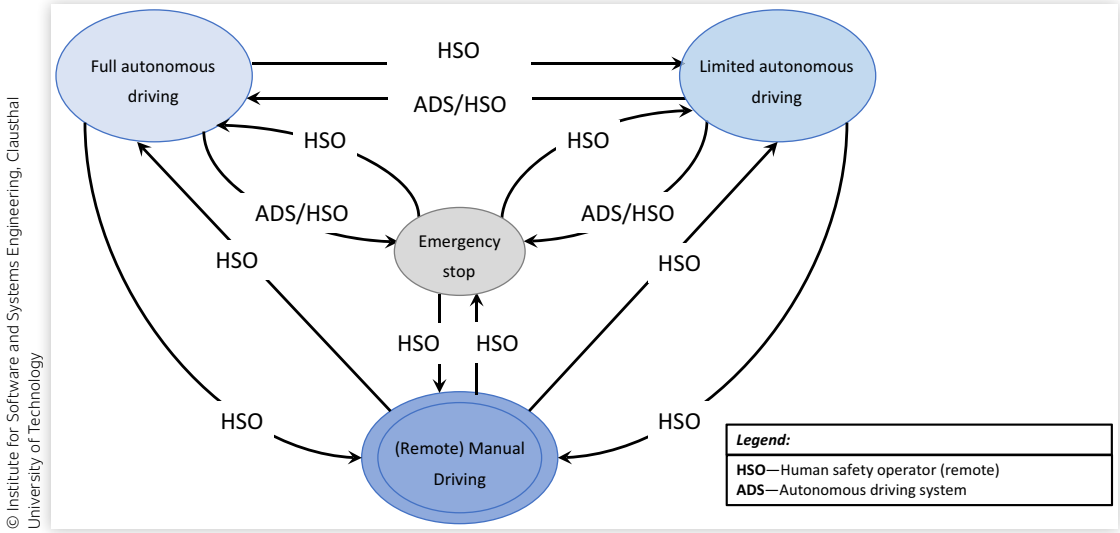
1. **Vehicle Loading:** The delivery vehicle is loaded at the delivery company branch according to predetermined sorting and route planning.
2. **Autonomous Transit to Meeting Point:** A meeting point near the delivery area is designated where the delivery vehicle meets the driver. The vehicle travels autonomously and unmanned to this location, allowing the delivery driver to dedicate more working time to the delivery process.
3. **Parcel Distribution Support:** During parcel distribution, the delivery driver is supported by the intelligent delivery vehicle. The driver and vehicle remain connected via a control interface, enabling the driver to issue commands or check the vehicle's status. Deliveries are conducted in "rendezvous mode," where the driver optimizes their route by taking a specific number of parcels from the vehicle. The driver then directs the vehicle to the next stop, which it autonomously reaches and waits for the driver.
4. **Return to Collection Point:** After completing the delivery tour, the driver and vehicle return to the original meeting point. At this point, the driver logs out, and the vehicle autonomously returns to the depot.
5. **Post-Delivery Operations:** At the depot, the control center directs returned vehicles to unload undelivered parcels at designated ramps or to proceed to charging stations. The vehicles manage these tasks autonomously, ensuring efficient utilization of resources.

## Practical Development of Graceful Degradation for ADS

As already depicted in the overall concept in Figure 1, graceful degradation of a system's functionality is realized through various intervention levels. Figure 3 illustrates an instantiation of the overall concept for ADS in the context of the last-mile parcel delivery case study. The levels defined for the autonomous parcel delivery vehicle define how responsibility for the vehicle's control and safety is distributed and transferred between the onboard ADS and the human safety operator in the remote CCC. Figure 3 shows these intervention levels and the transitions between them, with each transition's responsibility clearly indicated as belonging to either the human safety operator or the ADS. There is a clear correspondence to the concrete intervention levels defined in Figure 3 for the autonomous delivery vehicle and the abstract intervention levels introduced in Figure 1: (1) $IL_0$ corresponds to *full autonomous driving*, (2) $IL_{Intermmediate}$ represents the concrete intervention level *limited autonomous driving*, and (3) $IL_{Max}$ illustrates the intervention levels *(Remote) Manual Driving* and *Emergency Stop*.

We implemented the concept of graceful degradation, as illustrated in Figure 3, using a SCADE automaton modeled within the Ansys SCADE toolchain. Ansys SCADE

**FIGURE 3** Instantiation of the overall concept for graceful degradation of system functionality for autonomous driving systems.



is a model-driven development environment for creating reliable embedded software [61]. It uses the SCADE language to model both the data flow within software components and the control flow between them. The language is based on the declarative Lustre language [62] for data flow modeling, while hierarchical state machines in SCADE manage the control flow between components. The implementation was generated in C++ using KCG, a qualified code generator included in the toolchain. KCG ensures a one-to-one correspondence between the behavior modeled in the SCADE automaton and the generated C++ source code. The resulting code was integrated as the *Mode Control* component in the overall software architecture, as depicted in Figure 2.

The behavior defined by SCADE automata is inherently deterministic, making them well-suited for formal verification through model checking [63, 64]. Model checking is a computer-aided formal verification technique used to analyzse dynamic systems modeled as state-transition systems [65]. This method involves providing a model checker with a formal system model, such as a finite state machine, and a formal property specification, often expressed in temporal logic [65]. The model checker exhaustively explores the system's state space in search of system states that disprove the system property. If no such states are found, then the specified system property holds. If the model checker finds an error state, it returns a trace from the initial state of the system to the error state, to show why the error state occurred [65].

The SCADE automaton that implements the concept of graceful degradation can be formally verified against system safety requirements using the SCADE Design Verifier, a model checker integrated into the Ansys SCADE toolchain [63, 64]. By verifying the SCADE automation against the safety requirements, we demonstrate that the ADS operates within one of the following defined states:

1. **Full Autonomous Driving**: The ADS independently controls the delivery van.
2. **Limited Autonomous Driving**: The ADS operates with assistance and supervision from a remote safety operator.
3. **Remote Manual Driving**: The ADS relinquishes control entirely to the remote operator.
4. **Emergency Stop**: The vehicle comes to a complete stop to ensure safety.

This formal verification process ensures that the system consistently adheres to safety requirements across all operational states. Provided the latency between the AV and the remote CCC (see Section 1) as well as the latency between the vehicle sensors and the rest of the ADS components are negligible, formal verification of the SCADE automaton ensures that the AV remains in a safe state throughout the transfer of responsibilities between the ADS and the remote safety operator.

Additionally, proposed "*graceful degradation*" is aligned with key safety standards, i.e., ISO 26262 (FuSa) and ISO 21448 (SOTIF). At the core of the workflow is the ability to transition between different levels of autonomy in response to operational challenges, ensuring that the AV remains within safe boundaries, even when it faces unforeseen issues such as sensor failure/covered, environmental factors, and the like. In terms of SOTIF, when the AV encounters a failure caused by an adversary environment, such as a sensor blocked by leaves or the inability to navigate safely, it transitions to a fail-safe state (e.g., emergency stop or limited autonomous driving), preventing unsafe operation. This mechanism ensures the system remains within safety boundaries, allowing for human intervention when necessary, aligning with ISO 21448 standard.

## Application Scenarios

Two application scenarios were defined in the VanAssist project in order to demonstrate the concept of graceful degradation of the system functionality: (1) narrow road and (2) covered camera sensor.

***Scenario 1—Obstacles in the Vehicle's Path.*** The first scenario involves an obstacle that partially or completely blocks the ego-vehicle's path. The obstacle can be static, such as a garbage can sitting on the roadside, or dynamic, such as children playing on the street, which completely obstructs the ego-vehicle's lane. The AV must maintain a specified safety distance around these objects to prevent potential collisions, as outlined by safety requirements. However, adhering to this safety distance can prevent the AV from successfully navigating through narrow roadways.

As previously discussed, the DC functions as a runtime monitoring system designed to ensure that safety requirements are met during autonomous operation. In this scenario, the DC detects that the AV is unable to comply with the safety specifications due to the presence of obstacles in the vehicle's safe zone. Consequently, it triggers a fail-safe operation, initiating an emergency stop. Following this, the DC informs the remote CCC of the safety issue and requests an increase in the intervention level.

From this point onward, control and safety responsibilities for the autonomous driving task are transferred from the AV to the human safety operator in the remote CCC. The operator makes intervention decisions based on the live streaming of sensor data, such as camera images. Depending on the type of obstacle blocking the AV's path, the human safety operator has different handling alternatives at his disposal.

Thus, in case of a static obstacle partially obstructing the AV's lane, the operator decides to remotely reconfigure the ADS by activating the limited autonomous driving mode, which reduces the required safety distance. The intervention level is switched from emergency stop to the intermediate intervention level, limited autonomous driving. Consequently, the AV, now operating in limited autonomous mode, attempts to navigate through the

narrow road again. This scenario demonstrates that the safety assurance capability of the ADS is constrained by the manual reconfiguration performed by the human safety operator.

Control responsibility is then returned from the human operator to the AV. However, during the limited autonomous driving mode, both the human operator and the ADS share the responsibility for the safety of the vehicle. Thus, during this driving mode, the human operator monitors continuously the safety status of the AV via the live streaming of sensor data and can intervene manually to stop the vehicle if necessary.

Once the AV successfully passes through the narrow section, it requests a return to the initial intervention level, full autonomous driving. Given that the human operator remains in the loop and retains partial responsibility over the AV's safety, they must confirm that the issue has been resolved and reconfigure the ADS to its full autonomous driving mode with the original safety requirements.

In the case of dynamic obstacles in the AV path, the remote safety operator monitors the situation using live data streamed from the AV's camera sensors. Once the obstacles have cleared the path, the operator reduces the intervention level from **emergency stop** to **full autonomous driving**. Consequently, full control and responsibility for the AV's safety are returned to the ADS, allowing the AV to continue its journey autonomously.

***Scenario 2—Covered Camera Sensor.*** The second scenario involves the status of the AV's sensors. Onboard sensors may display reduced performance due to changes in environmental conditions. For instance, in autumn, fallen leaves can cover camera sensors, impairing their ability to accurately detect the environment, even if the sensors themselves are functioning correctly.

In this scenario, the DC on the AV is responsible for monitoring the quality of camera data to ensure it meets the specified safety requirements. If the data quality falls short of these requirements, the DC initiates a fail-safe operation by initiating an emergency stop. Consequently, the AV transitions from full autonomous driving mode to an emergency stop, triggered by a request to increase the intervention level.

Additionally, the DC communicates with the remote CCC to report the fail-safe operation. Based on the live streaming of the camera sensor data, the human operator at the CCC assesses the situation. Since the camera sensors are obstructed by fallen leaves, this issue cannot be resolved remotely. The human operator must request local human intervention to remove the leaves.

In this case, the intervention level is increased from full autonomous driving to emergency stop, indicating that the offboard human operator has fully assumed control and safety responsibility from the AV. The offboard operator then delegates the responsibility to a local operator near the AV. After the local operator removes the leaves, they contact the offboard safety operator at the CCC to return to the control.

Once the offboard safety operator confirms that the issue has been resolved through live streaming of sensor data, they request a decrease of the intervention level from emergency stop back to full autonomous driving. This restores the AV to fully autonomous mode.

Note that the definition of the two application scenarios is closely linked to the safety requirements outlined in Section 3. Specifically, the first application scenario is designed to check safety requirement **SR1**, while the second application scenario is to validate ODD constraint **ODD-C1**.

Both scenarios outlined demonstrate a comprehensive chain of transferring and distributing safety and control responsibilities for the AV. These scenarios address significant challenges associated with SAE Level 4+ fail-operational autonomous driving, e.g., legal liability, and the concept of graceful degradation of the AV's functionality along with the combination of onboard monitoring through the DC and offboard monitoring through the remote CCC is a possible solution approach, which is implemented and demonstrated.

# 5. Evaluation and Discussion of Results

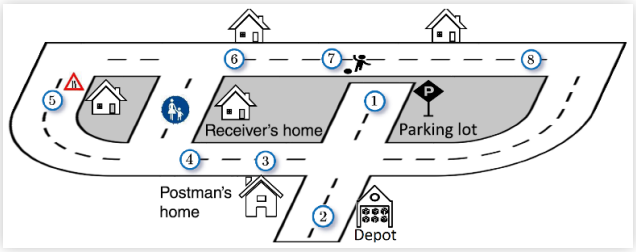
In this section, we present the evaluation process and discuss the results. We begin by introducing a comprehensive use case scenario designed to demonstrate and assess the concept. This overarching scenario is further divided into multiple steps to evaluate each component of the concept against the safety requirements specified in Section 3. The evaluation is carried out qualitatively in two stages:

1. **Controlled Lab Setting:** Initial assessments are performed in a controlled laboratory environment.
2. **Test Field Track:** Subsequent tests are conducted on a test field track.

## Overall Use Case for the Evaluation

The demonstration and evaluation of the graceful degradation concept focus on parcel delivery from a logistics center to end customers. The scenario comprises eight sequential steps, illustrated in Figure 4. The process begins with the AV parked in the parking area and driving out onto the road to the parcel depot (1). At the depot, the parcel is loaded, and the AV proceeds to pick up the postman at his house (2). After picking up the postman, the AV drives to the first recipient's home (3). The postman delivers the parcel on foot (4), while the AV circles the pedestrian zone to pick him up. As it circles the pedestrian zone, the AV detects obstacles in its path, which are

**FIGURE 4** Overall view of the evaluation scenario. (Reprinted with permission from Ref. [39].)





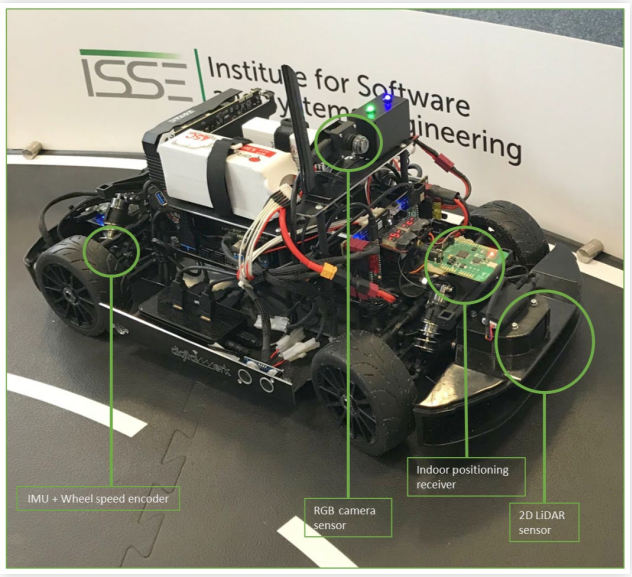

narrowing the road through its LiDAR sensor. Since the detected obstacles are inside the AV's safe zone, an emergency stop is triggered by the DC, and the remote safety operator at the CCC is notified (5). The remote driver switches the AV to a limited autonomous mode, allowing it to navigate the narrow road and reach the first meeting point (6). The postman retrieves the second parcel and delivers it, while the AV proceeds to the second meeting point. At this point, the AV encounters a person playing with a ball on the road. The DC triggers another emergency stop and alerts the remote operator (7). The operator waits for the person to leave and, once the road is clear, switches the AV back to fully autonomous mode.

While waiting at the second meeting point, the AV detects that its camera sensor is obstructed, triggering a fail-safe operation initiated by the DC, which causes the vehicle to perform an emergency stop. Remember that as a redundant offboard monitoring system, the human safety operator oversees the AV's status through live data streaming from the vehicle's sensors, facilitated by the remote CCC. Thus, the remote operator is able to recognize that there is a blockage on the front camera and instructs the postman to clear the camera sensor. Once the postman removes the obstruction from the camera sensor, the safety operator reactivates fully autonomous mode. The AV then returns to the parking area, completing the scenario (8).

Steps 5 and 7 from Figure 4 illustrate the first application scenario from Section 4, but they involve different types of objects. In step 5, a static obstacle such as a garbage can partially block the ego-vehicle's lane, while in step 7, a person playing with a ball fully blocks the lane. In both cases, the AV increases its intervention level from full autonomous driving mode to emergency stop.

According to the definition of the first application scenario in Section 4, the remote safety operator has different handling options for these two steps. In step 5, the operator switches to limited autonomous driving mode, allowing the AV to navigate the narrow road at a reduced speed. In step 7, the operator monitors the situation via the AV's camera sensors and, once the person clears the street, switches back to full autonomous driving mode, enabling the AV to continue its journey autonomously.

**FIGURE 5** Model car and its onboard sensor setup.






## Evaluation in a Controlled Lab Setting

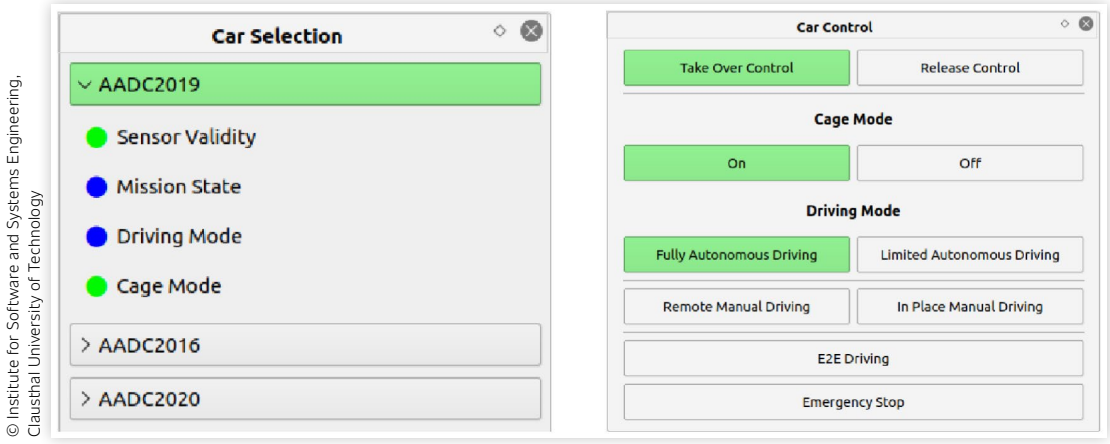
The evaluation of the graceful degradation concept in a controlled lab setting entails the evaluation of the HMI between the remote human safety operator and the AV on the CCC as well as checking the safety requirements defined in Section 4 based on the application scenarios defined for the lab environment.

***Evaluation Setup.*** For the evaluation conducted in the lab environment, a 1:8 scaled model vehicle was utilized (see Figure 5). This model is equipped with five primary sensors: a 2D LiDAR, an RGB camera, an inertial measurement unit (IMU), wheel encoders, and an indoor positioning receiver. These sensors enable monitoring of both the vehicle's current state and its surrounding environment. Additionally, the model features a wireless transmitter and receiver for remote communication.

In the lab, the road track used in the scenario was constructed with modular black mats measuring 1 m × 1 m each, featuring road markings that closely resemble real roads, as depicted in Figure 6.

**FIGURE 6** Track in the lab environment as a replica of the overall scenario.

**FIGURE 7** Panels in the remote command control center: car selection panel for fleet overview (left) and control panel for individual vehicles (right).






***Evaluation of the HMI on the Remote CCC.*** For this test, consider step 1 of the use case scenario shown in Figure 4. The graphical user interface of the remote CCC includes several panels: Car Selection and Car Control (Figure 7), Map (Figure 8), Destination List (Figure 9), and Sensor Visualization (Figure 10). The human safety operator utilizes these panels to monitor the vehicle's current state, analyze its surrounding environment, and interact with the AV in real-time.

Upon selecting a specific AV in the Car Selection panel (Figure 7, left), the remote operator can view the current state of the AV. Each attribute displayed represents specific information about the vehicle, as illustrated in Table 1.

Once the human safety operator selects an AV, control rights are granted to the remote CCC over the AV and all driving modes become available to the remote safety operator, and they can set the AV in a specific driving mode. In this way, the remote operator can supervise the safety of multiple AVs through the CCC.

At the start of the evaluation, the human safety operator activates the DC on the AV. With the cage active, the operator sets the vehicle to full autonomous driving mode using the car control panel (Figure 7, right) and selects the first destination, the parcel depot, on the destination control panel (Figure 9). As the AV navigates the track, its position is displayed on the CCC's mini-map panel, with the red dot indicating the vehicle's current location (Figure 8).

**FIGURE 8** Panel for the map visualization.

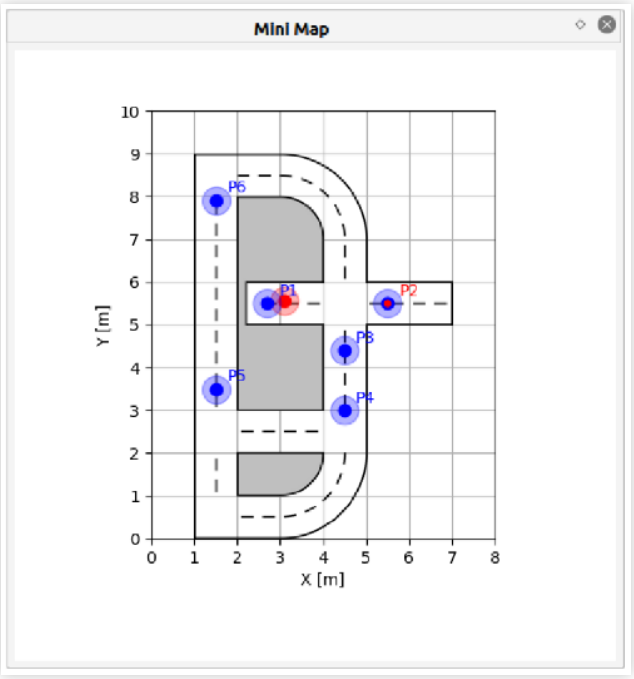





**FIGURE 9** Panel displaying the list of destinations for the selected autonomous vehicle.

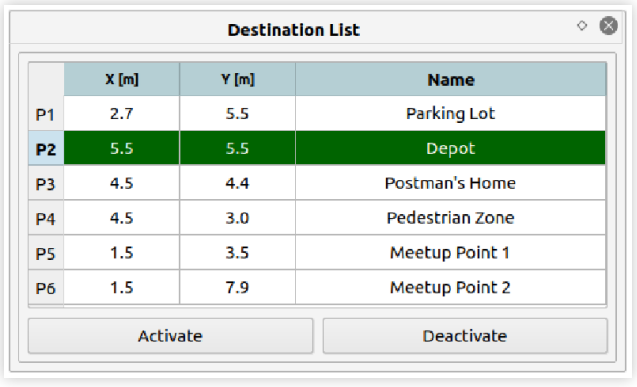


**TABLE 1** Information with respect to the current vehicle state depicted in the remote command control center.

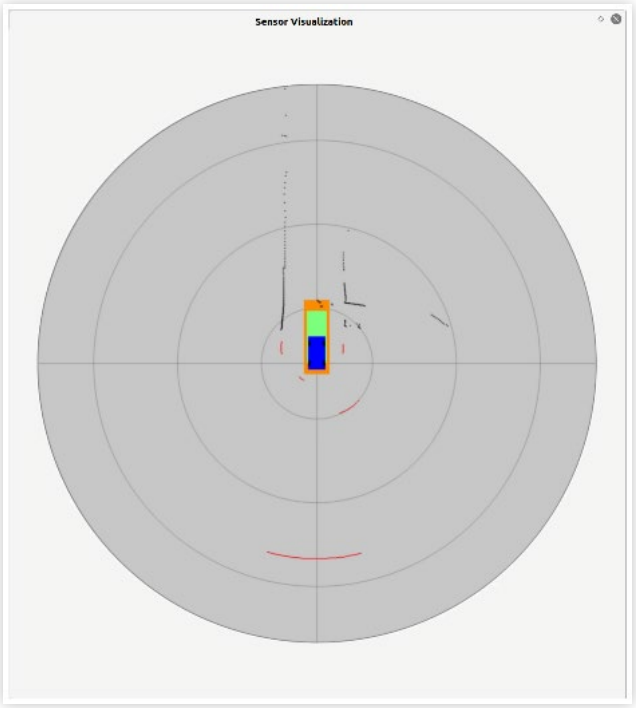
| Attribute name | Possible attribute values |
|---|---|
| Sensor validity | {Valid, invalid} |
| Mission state | {Inactive, active, blocked, complete} |
| Driving mode | {Fully autonomous driving, limited autonomous driving, remote manual driving, in-place manual driving, and emergency stop} |
| Cage state | {Safe zone free, focus zone occupied, clear zone occupied} |



***Scenario-based Testing of the Safety Requirements.*** For the test of the safety requirement, SR1 requires the components safe zone and LiDAR Detector of the qualitative monitor. The LiDAR Detector continuously monitors for obstacles in the AV's driving path. If an obstacle is detected inside the calculated vehicle's safe zone, then the DC triggers an upgrade of the intervention level from full autonomous driving to emergency stop (Figure 11, right). The calculated safe zone area along with the LiDAR points indicating obstacles are displayed on the Sensor Visualization panel of the remote CCC (Figure 10), where the human safety operator can view this information in real-time.

In addition to the sensor visualization panel, the CCC provides real-time access to front camera data via the camera panel (see Figure 11, left). This allows the human safety operator to assess the situation and, when the environment is safe, decreases the intervention level from emergency stop to full autonomous driving mode through the car control panel.

**FIGURE 10** Panel for the visualization of the safe zone and the LiDAR sensor data.






Testing the ODD constraint ODD-C1 makes use of the Camera Detector, which is part of the qualitative monitor and continuously checks the validity of images transmitted from the AV's front camera. For instance, in step 8 of the defined use case scenario, the Camera Detector detects obstruction by leaves on the lens (Figure 12), triggering an increase in the intervention level from full autonomous driving to emergency stop.

The human operator then uses the camera panel to view the issue and instructs the postman to clear the lens. Once the postman gives notice to the human safety operator that the issue has been resolved, the human safety operator decreases the intervention level from emergency stop to full autonomous driving, provided also that the vehicle's safe zone is clear of obstacles.

## Evaluation of the Test Field Track

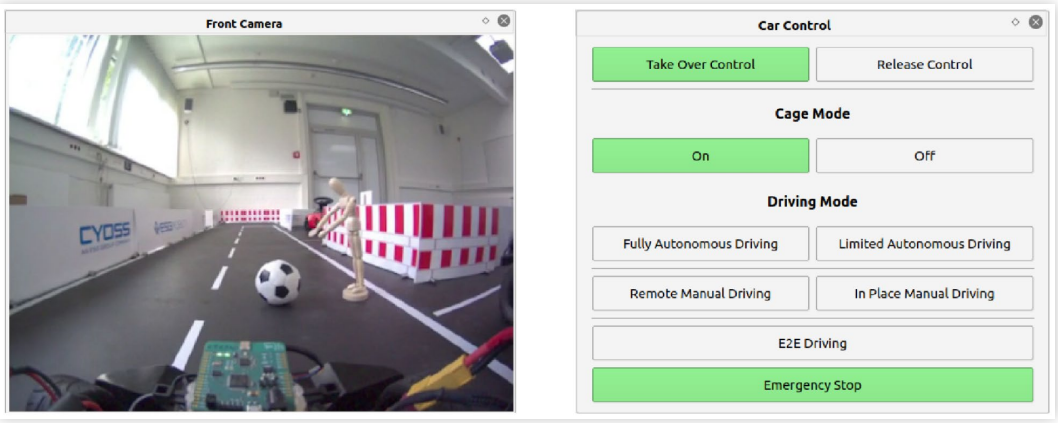
The evaluation on the test field track was done using a full-sized automated vehicle named PLUTO. The test track is situated at the NFF campus in Brunswick, Germany. PLUTO, an all-electric vehicle, was equipped with multiple LiDAR sensors, front and rear cameras, a GPS positioning system, and other sensors. More details on the setup of PLUTO can be found in [60], Section 3.4.

The transition from the model vehicle (see Figure 5) to the full-sized PLUTO vehicle ([60], Section 3.4) presented several challenges due to differences in sensor configuration and environmental conditions. PLUTO's sensors included a higher number and different types of LiDARs, which provided 360-degree coverage and generated significantly more data than the model vehicle's sensors. This increased data volume, combined with environmental factors such as sunlight, introduced additional noise and affected LiDAR functionality. Additionally, PLUTO's vehicle dynamics differed markedly from those of the model vehicle, impacting the calculation of the safe zone.

To address these issues, vehicle dynamics data for PLUTO were collected through multiple test drives, allowing for adjustments to the safe zone parameters. LiDAR data noise was reduced using a Z cut-off and a clustering algorithm to eliminate ghost points, see the work in [38] for more details.

Similar to the lab evaluation, a scenario-based testing approach was used to evaluate the graceful degradation concept on the PLUTO vehicle. To test the safety requirement SR1, PLUTO was driven at speeds of 5 m/s–20 m/s toward a static object. After adjusting the safe zone and LiDAR settings, the system successfully detected the obstacle and requested an increase in the intervention level from full autonomous driving to emergency stop 1 m before impact. The human safety operator could

**FIGURE 11** Emergency stop due to obstacle in the path of the vehicle: front camera with visible obstacles (left) and emergency stop on the car control panel (right).

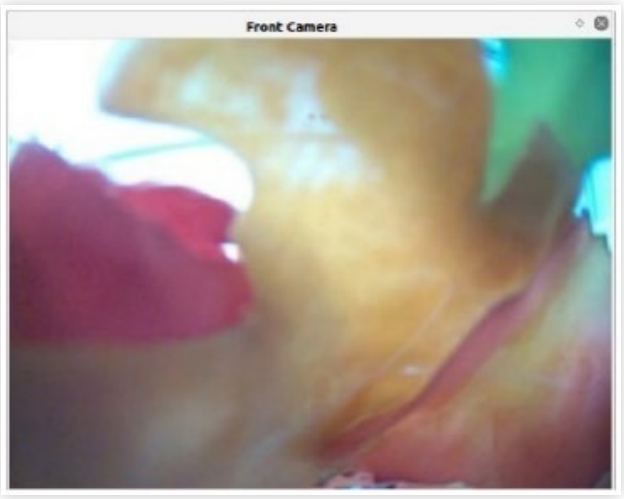





assess the situation and interact with the vehicle via the CCC.

Based on the definition of the first application scenario in Section 4, rather than choosing the lowest intervention level, full autonomous driving, the safety operator switches to the intermediate intervention level, limited autonomous driving, which reduces the required safety distance. Operating in limited autonomous mode, the AV attempts to navigate through the narrow road again. During the limited autonomous driving mode, both the human operator and the ADS share the responsibility for the safety of the vehicle, with the human operator monitoring continuously the safety status of the AV via the live sensor data streaming. Once the AV successfully passes through the narrow section, it requests a return to the lowest intervention level, full autonomous driving. since the human operator retains partial responsibility over the AV's safety, they must confirm that the issue vehicle's path is free of obstacles, before decreasing the intervention level to full autonomous driving mode.

**FIGURE 12** Front camera panel on the CCC showing the camera lens blocked by leaves.






For the test of the ODD constraint ODD-C1, a translucent bag was deliberately placed over the camera lens of the AV. The Camera Detector in the DC detected the obstruction and the DC requested an increase in the intervention level from full autonomous driving to emergency stop. Based on the definition of the second application scenario in Section 5, at this point, the offboard human operator has fully assumed responsibility for the AV's decision control and safety. The offboard operator then delegates the responsibility to a local operator near the AV to solve the issue of the camera sensor. After the local operator removes the leaves, they notify the offboard safety operator at the remote CCC to return control. Once they confirm that the issue has been resolved through live streaming of sensor data, the human safety operator requests a decrease of the intervention level from emergency stop back to full autonomous driving. this restores the AV to fully autonomous mode. The results reported in this section are also available in the form of videos [56, 65, 66].

## 6. Summary and Future Work

This article presented a concept for the graceful degradation of system functionality in ADSs accompanied by an integrated safety architecture for ensuring system safety using connected dependability cages. The integrated safety architecture supports the graceful degradation concept by providing two runtime monitoring systems: (1) the connected DC monitors the ADS onboard the AV and (2) the remote CCC supervises offboard an entire fleet of AVs with the cooperation of a remote human safety operator. The graceful

degradation of system functionality enables the reconfiguration of the ADS and the smooth share and transfer of responsibility over the DDT between the ADS and the remote safety operator. A qualitative evaluation of the graceful degradation concept was carried out both in a lab environment using a scale 1:8 model car and on a test track in Brunswick using a full-sized automated test vehicle. The results of the qualitative evaluation demonstrated the feasibility of the proposed graceful degradation concept for the ADS functionality through its application in scenarios from the domain of parcel delivery logistics.

Numerous promising routes for potential work include expanding the capabilities of DC. Currently, when a static obstacle detected by DC triggers a maximum intervention level, emergency stop is a fail-safe reaction for AV. In further developments, the aim is to enhance the dependability cage to support fail-operational reactions as well. We envision these fail-operational reactions to be akin to those of a human driver. For instance, the ADS might request an increase in the intervention level from full autonomous driving to limited autonomous driving, bypassing the emergency stop. This would allow the AV to gently steer away from the obstacle and maneuver around it while in limited autonomous driving mode. During this maneuver, the human safety operator would remain engaged, supervising the AV and ready to initiate an emergency stop if needed. After successfully driving through the obstacle, the AV could then request a return to full autonomous driving mode and continue its journey.

Additionally, we plan to conduct a quantitative evaluation involving a broader range of driving scenarios, including more classes of dynamic obstacles. We also intend to incorporate a quantitative monitor into the dependability cage, capable of assessing the novelty of current driving situations. The insights from this monitor will inform decisions regarding the graceful degradation of the system's functionality. Moreover, we aim to extend the remote CCC functionality to facilitate cooperation not only between the AV and the postman but also with a delivery robot, which would handle the transfer of parcels from the AV to the end customer.

# Acknowledgements

The research presented in this article is an outcome of the VanAssist project. The project was carried out between October 2018 and June 2021 under the project lead of ZENTEC Center for Technology, Business Start-ups, and Cooperation GmbH. The authors express their gratitude for the collaboration of all cooperative partners and acknowledge the funding from the Federal Ministry for Transportation and Digital Infrastructure (De.: Bundesministerium für Verkehr und digitale Infrastruktur) under the grant number 16AVF2139E.

# Contact Information

**Iqra Aslam**
iqra.aslam@tu-clausthal.de

**Meng Zhang**
meng.zhang@tu-clausthal.de

**Adina Aniculaesei**
adina.aniculaesei@tu-clausthal.de

# Definitions/Abbreviations

**ADS** - Autonomous Driving System

**AV** - Autonomous Vehicle

**CCC** - Remote Command Control Center to remotely supervise a fleet of vehicles

**DC** - Dependability Cage

**NFF** - Automotive Research Centre Niedersachsen (De.: Niedersächsisches Forschungszentrum Fahrzeugtechnik)

# References

1. Vijayenthiran, V., "Waymo's Self-Driving Taxis Will Cover 100 Square Miles of Phoenix," 2018, accessed March 20, 2025, https://www.motorauthority.com/news/1116055_waymos-self-driving-taxis-will-cover-100-square-miles-of-phoenix.
2. Abdel-Aty, M. and Ding, S., "A Matched Case-Control Analysis of Autonomous vs. Human Driven Vehicle Accidents," *Nature Communications* 15 (2024): 4931, doi:https://doi.org/10.1038/s41467-024-48526-4.
3. Ahangarnejad, A.H., Radmehr, A., and Ahmadian, M., "A Review of Vehicle Active Safety Control Methods—From Anti-Lock Brakes to Semi-Autonomy," *Journal of Vibration and Control* 27, no. 15–16 (2021): 1683-1712, doi:https://doi.org/10.1177/1077546320948656.
4. Bareiss, M., Scanlon, J., Sherony, R., and Gabler, H.C., "Crash and Injury Prevention Estimates for Intersection Driver Assistance Systems in Left Turn Across Path/Opposite Direction Crashes in the United States," *Traffic Injury Prevention* 20, no. S1 (2019): S133-S138, doi:https://doi.org/10.1080/15389588.2019.1610945.
5. Sun, Z., Bebis, G., and Miller, R., "On-Road Vehicle Detection: A Review," *IEEE Trans. Pattern Anal. Mach. Intell.* 28 (2006): 694-711.
6. Zang, S., Ding, M., Smith, D., Tyler, P. et al., "The Impact of Adverse Weather Conditions on Autonomous Vehicles: How Rain, Snow, Fog, and Hail Affect the Performance of a Self-Driving Car," *IEEE Vehicular Technol. Mag.* 14 (2019): 103-111.
7. Vargas, J., Alsweiss, S., Toker, O., Razdan, R. et al., "An Overview of Autonomous Vehicles Sensors and Their

Vulnerability to Weather Conditions," *Sensors* 21 (2021): 5397.

8. Van Brummelen, J., O'Brien, M., Gruyer, D., and Najjaran, H., "Autonomous Vehicle Perception: The Technology of Today and Tomorrow," *Transp. Res. Part C* 89 (2018): 384-406.
9. Radecki, P., Campbell, M., and Matzen, K., "All Weather Perception: Joint Data Association, Tracking, and Classification for Autonomous Ground Vehicles," arXiv preprint arXiv:1605.02196, 2016, https://arxiv.org/abs/1605.02196.
10. Filgueira, A., González-Jorge, H., Lagüela, S., Díaz-Vilariño, L. et al., "Quantifying the Influence of Rain in LiDAR Performance," *Measurement* 95 (2017): 143-148.
11. Yeong, D.J., Velasco-Hernandez, G., Barry, J., and Walsh, J., "Sensor and Sensor Fusion Technology in Autonomous Vehicles: A Review," *Sensors* 21 (2021): 2140.
12. Li, Y. et al., "Evaluation of the Impacts of Cooperative Adaptive Cruise Control on Reducing Rear-End Collision Risks on Freeways," *Accid. Anal. Prev.* 98 (2017): 87-95.
13. Adewale, A. and Lee, C., "Prediction of Car-Following Behavior of Autonomous Vehicle and Human-Driven Vehicle Based on Drivers' Memory and Cooperation with Lead Vehicle," *Transp. Res. Record.* 2678, no. 6 (2023): 248-266, doi:https://doi.org/10.1177/03611981231195051.
14. Li, Y., Wu, D., Lee, J., Yang, M. et al., "Analysis of the Transition Condition of Rear-End Collisions Using Time-to-Collision Index and Vehicle Trajectory Data," *Accid. Anal. Prev.* 144 (2020): 105676.
15. SAE International Recommended Practice, "Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles," SAE Standard J3016_202104, revised April 2021, https://doi.org/10.4271/J3016_202104.
16. International Organization for Standardization, "ISO: Road Vehicles—Functional Safety," Geneva, Switzerland, 2018, https://www.iso.org/standard/68383.html.
17. International Organization for Standardization, "ISO: Road Vehicles—Safety of the Intended Functionality," Geneva, Switzerland, 2022, https://www.iso.org/standard/77490.html.
18. Mauritz, M., "Engineering of Safe Autonomous Vehicles through Seamless Integration of System Development and System Operation," PhD thesis, Technische Universität Clausthal, 2019.
19. Levin, M.W. and Boyles, S.D., "Intersection Auctions and Reservation-Based Control in Dynamic Traffic Assignment," *Transp. Res. Rec.* 2497 (2015): 35-44.
20. Haris, M. and Hou, J., "Obstacle Detection and Safely Navigate the Autonomous Vehicle from Unexpected Obstacles on the Driving Lane," *Sensors* 20 (2020): 4719.
21. Endsley, M.R., "Toward a Theory of Situation Awareness in Dynamic Systems," *Hum. Factors* 37 (1995): 32-64.
22. Bhavsar, P., Das, P., Paugh, M., Dey, K. et al., "Risk Analysis of Autonomous Vehicles in Mixed Traffic Streams," *Transp. Res. Rec.* 2625 (2017): 51-61.
23. Fagnant, D.J. and Kockelman, K., "Preparing a Nation for Autonomous Vehicles: Opportunities, Barriers and Policy Recommendations," *Transp. Res. Part A* 77 (2015): 167-181.
24. Zhang, Q., Hong, D.K., Zhang, Z., Chen, Q.A. et al., "A Systematic Framework to Identify Violations of Scenario-Dependent Driving Rules in Autonomous Vehicle Software," *Proc. ACM Meas. Anal. Comput. Syst.* 5 (2021): 1-25.
25. Riedmaier, S., Ponn, T., Ludwig, D., Schick, B. et al., "Survey on Scenario-Based Safety Assessment of Automated Vehicles," *IEEE Access* 8 (2020): 87456-87477.
26. Zhou, D., Ma, Z., Zhang, X., and Sun, J., "Autonomous Vehicles' Intended Cooperative Motion Planning for Unprotected Turning at Intersections," *IET Intell. Transp. Syst.* 16 (2022): 1058-1073.
27. Wael, K.M.A., Miho, A., Hideki, N., and Dang Minh, T., "Stochastic Approach for Modeling the Effects of Intersection Geometry on Turning Vehicle Paths," *Transp. Res. Part C* 32 (2013): 179-192.
28. Noh, S., "Decision-Making Framework for Autonomous Driving at Road Intersections: Safeguarding against Collision, Overly Conservative Behavior, and Violation Vehicles," *EEE Trans. Ind. Electron.* 66 (2018): 3275-3286.
29. Grahn, H., Kujala, T., Silvennoinen, J., Leppänen, A. et al., "Expert Drivers' Prospective Thinking-Aloud to Enhance Automated Driving Technologies–Investigating Uncertainty and Anticipation in Traffic," *Accid. Anal. Prev.* 146 (2020): 105717.
30. Lake, B.M., Ullman, T.D., Tenenbaum, J.B., and Gershman, S.J., "Building Machines that Learn and Think like People," *Behav. Brain Sci.* 40 (2017): e253.
31. Schwarting, W., Pierson, A., Alonso-Mora, J., Karaman, S. et al., "Social Behavior for Autonomous Vehicles," *Proc. Natl Acad. Sci.* 116 (2019): 24972-24978.
32. Zhang, Y., Wang, W., Zhou, X., Wang, Q. et al., "Tactical-Level Explanation Is Not Enough: Effect of Explaining AV's Lane-Changing Decisions on Drivers' Decision-Making, Trust, and Emotional Experience," *Int. J. Hum. Comput. Interact.* 39 (2023): 1438-1454.
33. Rasouli, A. and Tsotsos, J.K., "Autonomous Vehicles that Interact with Pedestrians: A Survey of Theory and Practice," *IEEE Trans. Intell. Transp. Syst.* 21 (2019): 900-918.
34. Steinmeier, F., Merkel, A., and Scheuer, A.,"Bill Amending the Road Traffic Bill and the Compulsory Insurance Bill—Bill on Autonomous Driving," *German Federal Law Gazette* 2021, Part 1, no. 48: 3108-3114, Bundesanzeiger Verlag, 2021.
35. Aniculaesei, A., Grieser, J., Rausch, A., Rehfeldt, K. et al., "Graceful Degradation of Decision and Control Responsibility for Autonomous Systems Based on Dependability Cages," in *Proceedings of the 5th International Symposium on Future Active Safety Technology toward Zero Accidents*, Blacksburg, VA, September 2019.
36. Aniculaesei, A., Grieser, J., Rausch, A., Rehfeldt, K. et al., "Towards a Holistic Software System Engineering

Approach for Dependable Autonomous Systems," in *Proceedings of the 1st International Workshop on Software Engineering for AI in Autonomous Systems*, Gothenburg, Sweden, 2018, https://doi.org/10.1145/3194085.3194091

37. Grieser, J., Zhang, M., Warnecke, T., and Rausch, A., "Assuring the Safety of End-to-End Learning-Based Autonomous Driving through Runtime Monitoring," in *Proceedings of the 23rd Euro Micro-Conference on Digital System Design (DSD)*, Kranj, Slovenia, 2020, 476-483, IEEE, https://doi.org/10.1109/DSD51259.2020.00081
38. Helsch, F., Aslam, I., Buragohain, A., and Rausch, A., "Qualitative Monitors Based on the Connected Dependability Cage Approach," in *Proceedings of the 14th International Conference on Adaptive and Self-Adaptive Systems*, Barcelona, Spain,2022, 46-55, IARIA.
39. Aniculaesei, A., Aslam, I., Bamal, D., Helsch, F. et al., "Connected Dependability Cage Approach for Safe Automated Driving," in *Proceedings of the 23rd International Stuttgart Symposium*, Stuttgart, Germany, 2023, 3-21, Springer, https://doi.org/10.1007/978-3-658-42048-2_1.
40. Aslam, I., Aniculaesei, A., Buragohain, A., Zhang, M. et al., "Runtime Safety Assurance of Autonomous Last-Mile Delivery Vehicles in Urban-like Environment," SAE Technical Paper 2024-01-2991 (2024), doi:https://doi.org/10.4271/2024-01-2991.
41. Besser Smart – Das Innovationsportal, "Lower Saxony Test Field for Automated and Connected Mobility Opened," 2020, accessed December 28, 2024, https://www.braunschweig.de/innovationsportal/smarte-mobilitaet/testfeld-niedersachsen.php.
42. Besser Smart – Das Innovationsportal, "Brunswick as a Transport Lab," 2019, accessed December 28, 2024, https://www.braunschweig.de/innovationsportal/smarte-mobilitaet/artikel_aim.php.
43. Green, S.A., Billinghurst, M., Chen, X., and Chase, J.G., "Human-Robot Collaboration: A Literature Review and Augmented Reality Approach in Design," *International Journal of Advanced Robotic Systems* 5, no. 1 (2008): 1.
44. Stayton, E. and Stilgoe, J., "It's Time to Rethink Levels of Automation for Self-Driving Vehicles [Opinion]," *IEEE Technology and Society Magazine* 39, no. 3 (2020): 13-19.
45. Cooke, N.J., "Human Factors of Remotely Operated Vehicles," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 50 (Los Angeles, CA: SAGE Publications, 2006), 166-169.
46. Mutzenich, C., Durant, S., Helman, S., and Dalton, P., "Updating Our Understanding of Situation Awareness in Relation to Remote Operators of Autonomous Vehicles," *International Journal on Cognitive Research: Principles and Implications* 6, no. 1 (2021): 1-17.
47. Andersson, J., Rizgary, D., Söderman, M. and Vännström, J., "HAVOC Heavy Vehicle Operation Centre Project within Vinnova FFI Trafiksäkerhet och automatiserade fordon (TSAF)," 2022.
48. Kettwich, C., Schrank, A., and Oehl, M., "Teleoperation of Highly Automated Vehicles in Public Transport: User-Centered Design of a Human-Machine Interface for Remote-Operation and Its Expert Usability Evaluation," *Multimodal Technologies and Interaction* 5, no. 5 (2021): 26.
49. Fabris, E.J., Sangalli, V.A., Soares, L.P., and Pinho, M.S., "Immersive Telepresence on the Operation of Unmanned Vehicles," *International Journal of Advanced Robotic Systems* 18, no. 1 (2021): 1729881420978544.
50. Kalinov, I., Trinitatova, D., and Tsetserukou, D., "WareVR: Virtual Reality Interface for Supervision of Autonomous Robotic System Aimed at Warehouse Stocktaking," in *2021 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Melbourne, Australia, 2021, 2139-2145, IEEE.
51. Neumeier, S., Gay, N., Dannheim, C., and Facchi, C., "On the Way to Autonomous Vehicles Teleoperated Driving," in *AmE 2018—Automotive Meets Electronics; 9th GMM Symposium*, Dortmund, Germany, 2018, 1-6, VDE.
52. Shen, X., Chong, Z.J., Pendleton, S., James Fu, G.M. et al., "Teleoperation of On-Road Vehicles via Immersive Telepresence Using Off-the-Shelf Components," *Advances in Intelligent Systems and Computing* 302 (2016): 1419-1433.
53. Hosseini, A. and Lienkamp, M., "Enhancing Telepresence during the Teleoperation of Road Vehicles Using HMD-Based Mixed Reality," in *2016 IEEE Intelligent Vehicles Symposium (IV)*, Gothenburg, Sweden, 2016, 1366-1373, IEEE.
54. Graf, G., Palleis, H., and Hussmann, H., "A Design Space for Advanced Visual Interfaces for Teleoperated Autonomous Vehicles," in *Proceedings of the International Conference on Advanced Visual Interfaces*, Ischia Island, Italy, 2020, 1-3.
55. Kalamkar, S., Biener, V., Beck, F., and Grubert, J., "Remote Monitoring and Teleoperation of Autonomous Vehicles—Is Virtual Reality an Option?" in *2023 IEEE International Symposium on Mixed and Augmented Reality (ISMAR)*, Sydney, Australia, 2023.
56. Badescu, L., "Software for Fail-Operational Systems in Autonomous Vehicles," Elektrobit, accessed March 20, 2025, https://www.elektrobit.com/blog/software-for-fail-operational-systems-in-autonomous-vehicles/?utm_source=chatgpt.com.
57. Karakaya, B. and Bengler, K., "Minimal Risk Maneuvers of Automated Vehicles: Effects of a Contact Analog Head-Up Display Supporting Driver Decisions and Actions in Transition Phases," *Safety* 9, no. 1 (2023): 7.
58. Matute-Peaspan, J.A., Perez, J., and Zubizarreta, A., "A Fail-Operational Control Architecture Approach and Dead-Reckoning Strategy in Case of Positioning Failures," *Sensors* 20, no. 2 (2020): 442.

59. Dantuluri, N.A.V. and Pisu, P., "Safety Diagnostics and Degraded Operational Modes for Off-Road Unmanned Ground Combat Vehicles," in *Annual Conference of the PHM Society*, Vol. 13, 2021.
60. Seber, G., Czerwionka, P., Hegerhorst, T., Schappacher, M. et al., "Final Project Report VanAssist," Technical Report, 2021, accessed July 31, 2024, https://www.vanassist.de/ergebnisse/.
61. Anysys, "Anysys SCADE Suite—Model-Based Development Environment for Critical Embedded Software," accessed August 3, 2024, https://www.ansys.com/products/embedded-software/ansys-scade-suite.
62. Esterel Technologies SAS, "SCADE Language Reference Manual," ANSYS, Inc., 2018.
63. Bouali, A. and Dion, B., "Formal Verification for Model-Based Development," SAE Technical Paper 2005-01-0781 (2005), doi:https://doi.org/10.4271/2005-01-0781.
64. Esterel Technologies SAS, "SCADE Suite User Manual," vol. SCS-UM-19 – DOC/rev/35771-03, ANSYS, Inc., 2018.
65. Clarke, E.M., Henzinger, T.A., and Veith, H., "Introduction to Model Checking," in Clarke, E.M., Henzinger, T.A., Veith, H., and Bloem, R. (eds.), *Handbook of Model Checking* (Cham, Switzerland: Springer International Publishing, 2018), 1-26.
66. Institute for Software and Systems Engineering, "VanAssist: Use Case of Connected Dependability Cage," YouTube Video, accessed July 31, 2024, https://www.youtube.com/watch?v=iaM7iYJlJKA.
67. DPD Deutschland, "VanAssist: This Is What the Autonomous Delivery Vehicle of the Future Could Look Like," YouTube Video, accessed July 31, 2024, https://www.youtube.com/watch?v=6dgMxvnjZb8.