

# **A FRAMEWORK FOR AUTOMATED DRIVING SYSTEM TESTABLE CASES AND SCENARIOS**

## **Paul Rau**

National Highway Traffic Safety Administration  
United States

## **Eric Thorn**

Southwest Research Institute  
United States

Paper 19-0301

## **ABSTRACT**

Automated Driving Systems (ADS) are being developed to perform the primary functions of the dynamic driving task (DDT). These technologies hold great promise to improve safety and mobility for transportation. Test scenarios are critical for assessing the safety assurance of ADS in a range of operational environments and roadway conditions. The development of testing scenarios for ADS is proving to be an important challenge for the development of safety assurance requirements, certification and licensing frameworks, testbed services, standards, and international harmonization.

This paper summarizes foundational research undertaken to identify a sample preliminary, objective testing and evaluation approach for ADS. The paper considers technologies of interest that fall within Level 3 through Level 5 of the SAE International levels of driving automation and identifies a cross-section of prototype and conceptual ADS that are then categorized into seven generic ADS features.

This research also takes the first steps to partition the ADS performance space by identifying and assessing the primary variables that comprise an ADS test scenario. Those primary variables are described in detail, and include:

- Tactical and Operational Maneuvers
- Operational Design Domain (ODD)
- Object and Event Detection and Responses (OEDR)
- Failure Mode Behaviors

Tactical and operational maneuver capabilities largely focus on the control-related elements of the DDT (i.e., lateral and longitudinal control) that enable an ADS to navigate to reach its destination (e.g., lane centering / following, turning). A working list of these capabilities is presented. The ODD represents the operating conditions under which an ADS is designed to function (e.g., roadway types, weather conditions, etc.). A notional hierarchical ODD taxonomy is presented and described. OEDR capabilities include the elements of the DDT that involve monitoring the driving environment and implementing appropriate responses to relevant objects and events. A working list of OEDR capabilities is presented. Failure mode behaviors include fail-safe (FS) and fail-operational (FO) strategies that will allow an ADS to respond to a variety of failures, including DDT performance-relevant system failures that require the ADS or a DDT fallback-ready user to achieve a minimal risk condition.

The paper also considers the implementation of the proposed evaluation framework using existing test methods, including modeling and simulation (M&S), closed track testing, and open road testing. It further seeks to examine how each of the testing methods can be logically used to minimize the complexity of comprehensive safety assessments of ADS by leveraging each method's strengths to maximize the knowledge gained from each test. It also includes extensive discussion of challenges associated with testing ADS, including challenges related to the technology itself as well as challenges associated with test execution. This paper is based on research completed by NHTSA and its contractors, and is more fully documented in NHTSA Report DOT HS 812 623, "A Framework for Automated Driving System and Testable Cases and Scenarios"; September 2018.

## **INTRODUCTION**

Since 1975, the first year that the Fatality Analysis Reporting System began collecting data, the rate of traffic fatalities per 100 million miles traveled in the United States has decreased by 66 percent, according to the National

Highway Traffic Safety Administration's (NHTSA's) Traffic Safety Facts 2015 data (NHTSA, 2017b). Advancements in motor vehicle safety have been made through continuous engineering innovation, public education, industry agreements, safety regulations, and safety rating programs. There is, however, significant room for continued focus on motor vehicle traffic safety. In October 2017, NHTSA reported that traffic fatalities increased by 5.4 percent from 2015 to 2016 (35,485 to 37,461) for the United States (NHTSA, 2017c), which follows an 8.4 percent increase from 2014 to 2015 (32,744 to 35,485) (NHTSA, 2017b).

Many forces are at work in the automotive industry to advance safety technology. The worldwide automotive industry has recognized driver performance (e.g., error and choice) as a key factor that impacts safety and has begun to introduce systems that complement the driver in terms of enhanced perception with 360-degree vehicle views and rear video systems. Advanced Driver Assistance Systems that monitor the operational environment and enhance driver detection and response, such as Forward Collision Warning (FCW) and Lane Keeping Assist (LKA), are increasingly common in newer model vehicles. Additionally, 20 automakers have committed to making Automatic Emergency Braking (AEB) a standard feature in new vehicles by 2022 (IIHS, 2016).

Recently, research activities by several companies to develop ADS that can perform certain driving functions automatically have captured the nation's attention. ADS have been the subject of multiple congressional hearings and the public has provided numerous responses to NHTSA's Federal Automated Vehicles Policy (NHTSA, 2016b), including over 1,100 responses from industry participants, state and municipal transportation agencies, policy groups, and citizens (Kyrouz, 2017). The United States Department of Transportation (USDOT) and NHTSA recently released an update to their federal guidance for ADS that focused on their development and safe deployment and operation. NHTSA also continues to advance its ADS research. The research summarized in this paper sought to analyze aspects of ADS testing and develop examples of tests and evaluation methods for specific ADS features. A sample testing framework was developed that could further support the goals of improving safety for all users of the transportation network.

## **OBJECTIVE**

The purpose of this study was to analyze aspects of ADS testing to create a framework for developing test cases and test scenarios for ADS. Consideration was given to keeping the framework flexible and extensible such that it could be applied with different test approaches and methods. The ultimate goal of this framework is to support the safe deployment of ADS in the broader transportation system.

## **AUTOMATED DRIVING SYSTEM FEATURES**

As an initial step to develop this framework, sample concept ADS features that have been proposed for deployment were identified. This analysis focused on SAE International Levels 3-5 ADS (SAE International, 2018), such as Google's (Waymo's) self-driving car project and others like it that focus on next-generation automation. This step is critical because the sample concept ADS features are used to identify ODDs and OEDRs, develop preliminary tests and/or evaluation methods, and assess FS and FO mechanisms, which form a foundation to begin considering validation and verification approaches for ADS.

A four-stage approach was followed to identify ADS features: 1) review the literature, 2) define a framework for discussing ADS features, 3) define features and behaviors, and 4) categorize the features. To guide later analysis, priority ADS features on which to focus were identified. Over 50 literature sources were reviewed, including original equipment manufacturer (OEM) websites, press releases of vehicles being tested in specific domains, NHTSA pre-crash scenario analysis (NHTSA, 2007), NHTSA's Fiscal Year 2017 budget request (NHTSA, 2016c), NHTSA L2 and L3 Human Factors Concepts (NHTSA, 2015), Federal Highway Administration (FHWA) managed lane use cases (FHWA, 2008), and technical and international publications, including proceedings of the 2015 and 2016 Automated Vehicles Symposia and United Nations Economic Commission for Europe (UNECE) World Forum for Harmonization of Vehicle Regulations (WP.29) Automatically Commanded Steering Function working group, among others. Research sponsored by USDOT, such as the Crash Avoidance Metrics Partnership Automated Vehicle Research for Enhanced Safety (Christensen, et al., 2015; NHTSA, 2016d), which details functional descriptions for on-road driving automation levels, was also used.

Twenty-three concept ADS features were identified:

1. Audi Traffic Jam Pilot

2. Audi Highway Pilot
3. Auro Self Driving Shuttle
4. Baidu Automated TNC<sup>1</sup> Bosch Valet Parking
5. CityMobil2 Automated Shuttle
6. Bosch Highway Pilot
7. EZ10 Self Driving Shuttle
8. Ford Automated TNC
9. GM Cruise Automation TNC
10. Google Car
11. Honda Automated Drive
12. Mercedes Highway Pilot Truck
13. Navya Arma Shuttle
14. Nissan Autonomous Drive
15. Olli Local Motors Shuttle
16. Otto Trucking
17. Tesla Self-Drive
18. Toyota Chauffeur
19. Toyota Guardian
20. Uber Automated TNC
21. Varden Labs Self Driving Shuttles
22. Volkswagen I.D. Pilot
23. Volvo IntelliSafe Auto Pilot

These 23 features were categorized into the following seven generic categories:

1. L3 Conditional Automated Traffic Jam Drive
2. L3 Conditional Automated Highway Drive
3. L4 Highly Automated Low Speed Shuttle
4. L4 Highly Automated Valet Parking
5. L4 Highly Automated Emergency Take-Over
6. L4 Highly Automated Highway Drive
7. L4 Highly Automated Vehicle / TNC

Through the literature review and analysis, a working list of tactical and operational maneuvers related to ADS driving control was created. Some examples of these tactical and operational maneuvers included: parking, maintaining speed, lane centering, low-speed merge, right-of-way decision, following driving laws, and U-turns, among others.

Each of the identified generic ADS features was then described in terms of tactical maneuver behaviors, estimated commercial availability, and estimated level of automation. Figure 1 shows a sample analysis for the L4 Highly Automated Vehicle / TNC Feature. It should be noted that these commercial ADS features were identified several years ago and the list has changed quite significantly. It should also be noted that the estimates for commercial availability, level of driving automation, and tactical maneuver demonstration were deduced from the information available, which was limited, and as such should be considered notional.

---

<sup>1</sup> TNC: Transportation Network Company

<b>ADS Features and Tactical Maneuvers</b>  (X = demonstrated, ? = speculated)	Commercially Available? (Y/N)	Level of Automation (SAE 1-5)	Parking	Maintain Speed	Car Following	Lane Centering	Lane Switching/Overtaking	Enhancing Conspicuity	Merge	Navigate On/Off Ramps	Follow Driving Laws	Navigate Roundabouts	Navigate Intersection	Navigate Crosswalk	Navigate Work Zone	N-Point Turn	U-Turn	Route Planning
	Waymo Automated TNC	N	4	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Tesla Self-Drive	N	4	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Volkswagen I.D. Pilot	N	4?	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Volvo IntelliSafe Auto Pilot	N	4	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Nissan Autonomous Drive (2020)	N	4?	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
GM Cruise Automation	N	4	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Uber Automated TNC	N	4	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Honda Automated Drive (2020)	N	4	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Ford Automated TNC (2022)	N	4	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Baidu Automated TNC	N	4	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Toyota Chauffeur	N	4	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

**Figure 1. L4 Highly Automated Vehicle / TNC Features.**

## OPERATIONAL DESIGN DOMAIN

An operational design domain (ODD) describes the specific operating domain(s) in which an ADS feature is designed to function with respect to roadway types, speed range, lighting conditions (day and/or night), weather conditions, and other operations constraints. ODD will likely vary for each ADS feature, even if there is more than one ADS feature on a vehicle. The testing framework presented in this paper considers the potential range of ODDs and how ODDs factor into developing potential test cases.

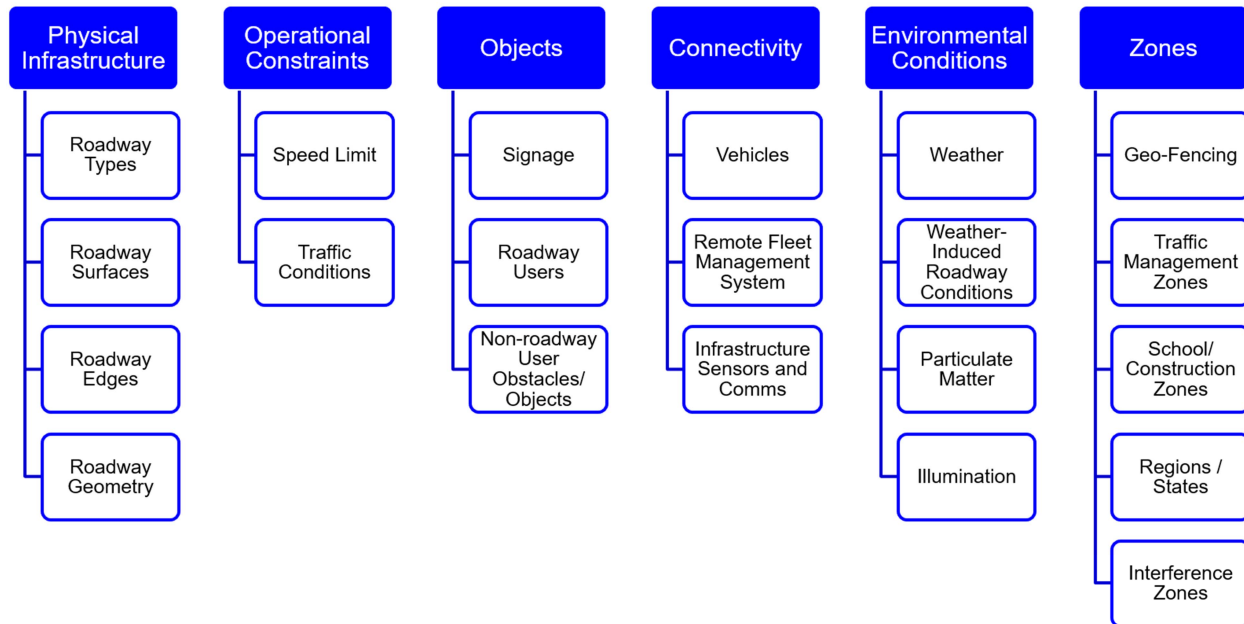
A three-stage approach was taken to define the ODDs:

1. Review the literature, including popular media, press releases, technical journals, and conference proceedings to identify key concepts, enumerate potential ODD characteristics, and examine approaches to ODD in other industries.
2. Define and categorize ODD into a sample taxonomy that can be used by departments of transportation (DOTs) and industry to discuss ADS.
3. Describe ODDs in which concept ADS features may operate based on literature review and engineering judgment.

Over 50 literature sources were reviewed, including OEM websites, press releases, USDOT documents, including NHTSA pre-crash scenario analysis and FHWA managed lane use case, as well as technical and international publications, including proceedings of the 2015 and 2016 Automated Vehicles Symposiums. Additionally, the NHTSA Fiscal Year 2017 Budget Request to Congressional Appropriations Committees (NHTSA, 2016c) identifies several ADS use cases that were considered when defining the ODD for this analysis. It should be noted that given the emerging and highly competitive nature of ADS technology, it is inherently difficult to obtain explicit and complete information about the intended ODD of an ADS feature. In the absence of information about an ODD,

engineering judgement was used at times to define the ODD taxonomy and identify the ODD for concept ADS features.

While the literature provided many examples of ODD elements, no classification framework was identified. This work takes an initial step towards developing a taxonomy to organize the many ODD elements identified in research. This sample ODD taxonomy takes the form of a hierarchy of categories and subcategories, each with definitions and, where appropriate, gradations. This taxonomy is meant to be descriptive, not normative, as it is envisioned that these elements may be organized into several different groupings. The taxonomy offers a structured approach to organize and identify various ODDs for ADS features, especially when there are several different possible combinations. Figure 2 **Error! Reference source not found.** shows the broad range of top-level categories and immediate subcategories. It should again be noted that this sample taxonomy was derived using available information at the time the research was conducted and should be considered notional.



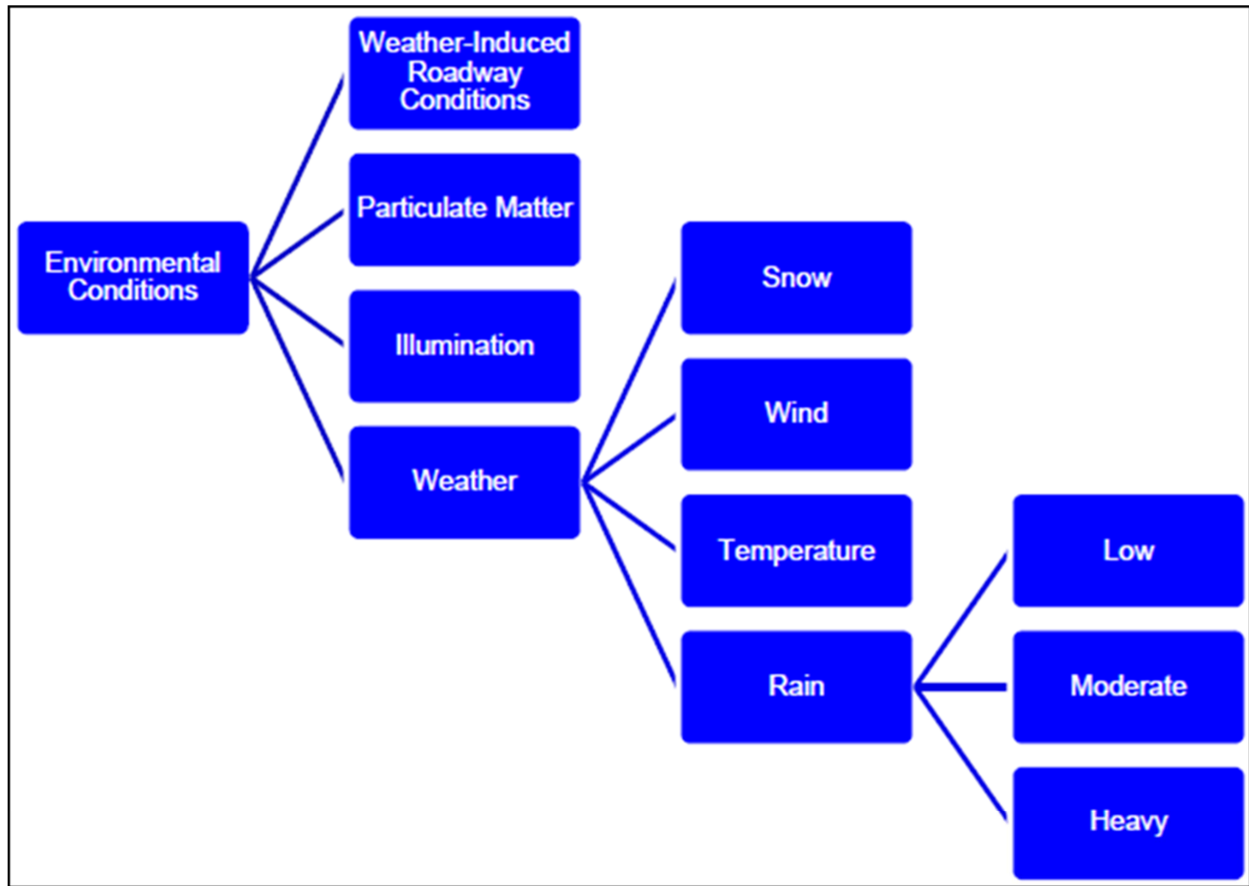
**Figure 2. ODD Classification Framework with Top-Level Categories and Immediate Subcategories.**

The hierarchy extends into multiple sublevels. For example, **Error! Reference source not found.** shows that the “Environmental Conditions” category was divided into four subcategories: weather, illumination, particulate matter, and road weather. Weather is further subdivided into rain, temperature, wind, and snow. For this research, it was helpful to further subdivide rain into gradations to capture the data that were collected on ADS features. For example, some ADS features had been tested in light rain, while others had been tested in heavy rain. Although the application of this sample taxonomy has been useful in the context of this research, further research and stakeholder engagement would be beneficial in refining and objectively quantifying the categories and gradations.

The sample ODD taxonomy lends itself to serving as a checklist for identifying the ODD of an ADS feature. A comprehensive ODD checklist was generated based on the ODD taxonomy described above. To demonstrate a potential application of the checklist, the checklist was filled out for three theoretical ADS features. It should be noted that the manufacturer determines the ODD for a feature, and the ODD may vary for similar ADS features. The theoretical features presented here are purely demonstrative, not representative of any commercially marketed ADS feature.

To test a vehicle’s ability to operate safely, ODD is considered in test development and execution. Scenarios consider a combination of ODD elements that can be used to describe conditions for test cases and scenarios; for example, a highway with a concrete surface with a light mist. Test facilities are limited in their ability to re-create certain ODDs (e.g., urban environments, hill crests) and may need to be upgraded with new infrastructure to support

testing. Some ODD elements are difficult to quantify and re-create (e.g., weather), though it is possible they could be addressed through functional safety design practices and on-road testing.



*Figure 3. Example of Hierarchy Levels within the Environmental Conditions Category.*

## **OBJECT AND EVENT DETECTION AND RESPONSE**

While performing tactical maneuver behaviors described previously, ADS will inevitably interact with a variety of static and dynamic physical objects that may alter how these behaviors are executed. SAE J3016 identifies the following real-time functions as elements of the DDT related to addressing these interactions with objects:

- Object and event detection, recognition, and classification
- Object and event response

These functions can be generalized under the term Object and Event Detection and Response (OEDR). OEDR represents the ability of the ADS feature to detect any circumstance that is immediately relevant to the driving task and implement an appropriate response. One of the factors that determines the level of driving automation of an ADS is whether the human driver or ADS is responsible for monitoring the driving environment. ADS, which were the focus of this research, range from SAE International L3 through L5, which means that the ADS feature is completing all aspects of monitoring the driving environment.

The elements of an ADS functional architecture that are specifically relevant to OEDR generally include hardware and software components that support:

- Sensing (e.g., radar, laser scanners, cameras, etc.)
- Perception (e.g., road feature classification, object segmentation and classification, etc.)

- World modeling (e.g., persistent data mapping, dynamic obstacle tracking, and prediction, etc.)
- Navigation and planning (e.g., path planning and motion control commands to implement responses)

The sensing and perception elements of the architecture specifically support detection of relevant objects. World modeling supports the aggregation of perception and other information to identify and understand events that may occur through interactions with those objects. Navigation and planning support determination of the appropriate response to those events and interactions, and the generation of control commands to implement that response.

Three of the generic ADS features were selected for an OEDR analysis (L3 Conditional Automated Traffic Jam Drive, L3 Conditional Automated Highway Drive, and L4 Highly Automated Vehicle / TNC). This allowed for an evaluation of a cross-section of operating environments and conditions, as well as driving scenarios. Following the evaluation of the operational needs of the selected ADS features, a focusing exercise established baseline ODDs for each feature to further refine the analysis to identify OEDR capabilities for the three selected features. This exercise served to frame the OEDR analysis to account for the potential variability of certain ODD elements, as well as the substantial number of combinations and permutations of ODD elements. It is reasonable to expect that different organizations developing similar ADS features will generate unique designs and implementations, and thus will ultimately define different ODDs for their respective systems. With the ODD baselines established for each feature, a survey and analysis of the driving scenarios resulting from the operations descriptions led to the identification of relevant objects and interactions that the ADS could encounter. These objects and events are derived from an evaluation of normal driving scenarios for a given ADS feature operating in its ODD.

The developed baseline ODDs were used to identify important objects and events that ADS could feasibly encounter within those ODDs. Aggregated OEDR behavior capabilities are shown in Table 1.

**Table 1. Summary of OEDR Behavior Capabilities.**

Detect & Respond to Speed Limit Changes	Detect & Respond to Relevant School Buses
Detect & Respond to Encroaching, Oncoming Vehicles	Detect & Respond to Relevant Emergency Vehicles
Perform Vehicle Following	Detect & Respond to Relevant Pedestrians
Detect & Respond to Relevant Stopped Vehicles	Detect & Respond to Relevant Pedalcyclists
Detect & Respond to Relevant Lane Changes / Cut-ins	Detect & Respond to Relevant Animals
Detect & Respond to Relevant Static Obstacles in Lane	Detect & Respond to Relevant Vehicle Cut-out / Reveal
Detect & Navigate Work Zones	Detect & Respond to Relevant Vehicle Roadway Entry
Detect & Respond to Relevant Safety Officials	Detect & Respond to Relevant Adjacent Vehicles
Detect & Respond to Relevant Access Restrictions	Detect & Respond to ODD Boundary Transition
Detect & Respond to Relevant Dynamic Traffic Signs	

## FAILURE MODE BEHAVIOR

ADS will utilize FO and FS mechanisms when the system does not function as intended. These mechanisms are intended to cause the ADS to attain a minimal risk condition (MRC) that removes the vehicle and its occupants from harm’s way, to the best extent possible. Defining, testing, and validating FO and FS strategies for achieving an MRC are important steps in promoting the safe operation and deployment of ADS.

The appropriate failure mitigation strategy and resulting MRC for a given ADS is largely dependent on the type and nature of failures the ADS experiences. To this end, an understanding of potential ADS failure modes is necessary. As such, a high-level failure analysis was performed. The results of this analysis informed the assessment of FO and FS mechanisms. A variety of failure and hazard analysis techniques exist, including fault tree analysis (FTA), system failure mode and effects analysis (FMEA), failure modes, effects, and criticality analysis (FMECA), system-theoretic process analysis, and hazard and operability analysis (HazOp). System FMEA was identified and selected

as an initial approach to develop the high-level analysis needed to identify potential failures in each subsystem of the representative functional architecture, as well as their causes and impacts.

Existing reports and literature on ADS failures, including from the Defense Advanced Research Projects Agency (DARPA) Grand and Urban Challenges (DARPA, 2008), as well as engineering judgments and prior experience in ADS development and testing were leveraged and considered. It was assumed that a detailed failure analysis employing a range of techniques noted above has been performed on the base vehicle platform, and therefore efforts were focused on components specifically related to the ADS. This allowed for a deeper dive into a representative ADS functional architecture. Furthermore, failures that could have safety implications, as opposed to failures that are merely an inconvenience, were prioritized. The FMEA was broken down by architecture subsystems to identify potential key failures at each step through the ADS “pipeline”:

- Sensing and communication
- Perception
- Navigation and control
- Human Machine Interface (HMI)

In general, many of the ADS failure modes described above could be attributed to some kind of failures by the ADS to obtain information needed to perform the DDT. These were summarized into three primary categories as failures attributed to:

- No data – Information is absent altogether
- Inadequate quality data – Information is of poor or degraded quality
- Latent data – Information is delayed or old

After completing the FMEA for the ADS architecture, the various failure modes and effects were summarized and mapped to the relevant tactical maneuver and OEDR behaviors for the three down-sampled ADS features (L3 Traffic Jam Drive, L3 Highway Drive, and L4 Highly Automated Vehicle/TNC). This notionally provides a mapping from the specific failures identified in the FMEA, to the generalized failures summarized in the previous section, to the behaviors implemented by various ADS features.

Based on the general failure modes identified, potential failure mode responses and strategies were identified. This effort focused on FS strategies for cases where the ADS cannot continue to operate due to a significant failure, and FO strategies for cases where the ADS could continue to operate even in the face of a failure. It should be noted that these potential FS and FO strategies were determined from engineering judgements and available literature, and as such should be considered notional.

The primary goal of an FS strategy is to rapidly achieve an MRC where the vehicle and occupants are safe. Three candidate FS mechanisms were considered for further evaluation:

- Transition vehicle control to fallback-ready user
- Safely stop in lane of travel
- Safely move out of travel lane and stop

FO strategies allow the ADS to continue to function, even in the event of one or more failures. It is important to note that this operation may only be supported for a limited duration, or potentially with a reduced set of capabilities. Three primary FO mechanisms were considered for further analysis:

- Hardware/software redundancy
- Adaptive compensation (e.g., ignore data coming from failed sensor or component and weight inputs from other sensors or components more heavily)
- Degraded operation(s)
  - Reduced top speed
  - Reduced level of automation
  - Reduced ODD
  - Reduced maneuver capabilities
  - Reduced OEDR capabilities



## PRELIMINARY TEST AND EVALUTION METHODS

After evaluating prototype ADS features, potential ODDs, potential OEDR capabilities, and potential failure mode strategies, a sample evaluation framework was developed to support the assessment of ADS for safe deployment. Sample test procedures were also developed using engineering judgements, previous test procedure development experience, and use cases. The test framework and procedures developed gave special consideration to achieving repeatability, reliability, and practicality. Lastly, many challenges associated with testing ADS and further research needed to help address these challenges were identified. Challenges included those related to the technology itself as well as test execution.

To identify appropriate methods to evaluate ADS, a review and assessment of existing testing methods and tools was performed. This evaluation served to develop an understanding of how testing is currently being executed for vehicles capable of various levels of automation. It also served to identify potential gaps in this existing testing framework, which led to the identification of additional and modified tools and methods to fill those gaps and helped create a testing framework. This assessment included a meeting with crash avoidance test engineers at NHTSA's Vehicle Research and Testing Center (VRTC) in Ohio to discuss their current testing of vehicles capable of SAE International L1 and L2 driving automation. Findings from the previous analyses were presented and initial thoughts on the steps to develop a useful set of test methods and actual tests were provided.

A common test scenario framework that could be used broadly across the various testing methods and tools was then established. This framework built upon the findings of the previous tasks to include the principal elements of ADS operation (tactical maneuver, ODD, OEDR, and failure behaviors) that are thought to have a direct impact on their overall safety. Each of these elements can be viewed as an input or integrated component in the overall test scenario. The framework was developed in such a way that it could be used for both black-box and white-box testing. Each of the core scenario components can be applied similarly for both black-box and white-box analyses; the differences come in the ability to inject inputs and take output measurements at various levels within the system under test. As part of this analysis, key interfaces where this injection and measurement could take place were identified.

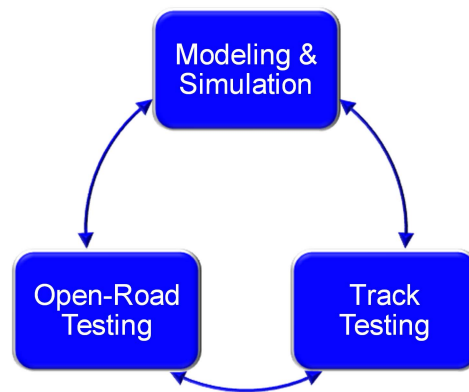
Available literature and reports on current ADS testing activities conducted by both government and industry were reviewed. The review identified three ways that these tests are primarily being conducted:

- Modeling and simulation (M&S)
- Closed-track testing
- Open-road testing

These three techniques offer a multifaceted testing architecture with varying degrees of test control, and varying degrees of fidelity in the test environment. In many cases, two or more of these techniques can be used in parallel or in an iterative fashion to progressively evaluate a complex system such as an ADS.

Simulation testing provides several advantages:

- Controllability – Simulation affords an unmatched ability to control many aspects of a test.
- Predictability – Simulation is designed to run as specified, so there is little uncertainty as to how the test will run.
- Repeatability – Simulation allows a test to be run many times in the same fashion, with the same inputs and initial conditions.
- Scalability – Simulation allows for generation of a large number and type of scenarios.
- Efficiency – Simulation includes a temporal component, which allows it to be sped up faster than real time so that many tests can be run in a relatively short amount of time.



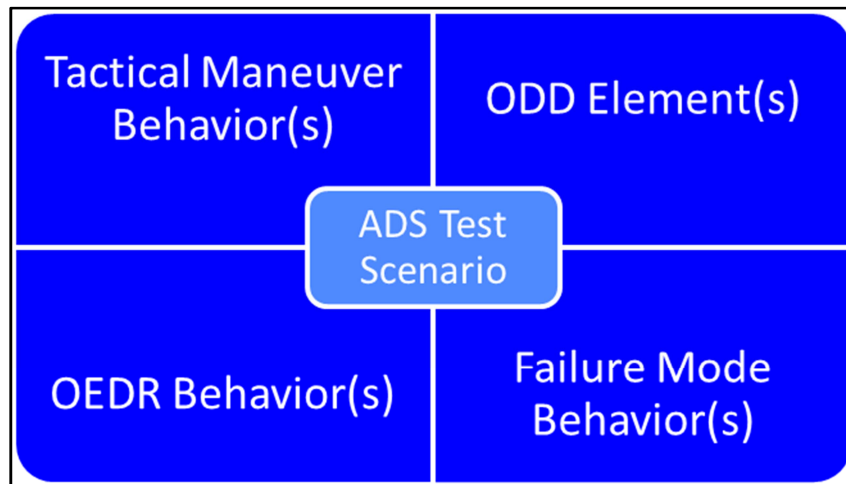
**Figure 4. Primary Testing Methods.**

The following components were identified as collectively making up the core aspects of a common ADS test scenario:

- Tactical maneuver behaviors
- ODD elements
- OEDR capabilities
- Failure mode behaviors

Tactical maneuver behaviors relate to the immediate control-related task(s) the ADS is executing as part of the test (e.g., lane following, lane change, turning). The relevant ODD elements generally define the operating environment in which the ADS is navigating during the test (e.g., roadway type, traffic conditions, or environmental conditions). OEDR capabilities relate directly to the objects and events the ADS encounters during the test (e.g., vehicles, pedestrians, traffic signals). Finally, some tests may include injection or simulation of errors or faults that induce failures at various stages within the ADS's functional architecture.

Test scenarios can be composed of one or more elements of each of these core components, visualized as the individual dimensions of the multidimensional test matrix in Figure 5. Each of these components may be included in a checklist identifying the aspects of each category that are incorporated in a given test.



*Figure 5. ADS Test Scenario Matrix.*

## CONCLUSIONS

This paper describes an example of a testing architecture and a scenario-based test framework to support the safe deployment of ADS and evaluate and assess their performance. Efforts focused on the testing of ADS (SAE International L3–L5), where the ADS is fully capable of all aspects of the DDT. To facilitate the identification of the testing architecture and framework, common and relevant operational components for ADS were identified and evaluated, specifically:

- ADS features
- ODD
- OEDR
- FO and FS strategies

The primary contribution of this research is the conceptual development of a test scenario framework that incorporates elements of each of these operational components. The framework uses a checklist-type approach to identify high-level scenario tests by specifying relevant tactical maneuvers, ODD, OEDR, and potential failures.

Each of these components are then further specified to develop a comprehensive set of procedures for a given scenario test. The scenario framework lends itself well to being applied across the three testing techniques identified for the testing architecture (M&S, closed-track testing, and open-road testing), although specific test procedures and implementations will vary, depending on the technique and tools used. This test scenario framework and the sample test procedures developed can provide a launching point to more comprehensive ADS test development and ultimately, test execution. Figure 6 shows a sample ADS test scenario visualization, with the principal elements notionally specified. (In this figure, SV stands for subject vehicle; POV stands for principal other vehicle.)

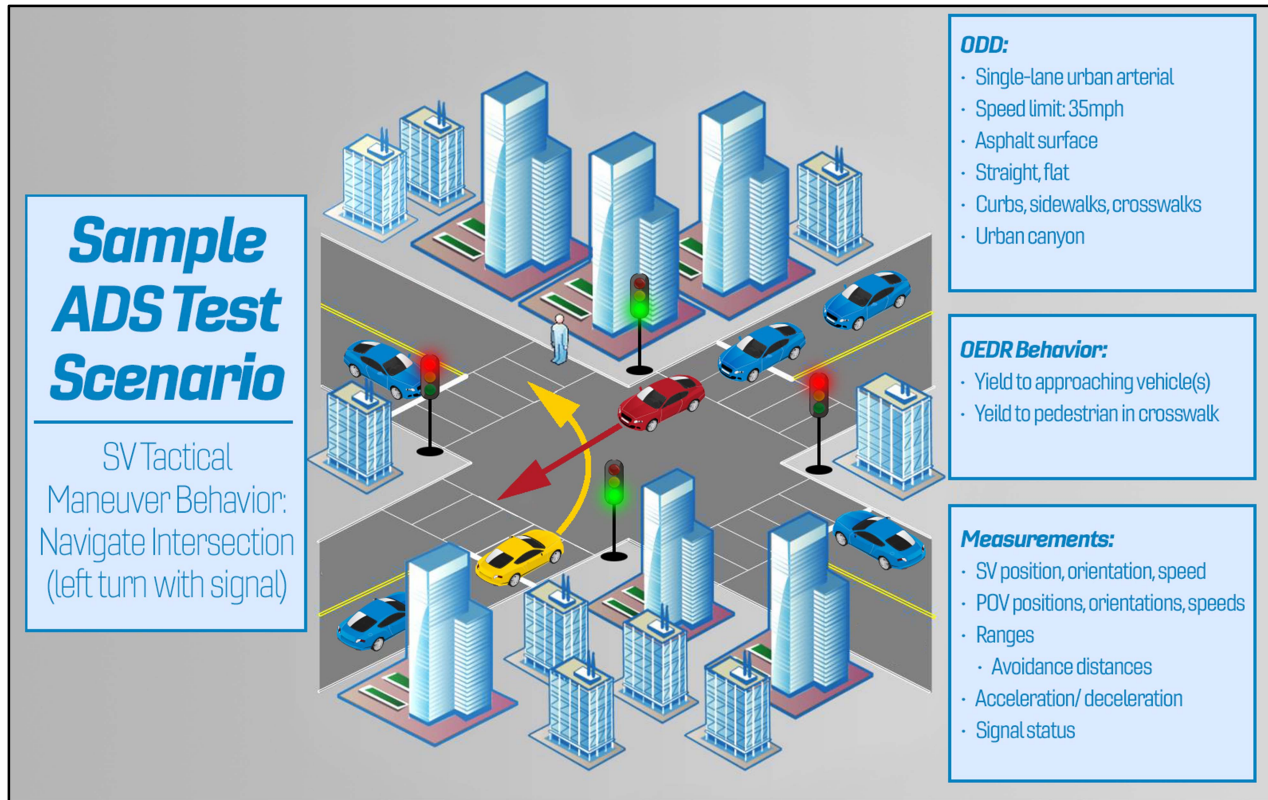


Figure 6. Sample ADS Test Scenario

The expansiveness of conceivable ODD, OEDR, and failure conditions presents a significant challenge to achieving comprehensive testing, even considering the test scenario framework identified during this research and described in this paper. The concept of risk associated with driving scenarios, notionally based on probability and severity of occurrence, has helped focus the analyses of ODD, OEDR, and failure modes to identify an appropriate testing process. A “reasonable worst case” approach may prove sufficient for general safety assessments; however, it is necessary to extend testing beyond the reasonable cases to understand the performance boundaries and limitations of ADS. This paper also identifies M&S capabilities and tools as a potential approach to addressing the expansiveness of these test components, as well as their potential combinations.

## REFERENCES

- Christensen, A., Cunningham, A., Engelman, J., Green, C., Kawashima, C., Kiger, S., . . . Barickman, F. (2015). Key Considerations in the Development of Driving Automation Systems. *Enhanced Safety Vehicles Conference*. Gothenberg, Sweden: NHTSA .
- DARPA. (2008). *Urban Challenge*. Retrieved from DARPA: <http://archive.darpa.mil/grandchallenge/>
- FHWA. (2008). *Managed Lanes: A Primer*.

- IIHS. (2016, March). *Automakers agree to standard AEB by 2022*. Retrieved from IIHS HLDI:  
<http://www.iihs.org/iihs/news/desktopnews/u-s-dot-and-iihs-announce-historic-commitment-of-20-automakers-to-make-automatic-emergency-braking-standard-on-new-vehicles>
- Kyrouz, M. (2017). *Medium*. Retrieved from <https://medium.com/smart-cars-a-podcast-about-autonomous-vehicles/industry-comments-to-nhtsas-federal-automated-vehicles-policy-436e7e24911a>
- NHTSA. (2007). *Pre-Crash Scenario Typology for Crash Avoidance Research*. NHTSA.
- NHTSA. (2015). *Human Factors Evaluation of Level 2 and Level 3 Automated Driving Concepts*. NHTSA.
- NHTSA. (2016b). *Federal Automated Vehicles Policy*.
- NHTSA. (2016c). *Budget Estimates - Fiscal Year 2017*. NHTSA.
- NHTSA. (2016d). *Automated Vehicle Research for Enhanced Safety - Final Report*. NHTSA.
- NHTSA. (2017b). *Traffic Safety Facts 2015*. NHTSA.
- NHTSA. (2017c). *Traffic Safety Facts - 2016 Fatal Motor Vehicle Crashes Overview*. NHTSA.
- SAE International. (2018). *J3016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*. SAE International.

# **ASSESSMENT, EVALUATION, AND APPROACHES TO TECHNICAL TRANSLATIONS OF FMVSS AND TEST PROCEDURES THAT MAY IMPACT COMPLIANCE OF INNOVATIVE NEW VEHICLE DESIGNS ASSOCIATED WITH AUTOMATED DRIVING SYSTEMS**

**Myra, Blanco**  
**Michelle, Chaka**  
**Clay, Gabler**  
**Loren, Stowe**  
**Warren, Hardy**  
**Joshua, McNeil**  
**Vikki, Fitchett**  
Virginia Tech Transportation Institute  
United States

**Ellen, Lee**  
National Highway Traffic Safety Administration  
United States

Paper Number 19-0261

## **ABSTRACT**

The project described in this paper provides research findings in terms of options regarding technical translations of select Federal motor vehicle safety standards (FMVSS) and related Office of Vehicle Safety Compliance (OVSC) test procedures. The research findings are based on potential regulatory barriers identified for self-certification and compliance verification of innovative new vehicle designs that may appear in vehicles equipped with Automated Driving Systems (ADSs). This paper documents the framework used to evaluate the regulatory text and OVSC test procedures with the goal of identifying possible options to remove regulatory barriers for the self-certification and compliance verification of ADS-Dedicated Vehicles (ADS-DVs) that lack manually operated driving controls. It also describes the research activities for 15 crash avoidance standards (100-series) and 15 crashworthiness/occupant protection standards (200-series). This research effort incorporates feedback obtained from stakeholders and subject matter experts (SMEs).

## **RESEARCH QUESTION/OBJECTIVES**

The goal of this project was to provide research findings in terms of options regarding technical translations of select Federal motor vehicle safety standards (FMVSS) and related Office of Vehicle Safety Compliance (OVSC) test procedures based on potential regulatory barriers identified for self-certification and compliance verification of innovative new vehicle designs that may appear in vehicles equipped with Automated Driving Systems (ADSs). A technical translation is a modification that would allow regulatory text and/or test procedures that are identified as potential barriers to be carried out with the same basic engineering performance without manual control-specific restrictions. Technical translations developed under this effort present options for the regulatory text (i.e., performance requirements and test procedures) and related OVSC test procedures when a regulatory barrier is present. This paper describes the option development process used to address the technical translations and the testing procedures for 30 select FMVSS, such that the identified potential regulatory barriers could be removed for vehicles operated exclusively by an ADS that do not have the traditional controls used by human drivers. These 30 FMVSS represent a mix of standards where potential straightforward translations are presented (e.g., FMVSS No. 125, "Warning devices") and other standards that could yield findings near-term that could be utilized for mid-term and long-term research (e.g., FMVSS No. 126, "Electronic stability control systems for light vehicles"). An initial set of 12 FMVSS was selected by NHTSA and the research team selected the remaining 18 FMVSS with a focus on how they could contribute to long-term research. Technical translations were used to either present potential modifications to the existing regulatory text or, alternatively, to create new regulatory language that would be capable of accommodating an ADS's functionalities. The FMVSS of focus for this study are illustrated in Figure 1 below.

Crash Avoidance			Crashworthiness & Occupant Protection		
<b>101</b> Controls and displays	<b>110</b> Tire selection and rims and motor home/recreation vehicle trailer load carrying capacity information	<b>124</b> Accelerator control systems	<b>201</b> Occupant protection in interior impact	<b>206</b> Door locks and door retention components	<b>216a</b> Roof crush resistance
<b>102</b> Transmission shift position sequence, starter interlock, and transmission braking effect	<b>111</b> Rear visibility	<b>125</b> Warning devices	<b>202a</b> Head restraints	<b>207</b> Seating systems	<b>219</b> Windshield zone intrusion
<b>103</b> Windshield defrosting and defogging systems	<b>113</b> Hood latch system	<b>126</b> Electronic stability control systems for light vehicles	<b>203</b> Impact protection for the driver from the steering control system	<b>208</b> Occupant crash protection	<b>222</b> School bus passenger seating and crash protection
<b>104</b> Windshield wiping and washing systems	<b>114</b> Theft protection and rollaway prevention	<b>138</b> Tire pressure monitoring systems	<b>204</b> Steering control rearward displacement	<b>210</b> Seat belt assembly anchorages	<b>225</b> Child restraint anchorage systems
<b>108</b> Lamps, reflective devices, and associated equipment	<b>118</b> Power-operated window, partition, and roof panel systems	<b>141</b> Minimum Sound Requirements for Hybrid and Electric Vehicles	<b>205</b> Glazing materials	<b>214</b> Side impact protection	<b>226</b> Ejection Mitigation

Figure 1. 100-series and 200-series FMVSS of focus

## DATA SOURCES

NHTSA recognizes that advanced-concept vehicle designs are on the horizon and may not be addressed throughout the current FMVSS. The findings from this project help identify potential regulatory barriers to self-certification and compliance verification of some of these advanced-concept vehicles that are equipped with ADSs. SAE International’s (SAE’s) Recommended Practice *J3016 Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles* [1] defines an ADS as “The hardware and software that are collectively capable of performing the entire DDT [Dynamic Driving Task] on a sustained basis, regardless of whether it is limited to a specific operational design domain (ODD); this term is used specifically to describe a level 3, 4, or 5 driving automation system.” The same Recommended Practice defines Automated Driving System-Dedicated Vehicle (ADS-DV) in this way: “A vehicle designed to be operated exclusively by a level 4 or level 5 ADS for all trips within its given ODD limitations (if any)” but goes on to say that level 3 systems could possibly be included under this term in the future [1]. However, this project’s development of FMVSS technical translation options focused on a particular type of ADS-DV; i.e., vehicles designed to be operated exclusively by an SAE level 4 or level 5 ADS for all trips, and which are not equipped with manually operated driving controls. Thus, level 3 ADS-equipped vehicles (i.e., vehicles equipped with a user interface that permits operation by a human driver) were outside of the scope of this project, even if they could be categorized as ADS-DVs under the SAE definition.

A report prepared by the United States Department of Transportation (USDOT) Volpe National Transportation Systems Center entitled *Review of Federal Motor Vehicle Safety Standards (FMVSS) for Automated Vehicles: Identifying Potential Barriers and Challenges for the Certification of Automated Vehicles using Existing FMVSS* [2]—referred to hereafter as the “Volpe Report”—included two reviews of the FMVSS: 1) a review to identify standards that include an explicit or implicit reference to a human driver, and 2) a review to identify standards that might pose a barrier for compliance verification of a wide range of concept vehicles that may be equipped with an ADS. From this review, 13 automated vehicle concepts were defined to reflect the identified barriers and potential future applications of automated vehicle technology. The 13 concepts differed in their design convention and speed classification. Design convention considered differences in the application of advanced features that take full advantage of automation (e.g., removing steering wheel). Speed classification regarded low-speed (e.g., speed restricted to 40 kmph/25 mph) and high-speed (i.e., no speed restriction).

The ADS-FMVSS project presented herein focused on design concepts similar to three design concepts from the Volpe Report [2] which do not have vehicle controls for human drivers. Those concepts are:

- *Highly Automated Vehicle with Advanced Vehicle Design*
- *Highly Automated Vehicle with Novel Design*
- *Low Speed Highly Automated Vehicle with Advanced Design*

The Volpe Report categorized certain types of regulatory barriers for ADS-equipped vehicles and linked them to corresponding standards and concepts [2; Appendix B]. It identified several regulatory barriers, highlighting uncertainty about how vehicles with innovative designs would execute some FMVSS test procedures and, therefore, how these vehicles would be tested to verify compliance with the standards. The Volpe Report was used during the current project to develop a framework to describe ADS-DV features. The vehicle features for each of the three concepts noted above were grouped into cohesive categories in the framework development process. These categories identified the main areas where ADS-DV concept designs could potentially need very specific terminology and specifications relating to FMVSS regulatory barriers (i.e., technical translation options). The framework focused on concepts that are impacted by the technical translations, concepts that helped the research effort anticipate how an ADS may perform the entire DDT without user intervention, and any safety-related aspects of interest. In addition, the work included expanding the features of interest to include features not described in the Volpe Report that may be necessary for the implementation of advanced and novel designs (Figure 2).



*Figure 2. Categories and features of interest*

## METHODS

The translation process that was used entailed analyzing the language of select 100-series (crash avoidance) and 200-series (crashworthiness/occupant protection) FMVSS for key terms or descriptions that might present regulatory barriers to vehicle compliance, in order to then develop options as to how the language could be altered. Crosscutting analyses were developed to drive consistency in the translation options and clarify when individual standards required unique options or approaches. Each FMVSS evaluation produced a set of options that NHTSA may consider for translating the FMVSS for ADS-DVs.

Potential ADS-DV barriers indicating a possible need for translations were analyzed at two levels: 1) regulatory language, and 2) implementation of test procedures. Several parts of the regulatory language include standards that are incorporated by reference (e.g., American National Standards Institute [ANSI], ASTM International [ASTM], International Organization for Standardization [ISO], SAE). The standards incorporated by reference are part of the

FMVSS regulatory language and were analyzed in the same way as the rest of the regulatory text. A taxonomy was then developed for completing and capturing the translation analysis.

Documents incorporated into the FMVSS by reference (49 CFR § 571.5 [3]) posed a unique challenge for translation, since they were issued by organizations outside of NHTSA (e.g., ASTM, SAE) and then became part of the regulatory text when incorporated by reference in the FMVSS. Through rulemaking, NHTSA can change its incorporation by reference of those documents, and can decide to no longer incorporate them, adopt them in part, or incorporate a different document provided by the external organization.

The process for developing the technical translation options for the FMVSS of focus is outlined in the steps below:

- 1) Transfer the standard and related test procedure(s) into a spreadsheet designed for this effort.
- 2) Identify relevant information and documents.
- 3) Obtain relevant incorporated references by external organizations (e.g., SAE, ANSI standards) and evaluate potential barriers to ADS-DV self-certification or compliance verification.
- 4) Evaluate the language of both the standard and the test procedure to identify references to the driver, driver-oriented displays, designated seating positions, bidirectionality, manual controls, or other language that could pose a barrier for ADS-DV self-certification or compliance verification.
- 5) Coding the translation type as 0, 1, or 2 (as shown in Figure 3 below).
- 6) Suggest potential translations of the standard text and test procedures for ADS-DVs, including investigating options for new testing methods.
- 7) Identify FMVSS requirements where a technical translation was evaluated but not performed. When not clearly evident why a translation was not performed, document the reasoning for which a translation either cannot occur (based on current knowledge of ADS-DVs) or was deemed unnecessary.
- 8) Document specific barriers in translating the standard/test procedure language to ADS-DVs.

Reason		Technical Translation Type Description
<b>0</b>	Not performed	Translation evaluated but not performed.
<b>1</b>	Translation is straightforward	The translation performed is straightforward.
<b>2</b>	Limited research may be beneficial	Can translate standards or provisions of standards, maintaining current performance levels, with some limited amount of research for NHTSA to conduct compliance verification for both conventional vehicle designs and new vehicle designs associated with Automated Driving System - Dedicated Vehicles (ADS-DVs).

**Figure 3. Technical translation taxonomy**

Every section within the FMVSS of focus was coded from the choices shown in Figure 3. The reasons and descriptions were based on the best forecast of what might need to be addressed during the course of the project. Those categorized as *0-Not performed* were deemed as non-problematic for ADS-DVs within the scope of this project. The code of *1-Translation is straightforward* is self-explanatory; i.e., the determination was made that the translation options provided allowed for a straightforward translation to be performed for ADS-DVs. Any translations of standards coded as *2-Limited research may be beneficial* may require additional testing and/or research to develop the appropriate translations.

By way of example, the spreadsheet for FMVSS No. 102 is shown in Figure 4. Translation options are included in the spreadsheet in red text. Note that driver definitions 1 and 2, referenced in Figure 4 below, are potential translation options provided for the driver definition in 49 CFR § 571.3. These definition options were created as the word “driver” is used throughout various FMVSS.



S3.1.4.2 Identification of shift positions and of shift position sequence			
Standard Text	Translation Options		Potential Considerations
<p>Except as specified in S3.1.4.3, if the transmission shift position sequence does not include a park position, identification of shift positions, including the positions in relation to each other and the position selected, shall be displayed in view of the driver whenever the ignition is in a position in which the engine is capable of operation.</p>	<p><b>Option 1</b></p>	<p>...shall be communicated to the driver ...</p>	<p>Uses driver definition 1.</p> <p>Eliminates the dependency on a display.</p> <p>Opens the possibility of other communication means to human drivers (e.g., auditory). May need to provide conditional language such as "via visual or electronic means."</p> <p>May need a means to confirm operation for ADS.</p>
	<p><b>Option 2</b></p>	<p>Except as specified in S3.1.4.3, if the transmission position sequence does not include a park position, identification of positions, including the positions in relation to each other and the position selected, shall be displayed in view of the driver in a vehicle with a transmission shift mechanism intended for operation by a human driver, and shall be communicated to the ADS driver in a vehicle equipped with such a system, whenever...</p>	<p>Uses driver definition 2.</p> <p>Separates the human and ADS.</p> <p>If taken out of context, exclusion of "shift" could be ambiguous. "Shift" could be kept as currently stated while keeping the distinction between human and ADS.</p>
	<p><b>Option 3</b></p>	<p>...shall be displayed in view of the human driver whenever the ignition is in a position in which the engine is capable of operation.</p>	<p>Use driver definition 2.</p> <p>Only display information for vehicle operated by a human driver.</p>

**Figure 4. FMVSS No. 102: Transmission Shift Position Sequence, Starter Interlock, and Transmission Braking Effect**

Work on the 100-series standards focused on addressing some of the fundamental aspects that cut across many of the FMVSS, such as definitions for driver and seating position, service brake application, and gear position/selection, as well as on developing initial considerations for translating requirements for telltales and addressing bidirectional vehicles. Work on the 200-series standards focused on occupant protection for ADS-DVs with conventional seating.

**Stakeholder Engagement**

The involvement of stakeholders and subject matter expert (SME) reviewers was a critical component of the translation process. Stakeholders included companies, organizations, and advocacy groups that were invited to be involved in this project in the early stages based on their experience with FMVSS and ADS-DVs. Additional stakeholder entities were later added; in some cases, organizations asked to be involved and in other cases a need was identified for additional expert feedback. The SME reviewers were a subset of the larger stakeholder group; these were individuals with demonstrated expertise in and knowledge of a particular FMVSS and/or laboratory test procedure along with how potential FMVSS barriers to innovative vehicle designs may be addressed. The SME reviewers for each FMVSS of focus were involved in providing input to the technical translation options developed;

as such, they were able to review the translation development work and provide feedback. In addition, several industry and research entities were engaged as collaborators on this project in order to obtain input and feedback, and produce prototype technology for testing and evaluation. Figure 5 illustrates the various organizations that participated in this project.



Figure 5. The project team, stakeholders, and SME reviewers

The SMEs were divided into working groups based on their expertise with a particular FMVSS and/or OVSC test procedure. The working group members assisted with the review process once technical translation options were developed or feedback was needed for the test methods. The purpose of the SME review process was to ensure that the options being developed did not produce more far-reaching or different regulatory barriers. The SMEs also provided feedback on alternative methods evaluated for test procedures of interest. In addition, stakeholders participated in open project meetings and provided input regarding this project during those events.

### Test Procedures

The goal was to identify the equipment and/or procedures that may help NHTSA perform compliance verification on ADS-DVs not equipped with manual controls. Similar to the regulation text translation assessment analysis, the same taxonomy was used to determine appropriate translation options or modifications to data sheet checklists. As an addition to the regulation text translation assessment framework, the test procedure analysis expanded the focus to vehicle functionalities. Developing and evaluating test methods to exercise the required vehicle functionalities may require one or more categories of functionalities. The functionalities, which are also shown in their respective categories later on in this paper, are: steering control, speed control (vehicle/engine), service brake application, parking brake, gear selection, telltales/warnings/indicators, key insertion/removal, ignition start/stop, accessory mode, door open/close, non-driving controls, and visibility.

The following steps illustrate the approach taken as part of the crash avoidance test procedure analysis:

1. Classification of standards
2. Selection of standards for inclusion
3. Implementation and execution
4. Evaluation of test methods
5. Select functionalities needed to verify compliance, if applicable

6. Iteration of testing and evaluation of results as necessary
7. Validation of test platform and execution

The implementation, execution, and evaluation of the testing was first applied to standards containing functionalities with less-demanding requirements to verify the test platform and test methods. The expectation was that this approach would provide a sufficient set of test cases to allow the selection of an appropriate test method that could be applicable for any requirements and associated test procedures.

Five potential methods were identified for verifying compliance; these fall into two general categories that are outlined below. Some are more appropriate for some standards than for others. The methods are:

#### **Vehicle-based**

*Human control:* Testing is performed using a controller console, connected either physically or through a wireless link (which could include teleoperation), to provide manual driving control.

*Programmed control:*

- Scripted control – A standard set of commands (e.g., “start engine,” “apply parking brake,” “speed =  $x$ ”) are used to define the actions the ADS is required to take to execute the test.
- Pre-programmed routine – The steps for executing the test are predefined and compiled into a script that can be run but not modified in the field.

*ADS normal operation:* The normal operation of the ADS is used to perform some or all of the test procedure.

#### **Non-vehicle-based**

*Simulation:* Simulation, either solely software-based or including a hardware-in-the-loop solution, is used to execute the test procedure.

*Technical design documentation:* Vehicle-specific technical design and/or build documentation which provides sufficient information and detail (e.g., a wiring diagram showing that a sensor signal is connected to an ADS electronic control unit) to show the system in question was designed to be in compliance with part or all of a particular standard. It should be noted that this is different than the Test Specification Forms that are provided to NHTSA when a vehicle is selected for potential verification testing. Instead, it is technical design documentation used by the manufacturer in the design, construction, and validation of the vehicle.

While the OVSC test procedures are not requirements, they do capture functionalities that are often implied by the regulatory text (e.g., to test the requirements of the backup camera the vehicle must be started and backed up) and which NHTSA currently uses to verify compliance. Bidirectionality provided a unique challenge for functionalities as they do not follow a standard rear vs. front direction determination of the vehicle. Further research is needed to translate test procedures for bidirectional vehicles; thus, this will be performed as part of long-term research.

Figure 6 shows the 15 crash avoidance FMVSS under study and the associated functionality requirements that are either specified in the FMVSS or that are necessary to execute the associated test procedures. These are organized into categories shown in the first column. The first four categories apply to vehicle operation and the last category (Environment Awareness) addresses items that allow the driver to perceive the environment outside of the vehicle. Within the categories, the functionalities are grouped (e.g., vehicle position control, braking) and ordered by use and occurrence within the standards.

Category	Functionality	101	102	103	104	108	110	111	113	114	118	124	125	126	138	141
Driving Tasks	Steering control						•	•		•				•	•	•
	Speed control (vehicle/engine)			•	•		•	•		•		•		•	•	•
	Service brake application						•	•		•				•	•	•
	Parking brake							•		•						•
	Gear selection		•	•	•		•	•		•				•	•	•
Vehicle Communications	Telltails/warnings/indicators	•	•			•				•		•		•	•	
Key/Ignition Function	Key insertion/removal									•						
	Ignition start/stop		•	•	•		•	•		•	•	•		•	•	
	Accessory mode									•	•					
	Door open/close									•	•					
Non-driving Tasks	Non-driving controls			•	•	•		•			•					
Environment Awareness	Visibility	•		•	•			•	•							

**Figure 6. Functionalities identified in standards and test procedures for the 15 crash avoidance FMVSS under study**

Test procedures from FMVSS No. 114, Theft protection and rollaway prevention and No. 138, “Tire pressure monitoring systems,” were selected first for testing as they capture many of the functionalities shown in Figure 6 above. These FMVSS also have less-demanding requirements than others (e.g., FMVSS No. 126, “Electronic stability control systems for light vehicles”) and, as such, allowed early verification of the test platform and test methods. Following the testing of FMVSS Nos. 114 and 138, more demanding standards—such as FMVSS No. 126—will be tested, and the test methods will be refined as appropriate.

## CONCLUSIONS

This paper describes the work conducted to create technical translation options for FMVSS and OVSC test procedures for innovative new vehicle designs. These options may assist with the self-certification and compliance verification of automated vehicles without manual controls with regard to existing FMVSS, and note where the existing standards may need to be modified. The test procedure portion of the project focused on the test methods used to exercise the required vehicle functionality (e.g., start/stop ignition, gear selection) for executing the test procedures. A range of test means was considered which included human control, programmed, normal ADS operation, simulation, and technical documentation methods. Multiple criteria were assessed; for example: ease of execution, test time, scalability, and standardization. For each FMVSS of focus during this research, the effort developed one or more potential options for NHTSA to verify compliance with FMVSS requirements for vehicles without manual controls.

With regard to the 100-series (crash avoidance) standards, the effort addressed some of the fundamental aspects that cut across many of the FMVSS and developed initial approaches to translating requirements for telltales, indicators, and alerts in addition to addressing bidirectional vehicles. Vehicle functionalities such as steering, transmission control, and service brake application were identified that are explicitly referenced in FMVSS and OVSC test procedures, and options were developed for potential alternatives that could be used in compliance verification.

Work on the 200-series (crashworthiness) standards focused on occupant protection for ADS-DVs with conventional seating. This included ADS-DVs with forward-facing seating, but without manually operated driving controls (e.g., steering wheel). For ADS-DVs without manually operated driving controls, researchers applied the test procedures that have been developed for the passenger seating positions to the left front outboard seating position, given that the main difference between the two front outboard seating positions in conventional vehicles is the presence or absence of these controls. Subsequent research as part of this effort will focus on knowledge gaps in several areas that could be beneficial since passenger seating preferences (e.g., rear seat) as well as translation considerations for unconventional seating configurations may begin to vary with different concept vehicles.

## **Limitations**

This research was built on current information, which is subject to change. In this complex regulatory and technological landscape, ADSs may continue to evolve and FMVSS may need to evolve along with them. It should also be noted that NHTSA may determine that the options that resulted from this project may be unworkable for legal or policy reasons.

## **REFERENCES**

- [1] SAE International (2018). J3016 *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*. Accessed on June 25, 2018.
- [2] Kim, A., Bogard, D., Perlman, D., & Harrington, R. (2016). *Review of Federal Motor Vehicle Safety Standards (FMVSS) for Automated Vehicles: Identifying potential barriers and challenges for the certification of automated vehicles using existing FMVSS*. Preliminary Report DOT-VNTSC-OSTR-16-03. Washington, DC: U.S. Department of Transportation.
- [3] 49 CFR § 571. Retrieved from <https://www.ecfr.gov/cgi-bin/ECFR?mc=true&page=browse>

# **BMW'S SAFETY GUIDELINES FOR THE TESTING AND DEPLOYMENT OF AUTOMATED VEHICLES**

**Paul Daman**

BMW AG  
Germany

**Dr. Martin Götze**

BMW AG  
Germany

**Dr. Christian Gold**

BMW AG  
Germany

**Prof. Klaus Kompass**

BMW AG  
Germany

Paper Number 19-0226

## **ABSTRACT**

As automobile manufacturers take the leap from Advanced Driving Assistance Systems and implement Automated Driving Systems into their vehicles, certain aspects of vehicle safety become increasingly important. Whereas in today's level 2 automation, the human driver is involved in the dynamic driving task, in level 3 and above, more technological measures are necessary to ensure safety, therefore requiring a newly designed electronic architecture. Nonetheless, analysis of human factors remain a key element to ensure the safe operation of the vehicle. Though conventional techniques may be employed to solve some of these challenges, others require new tools to be developed. In the absence of an international standard, the foundation for discussions of completeness is missing. With an expert analysis of topics and tools a focus can be brought into discussions and serve as a basis for further development. This analysis may also lead to uncover areas where final answers and methods are missing, but serves also to identify areas where effort must be concentrated. When members of the industry apply these principles to the development of automated driving systems, the number of accidents will be minimized following the testing and deployment of this new technology, therefore maximizing safety and customer acceptance.

This submission represents the culmination of multiple sessions within industry, but also with contracting parties and government agencies with the goal of the creation of a comprehensive list of guidelines for the safe development of automated driving systems.

BMW has defined 12 different areas that have been focused into guidelines for the development of a vehicle with a safe automated driving system. These areas include topics from functional safety through the human factors aspects of system handovers to the consideration of passive safety.

While the 12 guidelines are selected to be a comprehensive list of safety topics, they are general in form and do not contain the details necessary to apply it as a blue print for the development. As these automated driving systems are not on the roads in appreciable numbers, the data from real world events are missing. Also the projects to develop the methods to generate and analyze data are still underway, which also forces some guidelines to remain broadly formulated.

The proposed guidelines concentrate the capabilities and limitations of today's safety evaluation for vehicles when applied to automation. By following the guidelines, the industry can ensure that this technology meets an acceptable level of safety when it comes to market.

## INTRODUCTION

Automation has defined many areas of development for the past decades and will continue for many to come. From the automation of our digital daily planner to the robots used in manufacturing, our lives have been enabled to move more comfortably, faster and in many ways safer. This trend also continues in the cars we drive. Many areas secondary to the driving task such as automatic climate control and lighting simply make it easier for the driver to drive. Other areas of assistance have a more direct influence on safety as they take action to apply corrective measures to the brakes or steering to avoid an accident at the last moment. Still other features also actuate the brakes, accelerator and steering, but to increase comfort through constant input. Not surprising, these features are all examples of what are called Advanced Driver Assistance Systems, as they assist the driver, who remains in control and responsible at all times.

Based on German accident statistics [1], the errors that these human drivers make cause over 98% of recorded accidents. For that reason, further automation sounds like it would be a simple answer to have a major effect on the worldwide number of accidents. Many have claimed that removing the human from the equation would quickly result in safer streets. After further analysis of the statistics, it is apparent just how challenging this task would be. Overall, accidents are actually quite rare occurrences. Again according to German statistics, once the total life time mileage of 700,000km is taken into account, there is an average distance of approximately 300,000 km between two accidents with any severity. This number raises to 228 million km if fatal accidents are considered, and the distance increases to even 661 million km if we solely look at highways.

These statistics show that the human drivers are actually quite adept at handling the complexities of on-road traffic, and the endeavor of creating technology to accomplish this much is quite daunting. Just reaching this level could be considered difficult enough, but in June 2017, the German Ethical Commission [2] recommended that manufacturers show that the technology used to automate the vehicles perform better than the statistics indicate humans do today. Whereas humans have an amazing capacity to use intuition and anticipation for complex situations, technology has the advantage of offering a 360° view of surroundings, simultaneously processing the information and does not fatigue. When it comes to a safe development of automated vehicles, we need to understand and learn from both the capabilities and limitations of the human driver, while simultaneously taking the risks into account that may emerge from their interaction with an automated vehicle. That could be the handover between a driver and the automated vehicle, or the interaction of road users in a mixed traffic scenario. Therefore, even with higher levels of automation, taking the human factors into account is key to generate a safe system.

To better understand where automation technology in automobiles currently stands, as well as the areas that development is currently engaged in, a brief review of the accepted definitions is necessary. Presently in its 3<sup>rd</sup> iteration, SAE J3016 [3] is the internationally agreed upon standard to define different levels of automation. While a detailed discussion on the wide range of topics described in the standard is beyond the scope of this paper, several terms shall be described here and referred to in the guidelines. Divided into 6 discrete levels of automation and based upon the separation of tasks required to drive a vehicle, one of the key areas is the operative control of longitudinal and lateral systems (accelerator, brake, steering) which is referred to as the Dynamic Driving Task (DDT). Independent of whether the system or the human is performing this control, the decisions necessary are based on the recognition of objects and events that occur surrounding the vehicle (Object and Event Detection and Recognition- OEDR). In order to group the conditions such as environmental, geographic or similar which are necessary for the system to operate, the term Operational Design Domain (ODD) has been generated.

Level	Name	Narrative definition	DDT		DDT fallback	ODD
			Sustained lateral and longitudinal vehicle motion control	OEDR		
<i>Driver performs part or all of the DDT</i>						
0	No Driving Automation	The performance by the driver of the entire DDT, even when enhanced by active safety systems.	Driver	Driver	Driver	n/a
1	Driver Assistance	The sustained and ODD-specific execution by a driving automation system of either the lateral or the longitudinal vehicle motion control subtask of the DDT (but not both simultaneously) with the expectation that the driver performs the remainder of the DDT.	Driver and System	Driver	Driver	Limited
2	Partial Driving Automation	The sustained and ODD-specific execution by a driving automation system of both the lateral and longitudinal vehicle motion control subtasks of the DDT with the expectation that the driver completes the OEDR subtask and supervises the driving automation system.	System	Driver	Driver	Limited
<i>ADS ("System") performs the entire DDT (while engaged)</i>						
3	Conditional Driving Automation	The sustained and ODD-specific performance by an ADS of the entire DDT with the expectation that the DDT fallback-ready user is receptive to ADS-issued requests to intervene, as well as to DDT performance-relevant system failures in other vehicle systems, and will respond appropriately.	System	System	Fallback-ready user (becomes the driver during fallback)	Limited
4	High Driving Automation	The sustained and ODD-specific performance by an ADS of the entire DDT and DDT fallback without any expectation that a user will respond to a request to intervene.	System	System	System	Limited
5	Full Driving Automation	The sustained and unconditional (i.e., not ODD-specific) performance by an ADS of the entire DDT and DDT fallback without any expectation that a user will respond to a request to intervene.	System	System	System	Unlimited

Figure 1, table of SAE Automation levels [3]

Today, the technology available on large scale production vehicles allows a maximum of level 2 partial driving automation. As the driver is still responsible for the object and event detection the system can actually only assist them in driving the vehicle. The fact that this responsibility is transferred to the system in level 3 and beyond leads to a paradigm shift and a technological quantum leap is necessary to attain it. For simplification, systems capable of level 3 functionality and beyond can be referred to as Automated Driving Systems (ADS)[3]. As discussed in WP29 of UNECE [4] one of the major changes that an ADS brings is that at these levels of automation, activities secondary to the driving task would be explicitly allowed to be undertaken by the driver. Since the system performs the DDT, the driver no longer has this responsibility and is free for other activities such as watching a film on the vehicle displays. The driving task is no longer considered the primary task of the driver in these scenarios, therefore, secondary tasks are also referred to as Non-Driving-Related-Tasks, or NDRTs [5].

It is widely acknowledged that transition between level 2 and level 3 is not trivial [6], and for that reason a common language is necessary to discuss the challenges both inside and outside of the automotive industry. Expert groups within BMW gathered topics and clustered them to generate a comprehensive list of 12 guidelines for the development of automated driving systems. Through review of other recommendations and publications from government bodies or consumer associations such as NHTSA [7], Thatcham Research [8], NTSB [9], GDV [10], the German StVG [11] and the German Ethical Commission [2], it was found that there was much communality between the collections. Nonetheless, additional aspects as well as new viewpoints are introduced here.

To organize BMWs 12 guidelines, an arrangement in three overall groups with common areas of influence were found. The first four guidelines represent technological areas necessary for the system. As in all three groups, though initially simple in form, the details to develop the answer are currently engaging the entire automotive industry. Next is the area of human factors which are also extremely important even for higher levels of automation. While the last four guidelines do not directly create requirements for the automation system, they are areas necessary to be addressed during development of vehicles.



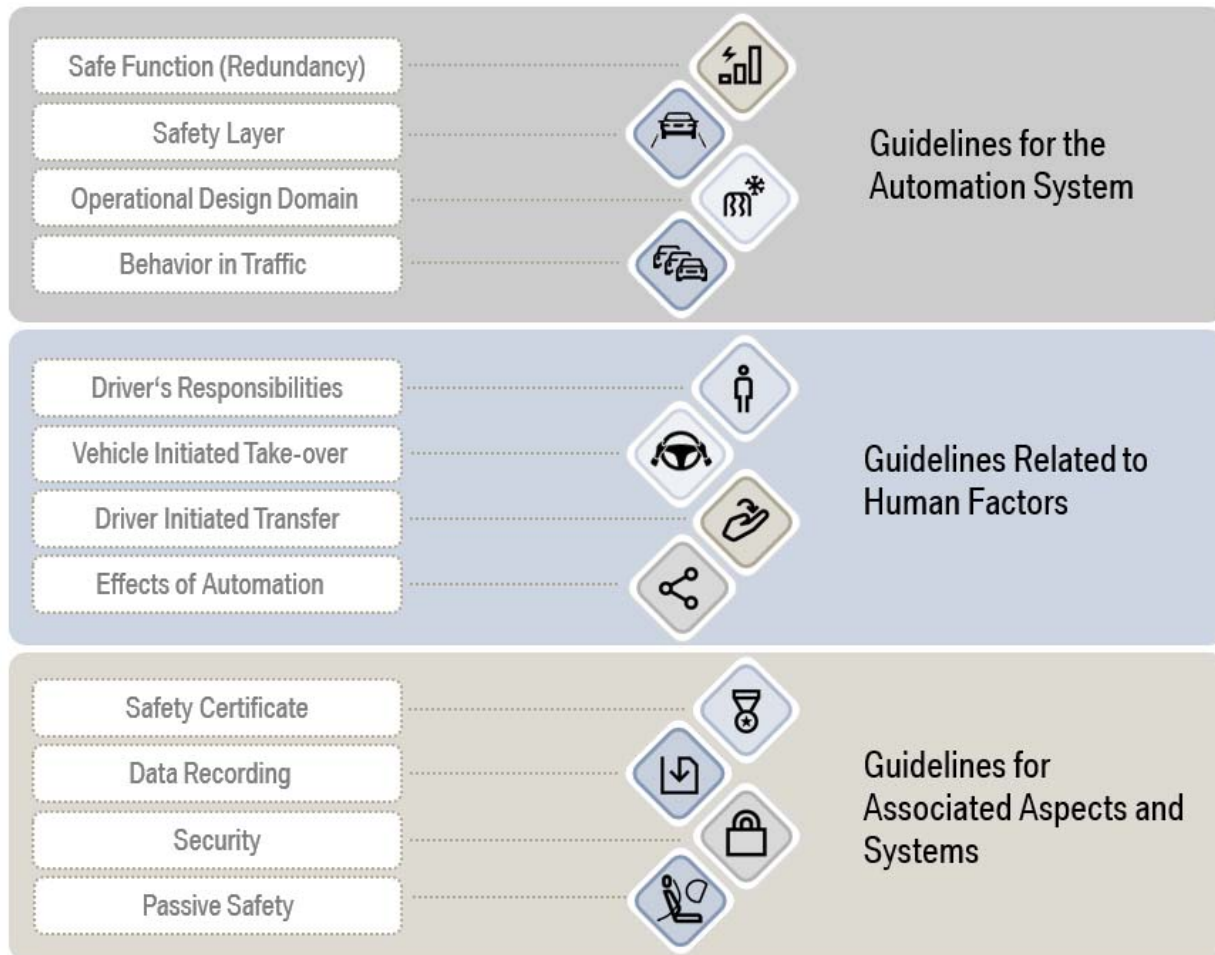


Figure 2 – BMW's 12 Guidelines for Safe Automated Driving Systems

## GUIDELINES FOR AUTOMATED SYSTEMS

### 1. Safe Function (Redundancy)

With automotive systems becoming ever more complicated, the concepts gathered under the term functional safety have become ubiquitous in all areas of automotive development. Either bundled under automotive best practices as ISO 26262-Road Vehicles Functional Safety [12] or other standards from other industries and the military, the processes as well as the measures which result from them have an even higher relevance for automated driving systems. In this list of guidelines, the following aspects gather two of the key elements.

#### Dealing with Degradation

If system components relevant to the function or individual functions become non-available, the automation system must be capable of compensating or ensuring a sufficient time budget for safe transfer of control to the driver.

This aspect embodies one of the major differences between how a level 2 and level 3 or higher automated driving system must be capable of reacting. As mentioned above, level 2 systems merely assist the human driver and therefore the driver must react if the system does not respond to a relevant object or event. For this reason they can never completely relinquish control and if an aspect of the assistance is no longer available, the driver continues to drive. Once the driver is involved in NDRTs at Level 3+, additional time is necessary before they can resume the responsibility of the DDT from the ADS.

While some have called for redundancy to be the only option to deal with the risk emerging from a degradation, there are also other strategies which can be followed to ensure a safe system behavior. As such, simply the reduction of speed, or avoiding a lane change are two examples of strategies to safely increase the time and reduce risks when aspects of the automated driving function are no longer available. The key is that some form of compensation is necessary.

### **Fail Operational**

The loss of sub functions or system components shall not lead to a safety critical situation.

Continuing along the same idea is that if any component or portion of the system fails, the result shall not be safety critical. This applies to both hardware malfunction which could come from mechanical damage or software/electronic errors.

Due to the new vehicle architecture necessary to fulfill this higher requirement, a level 3+ system is intrinsically different to a level 2 system, independent of the increased competence of the object detection and reaction. For that reason, a system designed as level 2 cannot become a level 3 system simply due to improvements in software. It is the way the system is networked and the measures in the actuators that make it inherently different.

## **2. Safety Layer**

To reduce the frequency of critical situations, automated driving systems of every level are generally designed to drive defensively. Unfortunately even at a reduced frequency, these events will occur and the system must react.

### **Safety Layer**

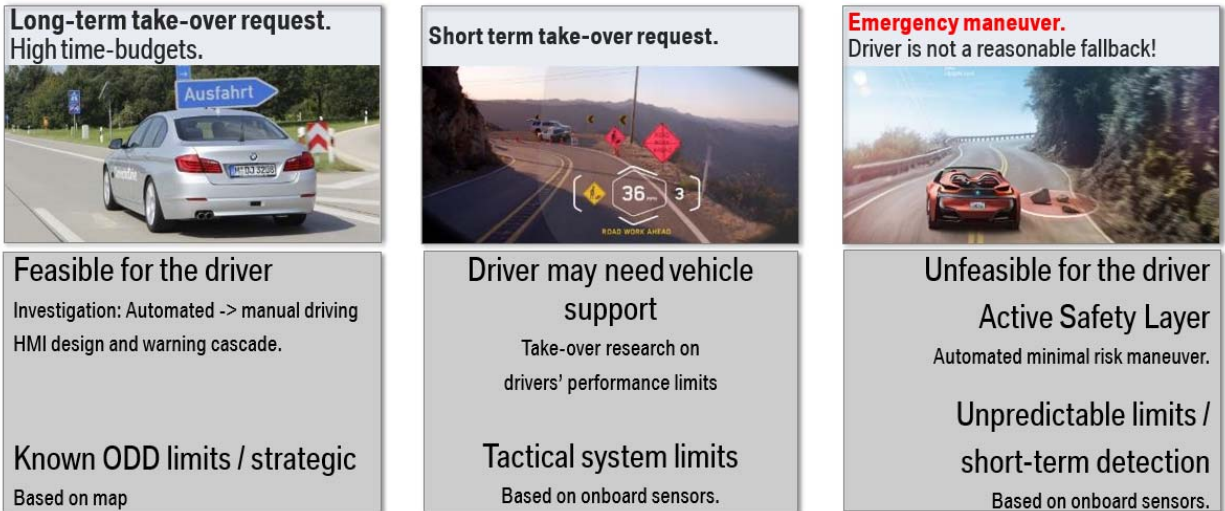
The automation system must recognize system limits, especially those that do not allow a safe driver take-over, and react to minimize the risk.

There has been a misunderstanding of level 3 automated driving systems in exactly this area. As stated in SAE J3016, it is expected that the fallback ready user regains control in short notice when the system requests it. Of course they are likely performing a task unrelated to driving, so the reaction by the human to an emergency situation may not be possible or inadequate [13]. Further has to be considered that the driver may need additional time for executing the required maneuver to react to the event. For this reason, even in a level 3 system, the system must react to minimize the risk of situations where a transition to the driver is not possible or reasonable, in order to reach an acceptable safety level.

This safety layer must be present below the system carrying out the long term control. Using humans as an analogy, we all have a cognitive layer that allows us to perform complicated activities. As critical situations are rare, a majority of the time is processed in this area. In emergency situations, a faster reaction is necessary to reduce following risk. This is akin to the nervous system, which must quickly react.

Just as human senses provide the information for these quick reactions, the sensors in automated driving systems provide the information for this layer. Therefore, these active safety systems can be found in all levels of automation, though their importance increases in level 3 and above.

Though discussed in further detail in the following section, other system limits may be observed and recognized by the system which are not immediately time critical, as illustrated in Figure 3. For this reason, the fallback ready user of a level 3 system must be able to intervene in these situations with a time allowance on the order of seconds.



**Figure 3 – Comparison of emergency maneuver with other situations**

### 3. Operational Design Domain

Another driving force behind the requirements on the system for higher levels of automation originate in the definition of the operational design domain (ODD). As previously mentioned, the ODD as defined by SAE J3016 is the collection of conditions where the system is designed to operate. Examples can be geographic as in the country or state, environmental as from sunshine to snow, or a collection of roadway characteristics such as a divided highway. As the function is designed to operate safely in this domain, sensors shall confirm at all times that the vehicle is still in that domain.

#### ODD recognition

As soon as system limits, which restrict the safe functionality of the automation system, are recognized, the system must react to compensate, or request a take-over from the driver with adequate time reserve.

Since the automated driving system is limited to an ODD and while activated in this domain, it is responsible for vehicle control until it requests the fallback ready user to intervene. While this may sound trivial, in lower levels of automation, it is ultimately the driver's responsibility to recognize when the limits are reached. The system may provide assistance to that effect, but only higher levels of automation need to definitively register the limits as a reaction is necessary.

#### Manage typical situations

The automated driving system must take situations into account, which can typically be expected to be encountered in the ODD and address the risks that may result.

The sensor arrays of vehicles equipped with automated driving systems need to register and classify much more than only the most common objects and the situations they are associated with. Even when they only make up a small percentage of the time spent on the road, there are a multitude of events such as an unexpected lane change, which happen often enough that they cannot be considered unusual. The system shall therefore be able to deal with all situations that are foreseeable to occur within the ODD which have an inherent risk of relevant magnitude.

### 4. Behavior in Traffic

In the near future, production vehicles capable of conditional automated driving will be on the road. Nonetheless that will only be the beginning of the phase of mixed driving with some conventional vehicles and some automated vehicles sharing the road. Even in today's traffic with solely conventional vehicles, one contributing factor to safe driving is the relatively similar behaviors of most drivers.

### **Manners on the road**

The behavior of the automated function needs to not only be comprehensible to the surrounding road users, but also predictable and manageable.

As mentioned in the introduction, human drivers are often able to apply their intuition and anticipate the actions of other road users based on their experiences. This predictability allows for traffic flow and cooperation between drivers with remarkably limited possibilities for communication. For instance, on the highway using only turn indicators and brake lights, a somewhat complicated coordination of maneuvers can be accomplished to allow a lane change in traffic. Additional lines of communication may even create confusion as human drivers learn how to interpret new signals. Furthermore, an unobtrusive behavior of the automated system reduces the implications emerging from new interaction patterns of a mixed traffic environment.

### **Conforming to Rules**

The applicable traffic rules are to be taken into account.

One method to ensure that driving behavior is similar among drivers is to establish rules. These traffic rules have developed over the last century of human driven vehicles and are often based on human traits such as average reaction time and visibility. Even with these rules there is room for interpretation of the applicable law and in certain situations, drivers are allowed to deviate to a certain extent in some aspects. This poses the question as to whether these rules apply to vehicles with automated driving systems with faster reaction times, a 360 degree field of view, and sensors such as radar, and how the applicable law is interpreted for ADS. As our society develops, the rules and interpretations may change, but the algorithms behind the automated driving systems need to bear them in mind.

## **GUIDELINES RELATED TO HUMAN FACTORS**

### **5. Driver's Responsibility**

Depending on the level of automation being offered by a vehicle, the driver's responsibilities may change. At lower levels, the driver is responsible for all actions of the vehicle except those attributed to a defect. At the highest level, the driver can be relegated to an operator. For the portions of the trip where it is active, an ADS is responsible for all parts of the DDT, but at a minimum the driver needs to ensure that vehicle maintenance has been taken care of. Other responsibilities of the driver may include a reaction after the failure of a suspension component, the correct loading of cargo and maintaining an appropriate seating position if a takeover may be necessary. Complicating matters further, a single vehicle can offer multiple levels of automation depending on the situation. For instance in one operational design domain limited to the highway, there may be a level 3 function available, but once the vehicle is in an urban environment only level 2 or 1 functions may be available.

### **Responsibilities**

The portions of the driving task which remain under the driver's responsibility must be clearly communicated to him/her.

From passages in the owner's manual to the way information is displayed in the vehicle, the manufacturer shall take care to take advantage of the various lines of communication so that the driver understands their responsibilities and act accordingly.

### **Driver's State**

To promote safety, systems need to be integrated that support the driver to recognize driver conditions that are not acceptable.

Though it does not obviate the driver's awareness of their responsibilities, technology can assist the driver if they are presenting characteristics, which conflict with system requirements on the driver. For instance, by using information provided by simple seatbelt contacts, the system can provide a reminder to the driver that they may not leave their seat. Nevertheless, as it is not possible to reliably detect all forms of misuse, no technology can replace the driver's conscious heeding of their responsibilities.

### **Mode Awareness**

The automated function must ensure that the currently active driving mode can be recognized explicitly and unmistakably at any time. If the driver must react, this must be clearly communicated.

As the single vehicle can offer multiple modes of operation, the driver must be aware of which level of automation is currently operational in the vehicle, in order to enable a correct use of the respective assistance or automation system. Through countless hours of simulator studies [14], measures are being defined and implemented in the human machine interface to give this awareness to the driver. While a level 2 system could expect the driver to recognize the necessity to take action, higher levels of automation must communicate whether there is a need for it.

## **6. Vehicle initiated handover**

Even for higher levels of automation, the vehicle may request that a driver take over control of the vehicle. One example is when a portion of the trip is no longer within the system's ODD, and the driver simply would need to once again takeover with the vehicle controls. Other extenuating circumstances may require a takeover in vehicle concepts without conventional controls in level 4. Here the human requested to drive the vehicle may do so remotely, continuing to use the vehicle's sensors and actuators.

### **Minimal Risk Condition**

If the driver does not comply with a take-over request, the ADS must perform a maneuver to minimize risk. The correct maneuver depends on the situation.

Though the reasons for initiating a handover may vary, automated driving systems need to follow a strategy between the time that the request is given and when the driver takes control. Depending on the technology available on the vehicle as well as the situation, the reaction can be as simple as reducing speed to reduce the risks, or as complicated as changing lanes and pulling over to a safe harbor parking space. It is important to note that this minimal risk condition may have a different character depending on whether it is an emergency maneuver, triggered by a loss of sub functions or system components, or a long term take-over request (Figure 3).

### **Take-Over requests**

Handovers must be manageable for the driver.

Hand in hand with the safety layer, time critical emergency situations would not be manageable if the driver is requested to take over in those situations. As with other guidelines associated with human factors, studies taking place in simulators [13] and other controlled environments indicate what time budget and take-over scenario is manageable for the average driver [15] and how an adequate take-over request should be designed [16], and how control elements and human machine interfaces [17] can be adopted to support the driver in taking over control.

## **7. Driver initiated transitions**

Often neglected when considering automated driving systems, there are situations when a driver would want to regain control of the vehicle. A simple example would be to have the full driving experience along an engaging stretch of road. However, there are situations where the driver may touch the controls without actually desiring to regain control.

### **Take-Over (driver)**

Activating and deactivating the automated driving system requires explicit driver's intent.

Differentiating the intent can mean the difference between accidentally contacting one of the driver controls (i.e. steering wheel) while reaching for an object, and explicitly taking the wheel to negotiate a curve. Relinquishing control in the former could result in a critical situation. While the driver should be able to take-over control if he intends to do so, an unintended take-over could result in a handover to a driver who is not ready or able to take on the driving task. For that reason concepts must be developed to differentiate between the two situations. Furthermore, there is a wide range of vehicle functions relevant or connected to the functioning of the ADS. Driver interaction with those functions should neither lead to an inexplicable hand-over, nor to a safety relevant change of the ADS state.

## **8. Effects of Automation**

Made evident from other industries with high levels of automation, such as the commercial aviation industry, humans adapt to the automation they experience.

### **Effects of Automation**

In the overall evaluation of system safety, effects on the driver due to automation need to be taken into account, even when they occur after the automated portion of the drive has ended, when a direct link to the drive while automated can be drawn.

Studies continue to be performed to analyze these effects in the automotive context [18]. Acknowledging that these occur is the first step to implementing measures to counteract them. These measures may include optimizations to the human machine interface [19], which further support mode awareness.

## **GUIDELINES FOR ASSOCIATED ASPECTS AND SYSTEMS**

### **9. Safety Assessment**

In addition to BMW's long history of striving to improve road safety, the German Ethics Commission [2] has also tasked the automotive industry to ensure that the automated driving system, which in some ways replaces the driver in performing the DDT, is safer than the average driver.

#### **Safety Assessment**

Verification and validation shall be used to ensure that the safety goals are met, in order to reach a consistent improvement of the overall safety balance, while minimizing new risks induced by the automation system.

In order to compare the performance of the system to that of human drivers, methods are being developed to quantify and assess how they perform. Simulation and prospective safety analysis [20] is playing a key role in generating the data. As this task affects a multitude of companies and institutions developing this technology, several cooperation projects have been initiated. One showing promise to deliver some of the answers is the PEGASUS project [21] supported by the German state. Summarized in Figure 4, a process of scenario collection, abstraction, database generation and validation is described. An international project titled L3 Pilot [22] is also poised to deliver pieces to the puzzle in quantifying safety and performance.

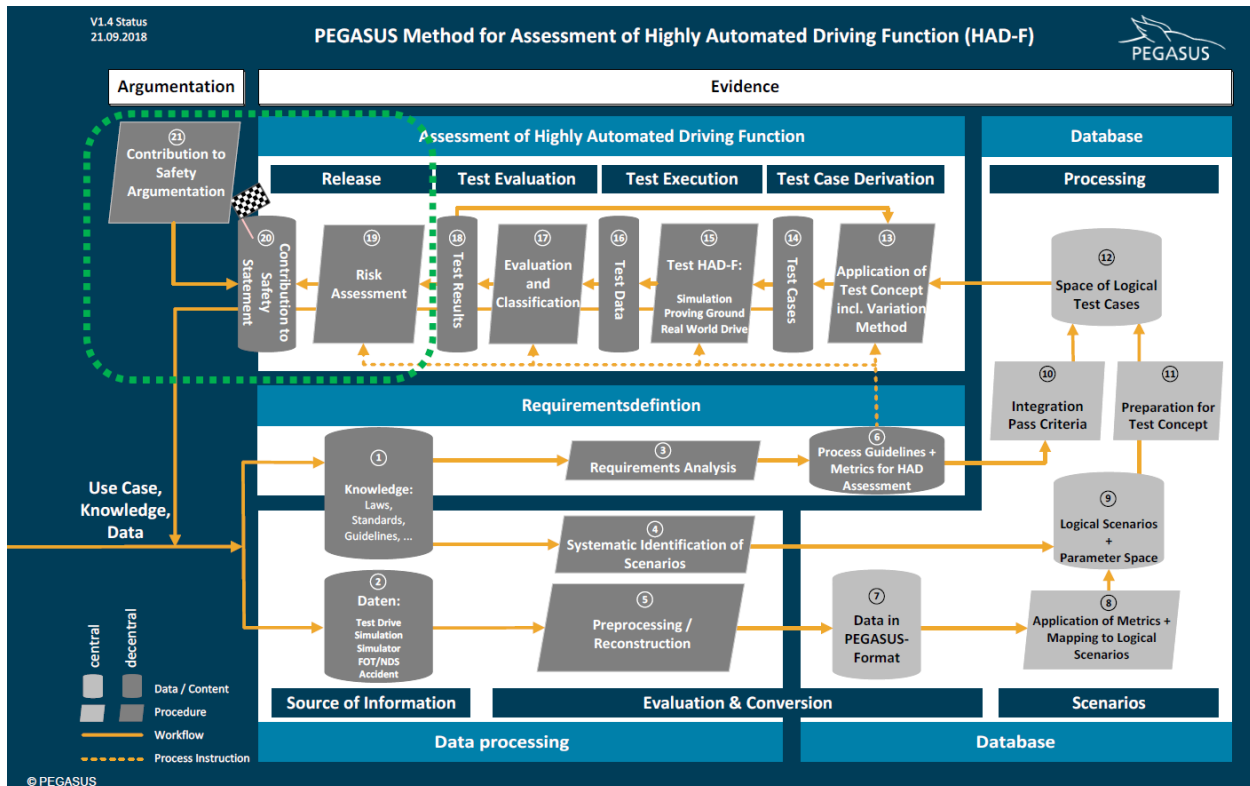


Figure 4 Summary of the Pegasus method [13]

## 10. Data Recording

Even with today's conventional vehicles, some markets have required that data is recorded in the event of an accident or similar situation. Information about the scenario leading up to the accident can be provided by the driver. Once the driver is no longer performing the DDT, this information will have to be recorded by the system.

### Data Recording

While conforming to the applicable data privacy laws, automated vehicles shall record the relevant data pertaining to the status of the functions when an unusual event is recognized.

Just as the today's driver is responsible for driving, their memory serves to aid in reconstructing what happened during a critical or emergency situation. Once this responsibility is transferred to the technology, it must also have the equivalent of a memory to provide information in those situations. As this data contains details, in accordance to privacy laws, access to the data will be limited.

## 11. Security

In a world of ever increasing connectivity, security is tantamount for information to only flow between appropriate places. In the financial industry or even online trade, the penalty for inadequate security is financial difficulties. In the automotive world, the consequences can be much more drastic.

### (Cyber-) Security

When offering an automated driving function, steps shall be taken to protect the function from threats.

With a history of connectivity, BMW has been addressing cyber security for decades. As control systems for the steering and brakes for even level 0 and 1 systems depend on the flow of information from sensor to actuator for a safe operation, even hardware access points are taken into account. Automated driving systems pose additional challenges as the actuators have even higher capabilities and the driver is further removed from the driving task. Just as the attacks evolve from year to year, so must the defense as security directly effects safety.

## **12. Passive Safety**

A motivation for the development of automated driving systems is the overall reduction of accidents which take place on public roads. Nonetheless due to unforeseen circumstances, unfortunately accidents will still occur and the passive safety necessary to protect the occupants will be necessary.

### **Crash Scenarios**

The vehicle layout shall accommodate modifications to crash scenarios brought about by vehicle automation.

The accident statistics stored in all of the databases around the world are generated by vehicles driven by human drivers. The accidents involving automated vehicles will be fewer in number, but it is likely that there will be a shift in the distribution. For that reason, a re-evaluation of relevant scenarios for the development of passive safety systems will be necessary.

### **Alternative Seating Position**

Occupant protection shall be ensured even when new uses for the interior are made possible by automation.

When the driver no longer needs to be involved in the dynamic driving task, new interior possibilities arise for the driver to fully take advantage of the situation. These new interior configurations will also need to be taken into account during the development and verification of passive safety systems.

## **CONCLUSION**

Though there is still much work to be done in the development of large scale automated driving systems, BMW's 12 guidelines for automated driving systems establish a framework and a baseline. Building upon them, a collective discussion can occur both within the industry as well as with important stakeholders outside. This discussion is necessary as questions still remain, and in order to answer them, research continues to take place. Together this common understanding will help bring us forward to a safer future.



## REFERENCES

- [1] N.N. 2018. "Verkehr - Verkehrsunfälle - 2017", Statistisches Bundesamt (Destatis).
- [2] N.N. 2017. "Ethics commission – automated and connected driving", Appointed by the Federal Minister of Transport and Digital Infrastructure, Final Report.
- [3] N.N. 2018. "Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles", SAE International, Document J3016\_201806.
- [4] N.N. 2017. „Proposal for the Definitions of Automated Driving under WP.29 and the General Principles for developing a UN Regulation on automated vehicles”, Informal Working Group (IWG) on Intelligent Transport Systems / Automated Driving (ITS/AD), UNECE.
- [5] Zeeb, K., Buchner, A., & Schrauf, M. 2016. „Is take-over time all that matters? The impact of visual-cognitive load on driver take-over quality after conditionally automated driving.” Accident analysis & prevention, 92, 230-239.
- [6] Petermann, I., & Schlag, B. 2010. „Auswirkungen der Synthese von Assistenz und Automation auf das Fahrer-Fahrzeug System“, Proceedings of the AAET, 257-266.
- [7] N.N. October 2018. "Preparing for the future of Transportation; Automated Vehicles 3.0", U.S. Department of Transportation.
- [8] N.N. July 2017. "Regulating Automated Driving the UK Insurer View", ABI and Thatcham Research.
- [9] N.N. 2017. "Collision Between a Car Operating With Automated Vehicle Control Systems and a Tractor-Semitrailer Truck Near Williston, Florida, May 7, 2016", NTSB/HAR-17/02.
- [10] N.N. 2018. "Technische Aspekte des automatisierten Fahrens und Verkehrssicherheit“, Gesamtverband der Deutschen Versicherungswirtschaft e. V.
- [11] N.N. 2018. „Strassenverkehrsgesetz (StVG) §1a Kraftfahrzeuge mit hoch- oder vollautomatisierter Fahrfunktion“, Bundesgesetzblatt.
- [12] N.N. 2018. "ISO 26262 Road vehicles – Functional safety", International Organization for Standardization.
- [13] Gold, C., Damböck, D., Lorenz, L., & Bengler, K. (2013). "Take over!" How long does it take to get the driver back into the loop? Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 57(1), 1938–1942. <https://doi.org/10.1177/1541931213571433>
- [14] Feldhütter, A., Segler, C., & Bengler, K. 2018. „Does Shifting Between Conditionally and Partially Automated Driving Lead to a Loss of Mode Awareness?”, In N. A. Stanton (Ed.): SpringerLink : Bücher, Advances in Human Aspects of Transportation: Proceedings of the AHFE 2017 International Conference on Human Factors in Transportation, July 17-21, 2017, The Westin Bonaventure Hotel, Los Angeles, California, USA (pp. 730–741). Cham: Springer.
- [15] Gold, C. G. 2016. "Modeling of take-over performance in highly automated vehicle guidance", (Doctoral dissertation, Technische Universität München).
- [16] Kerschbaum, P., Lorenz, L., & Bengler, K. 2014. „Highly automated driving with a decoupled steering wheel”, In Proceedings of the human factors and ergonomics society annual meeting (Vol. 58, No. 1, pp. 1686-1690). Sage CA: Los Angeles, CA: Sage Publications.
- [17] Lorenz, L., Kerschbaum, P., & Schumann, J. 2014. „Designing take over scenarios for automated driving: How does augmented reality support the driver to get back into the loop?” In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 58, No. 1, pp. 1681-1685). Sage CA: Los Angeles, CA: SAGE Publications.
- [18] Bainbridge, L. 1983. "Ironies of automation. In Analysis, Design and Evaluation of Man–Machine Systems" (pp. 129-135). Pergamon.
- [19] Van den Beukel, A. P., van der Voort, M. C., & Eger, A. O. 2016. „Supporting the changing driver’s task: Exploration of interface designs for supervision and intervention in automated driving”, Transportation research part F: traffic psychology and behaviour, 43, 279-301.
- [20] Fahrenkrog, F. 2016. „Wirksamkeitsanalyse von Fahrerassistenzsystemen in Bezug auf die Verkehrssicherheit”, Dissertation RWTH Aachen University, fka mbH Aachen.
- [21] Form, T. 2018. "PEGASUS Method for Assessment of Highly Automated Driving Function", SIP-adus Workshop 2018, 13-15 November 2018, Tokyo International Exchange Center, Tokyo, Japan.
- [22] N.N. 2018. "L3Pilot Driving Automation, Piloting Automation on European Roads", Self-driving vehicles: European automotive R&D leading the global race, Brussels, Belgium.

## **CERTIFICATION OF HIGHLY AUTOMATED VEHICLES FOR USE ON PUBLIC ROADS**

**John McDermid**

University of York and FiveAI  
UK

**Phil Koopman**

Carnegie-Mellon University  
USA

**Robert Hierons**

Brunel University  
UK

**Siddhartha Khastgir**

University of Warwick  
UK

**John A Clark**

University of Sheffield  
UK

**Michael Fisher**

University of Liverpool  
UK

**Rob Alexander**

University of York  
UK

**Kerstin Eder**

University of Bristol  
UK

**Pete Thomas**

University of Loughborough  
UK

**Geoff Barrett**

UK

**Philip Torr**

University of Oxford and FiveAI  
UK

**Andrew Blake**

FiveAI  
UK

**Subramanian Ramamoorthy**

University of Edinburgh and FiveAI  
UK

Paper Number 19-0343

## ABSTRACT

**Objective:** A number of different methods must be combined for the robust certification of highly automated vehicles (HAVs) for deployment in ODDs encompassing public roads. This paper, which is authored by a braintrust of the world's leading academics in validation, verification and certification and affiliated with Europe's largest autonomous vehicle developer FiveAI, proposes a core set of processes.

**Methods:** The paper discusses in detail: (1) requirements discovery; (2) behaviour requirements; (3) simulation as a tool for verification; (4) useful tools and methods.

**Results:** We propose a process centred around hyper-scale fuzzed scenario-based testing and the use of coverage driven verification methods in digital twins of the ODD and using generative models representative of each ODD. Testing must cover both full stack testing, which will require photo-realistic and sensor-realistic rendering of scenarios and objects, together with accurate sensor modelling and motion planning stack testing, will require robust beliefs over scenario actor behaviours to test predictive, planning and motion synthesis.

**Discussion and Conclusions:** The paper poses several questions for policy makers: (1) Could a validation, verification and certification system that incentivizes sharing of scenarios while protecting the value intrinsic to their discovery, improve safety across the industry? Could it be used by an approval body such as a national Certification Agency to establish a high standard for national certification? (2) Can the industry agree on a scenario description language that supports coverage-driven verification and is extensible? (3) What should the specification of an appropriate simulation environment be? (4) Could the specification for a test oracle be made available and could this be based on a formal description of 'good driving'? (5) Is auditable adherence to the IATF16949:2016 quality assurance process sufficient to satisfy 'Conformity of Production'?

Key questions also remain, including: (a) What machine learning methods should be applied to directed random testing in coverage driven verification? (b) Given the high dimensionality of the test space, what coverage measures are meaningful in generative and ODD digital twin verification? (c) Which computer vision methods can we apply to the 3D reconstruction of digital twin worlds from photogrammetry, LIDAR scans and other modalities that mean accurate, up-to-date digital twins are feasible? (d) What hardware acceleration beyond GPUs can we design and apply to enable faster-than-real-time full stack verification of HAVs? (e) How can we apply formal software checking to the complex integrated systems required for autonomous driving to ensure that each build achieves its goals without bugs or gaps? (f) How do we really apply formal mathematical methods to express the Digital Highway Code (DHC), vehicle dynamics and other road user expectations and behaviours to verify the behavioural safety of HAVs? (g) How can we verify HAV systems that comprise of one or more end-to-end neural networks with the requirements to explain failure modes and take corrective actions to improve their performance using human readability and intermediate outputs of modular processes? (h) How might we extrapolate randomized testing, including near collisions, into a measure of probability of collision generally?

## INTRODUCTION

The development of Highly Automated Vehicles (HAVs) capable of performing SAE Level 4 autonomous driving (AD) is a huge attractor of intellectual and capital investment across the world today. No single company has developed a complete system of hardware and software that can realistically be deployed in unconstrained urban environments yet, but several teams expect to attain a standard that they consider should be deployable in our cities within 3-5 years, perhaps sooner in simple, wide, well-lit and sparse urban zones.

If we are able to deploy such systems, they have the potential to unlock major economic and societal benefits for city dwellers and our economies as whole: the means to offer low cost universal demand-responsive mobility to every citizen, a tool for unlocking unproductive commuting time and enabling economic engagement for everyone, increased road safety for all road users and materially lower pollution, congestion and resources today wasted in manufacturing, assembling, parking and disposing of personal vehicles. In delivering safe, on-demand, shared end-to-end journeys across a city, including zero occupancy dispatch, the advent of HAVs will presage an inevitable and

dramatic shift away from the car ownership model which has prevailed for over 100 years towards a low cost, shared mobility-as-a-service world which can integrate more successfully with shared public transport services.

Reaching that goal is requiring large teams of computer scientists, mathematicians, engineers, roboticists and manufacturers to work together across disciplines to meet many engineering and implementation challenges. These are highly complex technologies which must be built using commercially feasible hardware and by selecting, hardening and integrating many recent, and still being developed, cutting-edge research breakthroughs from academia. Not only must those teams themselves test and validate the resulting systems to ensure they do not cause injury or death to humans and animals or endanger property, the public as a whole – along with their elected representatives – need the reassurance of a clear and rational means to validate the safety of these systems independently through an appropriate regime of validation and a process of certification.

What is already clear is that the combinatorial effects of different road topologies, road users, appearances, lighting, weather, behaviours, sensors, seasons, velocities, randomness and deliberate actions cannot be adequately experienced in on-road testing alone, even in the constrained operational design domain (ODD)[1] constraints implied by level 4 autonomy. And if they could, it would take billions of highly varied miles of drive testing on each individual build of hardware and software to reach a statistically reliable level of validation that the proposed system could even attain human levels of safety. The stakes are high: even a single bad character in one line of software code can, and has, caused catastrophic failure. Any such failures found in testing would require build change with the potential for regressive effects meaning that the testing process would need to start again. This means that a methodology that rests solely, or mainly, on on-road testing is infeasible.

Although international and national standards exist for the functional safety of individual components and sub-systems (e.g. ISO 26262), no regulatory authority today has a well-defined system for validation of HAVs as a complete system rooted in an understanding of the problem space. For example, measures set out by California's Department for Motor Vehicles (DMV) include the reporting of 'driven miles per disengagement' and this is sometimes presumed as a competitive measure of maturity and safety of proposed systems. Not only can these measures be statistically meaningless[2] – only a tiny fraction of the potential state space has been explored – but they are potentially harmful in encouraging premature and non-representative on-road testing, discouraging interventions and propagating a misleading perspective on safety, leading to loss of life. Our opportunity is to set out a framework and ensure our testing and validation processes are world-leading, thereby ensuring safety for our citizens, gaining economic advantage first and unlocking global business opportunity for our scientific and engineering companies who embrace the regime.

In light of the perceived benefits from HAVs, the UK government has indicated a willingness to provide an exemption from (or modification to) the construction and use regulations so that they can be used on public roads before 2021, with more wide-sweeping legislative reform targeted thereafter.

While nobody should expect these systems to be perfect, we should expect them to reach human driver safety levels and to be progressively tightened to significantly higher safety levels over time. In that quest, it's important that development and testing practices are established, are followed and that developers and regulators can measure the safety performance of each combination of technologies in representative environments to a statistically meaningful standard.

This paper therefore seeks to explore the problem space, propose appropriate practices and contribute to the establishment of a certification regime that will safely unlock the value of HAVs to our citizens.

## **SAFETY OBJECTIVE**

Once human levels of safety have been attained and surpassed, a primary objective for any HAV program should be to reduce the incidence of injury to humans, animals and property.

The UK's Department for Transport reported that in 2016, 327 billion vehicle miles were driven in the UK and there were 137,000 'accidents' reported to the police which are essentially collisions reported to insurance companies. That equates to one reported 'accident' every 2.4 million driven miles, with reported serious injury occurring every

12.6 million driven miles. Not all incidents are police-reported ‘accidents’ and collisions are likely to be significantly more frequent than the reported statistics indicate. The number of motor insurance claims in 2016 was 4.34 million[3], or one claim every 75,000 driven miles and many accidents are not reported to insurers.

The Institute of Advanced Motorists in their ‘Licensed to Skill’ report in 2010 estimated that around 94% of these incidents can be traced directly to human error but, in terms of public acceptance, HAVs that cause human injury or death are likely to be held to a higher standard than fellow humans, however irrational that may be. We do not know exactly how much higher these standards will need to be, but it seems likely that in order for the general public to accept the relinquishing of control to these emerging autonomous systems, halving the collision rate would be a minimum target. And that implies an incident rate of around once per 200,000 miles.

If the above were achieved, HAVs could halve serious injury and death on our roads, saving over a thousand lives each year in the UK alone, most in the 15-29 age bracket. The societal benefit is an overwhelming one.

## **REGULATORY CONTEXT**

Regulations governing the standards, testing and certification of product conformity of vehicles on public roads in Europe are governed by European Union (EU) Directives and, by virtue of the fact that the EU is a contracting party to global technical regulations coordinated by the United Nations (UN), are also governed by safety and environmental aspects of UN regulations too. The UN regulations are managed by the World Forum for Harmonization of Vehicle Regulations, a permanent working party of the United Nations Economic Commission for Europe (UNECE). UNECE and EU countries take part in the technical preparatory work of the Forum and UNECE exercises the right to vote in the Forum on behalf of the EU.

Directive 2007/46/EC provides that EU countries share a common legal framework and general technical requirements for the approval of new vehicles and of systems, components and technical units designed for them. It establishes a harmonized framework so as to facilitate the registration, sale and entry into service of new vehicles anywhere in the EU, as well as rules regarding the sale and entry into service of vehicle parts and equipment.

For vehicles to be approved for registration, sale and entry into service, the ‘whole vehicle’ must pass all applicable approvals and, for this purpose, a single production sample is selected and tested as representative of the type to be approved, hence the term Type Approval. In order to gain whole vehicle Type Approval, each of the various systems, e.g. brakes, emissions, noise, etc., must be tested and meet the standards set out in the relevant EU Directives and UNECE regulations. There are no additional whole vehicle tests; instead the sample vehicle will be considered as a whole by a designated approval body and if the production sample of the complete vehicle can be confirmed to match the specifications contained in all the separate Directive approvals, then on submission of the relevant manufacturer’s information documents, it will result in the issue of a European Whole Vehicle Type Approval Certificate (EWVTA).

EU Regulations permit any EU Member State to appoint an Approval Authority to issue those EWVTAs and to appoint a Technical Service to carry out the testing to the EU Directives and Regulations standards. In the UK, both the Approval Authority and Technical Service functions are performed by the Vehicle Certification Agency (VCA).

No technical Directive yet exists for the approval of HAVs. Moreover, existing Directives sometimes conflict with such operation: one example being the UNECE regulation no 79 on steering type approval which places an effective 12km/h limit on HAVs through clause 5.1.6.1 which states that ‘Automatically Commanded Steering .... action shall be automatically disabled if the vehicle speed exceeds the set limit of 10 km/h by more than 20 per cent’.

Several working groups have been established to seek consensus on how UNECE and EU Directives should be amended to permit HAV operation.

## **OBJECTIVE OF THIS PAPER**

The objective of this paper is not to identify conflicts within the existing Type Approval process or suggest amendments to the existing Directives – this work is already underway through the various working groups – but to

identify the key components of a validation, verification and certification process for HAVs that could be adopted to ensure their safe introduction on UK and European roads, along with highlighting the open research questions in relation to that process.

Until now, there have been no universally accepted dividing lines between validation (which checks that the required specification is complete and accurate), verification (which is the process used to gain confidence in the correctness of a design or system with respect to its specification) and certification (which is the legal recognition by a certification authority that a product or service complies with the requirements).

This paper therefore proposes the following approach:

- To propose a target general framework, to be achieved over time, which is capable of being applied to the discovery and establishment of adequate specifications for HAVs, which defines a process for validating those specifications (including safety properties) and which establishes a means of verifying that any candidate System under Test (SUT) is robust to all major classes of defects against those validated specifications to a measurable standard. This will permit HAV technology developers to attain and, over time, exceed human levels of driver safety
- To establish that framework as a code of practice that the UK (and by extension, if adopted, the EU) will require HAV technology developers to internally adopt for V&V, if they want to deploy in those regulatory environments
- To require that the UK (and by extension, if adopted, the EU) certification authorities adopt the same framework to independently verify a randomized subset of the design verification
- To require certification authorities (or an approval body) to conduct an audit of the quality assurance (QA) processes of the HAV technology vendor to ensure that the design and test methodology they employ is rigorous
- To require that there is a process whereby HAV technology developer software updates remain robust to regressions and conform to specifications as they are updated

This paper is structured in the above order, first identifying the key attributes of a V&V framework for HAVs and then discussing how this may be applied in the context of certification.

## **A FRAMEWORK FOR HIGHLY AUTOMATED VEHICLE SAFETY VALIDATION & VERIFICATION**

To ensure a HAV validation framework can establish and measure performance against necessary safety standards, it must address at least five types of defects. These are intended to cover all types of potential faults in the system, its environment or its use:

- **Requirements defect:** the system is specified to do the wrong thing (defect) or is not required to do the right thing (gap) or the Operational Design Domain (ODD) description is incomplete (gap) or inaccurate (i.e. a validation defect). These types of defects may manifest as product defects where the system does something unsafe or as process defects, i.e. where there is insufficient evidence of safety
- **Design defect:** the system design fails to meet a specified safety and/or functional requirement or fails to respond properly to violations of the defined ODD
- **Implementation defect:** the implementation of the system does not conform to its design specification
- **Verification plan defect:** the verification plan fails to exercise potential states (e.g. corner cases) in requirements or to identify instances in which the vehicle's interpretation of the external world is incorrect to the degree that safety is impaired

- **Safety or reliability defect:** an invalid input or a corrupted system state causes an unsafe system behaviour or failure (e.g. sensor noise, component fault, software defect) or an excursion beyond the ODD due to external forces

### **HAV Requirements**

A key challenge for the safety assurance of HAVs is in understanding the system requirements and validating that they sufficiently represent the ODD before verification of the system against those requirements can begin.

**Vehicle Road Testing for Requirements Discovery** Discovering the system requirements for HAVs in a target ODD is a huge and necessarily incomplete task, partly because the real world has high dimensionality and combination possibilities – objects, environment, behaviours, degradations, sensors, occlusions and so on – but also because the process of discovering precisely what is needed is never finished as the real world keeps changing.

Since no digital record exists anywhere that does or could possibly describe all the possible stand-alone and combinatorial possibilities that might exist in anything other than the simplest ODD the HAV could be presented with, any system specification will inevitably still present gaps to the real requirements.

Minimizing those requirement gaps is the primary motivation for on-road vehicle data-gathering and testing operations. These include:

- Detecting novel road hazards
- Detecting lighting, weather, specularities, sensor combinatorial failures in the ODD
- Discovering behaviours that violate normal traffic rules and finding exceptional but possible scenarios
- Learning accepted norms of driving
- Discovering unusual road user configurations, surfaces, aesthetics and behaviours
- Discovering how behaviours vary by time of day, weather, season
- Finding situations where sensing modalities fail, localization exhibits randomness or biases
- Finding and correcting misleading but well-formed map data
- Discovering types of novel road signs and traffic management mechanisms specific to a micro-location or event
- Finding unusual road markings and vandalism, degradations, mistakes
- Learning emergent traffic effects caused by the HAV and learning third-party behaviours due to the presence of the HAV
- Learning malicious third-party behaviours

Once a discovered requirement is identified by vehicle testing in the ODD and validated (distinct from an SUT verification failure against an existing system specification), there should be an update to the system requirements for that ODD, an update to the requirements for the fidelity of the simulation environment, the generation of one or more new test cases or a combination of all three.

The larger the ODD, the longer and more expensive the requirements discovery process will be. It is for this reason, amongst others, that we are a long way away from a true SAE level 5 autonomous driving capability.

**Hazard Analysis** While real-world discovery of requirements is an essential part of requirements capture, systems engineering methods like STPA (Systems Theoretic Process Analysis developed by MIT) or Functional Hazard Analysis (FHA) should also be adopted to better understand where defects of any kind can lead to hazards. STPA has been used in the aviation industry by Boeing, Embraer and NASA.

**Encoding Scenario Requirements** Efforts are underway in various countries to document the HAV's requirements as a curated set of vehicle behaviours and scenarios, the largest being the 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 supported by Germany's Federal Ministry for Economic Affairs and Energy (the Pegasus project).[4]

The capture and curation of such scenarios and behaviours provides a means not just to specify system performance but to develop and verify functionality that attempts to meet those system specifications. Such scenarios and behaviours can also be used to generate regression tests which can be replayed in simulated worlds to play a part in verifying some aspects of the behaviour of an entire system-under-test (SUT), as well as to provide a baseline from which to randomize variables to discover new failure modes of the SUT.

The Pegasus project, which has gained the broad support of many major participants in the German automotive industry, has the aim of developing procedures for the testing of AD functions, in order to facilitate the rapid implementation of HAVs into practice.

Scenarios are a key element of the Pegasus verification concept in that they are the basis for eliciting whether the HAV under test exhibits appropriately safe system-level behaviours. Scenarios have a functional view (described in free text), a logical view (with a set of ranges for the "interesting variables"), and a concrete view (with all these variables given concrete values).

Pegasus scenarios can be captured in a number of different ways but since the whole project is still at an early stage, today there is just one live capture method, **OpenSCENARIO**. This is an XML-based format proposed by Vires Simulations Technologie GmbH and capable of being interpreted on Virtual Test Drive, a widely-used simulation platform Vires has developed and marketed. OpenSCENARIO is therefore currently being adopted by all participants in Pegasus as a pro tem standard for capturing concrete test cases. Longer-term, the Pegasus project hopes that OpenSCENARIO might evolve to become a cross-platform industry-wide standard for encoding scenarios and behaviours that could be ported to many or all simulation and testing execution platforms (including software-in-the-loop simulators, hardware-in-the-loop simulators and test track setups).

### **Behaviour Requirements**

Encoding such scenarios and confirming the ability of the SUT to perform a manoeuvre that avoids collision in testing against each scenario has limitations unless we can also verify whether the SUT can conform to traffic laws and to driving codes of practice during that testing.

**Encoding Traffic Law & Driving Behaviours** For that, we need a publicly-available, machine-readable and complete set of those traffic laws and driving codes and conventions, a Digital Highway Code (DHC). That DHC must include exception handling rules, for example: when and how exactly can a vehicle cross a centre dividing line, if present, to avoid a lane obstruction; when would it be acceptable to mount a sidewalk; what should a driver be permitted to do if traffic lights are defective and so on. These conventions should extend to polite behaviour on the road in that jurisdiction, including when a HAV should let other road users merge into its lane, to what extent does the HAV have a responsibility to ensure the most efficient use of the road network, etc.

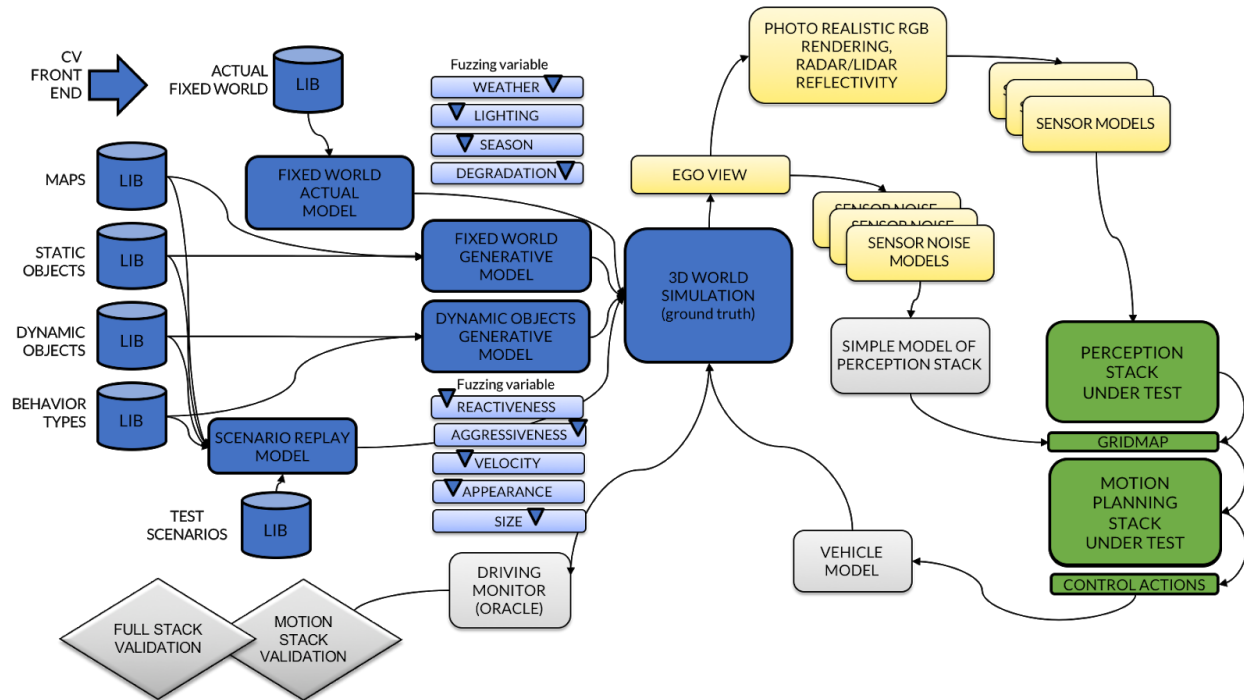
### **Simulation as a Tool for Verification**

The core of any effective verification program for HAVs will be the use of simulation.

One or more simulators must be developed to be capable of replaying scenarios in which the road, lighting, weather, degradations, objects, road user actions and interactions can be re-generated and used for verifying the SUT. How complete and representative of the real world a simulator needs to be depends on which parts of the SUT stack is being exercised and tested and how much testing is necessary to explore the state space. But at some level, the full SUT stack must be tested, which means that photo-realism, radar and Lidar reflectivity, sensor models, vehicle dynamics, road surface, human actions must be model variables on top of a baseline simulation capability. A critical issue is how good these simulations must be in order to be effective verification tools, when considered in conjunction with other verification methods including lab test, real-world driving, etc.



**Components** An example of the principal components of a simulation model suitable for HAV verification is shown in figure 1.



**Figure 1: Example simulation model to support HAV verification**

**Scenario Replay** The base point for using a simulator is the interpretation of a scenario and its re-creation in a simulated world, including the instantiation of all recorded dynamic agents and behaviours captured in that scenario. Given a model of road, layout, obstacles, occlusions, road users and behaviours, a simulator can test the predictive capability of the SUT stack, test its ability to plan the HAV motion in the context of road rules and uncertainties, set a trajectory and control the HAV safely, given a model of the HAV vehicle dynamics. A noise model is used to inject perception stack uncertainty into measurements and, at a base level, testing would confirm safe operation given that scenario and noise. Such behavioural tests could run much faster than real-time since the perception layers of the stack would be replaced with noise models. Types of noise as well as scene and user behaviours are varied to discover new failure modes in a process sometimes referred to as ‘fuzzing’.

**Coverage Driven Verification** In addition, simulation models can also be generative in the construction of new scenarios that are theoretically possible but have not yet been captured in road testing or in manual test case generation. Generative models allow the exploration of state space beyond fuzzing, either on a random or directed basis. Several useful techniques exist for exploring and finding new failure modes. These include (i) coverage metrics which then can direct random test generation to broaden that coverage and (ii) using machine learning to reward finding new combinations of layouts, objects, behaviours, velocities, lighting, weather, season etc. that cause the SUT to fail using the proximity of close or actual test failures from random test generation. These types of verification are usually referred to a coverage driven verification. Since the state space being explored for HAVs is extremely large, to all intents and purposes infinite, coverage driven verification using generative modelling would emphasize exploration over density of test coverage which would, by definition, remain sparse.

**Randomization & Direction** Hand-written tests can be created by focusing on expected corner cases and then automatically ‘fuzzing’ around them. This involves human generation of very general abstract scenarios which are then instantiated into many different concrete scenarios and coverage is typically clustered around these corner cases.

Another approach, currently favored by the Pegasus project, is to use randomization with expected distributions, often referred to as Monte Carlo simulation. This approach provides sparse coverage but will deliver estimates of the frequency of failures.

But directed or machine-learning randomization is the favored method for defect-finding. These techniques emphasize the capability to reach edge cases, at the expense of overall failure rate estimation and can also be used to support the systematic discovery of defects with respect to adversarial perturbations.[5]

It is important to note that the statistical distribution of test cases has to be driven both by the probability of occurrence and the magnitude of a potential loss (i.e., by risk, not just occurrence). Otherwise a relatively rare scenario that could result in a fatality will be under-represented. In other words, while some testing should concentrate on normal functionality, a substantial portion of testing will need to emphasize infrequent but dangerous situations.

**Verification in Digital Twins** As well as fuzzed scenario replay and the use of coverage driven verification in generative models, simulation models can also be built that replicate the real world ODD and the likely object types and behaviours in it. Applying coverage driven verification to such digital twins will find additional failure modes which may not be found in fuzzed test scenarios nor easily found in fully-generative models. It can also provide a higher level of coverage that, to some extent, is measurable in relation to the real-world twin the digital model represents. This approach is therefore an extremely useful addition to the first two techniques but requires the creation of a ‘digital twin’: literally a realistic model of the ODD along with a distribution of dynamic agents and behaviours that are representative, in absolute terms, of that specific ODD.

**Full Stack as well as Motion Planning** Not only must the predictive, behavioural and control aspects of the HAV stack be tested in simulation (motion planning) but the full stack must be tested too, since many failure modes are possible in the sensors, localization, perception, interpretation, classification and confidence measurement layers of the stack alone, or as they interact with the motion planning layers as a whole.

Full stack testing is a bigger task than behavioural testing, since the simulation model must now render the scene with photorealistic textures, lighting effects, reflections, specularities, shadows, weather and seasons. The same is true for all road users, pedestrians, cyclists and any other objects in the scene, and a library of such objects must be curated and maintained. Sensor outputs need to be modelled based on the placement of the sensors on the HAV and on accurate models of the behaviour of those sensors, including any dynamic range limitations, calibration limitations or errors, quantization, timing delays, race effects, color and lighting sensitivities, blur and other optical perturbations. And it’s not just RGB that needs rendering, it’s also radar, Lidar and other sensing outputs, given material, density, weather and other conditions. A useful contribution here may also come from the Pegasus project, in the shape of the proposed standard for defining weather, signs, sensor inputs and so on, called Open Simulator Interface (OSI). OSI could be used in the future to connect various simulated artefacts produced by different companies.

Not surprisingly, full stack testing is computationally expensive and may run well below real-time, meaning that attaining meaningful levels of coverage will require substantial datacenter resources to spin up multiple instances of the simulator, sensors and the SUT.

### **Useful Tools and Methods**

**A Scenario Language** A well-defined language to describe scenarios that can be interpreted by each simulator to re-create essentially the same scenario and behaviours with high fidelity is likely needed. Perhaps OpenSCENARIO is such a language, but if it is not suitable a new one will need to be created. One such initiative is being pioneered by Foretellix, an Israeli startup, and they simply call this language Scenario Description Language or SDL. But whether it is OpenSCENARIO, SDL or something different, a cross-industry agreement must be reached.

**A Scenario Sharing Library** A library of scenario test cases must be developed by or made available to each company building HAV technology. Of course, it needs to be as comprehensive as possible in many dimensions.

A suitable scenario library should:

- Cover cases where collisions are possible and must prove SUT avoidance within the boundaries of the DHC
- Monitor and report behaviour before, during and after collisions or near-collisions
- Pay specific attention to interactions between HAVs and humans and grade for collisions, near collisions, breaches of the DHC and any other behaviours where the SUT adversely affected any virtual passengers, traffic flow or other road users
- Emphasize the verification of inference or deep neural network-based algorithms and find failure cases where interpretability is poor
- Use (i) replayed scenarios (ii) fuzzed replayed scenarios (iii) generative models with directed or machine-learning randomization and (iv) replayed, fuzzed and generative behaviours in a digital twin of representative (or whole) digital twin instantiations of target ODDs
- Look for both “expected” and “unexpected” defects
- Employ configuration files that permit portability from city-to-city through tractable modification of vehicle, sensors, weather files, location, signage, human behaviours, road markings and DHC

These objectives must be met whilst maintaining transparency and maintainability. As the number of test scenarios grows and as they become ever more intricate, this will become a real problem unless tackled from the outset by the industry in initiatives, like the Pegasus project or by the adoption by several key players of a succinct means of encoding those scenarios.

**A Motion Language** A motion language with qualitative actions (e.g. "follow at a safe distance" or "pull in safely") could add significant value to the validation and verification processes. In the UK, learner drivers are tested on their knowledge of the Highway Code and advanced motorists are encouraged to follow the guidance set out in Roadcraft: The Police Driver’s Handbook.

Codifying what constitutes good driving as described in these manuals, as in the suggested DHC can serve the following uses:

- Engage with the public on target HAV behaviours on UK roads
- Complement scenario-based, coverage driven system testing
- Provide the basis behaviour for a test oracle
- Provide the basis functionality for low complexity monitoring systems to be used by HAVs in run time to improve safety robustness.[6]

Model-checking using a formal method might be used to automatically verify safety properties of the DHC using observation of behaviours from the real world.

**Application of Formal Methods** Important aspects of hardware design are already amenable to automated proof methods, making formal verification possible to introduce. But the application of these methods to software design is a more complex problem, although a number of mathematical methods do exist for proving a computer program satisfies a formal specification of its behaviour.

As development moves towards higher levels of autonomy then the need for stronger, formal software verification becomes acute. One of the fundamental steps that needs to be taken to understand and analyse HAVs is that we must assess not just what a system will do, but why it chooses to do it.[7] This, together with the need for explainability and responsibility leads towards systems with an identifiable central decision-making software component and, in this case, the formal verification of this software component can ensure that its decision-making is correct and allows us to analyse the decisions an autonomous system makes against the decisions that a human driver should

take. In complementary work, in aerospace[8], it is formally verified that an autonomous (air) vehicle always follows (selected) "Rules of the Air".

In the past 2-3 years, work has also started on how formal verification methods could be applied to making the problem of verifying HAVs easier. For example, by understanding and formalizing specific desired granular driving behaviours and checking by conventional means that any SUT can be verified to satisfy those granular behaviour requirements, the goal would be to eliminate collisions by design. Two notable contributions have come from TU Munich and MobilEye respectively as first attempts at producing a formal mathematical model for acceptable driving behaviour, using a concept of measuring and determining blame in the case of a collision.[9,10]

These are useful contributions to the process of HAV verification but the work so far is insufficient, not least in that proposed formulation for defining blame-free behaviour as set out in the most recent paper (for example in the presence of a child playing near parked cars) would imply a vehicle speed of just 10-15mph, yet humans can and do drive safely at 20-25mph in the same scenarios. Work is needed to consider how those formulations can discover and capture the more complex processes that humans are using for driving, including the social norms, customs and behaviours that are an essential (locally specific) element of the safe driving in mixed human/HAV environments.

## **COMPONENTS OF A HIGHLY AUTOMATED VEHICLE CERTIFICATION PROCESS**

### **New Type Approval Process**

The current Whole Vehicle Type Approval is well-suited to the present model where those component, system and vehicle specifications can be well-defined, stable, recorded, tested and approved.

But this process is clearly inadequate for HAVs, because:

- Many requirements will be highly specific to the ODD
- Requirements will change on a continuous basis as new vehicles, objects, behaviours, signage are emergent in the ODD over the life of the SUT and HAV
- There will always be a gap to the real-world requirements, necessitating a continuous process of requirements discovery through vehicle testing and/or live vehicle logging
- On discovery of a failure, HAV technology developers will be obligated to provide updated software and models to the vehicle and/or upgrade sensors, compute, communications technology or other AD capabilities and this could be very frequent and/or urgent
- Those updates, in improving performance on certain identified failure modes, may cause unexpected regressions or changes in others

The safety risks from AD operation are very different to those being managed in the current Whole Vehicle Type Approval process and a new testing and certification process is required.

To protect the public, improve road safety over time, assure public trust and ensure our economies and citizens reap the benefits of HAVs ahead of other developed economies:

- A new **HAV Type Approval** process must discover and establish a very high safety standard for the verification and certification of any SUT used on public roads in the UK and, if adopted, across the EU
- The certification of HAV Type Approval, at least initially, must be specific to the requirements of a well-defined ODD and a well-defined DHC; those requirements must represent a complete specification, following extensive discovery
- That high standard must be consistently applied to all HAVs seeking certification for any ODD/DHC pair

- Each certification of HAV Type Approval granted for any ODD/DHC pair must carry the obligation of Conformity of Production, meaning that all subsequent hardware and/or software changes must not reduce the overall safety of the design measured against the then current and most complete ODD/DHC requirements specification; the meaning of overall safety in this context will need to be established, likely as a high threshold pass rate of a statistically significant sample of regression and generative test cases in an ODD/DHC pair in full stack and motion planning simulation environments
- Any request for a HAV to operate outside its ODD/DHC pair must be accompanied by a further certification process for the changed ODD or DHC respectively

### **Practical Aspects of Validation, Verification and Certification**

**Scenario Sharing** As discussed, discovering scenarios that can inform safe system requirements for HAVs is expensive work spanning large scale, multi-fidelity simulation as well as physical testbed and public road testing. Much like the expensive process of drug discovery, no commercial organization could incur the expense and take the commercial risk unless they were assured some preferential use of the resulting outputs, which in the case of drug molecule development and testing, is achieved through patent protection. For the organizations developing HAV technology, requirements discovery is a similarly huge investment but also a source of competitive advantage.

Clearly a balance needs to be struck between sharing discovered requirements for the public good and that commercial imperative, without retreating to a legally enforceable patenting regime.

We propose a model by which HAV technology developers are encouraged to share the scenarios they discover with the UK certification authority (UKCA). Independent test houses would be commissioned by the UKCA and provided with controlled access to the scenarios for the purposes of evaluating HAV performance for both certification and also on behalf of regulated UK insurers, where required:

- Submitted scenarios are evaluated by UKCA for possible acceptance into an ODD certification test catalog, for example on the basis of probability in the target ODD or on the basis of more than one HAV technology developer executing the scenario and passing the test
- HAV technology developers can elect for submitted and accepted scenarios to be made public, but are not obligated to do so
- Any SUT for any target ODD must be tested in simulation by an independent test house against the full test catalog applicable for the ODD certification (whether publicly visible or not)
- A publicly described test oracle will determine whether a test has passed or failed, based on an overall safety threshold set by the UKCA in which the probability of occurrence of each scenario for the target ODD must be evaluated
- Where a SUT fails a private scenario, abstracted feedback would be provided to the HAV technology developer of that SUT, e.g. SUT failed in interaction with a cyclist.

A process along these lines has the following advantages:

- All HAV technology developers are encouraged to submit scenarios for testing in order to raise the bar for competitors seeking certification in an ODD
- Abstracted feedback from failed tests should encourage HAV technology vendors to generally improve their system safety performance rather than ‘gaming’ a solution to a specific scenario. However, the UKCA must ensure that vendors are not prevented from passing certification by being required to pass highly unlikely scenarios for which they are not provided details
- A market is created for non-competing HAV vendors, e.g. component suppliers or others, to find and submit private scenarios which, once accepted by the approval body have in themselves a value which can be licensed to technology vendors seeking system certification

- Independent test houses would not be subject to the same Freedom of Information (FOI) requests as a government body and could thus protect HAV technology vendors from being forced to disclose exhaustive details about their performance in relation to specific scenarios which could result in the disclosure of valuable trade secrets

**Scenario Validation Process** The validation of submitted scenario candidates into an ODD test catalog that becomes mandatory is a process which must be developed.

Lessons can likely be drawn from other sectors which have successfully tackled similar challenges of competitive technology development which must evolve standards and operate in a shared common environment.

Cellular wireless telecommunications is perhaps a good example, where the establishment of a cross-industry body, the Global Certification Forum (GCF) was established to define the priority of different work items (in their case dependent on Mobile Network Operators' deployment plans) and how to test conformance to relevant Third Generation Partnership Project (3GPP) wireless standards, such as 3G and LTE, so that the standard is met and there is a strong basis for expecting inter-operability between different networks and network equipment. GCF defines work items to prioritize specific test areas, working groups are drawn from industry participants to review those work items and to seek agreement on the ingredients of conformance test cases, pass criteria, parameters for simulation etc. and to be the final determinant of formal adoption of test cases as part of the mandatory program to be certified as GCF compliant by independent test houses. Obligatory test cases for each work item grow as standards are evolved and field failures are identified. In the example of 3G standards, the mandatory test program as a whole escalated quickly from tens of test cases to thousands of increasingly complex test cases over several quarters. In GCF's case, for any new test case to be adopted, it must be shown to be reproducible and repeatable, which normally means that two separate test and measurement organizations must demonstrate the implementation and execution of the same test. Cellular wireless technology development has different market and technology dynamics (global standards, established test and measurement companies, already a highly competitive market, contained functionality, and not safety critical, etc.), so an exact read across to HAVs will not work, but adaptation of some of these ideas for certifying HAVs could be instructive.

**Simulation and Test Tool Sharing** HAVs will ultimately operate over a wide range of real-world environments, some of which will be extremely complex with enormous possible state spaces and failure conditions to explore and verify. That leads to the conclusion that simulation must play a lead role in any effective testing procedure, in the generation of test conditions, in the parallelization and/or faster than real-time scaling up needed in the measurement of test coverage and in the defect-seeking capabilities of the randomization testing.

Closed course, physical testbed testing is one form of simulation that has a role to play in any meaningful testing regime. It serves an important purpose in that a real HAV's full stack response is measured with hardware in-the-loop within a full physical environment that has been designed to stress known specific risk aspects of the system and can not only identify system defects against those specific scenarios but can also pinpoint simulation modelling defects and gaps to the real world.

However, the dominant focus of any robust certification process should rest on system verification using high-fidelity software simulation at hyper-scale across a vast number of permutations and combinations. Moreover, this process must leverage tools to explore state space and seek defects, such as fuzzing and directed random testing as well as replaying regression suites of curated scenarios.

Engaging private enterprises in developing and contributing to the development and operation of this certification process is a real consideration, particularly in relation to parties who do not themselves plan to be operators of HAVs in the target ODDs, as may be the case for some HAV technology developers. Even in these cases, there may be a preference for reserving tools and models as trade secrets over sharing their utility across the industry as a whole.

Governments therefore may have an important role to play in enabling a market to exist for the licensing of tools or for their commercial use by practising entities. The objective needs to be to ensure that development expenses required for necessary and valuable independent simulation and tools are capable of being leveraged into meaningful

revenue streams by technology developers. One means of achieving this would be for government to signal and enable a market for such tools to be created, for example through the UKCA or to sponsor a cross-industry unit to step up to the important task, one possible candidate being the UK Government's Meridian initiative.

**Non-Deterministic Behaviour Verification Process** The behaviour of SUT for HAVs will exhibit non-determinism in the sense that if we repeat what is an identical test execution with what we believe to be an identical opening state, we might still get a different system behaviour. This non-determinism may be a result of e.g. random noise injection, race conditions, or some other aspects of operating system performance.

Therefore, in order to build confidence in system performance, an effective verification program may need to run a single test case multiple times. Where possible, that program must eventually reason about the number of test executions necessary to achieve a defined confidence level in the results, using probabilistic arguments.

Where possible, however, the industry should seek to build tools that offer repeatability and possibly even random stability to ensure that defects can be re-found and corrective actions can be proven to have been effective.

**Test Oracle** A test oracle is a mechanism for determining whether a system has passed or failed a test and usually is comprised of three capabilities:

- A generator, to provide predicted or expected results for each test
- A comparator, to compare predicted and obtained results
- An evaluator, to determine whether the comparison results are sufficiently close to be a pass

Any of the oracle capabilities may be automated and an automated test oracle will be required to generate, compare and evaluate the performance of the SUT across the test scenario catalog, and perhaps in a fully generative model within the ODD constraints, to ultimately determine if the system performed acceptably given the certification criteria.

The generator should make use of the DHC as extended and the comparator should compare the SUT results against the desired DHC and safety outturns. Evaluation is significantly more complex than simply determining if the SUT was involved in a collision since at one extreme bad driving behaviour doesn't always result in a collision and at the other, a collision is the safest choice for a given set of circumstances.

The specification for the test oracle should be made available to HAV technology developers seeking certification.

**Conformity of Production (CoP) Audit** Conformity of Production (CoP) is a means of evidencing the ability to produce a series of products that exactly match the specification, performance and marking requirements outlined in the type approval documentation.

In the context of HAVs and a new certification process, HAV technology developers will need to provide evidence to the satisfaction of UKCA that the HAV SUT is representative of all of that Type and that the process of developing and deploying design changes is robust. The form of evidence will need to be carefully considered but could follow the lines of a process review.

The International Automotive Task Force (IATF) together with the International Organization for Standardization (ISO) has developed a standard, IATF16949:2016.[11] This defines the quality management system requirements for the design and development, production, installation and service of automotive-related products.

To achieve IATF certification, an automotive supplier has to work according to automotive core tools, such as:

- Advanced Product Quality Planning – a structured approach to the design and development of products and processes
- Production Part Approval Process – formal release by the customer of a supplier's product and process

- Failure Mode Effect Analysis – risk analysis tool in which a supplier analyses the major risks of not fulfilling the required functions in the current design or process
- Measurement System Analysis – evaluation of the reliability of the measurement systems used by a supplier in its process
- Statistical Process Control – a method of quality control which uses statistical methods to monitor and control a process
- 8D Problem Solving – structural approach to analyze problems, including root causes analysis, containment and corrective actions[12]

Since IATF16949:2016 contains all the key elements for a QMS and is already centered on automotive applications, it is a strong candidate to deliver the framework for the CoP audit compliance of HAVs.

## **PROMISING NEW RESEARCH AREAS**

**Swiss Cheese Model** Recent promising research at TU Darmstadt has centered on applying a technique known as the Swiss Cheese Model to HAV verification for assessing the probability of collision. In essence, each sensing modality, process, behavioural or environmental variable has ‘holes’ which could permit a failure and when those holes line up, a collision can occur. One of the key unknowns for assessing the safety of HAVs versus human drivers is a strong understanding of the gap between the probability of critical situations arising in driving scenarios and probability that those critical situations do actually result in a collision. In human driven cars, this difference is a representation of the driving skill and attention of the driver themselves. But on replacing the human with the SUT, those human failure modes (which could be inattention, blind spots etc.) are replaced with new failure modes (which could be detection and classification accuracy, prediction failures etc.). The replacement of one set of cheese slices with another can exhibit quite different failures which demands further research.

Quantifying and measuring these impacts has the potential for us to measure the probability of collision and to compare the two in quantifiable ways and deserves further research.[13]

**Extreme Value Theory** In another initiative, this time from a research team at Volvo Cars, studies into the use of near-collision measurement as a means of estimating the frequency of actual collisions show good promise. Their approach uses a technique called Extreme Value Theory but more importantly highlights the need for further research into capturing and using near collision data for robust collision rate estimation.[14]

These ideas, and many others, should be reviewed and considered for the on-going development of HAV validation, verification and certification processes.

**Remaining Research Questions** Key research questions remain, and industry participants can and should work together with leading academics in UK and EU to address them, including:

- What machine learning methods should be applied to directed random testing in coverage driven verification?
- Given the high dimensionality of the test space, what coverage measures are meaningful in generative and ODD digital twin verification?
- Which computer vision methods can we apply to the 3D reconstruction and annotation of digital twin worlds from photogrammetry, Lidar scans and other sensing modalities that mean accurate, up-to-date digital twins are feasible?
- What hardware acceleration beyond GPUs can we design and apply to enable real-time and faster-than-real-time full stack verification of HAVs?



- How can we apply formal software checking to the complex integrated systems required for autonomous driving to ensure that each build achieves its goals without bugs or gaps?
- How do we really apply formal mathematical methods to fully express the DHC, vehicle dynamics and other road user expectations and behaviours to allow us to verify the behavioural safety of HAVs?
- How can we verify HAV systems that comprise of one or more end-to-end neural networks with the requirements to explain failure modes and take corrective actions to improve their performance using human readability and intermediate outputs of modular processes?
- How might we extrapolate randomized testing, including near collisions, into a measure of probability of collision generally?

## QUESTIONS FOR POLICY MAKERS

This paper makes a number of suggestions that fall into the realm of policy making, including:

- Could a validation, verification and certification system, such as that outlined in this paper, that incentivizes sharing of scenarios while protecting the value intrinsic to their discovery, improve safety across the industry? Could it be used by an approval body such as UKCA to establish a high standard for UK certification?
- Can the industry agree on a scenario description language that supports coverage-driven verification and is extensible? Is Pegasus a suitable basis for extension to meet this?
- What should the specification of an appropriate simulation environment be and would the government request to tender for delivery of such a tool?
- Could the specification for a test oracle be made available and could this be based on a formal description of ‘good driving’ in accordance with a DHC?
- Is auditable adherence to the IATF16949:2016 quality assurance process sufficient to satisfy ‘Conformity of Production’?

## CONCLUSIONS

A number of different methods must be combined for the robust certification of HAVs for deployment in ODDs in the United Kingdom and, by extension, other jurisdictions in Europe.

At the centre of this process is hyper-scale fuzzed scenario-based testing and the use of coverage driven verification methods in digital twins of the ODD and using generative models representative of each ODD. Testing must cover both full stack testing, which will require photo-realistic and sensor-realistic rendering of scenarios and objects, together with accurate sensor modelling and motion planning stack testing, which will require robust beliefs over actor behaviours to test predictive, planning and motion synthesis capabilities. A method for sharing scenarios to a UKCA for industry-wide testing will be required and a means of balancing that sharing for the public good with the need to retain economic leverage over the necessary costs of discovering those requirements will need to be devised. A DHC to include good driving behaviours will be needed and a test oracle will be required to evaluate and publish certification performance.

## REFERENCES

- [1] The specific conditions under which a given driving automation system or feature thereof is designed to function, including, but not limited to, driving modes is known as the ODD, in accordance with SAE J 3016
- [2] “Even if the safety of autonomous vehicles is low—hundreds of failures per 100 million miles, which is akin to human-driven injury and crash rates—demonstrating this would take tens or even hundreds of millions of

- miles, depending on the desired precision.” Kalra, Nidhi and Susan M. Paddock, *Driving to Safety: How Many Miles of Driving Would It Take to Demonstrate Autonomous Vehicle Reliability?*. Santa Monica, CA: RAND Corporation, 2016. [https://www.rand.org/pubs/research\\_reports/RR1478.html](https://www.rand.org/pubs/research_reports/RR1478.html).
- [3] Number of motor insurance claims notified in the United Kingdom (UK) from 2010 to 2016 (in millions), Statista 2018
  - [4] <http://www.pegasus-projekt.info/en/>
  - [5] Huang X., Kwiatkowska M., Wang S., Wu M. (2017) Safety Verification of Deep Neural Networks. In: Majumdar R., Kunčák V. (eds) *Computer Aided Verification. CAV 2017. Lecture Notes in Computer Science*, vol 10426. Springer, Cham
  - [6] Monitor/actuator pair architectures can be used in-vehicle to separate the most complex autonomy functions from simpler safety functions. The primary AV functions are performed by the high complexity ‘actuator’ system, and a paired module (the ‘monitor’) performs an acceptance test / behavioural validation. The low complexity monitor system should be more straightforward to verify and therefore could, potentially, be verified to ISO 26262 ASIL-D
  - [7] Fisher, Dennis, Webster: *Verifying Autonomous Systems*. *Communications of the ACM* 56(9):84-93, 2013. <http://doi.acm.org/10.1145/2494558>
  - [8] Webster, Cameron, Fisher, Jump: *Generating Certification Evidence for Autonomous Unmanned Aircraft Using Model Checking and Simulation*. *J. Aerospace Inf. Sys.* 11(5):258-279, 2014. <https://doi.org/10.2514/1.I010096>
  - [9] Rizaldi, A., & Althoff, M. (2015, September). Formalising traffic rules for accountability of autonomous vehicles. In *Intelligent Transportation Systems (ITSC), 2015 IEEE 18th International Conference on* (pp. 1658-1665). IEEE.
  - [10] Shalev-Shwartz, S., Shammah, S., & Shashua, A. (2017). On a Formal Model of Safe and Scalable Self-driving Cars. arXiv preprint arXiv:1708.06374.
  - [11] <http://www.aiag.org/quality/iatf16949/iatf-16949-2016>
  - [12] “Working in the automotive industry” H. Broekman; D. Ekert; M.I. Kollenhof A.E. Riel; H.C. Theisens; R. Winter, 2017
  - [13] Winner, H., Wachenfeld, W., & Junietz, P. (2018). Validation and Introduction of Automated Driving. In *Automotive Systems Engineering II* (pp. 177-196). Springer, Cham
  - [14] Åsljung, D., Nilsson, J., & Fredriksson, J. (2016). Comparing Collision Threat Measures for Verification of Autonomous Vehicles using Extreme Value Theory. *IFAC-PapersOnLine*, 49(15), 57-62

## **CHALLENGES FOR OCCUPANT SAFETY IN HIGHLY AUTOMATED VEHICLES ACROSS VARIOUS ANTHROPOMETRIES.**

**Bronislaw Gepner, Katarzyna Rawska, Rachel Richardson, Shubham Kulkarni, Kalle Chastain, Junjun Zhu, Jason Forman, Jason Kerrigan**

University of Virginia, Center for Applied Biomechanics  
4040 Lewis and Clark Dr., Charlottesville, VA 22911 USA

Paper Number 19-0335

### **ABSTRACT**

The introduction of automated driving systems (ADS) is likely to change the very nature of personal transportation. Without the need to drive, occupants will have more freedom to engage in other activities, which could result in major changes to vehicle interiors, controls, and seating configurations. Reclined posture seating may be an option that manufacturers consider in the relatively near term. The goal of this study is to evaluate how varying occupant anthropometry, distance to the knee bolster, and seatback angle affect occupant response.

A finite element model of a vehicle occupant compartment with the state-of-the-art seatback integrated restraint system was used, to evaluate three different simplified Global Human Body Model Consortium (GHBMC) occupant models (small female, midsize and large male) in frontal crashes. A full factorial sensitivity study was performed with four different levels of seatback recline (0, 10, 20, 30 deg) and four different distances to the instrument panel knee bolster resulting in total of 40 simulations.

Increasing the seatback recline angle caused the occupants' pelvis to submarine under the lap belt, which, in turn, resulted in poor pelvis-belt engagement and increased occupant excursion. Larger occupants tended to be able to withstand higher seatback recline angles without submarining than smaller occupants. Additionally, across all occupants, increased recline angle resulted in increased lumbar compression and shear force.

The new ADS environment is likely to pose substantial challenges to occupant restraints systems. Increased seatback angle increases the propensity of occupants to submarine, and results in increased lumbar spine load.

### **INTRODUCTION**

The introduction of automated driving systems (ADS) is likely to influence almost every aspect of personal transportation. With Level 3 autonomy, the occupants will no longer be required to constantly interface with the vehicle controls [1-3]. Consequently, they may no longer be constrained to traditional seating postures. They will have more time and freedom to engage in other activities, which could result in major changes to vehicle interiors, controls, and seating configurations. While it will take time to develop the new automated technology, and revolutionize the layout of the occupant compartment, the greatest near-term changes will likely occur with drivers choosing to recline their seats and move them away from the knee bolster (KB) to rest during periods where autonomous modes are engaged. Thus, these seating choices may soon challenge the ability of current vehicle safety systems to adequately protect the occupants.

There are few studies focusing on occupant kinematics and restraint performance in reclined postures [4-7]. Those studies indicate that higher recline angles as well as increased distance to the KB may result in higher risk of submarining. Submarining occurs when the lap belt loads the abdominal area, after passing over the iliac crest of the pelvis to load the abdominal soft tissues without engaging, or after disengaging, the pelvis. This in turn results in series of adverse effects onto occupant-restraint engagement, occupant kinematics and occupant injury risk. These studies identified pelvis motion and lumbar spine loads as areas of particular interest. Additionally, some studies considered the differences between traditional b-pillar-mounted 3-point belt, and seat integrated restraint [4, 7]. While a seat-integrated D-ring resulted in earlier engagement of the torso, and less forward head motion, the b-pillar-mounted belt resulted in lower resultant force and flexion angle in the lumbar spine. However, none of these studies considered the effect of occupant anthropometry on occupant response.

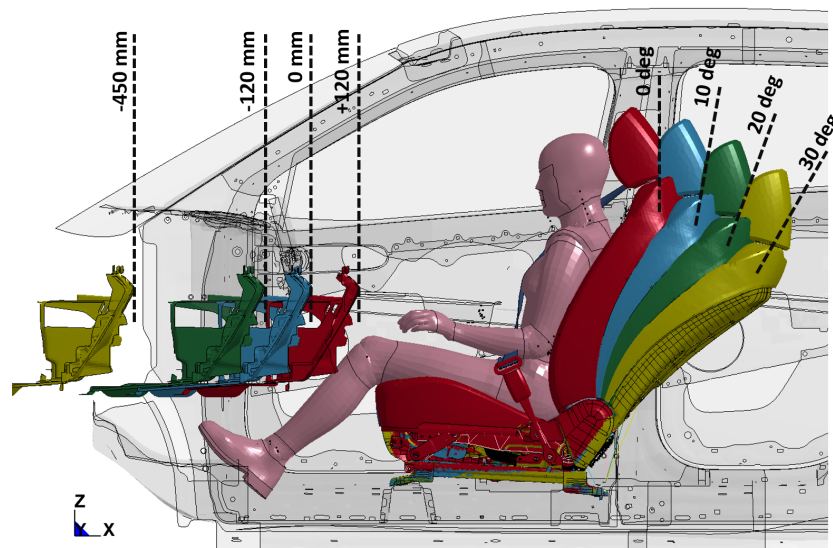
The goal of this study was to evaluate the response for reclined occupants in frontal impacts across variations in occupant anthropometry, recline angle and the KB position. The specific goal of this study was to provide general overview of occupant, and restraint system responses across all varied conditions. This was accomplished using the family of Global Human Body Models Consortium (GHBMC) simplified human body models (HBM): mid-sized male, large male, and small female, subjected to 56 km/h frontal-impact simulations in a finite element model of a generalized vehicle interior.

## METHODS

### Overview

The simulation environment was developed based on the finite element (FE) model of the prototype vehicle provided by the OEM. Several changes were incorporated into the original model in order to make it suitable for the current study. First, the seatback integrated 3-point seatbelt system was developed. The seatbelt included lap belt pre-tensioner, shoulder retractor pre-tensioner and force limiter. Second, the seatback was reinforced with additional beam elements to provide appropriate structural support for the loads expected from the seatback integrated restraint system. Third, the KB was decoupled from the vehicle interior to facilitate rapid and parametric interior configuration adjustment. All simulations were performed with the occupant seated in the right front passenger seat, with generic passenger airbag, subjected to a USNCAP 56 km/h frontal crash pulse.

A full factorial design of experiments (DOE) was performed with respect to the parameters including, occupant anthropometry, seatback recline and KB position. Three different occupant anthropometries, small female (F05), midsize (M50) and large male (M95) were considered in this study. Seatback recline angle was defined as the angle between the headrest post and vehicle side sill. Four different recline angles were considered: 0, 10, 20 and 30 deg. recline (Figure 1). The distance between the occupant and KB was adjusted by moving the entire KB assembly relative to the vehicle frame (Figure 1). This was done in order to isolate the effect of the KB's position without altering any other restraint components such as belt anchorage position, or the distance to the frontal airbag. Four KB positions were considered, three positions representing a distance to a KB when the seat is placed at forward-track (fIP, +120mm), mid-track (sIP, 0mm) and back-track (bIP, -120mm) position, and one position when the KB is removed from the vehicle (nIP, -450mm). Since midsize and large male did not fit into the seat with the forward KB position, these conditions were removed from the simulation matrix. Consequently, the DOE resulted in total of 40 FE simulations (Table 1).



**Figure 1. Simulation environment. Investigated seatback recline angles (0, 10, 20, 30 deg.) and knee bolster positions: fIP (+120 mm), sIP (0 mm), bIP (-120 mm), and nIP (-450 mm).**

**Table 1. Simulation matrix.**

	Parameters			
Occupant anthropometry (version)	F05-OS (2.0)	M50-OS (1.8.4.1)	M95-OS (1.2)	
Seat recline angle (deg)	0.9	10.9	20.9	30.9
Knee bolster position (position)	Forward (fIP)*	Standard (sIP)	Backward (bIP)	No knee bolster (nIP)
	(+120 mm)	(baseline)	(-120 mm)	(-450 mm)
TOTAL	40 simulations*			

All of the simulation in this study were performed using LS-Dyna (R9.1.0) explicit finite element (FE) solver and the high performance computational cluster (Intel Xeon E5-2670v2, 2.5 GHz, 20 core). In order to eliminate decomposition performance variability, all jobs were run using two computational nodes.

### Simulation setup

All occupant models were positioned in the vehicle seat following the methodology described in [7]. Additionally, care was taken to ensure that occupants' pelvis was positioned as close as possible to the seatback, thus avoiding unnecessary slouching that could lead to unfavorable belt placement and consequently submarining. The HBM and seat stress and strain data was carried through the positioning phase to the final simulations in order to achieve proper boundary conditions and contact initiation. The seat belts were fitted individually for each occupant size and each seat recline angle.

Additionally, throughout the setup process and during initial shakedown simulations several modeling issues/discrepancies were discovered in the utilized HBMs. First, M50 and M95 had several redundant single surface contact definitions, which impacted the overall stability of these models, and forced premature error termination. Second, it was discovered that male models had inverted polarities of the zero length discrete beam definitions in the lumbar spine, affecting the kinematic response as well as polarity of the obtained signal. Third, male models had a misaligned coordinate systems used for measuring forces in the occupant's femurs. Fourth, small female model carried additional attachment between pelvic flesh and pelvis which made it different from the male models. All discovered issues were addressed and the models were modified to unify the modeling approach.

### Post-processing

A custom automated post-processing code was developed to analyze the results from all of the performed simulations. The occurrence of submarining was assessed through visual assessment of simulation results. The submarining was identified if the belt passed either of left, right or both iliac wings and moved above the anterior superior iliac spine (ASIS) into the abdomen.

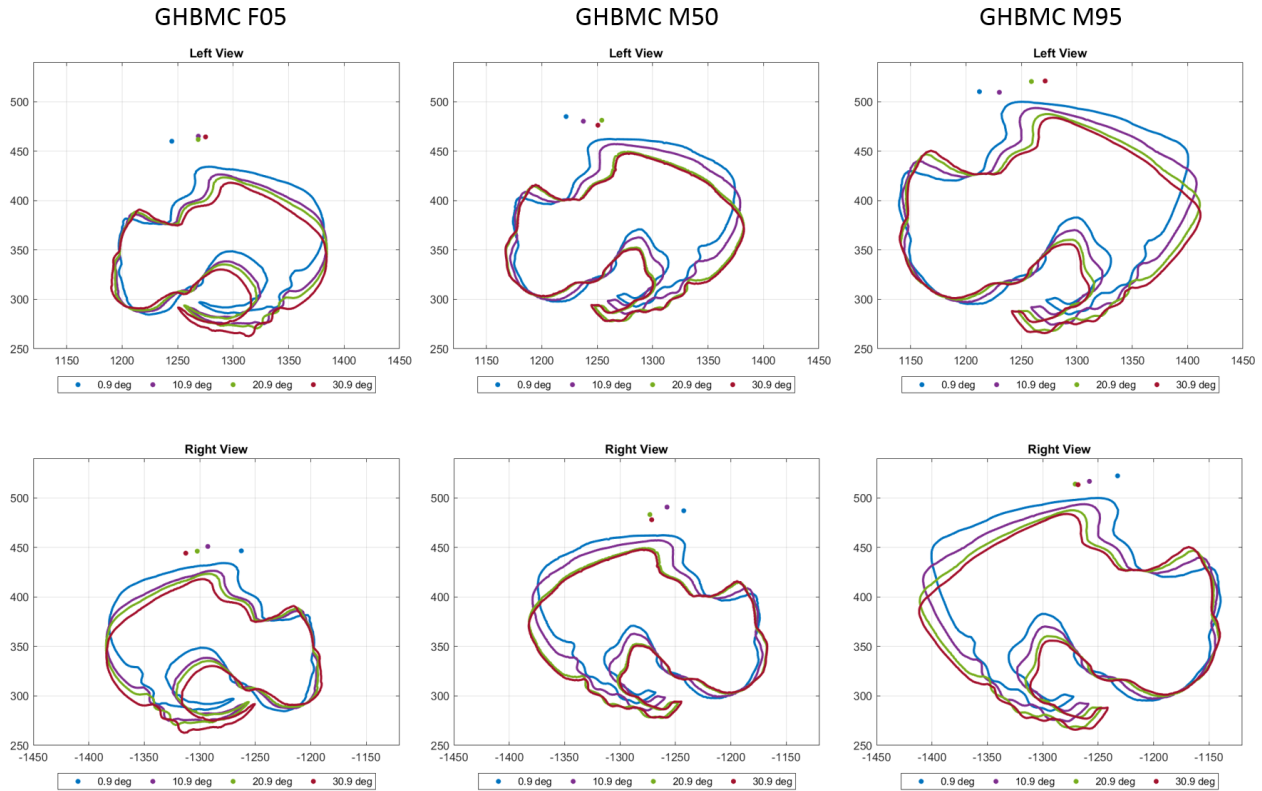
### RESULTS

A total of 40 simulations were performed in this study. Since some of the simulations did not proceed through a maximum of 150 ms, and terminated in error, the termination times were evaluated to identify trends with respect to simulation parameters (Table 2). The completion rate declined with the increase of the seatback angle. Forward and standard KB positions had the highest completion rate followed by the back and no KB condition. The M50 model had the highest percentage of normal terminations, followed by the M95 and F05 models.

**Table 2. Termination times (out of 150 msec.) for all investigated cases.**

HBM	IP Position	Recline Angle				Completion rate (IP)	Completion rate (HBM)
		0	10	20	30		
F05	fIP	150	150	82	90	50%	44%
	sIP	150	150	74	90	50%	
	bIP	150	150	110	78	50%	
	nIP	102	150	118	82	25%	
M50	fIP	N/A	N/A	N/A	N/A		67%
	sIP	150	150	150	84	75%	
	bIP	110	150	150	150	75%	
	nIP	150	150	70	74	50%	
M95	fIP	N/A	N/A	N/A	N/A		50%
	sIP	150	150	150	150	100%	
	bIP	150	88	88	96	25%	
	nIP	150	80	82	86	25%	
<b>Completion rate (Rec.)</b>		80%	80%	30%	20%		

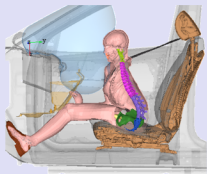
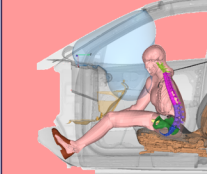
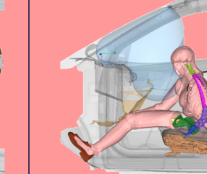
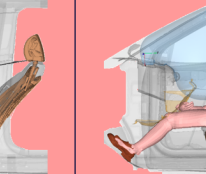
For all occupants, increased occupant recline angle lead to increased posterior tilt of the pelvis. Additionally, with increased angle of recline, the lap belt moved vertically up and away from the ASIS (Figure 2).



**Figure 2. Lateral view of the pelvis with respect to the recline angle along with the top edge of the lap belt relative to the ASIS, shown for all three HBM models.**

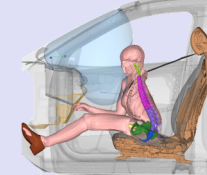
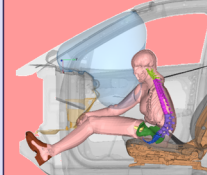
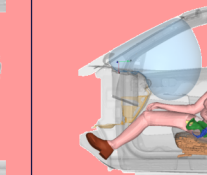
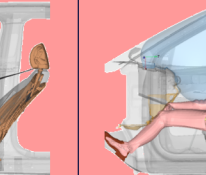
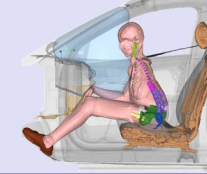
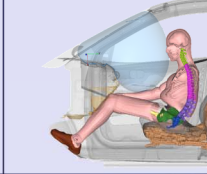
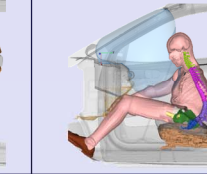
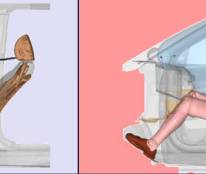
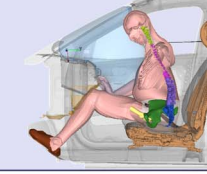
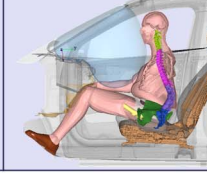
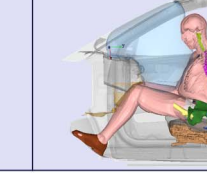
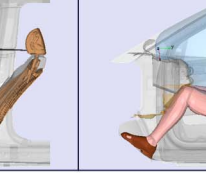
The occurrence of submarining was evaluated across all 40 of the simulations (Table 3, Table 4, Table 5, and Table 6). In general, submarining was observed more frequently at higher recline angles. The small female model submarined in the most cases, followed by the mid-size, which submarined in fewer cases, and then the large male, which submarined in the fewest cases. The KB distance also played a role in limiting the occurrence of submarining. In several cases where the submarining was observed in the back KB position it was effectively eliminated by moving the KB into the standard position (Table 4 and Table 5).

**Table 3. Submarining outcome for the fIP knee bolster position. Cases highlighted with a red/pink background were cases where at least partial submarining occurred.**

	0.9 deg	10.9 deg	20.9 deg	30.9 deg
F05				
M50	N/A	N/A	N/A	N/A
M95	N/A	N/A	N/A	N/A

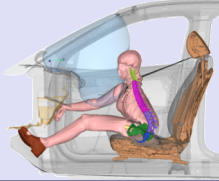
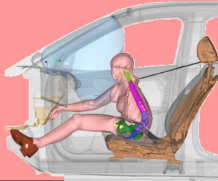
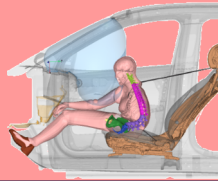
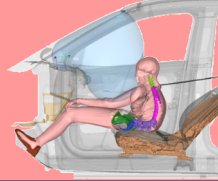
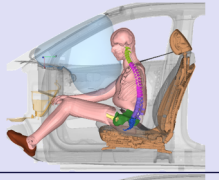
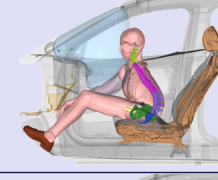

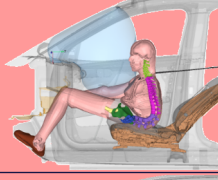
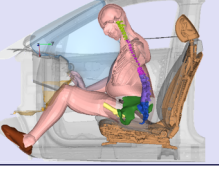
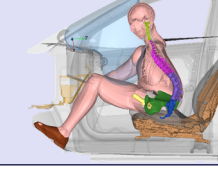
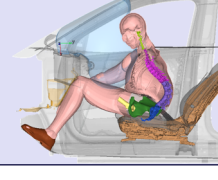
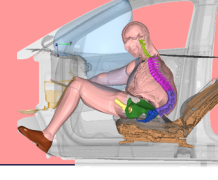
 No Submarining       Submarining

**Table 4. Submarining outcome for the sIP knee bolster position. Cases highlighted with a red/pink background were cases where at least partial submarining occurred.**

	0.9 deg	10.9 deg	20.9 deg	30.9 deg
F05				
M50				
M95				

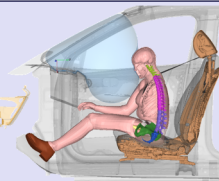
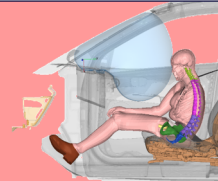
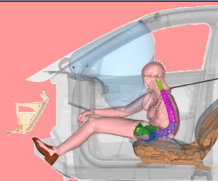
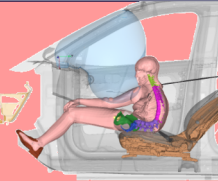
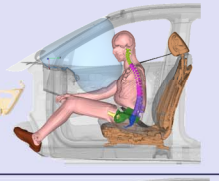
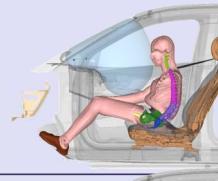

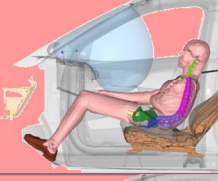
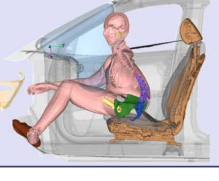

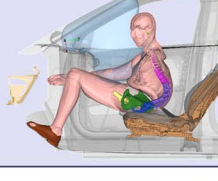

 No Submarining       Submarining

**Table 5. Submarining outcome for the bIP knee bolster position. Cases highlighted with a red/pink background were cases where at least partial submarining occurred.**

	0.9 deg	10.9 deg	20.9 deg	30.9 deg
F05				
M50				
M95				

No Submarining
  Submarining

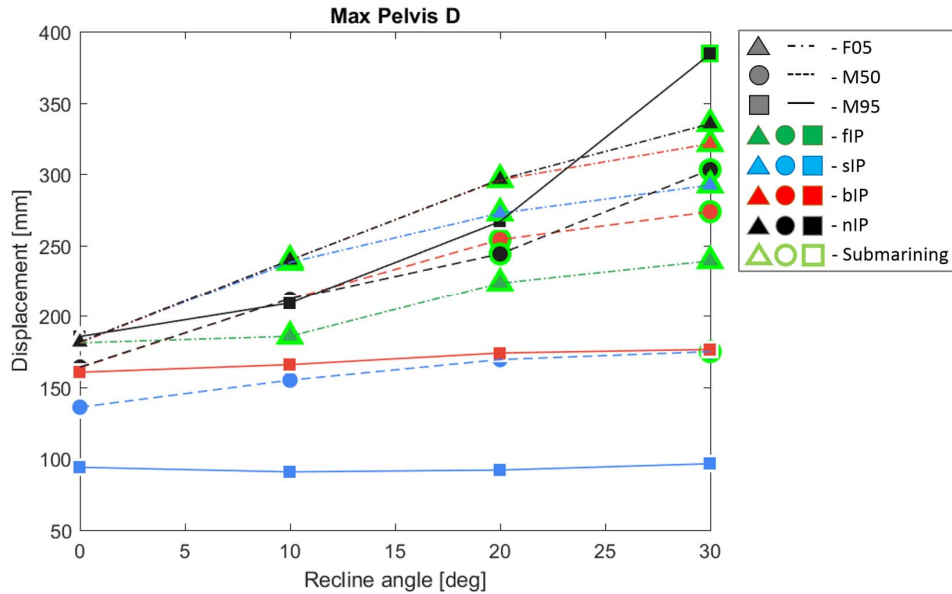
**Table 6. Submarining outcome for the nIP knee bolster position.**

	0.9 deg	10.9 deg	20.9 deg	30.9 deg
F05				
M50				
M95				

No Submarining
  Submarining

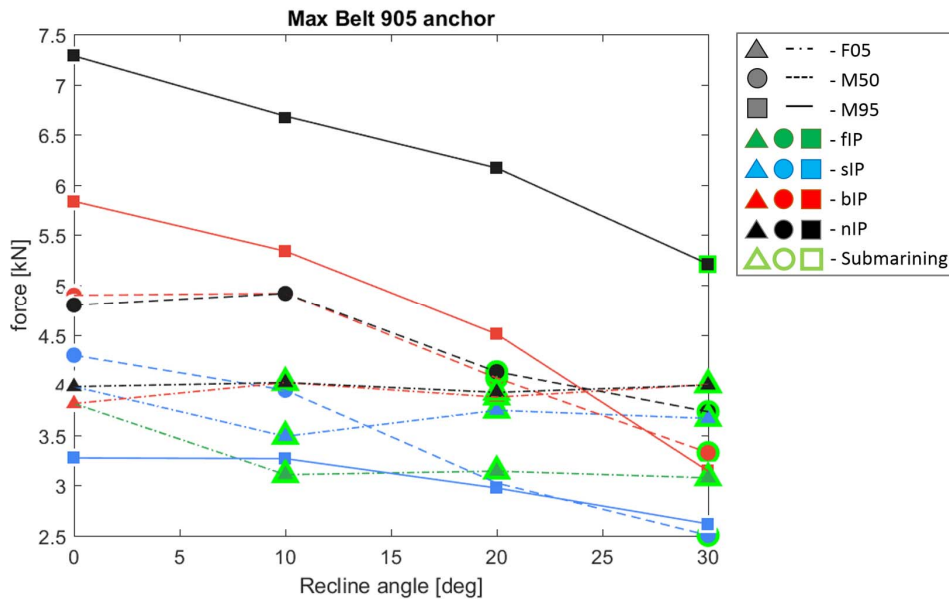
In all cases, pelvis excursion increased with an increase of seatback recline angle and the increase of distance between the occupant and KB. In comparable cases with the KB present (fIP, sIP or bIP) larger occupant experienced smaller forward pelvis excursion (Figure 3).





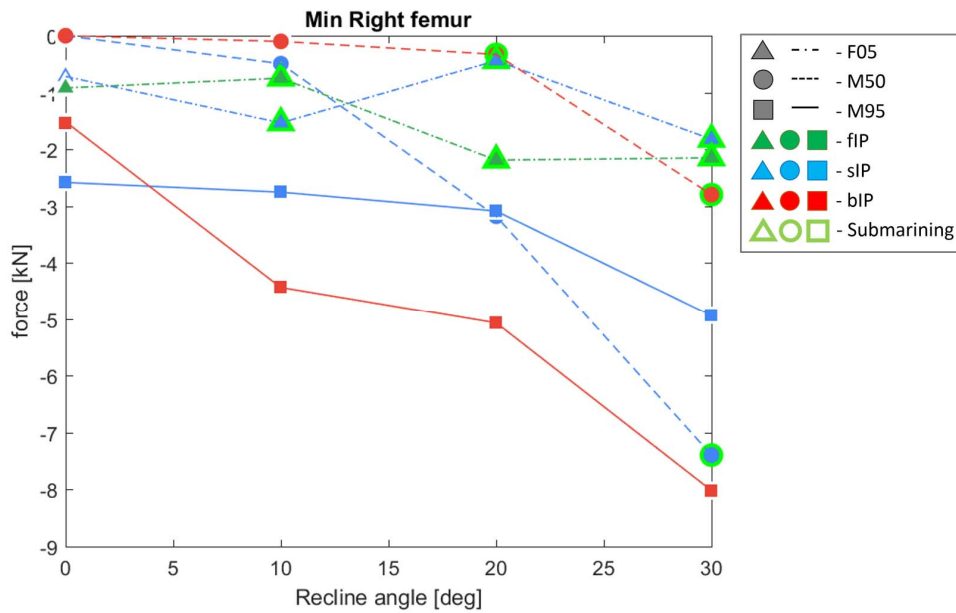
**Figure 3. Maximum forward pelvis motion relative to the vehicle across all anthropometries, knee bolster positions, and recline angles.**

As expected, the maximum lap belt force (measured at the anchor) increased with the increased size of the occupant. An increase in the lap belt force was observed with the increase distance between the occupant knees and KB. Interestingly the maximum lap belt force showed general decrease with the increased level of seatback recline (Figure 4).



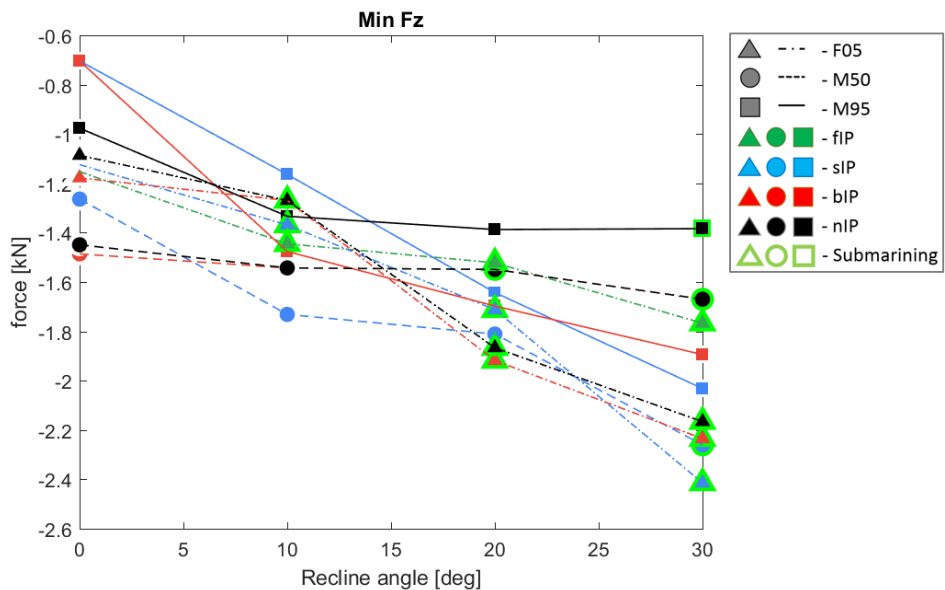
**Figure 4. Maximum recorded lap belt force measured at the outboard anchor across all anthropometries, knee bolster positions, and recline angles.**

The maximum femur compression force, used as a surrogate for knee to KB contact, showed an increase with the increase of the seatback recline angle. Only F05, siP, 20 deg. and 30 deg. recline cases showed the opposite trend, however upon in depth review it was discovered that these simulation terminated prematurely, before the maximum femur force was recorded (Table 2). Interestingly the maximum femur compression force didn't show consistent trend with the size of the simulated occupant (Figure 5).

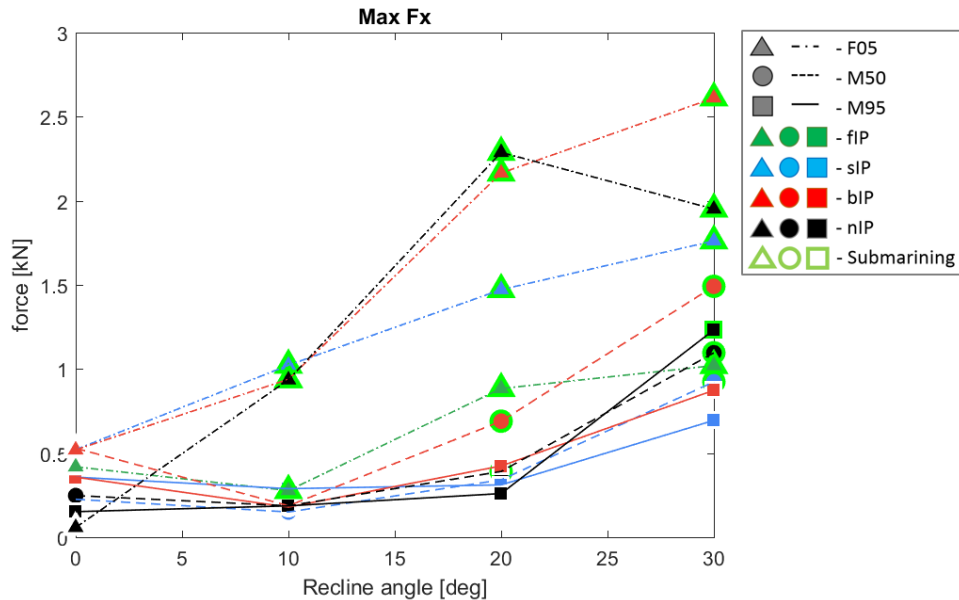


**Figure 5. Maximum femur compression force across the cases where knee to knee bolster contact was present. No IP cases (nIP) for all anthropometries, and back IP (bIP) for F05 didn't have knee bolster contact and were removed for brevity.**

The maximum lumbar spine forces were obtained by finding a maximum force across all vertebral levels in the lumbar spine. The maximum compression and anterior posterior (AP) shear force in lumbar spine increased with the increase of the recline angle (Figure 6 and Figure 7). Additionally, cases where submarining was observed, showed a substantial increase in a maximum lumbar spine shear force (Figure 7).



**Figure 6. Maximum compression force in the lumbar spine measured for all lumbar vertebral levels (T12-S1), across all anthropometries, knee bolster positions, and recline angles.**



**Figure 7. Maximum anterior-posterior shear force in the lumbar spine measured for all lumbar vertebral levels (T12-S1), across all anthropometries, knee bolster positions, and recline angles.**

## DISCUSSION

This study provides an overview of occupant responses in the environment relevant to the future of personal transportation. The initial results indicate that current state-of-the-art restraint systems will require additional research and development to offer an adequate level of occupant protection in the future ADS environment. Additionally, the results of this study show that current numerical tools need additional development, for evaluating occupant safety in nontraditional seating postures. Several modeling errors, which influenced either the stability or the actual response of the model were discovered. These modeling discrepancies have been addressed, and the modified models were used for this study.

The results show that these models perform best in the conditions that cover their development and validation regime, which is based on the current vehicle environment (upright occupant with KB). All models were also more stable in simulations with more upright occupants, and where traditional knee support was present. This is not surprising given that they were developed to be used in such environment [8]. However when used outside the development regime their stability decreases.

The occurrence of submarining was highly related to the setback recline angle and pelvis posterior rotation. All occupants were more likely to submarine with the increase of seatback recline, however each occupant had a different submarining threshold. The smallest occupants were most likely to submarine. When submarining was observed for larger occupants it was at higher seatback recline angles. All non-upright F05 simulations resulted in the model submarining under the lap belt, even in cases when the occupant was in contact with KB. This suggests that the occupant size, and consequently pelvis size and pelvis orientation may play a role in influencing occupant propensity to submarine (Figure 2). This also suggests that the current state-of-the-art restraint systems will be especially challenged by small occupants in recline configurations.

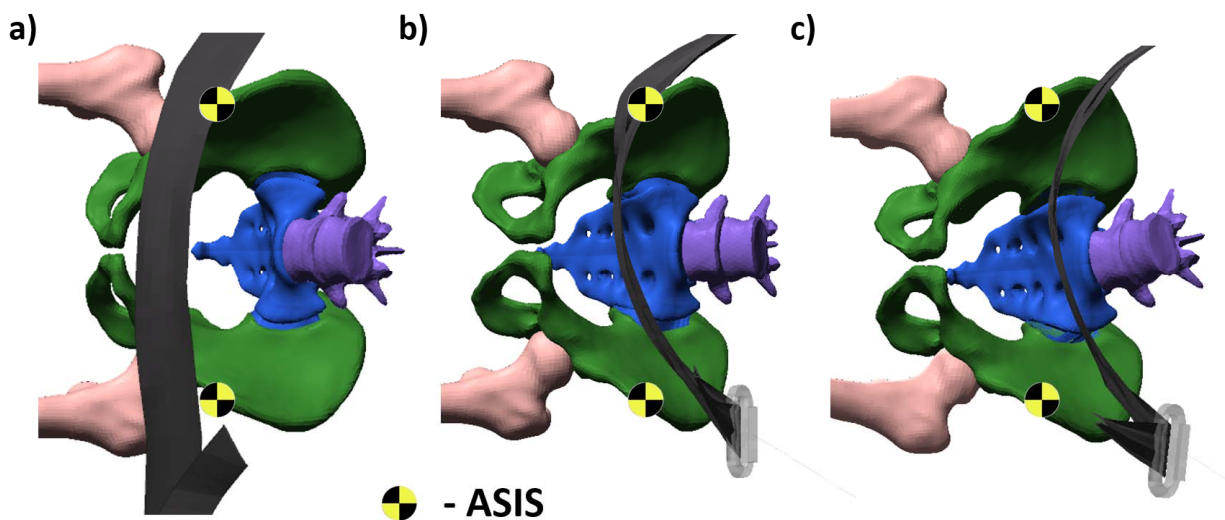
The KB was an effective measure controlling occupant's pelvis motion. The shorter the distance to the KB, the fewer submarining cases were identified. In cases where the occupant interacted with the KB (Figure 5), its pelvis forward motion was limited. Consequently, the pelvis forward excursion remained constant, or increased only slightly for the cases with increased seatback recline angle (Figure 3, F05:fIP, M50:sIP, M95:sIP, bIP). The cases with limited or no KB engagement showed substantial increase in pelvis forward

excursion and increased submarining occurrence with increase of the seatback recline angle (Figure 3, Table 4 and Table 5). This suggests that the KB could be an effective countermeasure for controlling occupant kinematics, and reducing submarining likelihood for reclined occupants in the ADS environments.

The results indicate that reclined positions may lead to the increase in lumbar spine compressive loads (Figure 6). The increase of seatback recline angle aligns the occupant's lumbar spine with the direction of the acceleration pulse, resulting in increased lumbar compressive load from upper body inertia. Establishing lumbar spine biofidelity targets and injury tolerance should be at the center of future research. Especially, given limited development, biofidelity and validation data available for GHBMC's lumbar spine model, which is shared between simplified and detailed models [8, 9]. In author's understanding, the stiffness functions in the current model were calibrated to match a set of whole body PMHS sled tests [10, 11] without using data from component tests. Few studies attempted to address this issue by using available tests data. However, these studies used either data from unidirectional tests on functional spinal units without ligamentous structure [12], or whole spine experiments that had unrealistic boundary conditions and failed to apply and maintain follower load [13, 14].

The maximum lap belt force was dependent on occupant size and KB position (Figure 4). Naturally, larger occupants subject the belt system to higher restraint forces. Additionally, the contact with the KB creates an alternative load path through occupant femurs, further offloading the belt system (Figure 5). Interestingly, the lap belt forces obtained for both male HBMs showed a force reduction with an increase of initial recline angle. This was a consequence of the substantial belt transfer from the shoulder to the lap belt. The increase of seatback recline angle resulted in the increased flexion in the lumbar spine and reduction in seated height during torso forward motion (Table 6, M95:30:nip). The shortened distance between the occupant's shoulder and the buckle facilitated shoulder-lap belt transfer, and reduced the restraint of the pelvis allowing further forward excursion. This effect could be eliminated with the belt locking tongue, however an increase in lumbar spine forces (Figure 6) suggests that aggressive pelvic restraint may lead to increased lumbar spine injuries.

Lumbar spine AP shear force was a good predictor for submarining (Figure 7). In the model, when the belt slips off the ASIS it penetrates the abdomen and load is transferred directly to the lumbar spine. Out of all cases where submarining was observed, only two (F05:10:fIP, M50:20:nIP) did not show a substantial increase in the lumbar shear force. In both of these cases, the lap belt only slipped off one side of the pelvis, but remained hooked on the other (Figure 8), stopping the belt from engaging the lumbar spine. Interestingly, in all cases the buckle side, which was not pre-tensioned, was more prone to disengaging first. This indicates that pre-tensioning on both sides of the lap belt might be an effective countermeasure to ensure lap belt-pelvis engagement.



**Figure 8. Comparison of different submarining mechanisms. Superior view, a) initial belt placement, b) unilateral submarining, c) bilateral submarining.**

## **CONCLUSIONS**

This study provides an overview of occupant responses in non-traditional vehicle environment relevant to the future automated vehicles. It focused on evaluating the occupant response with respect to anthropometry, recline angle and distance to the KB. The results lead to the following conclusions:

1. Current numerical tools need additional development, for evaluating occupant safety in nontraditional seating postures.
2. Reclined postures pose a challenge for the current state-of-the-art restraint systems.
3. Increased recline angles lead to more submarining cases.
4. Smaller occupants may be more prone to submarining.
5. The knee bolster could be an effective countermeasure for controlling occupant kinematics and preventing submarining.
6. Higher recline angle results in a high compression force in the lumbar spine
7. Submarining results in large shear force recorded in the lumbar spine.

## **ACKNOWLEDGEMENT**

This study was supported by Hyundai-Kia America Technical Center Inc. (HATCI). Views or opinions expressed or implied are those of the authors and are not necessarily representative of the views or opinions of HATCI.

## REFERENCES

- [1]. SAE On-Road Automated Vehicle Standards Committee, (2014) Taxonomy and definitions for terms related to on-road motor vehicle automated driving systems. SAE International.
- [2]. U.S. Department of Transportation, 2017. Automated Driving Systems 2.0 - A Vision for Safety. Available at: [https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0\\_090617\\_v9a\\_tag.pdf](https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf) Accessed February 21, 2019.
- [3]. U.S. Department of Transportation, 2017. Automated Driving Systems 3.0 - Preparing for the Future of Transportation. Available at: <https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf> Accessed February 21, 2019.
- [4]. Forman, J., Lin, H., Gepner, B., Wu, T., Panzer, M. (2018) Occupant safety in automated vehicles: effect of seatback recline on occupant restraint. Japan Society of Automotive Engineers.
- [5]. Ji, P., Huang, Y., & Zhou, Q. (2017). Mechanisms of using knee bolster to control kinematical motion of occupant in reclined posture for lowering injury risk. *International journal of crashworthiness*, 22(4), 415-424.
- [6]. Kitagawa, Y., Hayashi, S., Yamada, K., & Gotoh, M. (2017). Occupant Kinematics in Simulated Autonomous Driving Vehicle Collisions: Influence of Seating Position, Direction and Angle (No. 2017-22-0005). SAE Technical Paper.
- [7]. Lin, H., Gepner, B., Wu, T., Forman, J., (2017) Effect of Seatback Recline on Occupant Model Response in Frontal Crashes. 2017. Available at: <http://www.ircofi.org/wordpress/downloads/irc18/pdf-files/64.pdf>. Accessed February 21, 2019.
- [8]. Gayzik, F.S., Moreno, D.P., Vavalle, N.A., Rhyne, A.C. and Stitzel, J.D., 2011. Development of the Global Human Body Models Consortium mid-sized male full body model. In *International Workshop on Human Subjects for Biomechanical Research* (Vol. 39). National Highway Traffic Safety Administration.
- [9]. Schwartz, D., Guleyupoglu, B., Koya, B., Stitzel, J.D. and Gayzik, F.S., 2015. Development of a computationally efficient full human body finite element model. *Traffic injury prevention*, 16(sup1), pp.S49-S56.
- [10]. Global Human Body Models Consortium, 2016, User Manual: M50 Detailed Occupant Version 4.5 for LS-DYNA. Document Revision 5.1
- [11]. Luet, C., Trosseille, X., Drazétić, P., Potier, P. and Vallancien, G., 2012. *Kinematics and Dynamics of the Pelvis in the Process of Submarining using PMHS Sled Tests* (No. 2012-22-0011). SAE Technical Paper.
- [12]. Arun, M.W., Hadagali, P., Driesslein, K., Curry, W., Yoganandan, N. and Pintar, F.A., 2017. *Biomechanics of lumbar motion-segments in dynamic compression* (No. 2017-22-0001). SAE Technical Paper.
- [13]. Zheng, J., Tang, L. and Hu, J., 2018. A numerical investigation of risk factors affecting lumbar spine injuries using a detailed lumbar model. *Applied bionics and biomechanics*, 2018.
- [14]. Katagiri, M., Zhao, J., Kerrigan, J., Kent, R. and Forman, J., 2016. Comparison of whole-body kinematic behaviour of the GHBM occupant model to PMHS in far-side sled tests. In *Proceedings of IRCOBI Conference* (pp. 679-693).

APPENDIX

Table A1: Data extracted from the simulations.

ID	Occupant	Recline Angle	IP location	Submarine (Yes = 1, No =0)	Max. Pelvis X Excursion [mm]	Max belt force (anchor) [kN]	Max femur comp. force [kN]	Max lumbar comp. force [kN]	Max lumbar AP shear force [kN]
1	M50	0	sIP	0	136	4.30	0.00	-1.26	0.23
2	M50	10	sIP	0	155	3.95	-0.49	-1.73	0.15
3	M50	20	sIP	0	169	3.02	-3.18	-1.81	0.34
4	M50	30	sIP	1	175	2.50	-7.40	-2.26	0.92
5	M50	0	bIP	0	164	4.90	0.00	-1.49	0.53
6	M50	10	bIP	0	212	4.92	-0.10	-1.54	0.19
7	M50	20	bIP	1	254	4.07	-0.33	-1.55	0.69
8	M50	30	bIP	1	274	3.33	-2.80	-1.67	1.49
9	M50	0	nIP	0	164	4.80	-	-1.45	0.25
10	M50	10	nIP	0	212	4.92	-	-1.54	0.19
11	M50	20	nIP	1	244	4.13	-	-1.55	0.39
12	M50	30	nIP	1	303	3.73	-	-1.67	1.10
13	M95	0	sIP	0	94	3.27	-2.58	-0.70	0.36
14	M95	10	sIP	0	91	3.27	-2.75	-1.16	0.29
15	M95	20	sIP	0	92	2.97	-3.09	-1.64	0.31
16	M95	30	sIP	0	96	2.62	-4.93	-2.03	0.69
17	M95	0	bIP	0	160	5.84	-1.51	-0.70	0.36
18	M95	10	bIP	0	166	5.34	-4.44	-1.48	0.18
19	M95	20	bIP	0	174	4.51	-5.07	-1.70	0.42
20	M95	30	bIP	0	176	3.14	-8.02	-1.89	0.87
21	M95	0	nIP	0	185	7.29	-	-0.98	0.15
22	M95	10	nIP	0	209	6.69	-	-1.33	0.19
23	M95	20	nIP	0	267	6.17	-	-1.39	0.26
24	M95	30	nIP	1	384	5.21	-	-1.38	1.23
25	F05	0	sIP	0	182	3.98	-0.72	-1.12	0.52
26	F05	10	sIP	1	238	3.49	-1.53	-1.37	1.02
27	F05	20	sIP	1	273	3.75	-0.44	-1.71	1.47
28	F05	30	sIP	1	292	3.67	-1.82	-2.41	1.76
29	F05	0	flP	0	181	3.81	-0.92	-1.15	0.42
30	F05	10	flP	1	186	3.11	-0.75	-1.45	0.28
31	F05	20	flP	1	223	3.14	-2.19	-1.52	0.88
32	F05	30	flP	1	239	3.08	-2.15	-1.77	1.02
33	F05	0	bIP	0	181	3.81	-	-1.18	0.52
34	F05	10	bIP	1	240	4.02	-	-1.27	0.94
35	F05	20	bIP	1	296	3.88	-	-1.92	2.17
36	F05	30	bIP	1	321	4.00	-	-2.23	2.61
37	F05	0	nIP	0	182	3.98	-	-1.09	0.06
38	F05	10	nIP	1	240	4.02	-	-1.27	0.94
39	F05	20	nIP	1	296	3.93	-	-1.87	2.29
40	F05	30	nIP	1	335	4.00	-	-2.17	1.95

# DEVELOPMENT AND APPLICATION OF AN EXPERT ASSESSMENT METHOD FOR EVALUATING THE USABILITY OF SAE LEVEL 3 ADS HMIS

**Naujoks, Frederik**  
**Hergeth, Sebastian**  
**Keinath, Andreas**  
BMW Group  
Germany

**Wiedemann, Katharina**  
**Schömig, Nadja**  
Wuerzburg Institute for Traffic Sciences (WIVW)  
Germany

Paper Number 19-0026

## ABSTRACT

With the Federal Automated Vehicles Policy, the U.S. National Highway Traffic Safety Administration (NHTSA) has provided an outline that can be used to guide the development and validation of Automated Driving Systems (ADS). Acknowledging that the Human-Machine-Interface (HMI) – identified as one of the 12 priority safety design elements in this voluntary guidance – will be crucial for the success of ADSs, we developed a two-step iterative test procedure that serves to evaluate the conformity of SAE level 3 ADS HMIs with the requirements outlined in NHTSA's Automated Vehicles policy. The aim of this assessment is to evaluate whether minimum HMI requirements are met that facilitate a safe and efficient use of AVs. The present contribution describes the development of an expert-based checklist, how it was compiled from existing literature, how its content and application were refined in simulator and real-world studies, and how it can be employed as a complimentary or stand-alone tool to assess the conformity of SAE Level 3 ADS HMIs with NHTSA's AV policy. It also discusses boundary conditions for the application of the method and the generalization of findings. The described method can be employed in a variety of settings to evaluate SAE Level 3 ADS HMIs, therefore making it a valuable tool for both researchers and practitioners alike.

## INTRODUCTION

Conditionally automated driving (SAE L3; [1]) will change how vehicles are used. Depending on the Operational Design Domain (ODD), user of ADS may no longer be required to monitor the driving situation continuously when the system is engaged in automated mode. However, the driver still needs to take back control over the vehicle as soon as a Request to intervene (RtI, also called take-over request) is issued. Therefore, the Human-Machine Interface is of crucial importance to enable a safe and efficient use of the ADS. The ADS has to inform the user through HMI indicators about the current system mode and support the user's awareness about their responsibilities corresponding with the respective mode. Therefore, the NHTSA has proposed that an AV HMI at minimum shall inform the user that the system is (NHTSA, [2]):

- (1) Functioning properly
- (2) Engaged in automated driving mode
- (3) Currently 'unavailable' for use
- (4) Experiencing a malfunction and/or
- (5) Requesting a control transition from ADS to the operator

A suitable design of mode indicators should effectively support the driver in using an ADS and prevent a false understanding of the current driving mode. This is especially important when considering that a given vehicle may be equipped with different driver assistance systems as well that may be confused with ADSs. As this may produce undesired consequences, there is an urgent need to establish test and evaluation methods that can be applied during product development to ensure that these basic HMI requirements are met.

We developed a heuristic evaluation method that can be used by Human Factor and Usability experts to evaluate and document whether an HMI [3] meets the above-mentioned minimum requirements. In Usability Engineering, such heuristic assessment methods are commonly applied during the product development cycle [4] and can be used as a quick and efficient tool to identify and correct potential usability issues associated with the HMI. The heuristic assessment method consists of a set of AV HMI guidelines together with a checklist that can be used as a systematic HMI inspection and a problem reporting sheet. This paper describes the background and application of the checklist.



## METHOD DESCRIPTION

### Evaluators

The method should be conducted by a pair of HMI experts. Experts should have received formal training in Human Factors and Usability Engineering and have demonstrable practical experience in HMI assessment and evaluation.

### Procedure

The HMI inspection is conducted in an on-road assessment of a production vehicle or a high-fidelity prototype. The aim of the assessment is to evaluate whether a set of pre-defined HMI principles (the “heuristics”) are met. Therefore, each of the two evaluators completes a set of fixed use-cases, observes the visual, auditory and haptic HMI output and records potential usability issues arising from non-compliance with the HMI heuristics that have been compiled into a checklist (see [3] for a detailed description of the checklist). The use-case set depends on the specific design of the ADS with respect to the available levels of automation (e.g., whether only manual or conditional automation are available, or if driver assistance is also available within the same vehicle). For an extensive assessment, the use-case set presented in Table 1 should be completed (for a detailed description, see [5]). The aim of the heuristic assessment is twofold:

- (1) For the minimum HMI requirements to be fulfilled, each of the use-cases presented in Table 1 should be reflected in a mode indicator or the change of a mode indicator that must be present in the in-vehicle HMI. The mode indicator can be presented visually, auditory and/or tactile.
- (2) The design of the respective mode indicator should be in accordance with common HMI standards and best practices that are the basis of the checklist (see Table 2; an extended version of the checklist with corresponding examples and background literature can be found in [3]).

### Reporting and documentation

Checklist compliance and identified usability issues should be initially documented independently by each of the raters. Each of the checklist items should be answered using the following rating categories:

- “*major concerns*”: non-compliance with guideline
- “*minor concerns*”: partial fulfillment of guideline, but some aspects of the HMI are non-compliant
- “*no concerns*”: compliance of all HMI aspects with guideline
- “*measurement necessary*”: no definite conclusion can be given on the basis of the checklist and empirical testing is needed; this may be the case when very innovative designs are used that are not covered by current standards and best practices.

Reasons for “major” and “minor” concerns should be documented. A problem reporting sheet can be found in [3]. After the individual assessment, the results should be discussed between the evaluators to come to a joint assessment that should also be documented. Figure 1 summarizes the rating procedure.

Table 1: Use-Case set (adapted from Naujoks et al., 2018). Note that some use cases might not be applicable if a vehicle is not equipped with a respective system.

Minimum HMI requirement	Use Case	Description
Functioning properly	L3	Steady driving in L3 mode
Engaged in AD mode	L3 → L2	Driver voluntarily switches from L3 to L2
	L2 → L3	Driver voluntarily switches from L2 to L3
	L2	Steady driving in L2
Currently unavailable for use	L3 <sub>unavailable</sub>	Driving outside the system’s ODD, L3 is not available; this use case applies to all lower levels of automation (i.e., L0, L1, L2)
Experiencing a malfunction	L3 <sub>degraded</sub>	Driving in or outside the ODD, L3 is not available because of a malfunction such as a sensor degradation; this applies to all lower levels of automation (i.e., L0, L1, L2)
Requesting a control transition from ADS to operator	L3 → L2	System initiated transition to L2
	L3 → L1	System initiated transition to L1 (either longitudinal or lateral assistance)
	L3 → L0	System initiated transition to L0

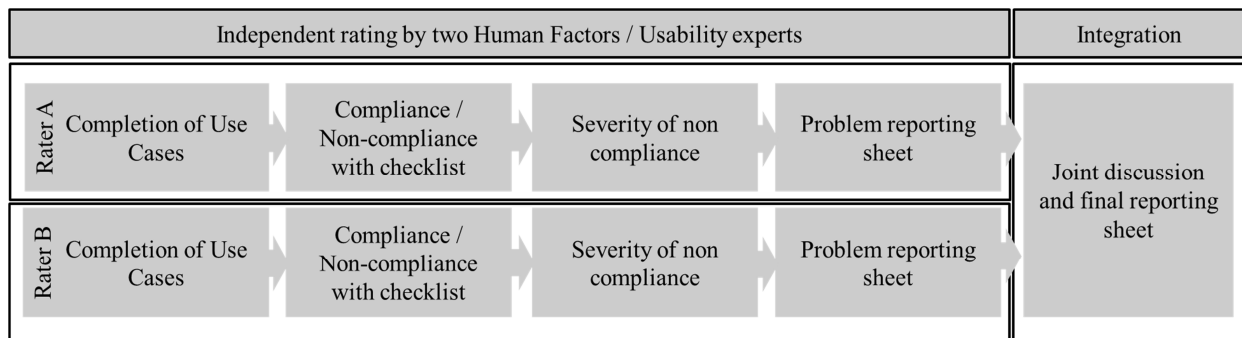


Figure 1: Rating procedure.

Table 2: Checklist items (adapted from [3]).

#	Item
1	Unintentional activation and deactivation should be prevented.
2	The system mode should be displayed continuously.
3	System state changes should be effectively communicated.
4	Visual interfaces used to communicate system states should be mounted to a suitable position and distance. High-priority information should be presented close to the driver's expected line of sight.
5	HMI elements should be grouped together according to their function to support the perception of mode indicators.
6	Time-critical interactions with the system should not afford continuous attention.
7	The visual interface should have a sufficient contrast in luminance and/or colour between foreground and background.
8	Texts (e.g., font types and size of characters) and symbols should be easily readable from the permitted seating position.
9	Commonly accepted or standardized symbols should be used to communicate the automation mode. Use of non-standard symbols should be supplemented by additional text explanations or vocal phrase/s.
10	The semantic of a message should be in accordance with its urgency.
11	Messages should be conveyed using the language of the users (e.g., national language, avoidance of technical language, use of common syntax).
12	Text messages should be as short as possible.
13	Not more than five colours should be consistently used to code system states (excluding white and black).
14	The colours used to communicate system states should be in accordance with common conventions and stereotypes.
15	Design for colour-blindness by redundant coding and avoidance of red/green and blue/yellow combinations.
16	Auditory output should raise the attention of the driver without startling her/him or causing pain.
17	Auditory and vibrotactile output should be adapted to the urgency of the message.
18	High-priority messages should be multimodal.
19	Warning messages should orient the user towards the source of danger.
20	In case of sensor failures, their consequences and required operator steps should be displayed.

## METHOD EVALUATION

The method has been evaluated and refined with various approaches. The use of expert assessments may be practical and efficient, but it also comes with limitations. Expert raters might differ in their assessment, resulting in an unreliable outcome of the assessment. Furthermore, the validity of the assessment depends on the capability of the checklist items to predict the usability issues that would arise from non-compliance with them. Therefore, a series of validation experiments were conducted by the authoring team.

### Study I: Inter-rater agreement [6]

The aim of the first evaluation study was to assess the *reliability* of the rating outcome in a realistic setting. Demonstrating inter-rater agreement is crucial to the generality of the findings generated from the heuristic assessment, as it is inherently influenced by the raters' subjective experiences and opinions. Therefore, it should be ensured that the ratings were not merely based on idiosyncratic judgements, but that different evaluators

would arrive at similar conclusions when using the method. Three teams of raters (i.e., six individual raters in total) conducted the heuristic assessment in an on-road setting. The employed checklist included two additional items<sup>1</sup>. As L3 systems are not yet available to consumers, a L2 system was used to validate the checklist instead. Each of the evaluators drove a section of a German motorway while switching between different automation levels (A70/A71 Schweinfurt/Bamberg; 2 lane-motorway with mainly unrestricted speed limit, including sections with partially missing lane markings and a tunnel). The heuristic evaluation including the final discussion took about six hours per rater pair. All evaluators were employees of the Wuerzburg Institute for Traffic Sciences (WIVW GmbH). They hold a university degree in Psychology or Computer Science and had several years of experience in Human Factors and Usability research.

Table 3: Use cases driven in the on-road evaluation study.  $L1_{Long}$  = ACC,  $L1_{Lat}$  = Steering Assistance. The use-cases were adapted to the available automation levels in the test vehicle.

Category	Use Case
Activation (driver initiated)	$L0 \rightarrow L1_{long} \rightarrow L2$ $L0 \rightarrow L1_{Lat} \rightarrow L2$ $L0 \rightarrow L2$
Deactivation/ transition to lower level (driver- or system initiated)	$L2 \rightarrow L1_{Long} \rightarrow L0$ $L2 \rightarrow L1_{Lat} \rightarrow L0$ $L2 \rightarrow L0$
Driving steady in a system state	$L0, L1_{long}, L1_{Lat}, L2$
Higher level not available (e.g., sensor failure)	$L0, L1_{long}, L1_{Lat}$
Re-activation of passive system state (system-initiated)	$L0 \rightarrow L1_{Lat}$ $L1_{long} \rightarrow L2$

During and after the test drives, the evaluators recorded their individual assessment before discussing with the other rater. After the team discussion, a final rating was given by every rating team. The main interest of the study was to assess the inter-rater agreement between the individual raters and rater pairs before and after the joint discussion of the rating outcome. Brennan & Prediger's Kappa  $\kappa$  was used to evaluate the reliability of the ratings ([7]; for more details on differences to Cohen's Kappa  $\kappa$ , see [8]).

Table 4: Inter-rater agreement with an evaluation of the quality of the rating according to [9]. Rater pairs were Rater 1/2, Rater 3/4 and Rater 5/6.

Brennan's $\kappa$		R1	R2	R3	R4	R5	R6
Pre	R1	-	0.29	0.36	0.08	0.14	0.13
	R2		-	0.55	0.37	0.48	0.42
	R3		"fair"* = $\kappa > 0.21$	-	0.21	0.37	0.48
	R4		"moderate" = $\kappa > 0.41$		-	0.45	0.12
	R5		"good" = $\kappa > 0.61$			-	0.48
	R6		"very good" = $\kappa > 0.81$				-
		R1	R2	R3	R4	R5	R6
Post	R1	-	0.79	0.48	0.48	0.40	0.40
	R2		-	0.40	0.40	0.48	0.48
	R3		"fair"	-	0.86	0.38	0.50
	R4		"moderate"		-	0.36	0.36
	R5		"good"			-	1
	R6		"very good"				-

As can be seen in Table 4, the inter-rater agreement was not sufficiently high on an individual level before the joint discussion. However, after the discussion among the rater pairs, agreement levels within each rater pair and between different rater pairs increased. This finding demonstrates that different rater pairs come to comparable

<sup>1</sup> The checklist used included two more items in addition to the initial item-set: "Instructions and information of the user manual facilitate the interaction with the HMI" (item #21) and "Interaction with the system is easy" (item #22). Note that these items do not directly pertain to the minimum HMI requirements as proposed by NHTSA.

conclusions using the heuristic evaluation approach, showing that it is a reliable tool to assess the HMI of AVs. However, the findings also highlight that the heuristic evaluation should always adhere to a four-eyes principle to ensure the quality of its outcome.

### Study II: Predictive validity [10]

The usefulness of the heuristic HMI assessment not only depends on the reliability of the method, but also on its ability to *predict* usability problems that arise when the heuristics are violated. To test the predictive validity of the heuristics, we constructed two HMIs that are either compliant or non-compliant (“high-compliance” and “low-compliance” HMI) with several checklist items and ran a simulator study with N = 57 participants in the BMW Group’s simulator facilities. A fixed-based driving simulator was used. A detailed description of the study is provided in [10].

The simulated ADS had four modes: (1) manual driving, L3 unavailable for use, (2) manual driving, L3 available for use, (3) L3 engaged, (4) system-initiated take-over request in L3 mode due to system limits. The mode indicators were presented in the instrument cluster. The high compliance HMI (see Figure 2, left) communicated information redundantly by means of pictograms and a textbox. Textual information was displayed in German language. During the approach of the system limits, the HMI announced system limitations through a take-over cascade in form of an announcement, a cautionary take-over request (“*cautionary TOR*”) and an imminent take-over request (“*imminent TOR*”). The request to intervene was shown by animated hands grasping a steering wheel in both HMI variants.

The low-compliance HMI differed from the high-compliance HMI in various aspects (see Figure 2 and Table 5) of non-compliant colour coding, symbol size and labelling. Use-cases included driver initiated activations and deactivations of L3 mode, steady driving in L3 mode and two take-over requests resulting in a transition from L3 to manual driving. The ADS under investigation did not contain L2 or L1 driving assistance. One drive lasted approximately 15 minutes. The study results support the predictive validity of the heuristics in several ways:

- *Perceived usability*: Participants rated the usability of the low-compliance HMI to be statistically significantly lower than the high compliance HMI on the System Usability Scale (SUS, [11]).
- *Observer usability ratings*: Trained observers rated the frequency and severity of usability problems during interactions with the ADS from video footage on a five-point scale ranging from “no problems” to “help from experimenter needed”. Observed usability problems were significantly higher with the low compliance HMI.
- *Take-over time*: Participants reacted significantly slower to RtIs in the low compliance condition compared with the high compliance condition.

### Study III: Predictive validity [12]

The predictive validity of the heuristics was further tested in another simulator study at the facilities of the WIVW GmbH. Again, two HMIs were designed that were either compliant or non-compliant with some of the checklist items (e.g., with regard to prominence of task responsibility in L2 assisted driving mode (item #2), color contrast coding (item #7 and item #14), readability of icons and text (item #8), additional explaining text (item #9), usage of understandable language (item #11), multimodality of urgent warnings/take-over requests (item #18) and button labeling consistent to functionality (“additional” item #22)). The HMI variant was varied as a between-subject factor. Twelve drivers completed a simulator drive either with the low- or high-compliant HMI. The participants experienced the HMI in a 30-minutes-driving course containing several use-cases, including driving in each available automation mode (L0 vs. L2 vs. L3), driver initiated-upwards and system-initiated downwards transitions between these levels. The results revealed that the classification of the HMI variants as low vs. highly compliant based on the heuristic evaluation was also reflected in participants’ behavior and subjective ratings of the system and the HMI. The results further support the predictive validity of the heuristics. Differences between the two HMI variants were observed in the following measures:

- *Take-over reaction times*: Participants of the low compliance condition reacted significantly slower to a RtI (hands-on times and take-over times)
- *Usability problems in activating either L2 or L3 system*: participants in the low-compliance condition required more frequent support by the experimenter to successfully activate/reactivate the L3 system
- *Number of handsoff-warnings*: the number of participants experiencing at least one hands-off warning during L2 driving was higher in the low compliance condition
- *Perceived understandability and difficulty in system usage*: Participants in the low-compliance condition reported worse system understanding and perceived it as more difficult to activate the L3 system, to react to a take-over requests in L3 and to react to a system-initiated transition from L3 to L2

- *Global evaluation of the HMI:* Global ratings of the acceptability of the HMI by participants into three categories (very good, acceptable or not acceptable) showed a higher percentage of non-acceptable ratings for the low compliant condition after experiencing the HMI in the driving scenarios.









Mode	High-compliance HMI	Low-compliance HMI
L3 ADS active		
Cautionary TOR		
Imminent TOR		
L3 ADS not available for use		

Figure 2: HMI for high-compliance (left) and low-compliance (right) during normal functioning (top) cautionary TOR (2nd row), imminent TOR (3rd row) and L3 ADS not available (bottom). Figure adapted from [10].

Table 5: Variations for low compliance HMI for the two components with respective criterion and reference to heuristics; adapted from [10].

Variation of low-compliance HMI	Guideline violation
Activation and deactivation through long-press (i.e., 0.8 seconds)	System state changes should be effectively communicated.
Pictograms are 60% of the original size	Texts (e.g., font types and size of characters) and symbols should be easily readable from the permitted seating position.
No text information except for L3 ADS availability	The system mode should be displayed continuously System state changes should be effectively communicated. Commonly accepted or standardized symbols should be used to communicate the automation mode. Use of non-standard symbols should be supplemented by additional text explanations or vocal phrase/s.
No color coding for cautionary and imminent TOR	System state changes should be effectively communicated. The visual interface should have a sufficient contrast in luminance and/or colour between foreground and background. The colours used to communicate system states should be in accordance with common conventions and stereotypes.
No blue color coding for active L3 ADS	System state changes should be effectively communicated. The visual interface should have a sufficient contrast in luminance and/or colour between foreground and background. The colours used to communicate system states should be in accordance with common conventions and stereotypes.

Mode	High-compliance HMI	Low-compliance HMI
L3, ADS active		
L2 assisted driving active		
L2 Handsoff-warning		
Take-over request in L3		

Figure 3: HMI for high compliance (left) and low compliance (right) in selected system modes. Figure adapted from [12].

## SUMMARY

This paper presented a heuristic method for the assessment of in-vehicle HMIs for automated vehicles. The aim of the heuristic assessment is to provide a quick but reliable and valid tool that can be used during the product development cycle. It was developed to include common standards and practices and apply them to the in-vehicle interface of AVs [3]. In a series of studies, the reliability and predictive validity of the heuristic assessment was investigated and demonstrated. In view of the minimum HMI requirements proposed in NHTSA's automated vehicle's policy, the method can be used to verify compliance on an analytical level.

It should be noted, however that the method should be applied with care and thought. A thorough application of the method requires (1) the selection and adequate training of HMI evaluators and (2) quality control by periodically checking the agreement between rater pairs as demonstrated in this paper. Otherwise, the outcome of the heuristic assessment might suffer from subjectivity of evaluations and resulting low reliability. It must also be emphasized that the heuristic assessment should be combined with empirical test methods such as simulator or test track studies involving potential users of AVs. The combination of expert evaluations and empirical user tests has a long and successful history in the general Human Factors and Usability context, but has not seen wide-spread application to the domain of AV HMIs in the scientific and technical literature so far.

## REFERENCES

- [1] Society of Automotive Engineers International J3016 (2018). Taxonomy and definitions for terms related to on-road motor vehicle automated driving systems. Warrendale, PA: SAE International.
- [2] National Highway Traffic Safety Administration (2016). Automated Driving Systems 2.0: A Vision for Safety. Washington, DC: NHTSA.
- [3] Naujoks, F., Wiedemann, K., Schömgig, 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.
- [4] Nielsen, J. (1994). Usability inspection methods. In Conference companion on Human factors in computing systems (pp. 413-414). ACM.

- [5] 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.
- [6] Wiedemann K., Schömig N., Naujoks F., Hergeth S., Neukum A. & Keinath, A (2018). Expert evaluation of automated driving HMI – does a checklist-based method work? Paper presented at: HFES Europe Chapter Annual Meeting. Berlin, Germany.
- [7] Brennan, R. L. & Prediger, D. J. (1981). Coefficient  $\lambda$ : Some Uses, Misuses, and Alternatives. Educational and Psychological Measurement, 41, pp. 687-699.
- [8] Umesh, U. N., Peterson, R.A., & Sauber M. H. (1989). Interjudge agreement and the maximum value of kappa. Educational and Psychological Measurement, 49, pp. 835-850.
- [9] Landis, J.R. & Koch, G.G. (1977). The measurement of observer agreement for categorical data. Biometrics, 33 (1), pp. 159-174.
- [10] Forster Y., Hergeth S., Naujoks F., Krems J.F. & Keinath A. (2019). Empirical Validation of a Checklist for Heuristic Evaluation of Automated Vehicle HMIs. In: International Conference on Applied Human Factors and Ergonomics. Cham: Springer.
- [11] Brooke, J. (1996). SUS-A quick and dirty usability scale. Usability evaluation in industry, 189(194), 4-7.
- [12] Schömig N., Wiedemann, K., Naujoks, F., Hergeth, S. & Keinath, A. (in preparation). The heuristic evaluation of HMI requirements for Automated Driving Systems – a validation study.

# EURO NCAP'S FIRST STEP TO ASSESS AUTOMATED DRIVING SYSTEMS

**Richard Schram**

European New Car Assessment Programme  
Belgium

on behalf of the Euro NCAP Working Group on Automated Driving

Paper Number 19-0292

## ABSTRACT

Technology is evolving quickly and more and more of the driving function is being handed to the vehicle. Given that a significant portion of road accidents are attributable to "driver error", the potential safety benefits of increased automation are clear, if the automation is at least as competent as the driver in complex traffic situations. It is therefore in Euro NCAP's interests to raise awareness of the technologies that exists and to promote their introduction in such a way that these safety benefits are realised.

Based on the Euro NCAP's existing active safety testing protocols, extended test scenarios were derived that cover the Operational Design Domain of currently available SAE Level 2 systems. These systems are designed for use on motorways where speeds up to 130 km/h are most typical on European roads. With the first round of evaluating Assisted Driving technologies, Euro NCAP is entering a whole new area of safety and safety assessments where public expectations are high yet understanding may be low. Euro NCAP is striving to promote automated driving technologies while at the same time raise awareness of their safety benefits and moreover their limitations.

## BACKGROUND

More than 70% of car drivers believe that it is already possible to purchase a car that can drive itself, according to a consumer survey commissioned by Euro NCAP, Global NCAP and Thatcham Research in 2018. The findings of the survey, which coincided with Euro NCAP's first assessment of automated driving technology, are in stark contrast to the current capabilities of such systems and highlight the significant confusion that exists amongst motoring consumers when it comes to the reality of automated or autonomous driving.

On the question: "Which of the following brands currently sell cars with technology that enables the car to drive itself, without the driver having to do anything?", 1107 respondents from Europe (France, Germany, Italy, Spain and UK), US and China believed that this type of technology is currently available, depending on the vehicle brand 10-40%. Only 11% of the respondents clearly stated that this is not offered in any of these brands. This underlines the need for better and more objective information for consumers on state of advanced driving technology.

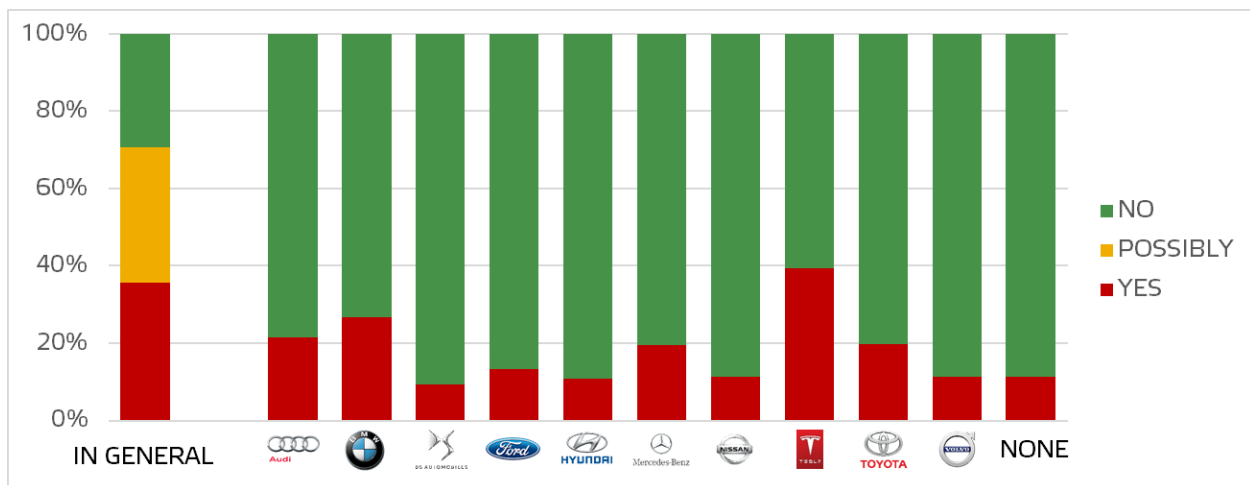


Figure 1. Survey results on the consumers perception on the availability of self-driving technology



As part of its ongoing commitment to independently assess the benefits of new vehicle safety technologies, Euro NCAP has tested the comparative performance of so-called Highway Assist systems in ten cars: the Audi A6, BMW 5 Series, DS 7 Crossback, Ford Focus, Hyundai NEXO, Mercedes-Benz C Class, Nissan LEAF, Tesla Model S, Toyota Corolla and the Volvo V60. The Highway Assist tested combine Adaptive Cruise Control, Lane Centering and Speed Assist Systems to support the driver in driving situations on motorways.

Dedicated test and assessment procedures were developed to grade different driver assistance systems that are currently available by a Working Group consisting of Euro NCAP members, labs and supported by car manufacturers and suppliers.

## LEVELS OF AUTOMATION

It is difficult enough for engineers to understand the different levels of automation as defined by Society of Automotive Engineers in SAE J3016 [1], let alone for the typical consumer. For that reason, it was decided to develop a simpler and easier to understand definition around the possible levels of Automation in a car.

### SAE J3016 Levels of Driving Automation

The latest update of the SAE J3016 Levels of Driving Automation already provide a clear distinction of driver support and automated driving, but Euro NCAP believes that further simplification is needed for the general public to understand the limitations and proper use of the systems they may have available on their vehicle.

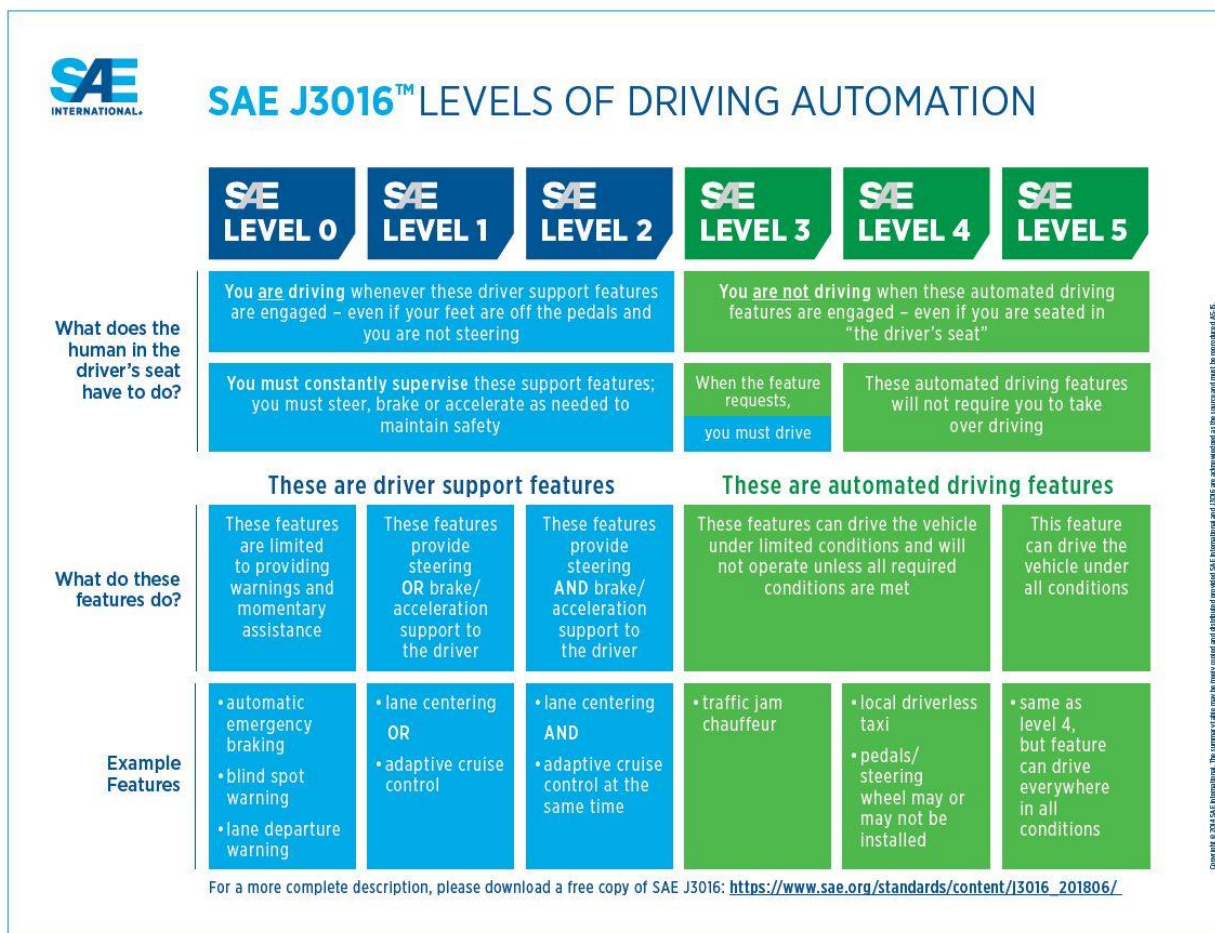


Figure 2. SAE J3016 Levels of Driving Automation

### Euro NCAP Driving Modes

The clear separation between driver support and automated driving which is now part of SAE J3016 is supported by Euro NCAP, but a clear understanding of the Operational Design Domain is still missing as this may be different per system and per OEM. Therefore, Euro NCAP decided to define the Levels of Automation as Driving Modes and combine this with defined Operational Domains.

Three Driving Modes exist for Euro NCAP; Assistance, Automation and Autonomous, where the difference between the Automated Driving Mode and the Autonomous Driving Mode is subtle.

**Table 1.**  
**Euro NCAP Driving Modes**

DRIVING MODE	
Assisted	<ol style="list-style-type: none"><li>1. Driver retains full responsibility and shares control with the Vehicle</li><li>2. Vehicle &amp; Driver share Object and Event Detection and Response [OEDR]</li><li>3. Driver may not perform secondary tasks over and above those permitted during normal driving</li></ol>
Automated	<ol style="list-style-type: none"><li>1. Vehicle has full responsibility for control in Operational Design Domain [ODD] defined by the OEM</li><li>2. Vehicle performs OEDR</li><li>3. Driver may perform certain other non-driving tasks</li><li>4. Driver needs to be available for safe transition of control</li></ol>
Autonomous	<ol style="list-style-type: none"><li>1. Vehicle has full responsibility for control in Operational Design Domain [ODD] defined by the OEM</li><li>2. Vehicle performs OEDR</li><li>3. Driver is effectively a passenger</li><li>4. Driver has no ability to control [apart from switching to another mode]</li></ol>

In the Assisted Driving Mode, the driver is fully responsible but shares control with the vehicle. The Object and Event Detection and Response (OEDR) is performed by the both vehicle and driver, where the driver is not allowed to perform any secondary task over and above those permitted during normal driving. In short this means that the driver is driving and the vehicle provides support where it can.

The Automated Driving Mode gives full responsibility to the vehicle and the vehicle will have full control. As the driver is allowed to perform certain other non-driving tasks, the vehicle has to perform the OEDR, but the driver needs to remain available for a safe transition of control.

Vehicles function which take away the ability of the driver to take control of the vehicle are called Autonomous Driving modes. In this mode pedals and steering wheels may be retracted, which effectively will change the driver to a passenger in this specific driving mode.

These driving modes are combined with Operational Domains that are understandable by a consumer and moreover give Euro NCAP a defined range of assessment of different systems that the car manufacturers may offer to their costumers. The Operational Domains considered are: Parking, City, Inter-Urban and Highway. Combining Driving Modes and Operational Domains result in a matrix of possible systems, e.g. Assisted Highway systems or Automated City systems.

**Table 2.**  
**Euro NCAP Automated Driving Matrix**











<b>AUTOMATED DRIVING</b>	<b>Parking</b>	<b>City</b>	<b>Inter-Urban</b>	<b>Highway</b>
Assisted				
Automated				
Autonomous				

The Euro NCAP Working Group on Automated Driving is detailing the test and assessment procedures for each cell in the matrix for Euro NCAP to be able to comparatively provide consumer information on the different driver assist or automated systems offered by the car manufacturers.

### **HIGHWAY ASSIST SYSTEMS**

A first set of evaluations of Highway Assist systems was published with the goal to highlight the current level of performance and limitations of Highway Assist systems in the area of longitudinal, lateral and speed control. Highway Assist systems are supposed to support the driver in monotonous driving situations on motorways and adapt to the traffic conditions. The first publications investigated three different aspects of these assist systems; Human-Machine-Interaction (HMI), Adaptive Cruise Control (ACC) and Lane Centering (LC). For both ACC and LC, the Euro NCAP Working Group developed test scenarios where the limitations of the systems would be highlighted.

**Table 3.**  
**Automated Driving test vehicles with their Highway Assist system names**

<b>AUTOMATED DRIVING</b>		
	Audi A6	Adaptive Cruise Assist
	BMW 5-series	Active Driving Assistant Plus
	DS 7 Crossback	Connected Pilot
	Ford Focus	Co-Pilot360 (ACC,LC & SAS)
	Hyundai Nexo	Smart Cruise Control with Lane Following Assist
	Mercedes-Benz C-Class	Active Distance Assist DISTRONIC with Active Steering Assist
	Nissan Leaf	ProPILOT
	Tesla Model S	Autopilot
	Toyota Corolla	Toyota Safety Sense (ACC & LTA)
	Volvo V60	Pilot Assist

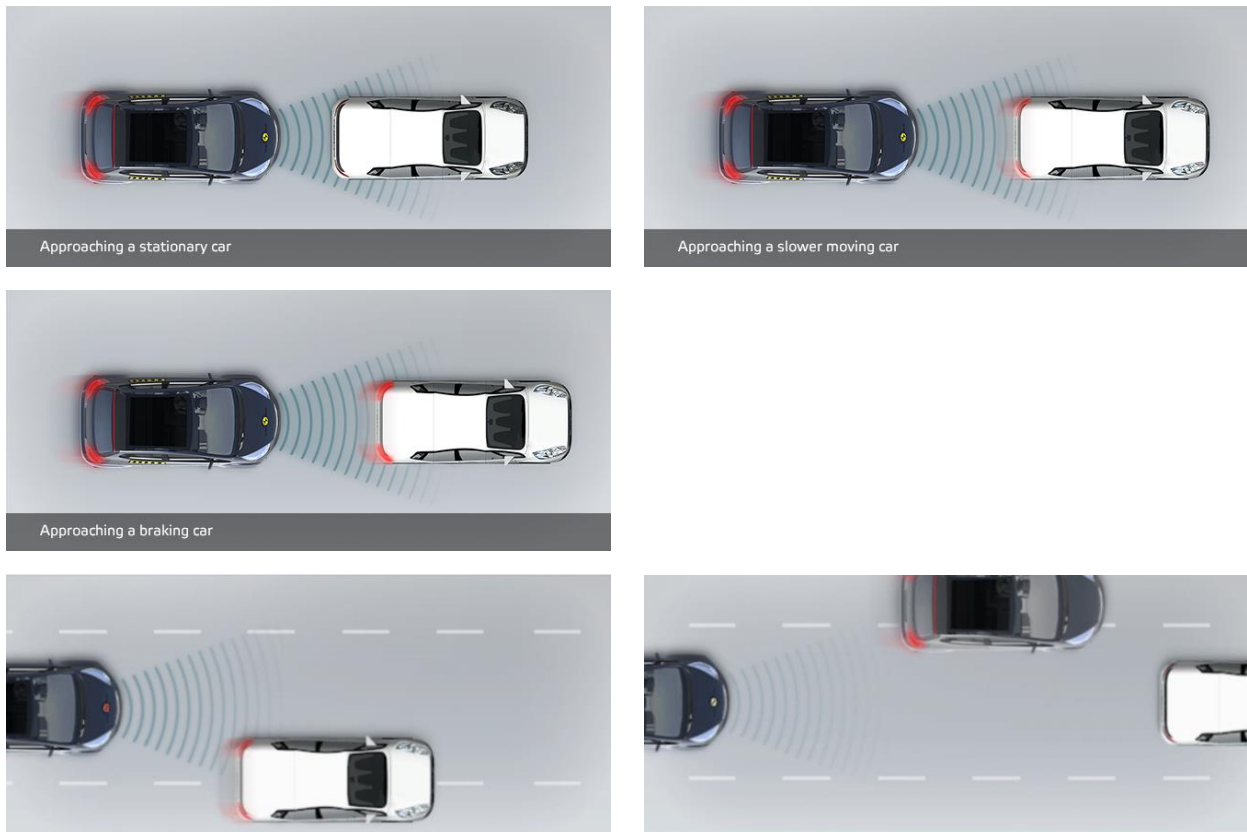
### Human-Machine-Interaction

In addition to physical testing, Euro NCAP reviewed the system names, official media from the car manufacturers as well as the vehicle handbooks to verify how the consumers are informed about these Highway Assist systems in the areas of marketing and technical details. For information purposes, additional features available in the different systems were published but not verified, like automatic speed adaptation. Finally, the vehicle response in case of no driver input (hands-off) was monitored.

### Adaptive Cruise Control Tests

The ACC tests use the Autonomous Emergency Braking tests as a basis because these procedures are well known and represent the typical situations that ACC systems have to cope with on Highways. The speed ranges that are currently used for AEB were extended to cover the typical driving speeds on European Highways.

In addition to the stationary, slower moving and braking vehicles ahead, a so-called cut-in and cut-out scenario were added which were aimed to cover realistic driving situations and were knowingly ACC systems are responding well.



**Figure 3. Highway Assist test scenarios for Adaptive Cruise Control (Left top: Approaching a stationary car, Right top: Approaching a slower moving car, Middle left: Approaching a braking car, Left bottom: Other car cuts-in into your lane, Right Bottom: Car in front changes lane to avoid a stationary car)**

### Lane Centering

Steering Support systems were evaluated in two very simple tests where the level of steering support was evaluated by hands-off driving through an S-curve and a second test where the driver steered the car away from the middle of the lane to avoid a small obstacle to identify the interaction between car and driver.

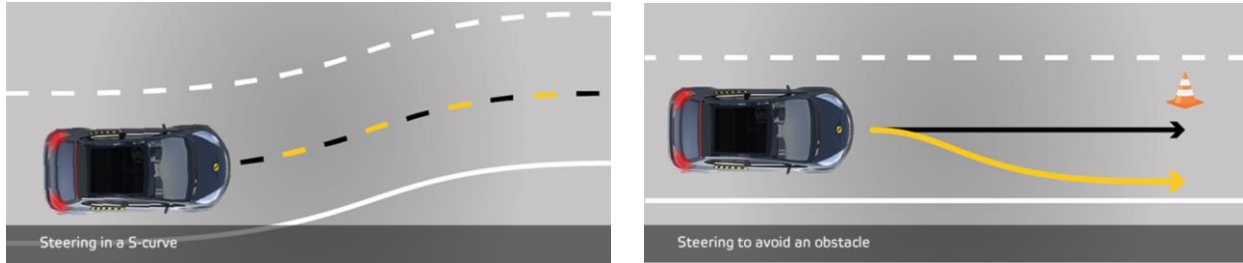


Figure 4. Highway Assist test scenarios for Lane Centering (Left: Steering in a S-curve, Right: Steering to avoid an obstacle)

### RESULTS

The main goal of the first series of tests was to highlight that all Highway Assist systems currently offered have a limited performance and they all need a vigilant driver to avoid the vehicle ending up in a critical situation. A vehicle which can comfortably, by ACC level braking, avoid all of the situation is not per se seen as a safe vehicle as the risk of overreliance is prominent. A balanced result where the role of the driver is clear, and where the vehicle merely provides support is what is expected of these systems. This paper will not go into the detailed test results of all vehicles separately but will provide the general observations and main conclusions from Euro NCAP’s first Automated Driving publication.

Detailed results can be found on the Euro NCAP Automated Driving campaign website.[2]

### Human-Machine-Interaction

Often system names will instantly give the consumer the wrong idea about the system’s capabilities as they do not clearly state whether the system is an assist system or not. Names like “Pilot” will give a false impression that the system is able to drive by itself, without the need of a driver. Of the ten systems verified, only three system names contained the word “Assist”; Adaptive Cruise Assist on the Audi A6, Active Driving Assistant Plus on the BMW 5-series and Pilot Assist on the Volvo V60. Hyundai, Mercedes and Toyota have non-specific for their Highway Assist systems and simply combine the separate functions. Four system names however, were perceived as misleading as they all contained the word “Pilot” without adding the word “Assist”; Connected Pilot in the DS 7 Crossback, Co-Pilot360 in the Ford Focus, ProPilot in the Nissan Leaf and Autopilot in the Tesla Model S.

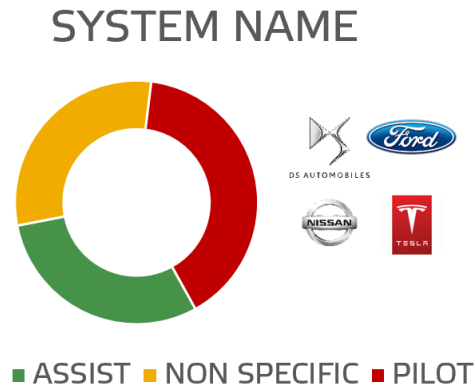
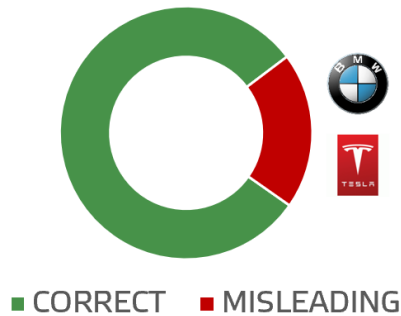


Figure 5. Highway Assist system name assessment

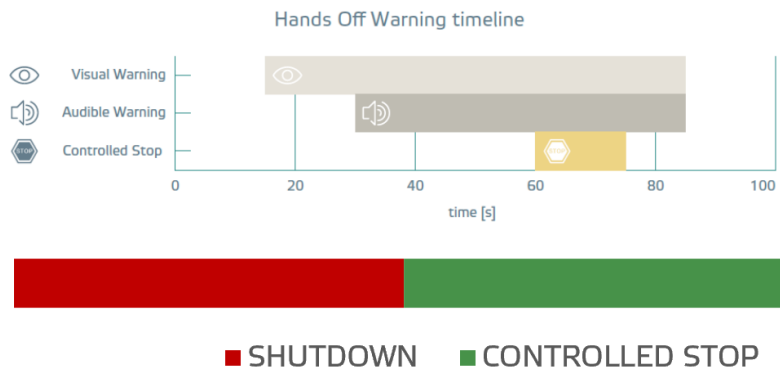
In general terms it was found that user manuals were extremely conservative and cautious regarding the role of the driver stating that the driver always has full responsibility. Contrary to this, marketing videos that were provided to Euro NCAP were seen as misleading for both the BMW and the Tesla where the drivers were shown to take their hands off the steering wheel and hand over control to the vehicle.

## OFFICIAL MEDIA



**Figure 6. Highway Assist system official media assessment**

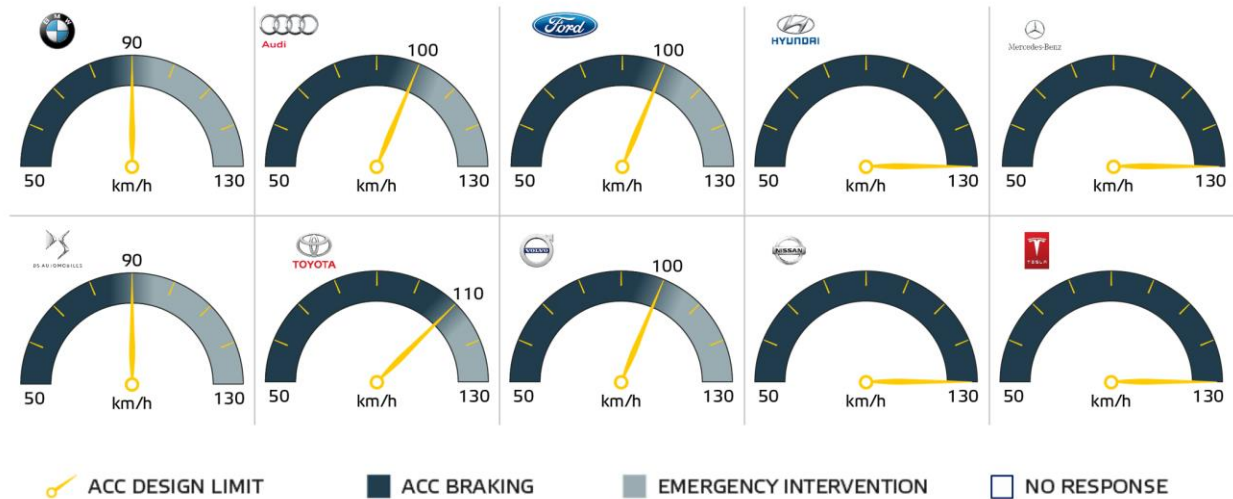
UNECE Regulation 79 requires all vehicles to have a monitor driver input on the steering wheel and warn the driver when the system detects that the driver is not in the loop. Two main strategies were applied by the vehicle manufacturers tested. In case the driver does not take back control after a certain warning sequence, half of the vehicles simply switched off their lane support and ACC, leaving the vehicle in principle uncontrolled. In case of sudden sickness or a driver falling asleep, this may have catastrophic results. The other half of the vehicles would bring the vehicle to a controlled stop within the lane, which was perceived as safer solution than simply cancelling the vehicle support functions.



**Figure 7. Highway Assist system Hands Off Warnings**

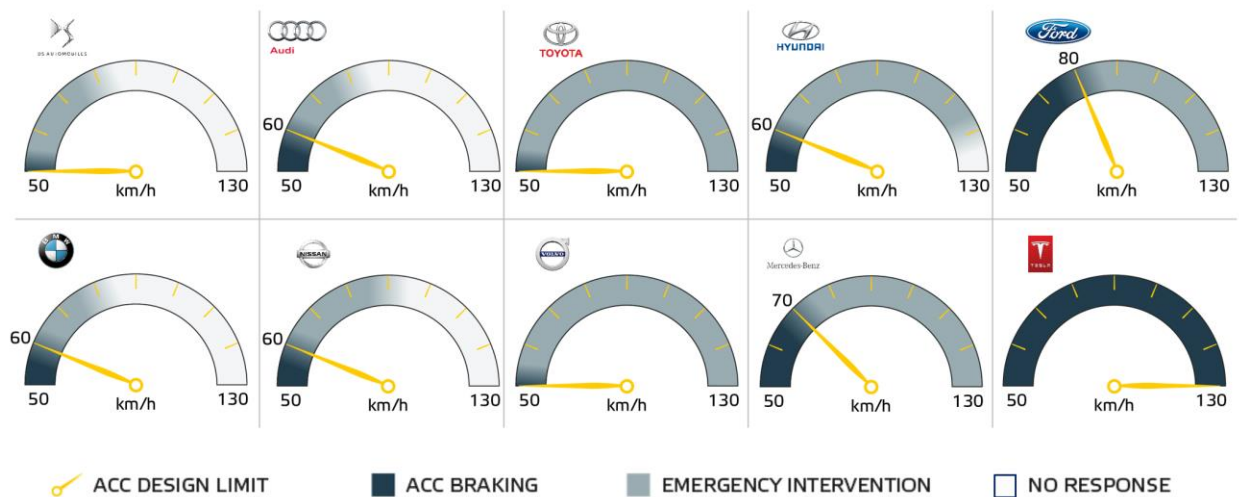
## Adaptive Cruise Control Tests

The performance in the ACC test scenarios revealed the strategies implemented by the different manufacturers, but also clearly shows that these systems are designed to work best in the slower moving scenarios.



**Figure 8. Results of the Approaching a slower moving car scenario**

In the stationary car in front scenario, most systems were very conservative and provide ACC level braking only upto 60 km/h to safely avoid the collision. DS, BMW, Audi and Nissan provided emergency support (FCW and/or AEB) only upto a speed of 80 to 90 km/h, where Toyota, Volvo, Hyundai, Mercedes, Ford provided emergency support over the whole speed range. Tesla however provided ACC level braking over the full speed range in this scenario which may lead to a consumer perceiving the system as full automation, with a high risk of the driver over relying on the system. Assist systems offering such a high level are expected to have a direct driver monitoring system to ensure the driver is in the loop but this was not the case for this vehicle.



**Figure 9. Results of the Approaching a stationary car scenario**

In the most challenging scenarios, the cut-in and cut-out of a vehicle in front, all vehicles highlighted limitations showing that a driver is always needed to respond to the situation before the vehicle does to avoid a collision.

### Lane Centering

The steering tests showed that all manufacturers apart from one, apply the same strategy where the driver keeps control of the lateral control and where the vehicle offers lane centering. This strategy is what one would expect from an assist system to avoid the driver thinking he is not required which can ultimately result in overreliance.

Tesla's Autopilot is not designed to work together with the driver and will not allow any driver input. As soon as the test driver steered around the obstacle in the lane, the system disengaged and stopped the steering support.

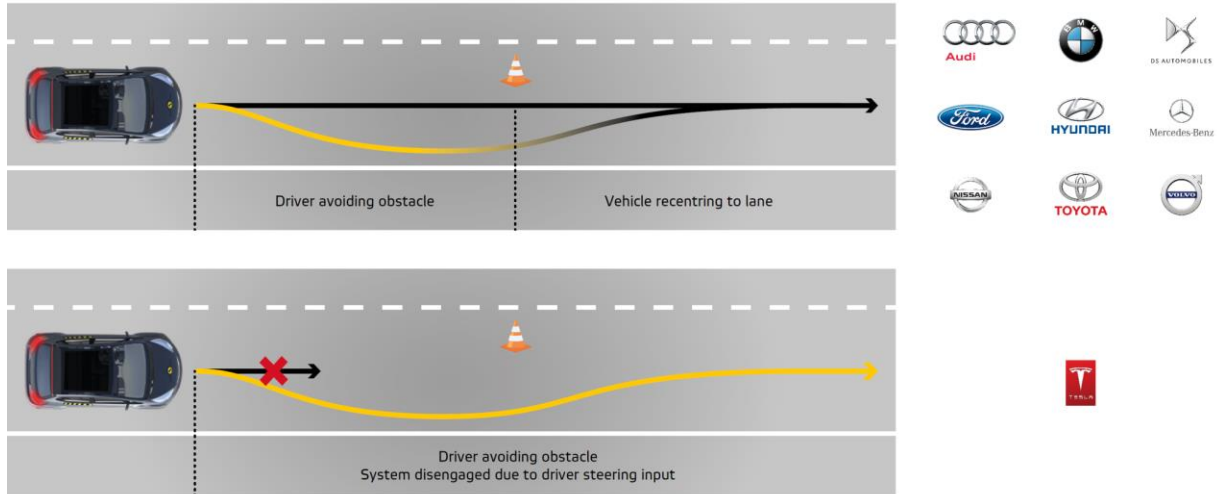


Figure 10. Results of the Steering to avoid an obstacle scenario

### Summary of results

In general terms all vehicles, apart from Tesla, behaved very similar with different levels of steering support and ACC performance. Overall, both BMW and DS were judged to be too conservative, where a consumer may not see the added value of the support function. On the other extreme, Tesla was seen as providing too much support for a Highway Assist system which results in the risk of a driver over relying on the system. The Highway Assist systems of the other seven manufacturers provided different levels of support but were all seen as balanced systems where the driver will clearly understand its role while the function is engaged.



Figure 11. Overall Highway Assist system results



## **DISCUSSION**

The different scenarios for testing the ACC performance are extended AEB scenarios but there is only an intuitive link to accident data or potential risk at crashes at the moment. More research is needed on the relevance of certain scenarios within the ODD of the systems assessed.

Clear and objective criteria need to be developed that can quantify and/or assess over-reliance so that car manufacturers can take this into account while developing these systems. Over the next years, when more automation is expected to penetrate the market, requirements need to be reviewed and updated to incentivise better, safer and more intuitive assist systems that support the driver in normal driving conditions.

## **CONCLUSION**

With the first round of evaluating Assisted Driving technologies, Euro NCAP is entering a whole new area of safety and safety assessments where public expectations are high, although understanding may be low. Euro NCAP is striving to promote automated driving technologies while at the same time raise awareness of their safety benefits and moreover their limitations.

For future assessments a clear and understandable definition to classify different driving modes so that consumers will have no problems understanding the capabilities of these systems and what the role of the driver is once the system is engaged. By combining these Driving Modes with well-defined Operational Domains, a solid foundation is available for Euro NCAP to develop specific test and assessment procedures for different levels of automation.

## **REFERENCES**

- [1] Society of Automotive Engineers, 2014 - Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems J3016
- [2] Euro NCAP Automated Driving campaign website, [www.euroncap.com/en/vehicle-safety/safety-campaigns/2018-automated-driving-tests](http://www.euroncap.com/en/vehicle-safety/safety-campaigns/2018-automated-driving-tests)

# **FAULT TREE-BASED DERIVATION OF SAFETY REQUIREMENTS FOR AUTOMATED DRIVING ON THE EXAMPLE OF COOPERATIVE VALET PARKING**

**Valerij Schönemann, Hermann Winner**

Institute of Automotive Engineering, Technische Universität Darmstadt  
Darmstadt, Germany

**Thomas Glock, Eric Sax**

Research and Engineering Center, FZI Research Center for Information Technology  
Karlsruhe, Germany

**Bert Boeddeker, Sebastian vom Dorff**

Research and Engineering Center, DENSO AUTOMOTIVE Deutschland GmbH  
Eching, Germany

**Geert Verhaeg<sup>1</sup>, Fabrizio Tronci<sup>2</sup>, Gustavo G. Padilla<sup>3</sup>**

TNO<sup>1</sup>, Magneti Marelli<sup>2</sup>, Hella Aglaia Mobile Vision<sup>3</sup>  
Netherlands<sup>1</sup>, Italy<sup>2</sup>, Germany<sup>3</sup>

Paper Number 19-0099

## **ABSTRACT**

Developing safe vehicle automation systems is crucial for the commercialization of automated driving. One of the major challenges for the release of fully automated driving is functional safety. Automated driving systems explode in complexity due to an infinite number of occurring scenarios. Thereby, the derivation of safety requirements for complex automated driving functions lacks a categorization to tackle the completeness issue. This work presents a structure for a fault tree-based approach to derive safety requirements from safety goals systematically in compliance with the international standard of functional safety for road vehicles known as ISO 26262. The investigation of the state of the art reveals that a functional safety concept for fully automated valet parking (AVP) has not yet been targeted. The methodology is therefore applied on the example of automated valet parking to elaborate a safety concept which was not yet investigated.

Beforehand, the AVP system was split into a manageable amount of relevant functional scenarios to decrease complexity. For each scenario, a Hazard Analysis and Risk Assessment (HARA) was performed. A set of safety goals was elaborated. The approach utilizes a fault tree-based Sense-Plan-Act architecture to achieve a large coverage of possibly derivable safety requirements from safety goals. The sense phase contains the acquisition of sensor data and leads to three uncertainty domains: state, existence, and class uncertainty. The plan segment includes the situation comprehension and action planning. Thereby, the transportation mission can be split into five tasks. The act block represents the execution of the planned trajectory. Longitudinal and lateral vehicle dynamics such as steering, shifting, accelerating, and braking are performed. A violation of a safety goal occurs if at least one of the failure events in the sense-, plan-, and act-phase is present. The methodology is suitable for safety goals which follow the specified Sense-Plan-Act pattern.

## **INTRODUCTION**

The globally leading cause of death among people aged 15-29 in the year 2012 are road traffic accidents [1]. 94 % of crashes can be tied back to human error [2]. In 2015, the United Nations agreed to global goals for sustainable development. The goal “good health and well-being” concerns road safety in which the number of global deaths and injuries from road traffic accidents shall be halved by 2020. Safe automated systems that intervene in case of a proximate accident and release the driver from the responsibility are required. Thereby, functional safety is one of the major challenges for the release of automated driving [3]. An automated driving function shall be harmless in all operating states. The system shall identify hazards and reach a safe location in which the vehicle is no hazard for other participants. The international standard for functional safety ISO 26262 specifies a systematic procedure for designing functionally safe electrical and electronic systems [4]. ISO 26262 and international standards for other domains are derived from the IEC 61508 [5].

Automated systems from different domains have a common denominator: exploding complexity. A nearly infinite number of possible scenarios has to be tested. The European Union (EU) project ENABLE-S3 focuses on the reduction of today’s cost-intensive verification and validation process to establish efficient methods for the commercialization of automated cyber-physical systems. Different approaches have to be targeted in order to cope with the increasing complexity regarding the development of safe automated systems.

A major challenge is to develop a functionally safe distributed system in which independent subsystems share responsibility for the automation task. Such a distributed system is fully Automated Valet Parking (AVP). AVP is realized through cooperation between the automated vehicle and a Parking Area Management system (PAM). The automated vehicle operates driverless and is classified as level 4 of SAE International’s taxonomy of driving automation [6]. The use case provides an automated parking procedure. In previous work, a scenario-based methodology for functional safety according to ISO 26262 was presented and applied on the safety analysis of AVP [7]. The following pre-conditions were assumed for AVP:

1. Parking management system and automated vehicle manage the driving task in cooperation.
2. The handing over and requesting back procedure of the automated vehicle to/ from the PAM is instructed via a terminal (human-machine interface, HMI).
3. Manually and automatically operated vehicles are allowed to enter the parking garage.
4. Pedestrians, animals, obstacles, etc. sojourn in the car park.
5. Drivers and passengers have to leave the automated vehicle before AVP is activated.
6. Parking construction prevents dangers caused by running engines.

The described constraints served as an input to break down the system’s functional behavior into scenarios. Thereby, the AVP system was split into a manageable amount of relevant functional scenarios to decrease complexity. For each scenario, a Hazard Analysis and Risk Assessment (HARA) is performed. As a result, a more complete set of safety goals was elaborated as indicated in Table 1.

This work is structured as follows: Section 2 contains the related work of functional safety. Section 3 illustrates a structure for a fault-tree-based approach to derive functional safety requirements for automated driving. Thereafter, the presented methodology is applied using the example of fully automated valet parking. Section 4 shows the elaborated safety requirements from safety goals for AVP. Section 5 summarizes the results of the safety requirements and gives a brief outlook for developing a safety concept.

**Table 1.**  
**Safety Goals for Automated Valet Parking [7]**

ID	Safety Goal	ASIL
SG01	Unintended activation of the valet parking function outside of the PAM-controlled parking area shall be prevented.	D
SG02	The integrity of the communication between the PAM and the vehicle shall be ensured.	D
SG03	The system shall prevent a collision between automated vehicles and persons.	C
SG04	The vehicle shall not start moving during embarkment and disembarkment.	C
SG05	The system shall prevent collisions with other vehicles.	B
SG06	The system shall notify a human supervisor in case of a collision or fire.	B
SG07	The system shall ensure that the vehicle stays within the (statically defined) drivable area during AVP.	B
SG08	The valet parking function shall be disabled if people are inside the vehicle.	A
SG09	The system shall prevent collision of automated vehicles with objects.	A

## RELATED WORK

A major challenge for the release of automated driving is the issue of testing. Up to now, only the international standard ISO 26262 illustrates a systematic process for developing functionally safe electrical and electronic systems in the automotive domain. Neither a standard, nor a methodology is specified to elaborate a safety concept specifically for automated driving. However, functional safety as well as a corresponding methodology for developing a safety concept for such complex systems is crucial for the release of automated driving [8].

Alexander et al. [9] combined several existing approaches to develop a methodology for deriving safety requirements for autonomous systems. The authors describe the derivation of safety requirements as a three-stage process. In the first step, harmful events are determined (hazard identification). Causes of the hazards are explored (hazard analysis) and finally safety requirements can be derived from causes. The system is seen as a combination of operators (Combined Autonomous Systems, CAS) in which hazards may occur. High-level capabilities of CAS are determined and hierarchically decomposed in lower level capabilities until these can be analyzed for safety (Hall-May [9]). The authors consider autonomous systems in general. Autonomous systems from other domains will lead to different safety requirements e.g. by comparing automated systems in the health domain with automated driving functions.

The fault tree analysis is a deductive approach starting with a top undesired event and is suggested in the ISO 26262 beside a Failure Modes and Effects Analysis (FMEA) and Hazard and Operability study (HAZOP) for safety analysis. FTA is also used in the nuclear power and aerospace sector. Failure events can be identified by considering Boolean logic. The main advantage of a FTA is that it displays interactions between events in a graphical format [11]. The interaction cannot be seen from a FMEA. A FMEA is more suitable for an inductive failure analysis of components and subsystems. Furthermore, the FTA should contain all failure modes of a FMEA.

Lambert applied a qualitative FTA on a car starting system [12]. Thereby, the applier has to identify the failure modes that cause the top event. Starting from the top undesired event that the car does not start, the author shows a logical progression of undesired events connected via AND and OR logic. However, a vast number of undesired events may occur with increasing system complexity. The elaboration of a FTA for automated driving systems without providing any structure is challenging.

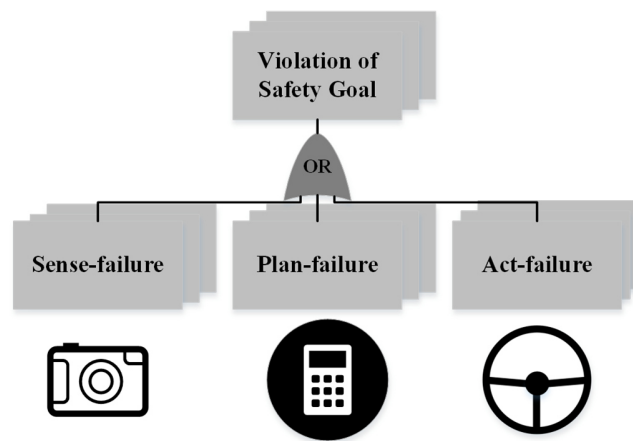
Stolte et al. [13] derived safety goals and functional safety requirements of actuation systems for automated driving by applying a system theory-based methodology. The authors used a System-Theoretic Process Analysis (STPA) to identify unsafe control actions and its causes which serve as an input for a HARA. Furthermore, safety requirements are derived from a control structure and corresponding unsafe control actions. The authors do not determine safety requirements for perception or planning modules of automated vehicles. The trajectory input was assumed to be correct and only actuation systems of automated vehicles were analyzed.

The national project PEGASUS [14] applies a scenario-based approach to reduce driving test distances for a statistical approval of highly automated driving. It is assumed that the majority of the driven mileage is uncritical and only critical scenarios are required to be investigated. Amersbach and Winner [15] proposed a six-layer decomposition of the automated driving function. The six layers are Information Access, Information Reception, Information Processing, Situational Understanding, Behavioral Decision, and Action. A matrix to allocate fail criteria to functional layers and relevant scenarios is built. Fail criteria are identified by using a FTA. Redundant fail criteria that are “subsets or intersecting sets of each other” are combined and thus the testing effort is reduced. Test cases and environments are derived from fail criteria for the use of safety approval. However, the authors propose a different approach and do not relate to the ISO 26262 standard. The interaction of different subsystems is not targeted.

Furthermore, there is still a risk of a violation of a safety goal without any malfunction. It is therefore required to consider the safety of the intended function (SOTIF). A sub-working group was built within ISO 26262 to specify when a target function behaves safely. The results are present in the ISO/WD PAS 21448. This work aims to cover critical scenarios, which are not only a result of malfunction, but also the safety of the intended functionality.

Reschka et al. [16] investigated safety concepts for automated driving without driver monitoring. The analysis leads to high-level safety mechanisms to handle potential hazards for AVP systems. More specific safety requirements are not presented. Bosch and Daimler [17] released the first prototype for infrastructure-based AVP in a mixed traffic parking garage. However, further specification concerning the safety are missing. Chirca et al. [18] and Schwesinger et al. [19] provide mainly a technical description of an AVP service in which safety is not of major focus.

The state of the art reveals that a structure for breaking down highly complex and self-driving automation systems is missing. This work aims to overcome the lack of a recipe for deriving safety requirements from safety goals. This work presents a methodology how such a specification can be achieved by deriving safety requirements for automated driving systematically in compliance with the international standard ISO 26262. The approach utilizes a fault tree-based technique to achieve a large coverage of possibly derivable safety requirements. The issue of completeness is targeted qualitatively by applying a deductive



**Figure 1.** The violation of a safety goal occurs if at least one of the failure events in the sense-, plan-, and act-phase is present.

method. The methodology is applied on cooperative valet parking for which a safety concept is still missing in the state of the art.

## METHODOLOGY

The methodology presented in this work provides a path to systematically derive safety requirements from safety goals. A fault tree-based approach is proposed to ensure a more complete set of safety requirements. Sequential robot control architectures are known as Sense-Plan-Act or Sense-Model-Plan-Act architectures. Thereby, the signal processing steps of the sensor data acquisition, the environment modeling, the planning, and finally the actions are executed sequentially. Sequential architecture elements serve for achieving a long-term goal, e.g. the execution of a driving mission [20]. In the following the terms Sense, Plan, Act and the corresponding breakdown into segments are introduced. Figure 1 indicates the safety analysis of a Safety Goal's violation.

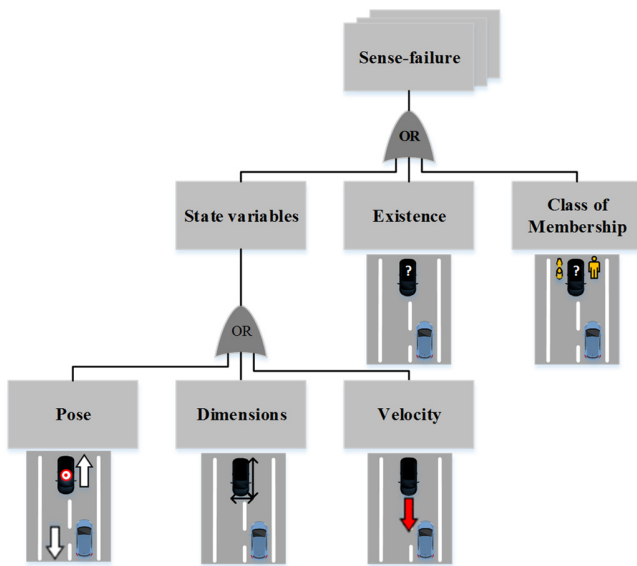
*Sense:* The Sense phase contains the acquisition of sensor data and modelling of the environment. According to Dietmayer et al. [21] detecting static and dynamic objects and physically measuring them as precisely as possible, leads to three uncertainty domains visualized in Figure 2:

- **State uncertainty:** Represents the measuring errors of physical measured variables, especially the object's dimensions (length, width, height), the object's pose and the object's velocity.
- **Existence uncertainty:** Outlines the uncertainty whether an object captured by the sensors and mapped into the representation actually exists. This concerns mainly false positives and false negatives. For example, emergency braking should only be executed in case of a high existence probability.
- **Class uncertainty:** Describes uncertainty of the capability to classify the object's membership in order to predict the object's behavior. Type of object might be for example pedestrians, bicyclists, trucks, or cars. The degree of granularity is dependent on the use case.

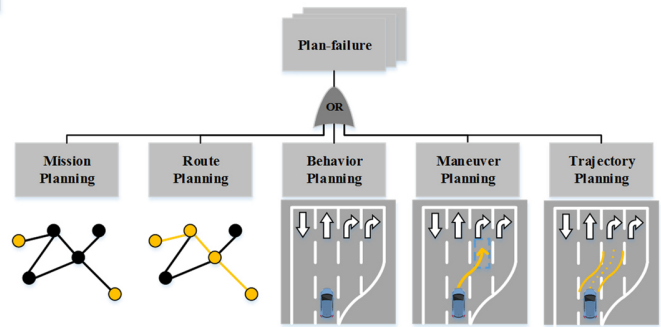
*Plan:* The Plan segment includes the situation comprehension and action planning. The transportation mission can be split into five tasks which are partly computed by today's navigation systems. These five steps are given in Figure 3:

- **Mission Planning:** In the first step, a mission has to be planned from the current location to the destination.
- **Route Planning:** A route has to be determined in order to get to the destination.
- **Behavior Planning:** Selects a sequence of maneuvers by considering other traffic participants, traffic rules and restrictions.
- **Maneuver Planning:** Maneuvers such as lane changes have to be executed.
- **Trajectory Planning:** A trajectory has to be calculated to perform necessary maneuvers.

Timing constraints for the start and end of each maneuver and the calculation of the maneuver trajectory have to be specified.



**Figure 2.** According to Dietmayer [17] an uncertainty in the sense phase occurs if the object’s state variables such as the object’s pose, the object’s dimensions, and the object’s velocity are not measured with sufficient precision or if the object’s existence or its class of membership are uncertain.



**Figure 3.** According to Lotz [22] the driving mission can be split into mission planning, route planning, behavior planning, maneuver planning, and trajectory planning. For maneuver and trajectory planning, timing constraints for calculation and execution are crucial.

*Act:* The Act block represents the execution of the planned trajectory. The following vehicle control inputs are required for performing longitudinal and lateral vehicle dynamics: Steering, shifting, accelerating, and braking. A complete electrification of actuators is mandatory. This is realized by today’s X-by-Wire concepts: Throttle-by-Wire, Brake-by-Wire, Shift-by-Wire, and Steer-by-Wire [19]. Thereby, either the targeted steering, shifting, acceleration, and braking parameters are not plausible for the executed maneuver in terms of range and time or corresponding vehicle components are corrupted. The breakdown of possible Act-failures is illustrated in Figure 4.

The presented structure can be further broken down into use case-specific safety requirements. The safety requirements can be derived systematically by covering a more complete set of safety requirements due to the application of a deductive fault tree-based approach. The methodology is not suitable for all derived safety goals since for example C2X-communication does not follow the specified Sense-Plan-Act pattern.

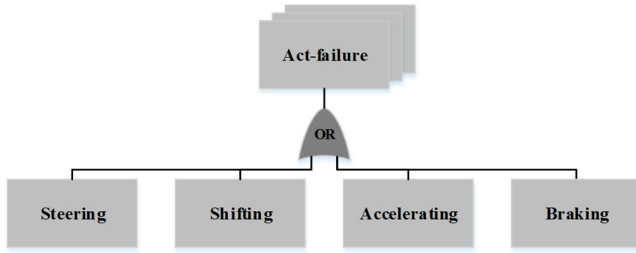
### DERIVATION OF SAFETY REQUIREMENTS

In the following, the elaborated methodology is applied to the safety goal “SG03: *The automated driving system shall prevent a collision between automated vehicles and persons*”. Furthermore, the derivation is similar for SG05 and SG09 only with a different ASIL inheritance for derived safety requirements and decomposition to architectural elements.

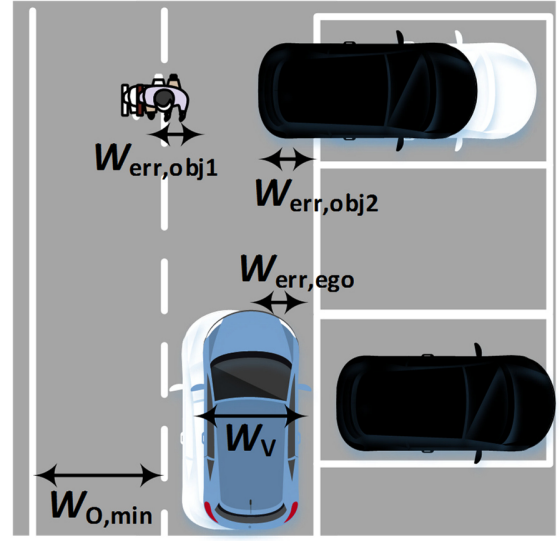
The division in sense, plan, and act leads to the following high-level Functional Safety Requirements (FSR):

- FSR3.1: The system shall detect objects in its required sensor perception area
- FSR3.2: The system shall not plan a harmful trajectory
- FSR3.3: The vehicle shall prevent unintended control actions

Each high-level FSR will be further broken down into low-level FSR.



**Figure 4.** Steering, shifting, accelerating, and braking are primitives that are required for vehicle control mechanisms.



**Figure 5.** Maximum accepted total error of size determination and object localization is given by the narrowest part in the operational domain and measurement inaccuracies

#### A. Sense

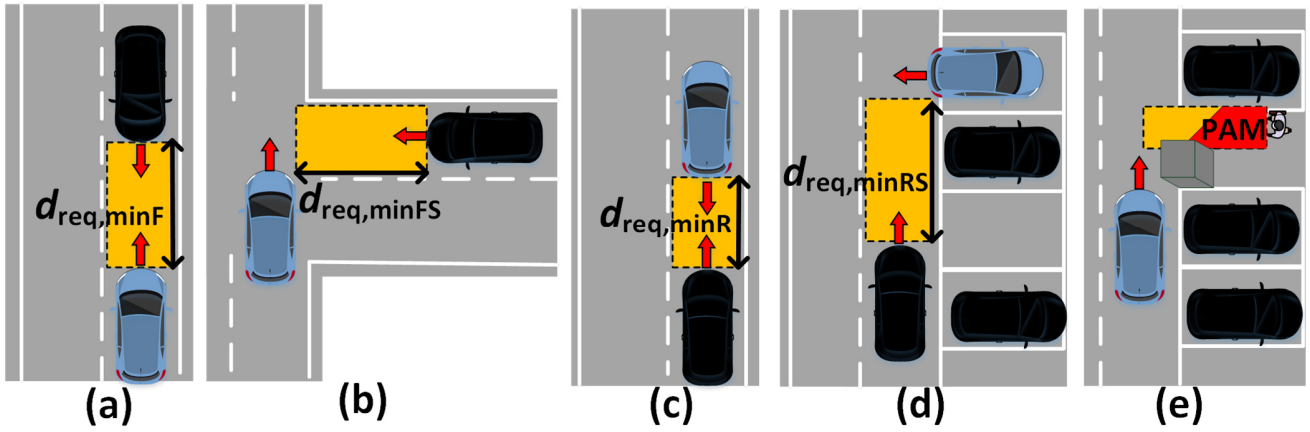
Since no standard exists specifically for safety requirements of automated driving, other regulations have to be considered as a basis. State uncertainty is represented by the functional safety requirement FSR3.1.1 - FSR3.1.3 of Table 3. and corresponding derived functional safety requirements. The system has to detect the object's position by localizing it. The precision of localization is given by the narrowest part of the operational design domain  $W_{O,min}$ , the vehicle width  $W_V$ , and corresponding measurement inaccuracies  $W_{err}$  which may appear on both sides in worst-case. Figure 5 indicates an ego-vehicle driving straight and approaching two objects. Beside the ego-vehicle's localization error  $W_{err,ego}$ , the object's localization errors  $W_{err,obj}$  are present. The ego-vehicle assesses a collision-free area due to localization errors, but in reality the ego-vehicle would collide with a traffic participant. The total accepted localization error  $W_{err,total}$  is given by

$$W_{err,total} \leq W_{err,ego} + W_{err,obj} = \frac{W_{O,min}}{2} - \frac{W_V}{2} \quad (\text{Equation 1})$$

$$W_{err,obj} \leq \frac{W_{O,min} - W_V}{4} \quad \text{for } W_{err,ego} = W_{err,obj} \text{ (infrastructure-based)}$$

Considering Germany's road construction regulation and Germany's traffic regulation, a minimum lane width  $W_{L,min} = 2.75$  m [25][26] and a maximum vehicle width of  $W_{V,max} = 2.50$  m [27] can be found. The overall error of size determination and object localization for  $W_{err,ego} = W_{err,obj}$  shall be less than  $W_{err,total} = (W_{L,min} - W_{V,max})/2 = 12.5$  cm and  $W_{err,obj} \leq 6.25$  cm. However, for AVP systems a parking lot width of  $W_{P,min} = 2.75$  m is not profitable for the operator and a minimum parking lot width of Germany's parking garage regulation  $W_{P,min} = 2.30$  m [26] could be considered by not allowing to enter oversized vehicles. In that case, a look on the European's average passenger car size of 2016 could be done [24]. Adding a safety margin of 10 cm for withdrawn car mirrors on each side, we end up with an average vehicle width of around  $W_{V,avg} = 2$  m and therefore an overall error of size determination and object localization of less than  $W_{err,total} \leq (W_{P,min} - W_{V,avg})/2 = 15$  cm and  $W_{err,obj} \leq 7.5$  cm.

The object can only be detected if it appears in the system's sensor perception area. Safety-relevant areas of interest for collision avoidance can be specified dependent on the dynamic driving parameters of the engaged traffic participants such as velocities, timing constraints and deceleration capabilities. A definition of an area, in which the perception of objects for collision avoidance is mandatory, has to be given. Furthermore, maneuvers that can occur in the defined operational domain as illustrated in Figure 6 have to be identified. The superposition of the maneuver-based stopping distances shows that the overall safety zone is created by the ego-vehicle's and the object's travelled envelopes given by their widths and stopping distances [28].



**Figure 6. Identified maneuvers that lead to a minimum required sensor perception area: (a) driving straight with potential frontal collision between an automated and manually driven vehicle and both vehicles are braking, (b) intersection crossing and approaching collision partner, (c) driving in reverse with potential rear collision and both vehicles braking, (d) leaving the parking spot in reverse, (e) covered object and required infrastructure support.**

The worst-case concerning the stopping distance is defined as a frontal collision of an automated and manually operated vehicle driving with  $v_{\max}$  and both vehicles are braking. It is assumed that both vehicles react at the same time. The minimum required sensor range  $d_{\text{req}}$  is theoretically given by the stopping distance until frontal collision and can be calculated according to

$$d_{\text{req,min}} \geq (v_{\text{ego}} + v_{\text{obj}}) \cdot (t_{\text{B,lag}} + t_{\text{R,ad}}) + v_{\text{obj}} \cdot (t_{\text{R,md}} - t_{\text{R,ad}}) + \frac{v_{\text{ego}}^2 + v_{\text{obj}}^2}{2 \cdot D_{\text{min}}} + d_{\text{tol}} \quad (\text{Equation 2})$$

Thereby, the worst-case constraints are defined as presented in Table 2. Considering rather conservative values of a nearly dry road surface and a resulting minimum deceleration of  $D_{\text{min}} = 8 \text{ m/s}^2$ , a free running time  $t_{\text{B,lag}} + t_{\text{R,ad}} = 0.5 \text{ s}$ , worst-case driver reaction time  $t_{\text{R,md}} = 1.5 \text{ s}$  and  $d_{\text{tol}} = 0.5 \text{ m}$ , we get  $d_{\text{req,minF}} \geq 27.51 \text{ m}$ . A worst case for a rear collision is a collision at a maximum allowed reverse velocity of the ego-vehicle  $v_{\text{ego}} = v_{\text{maxR}}$ , an object forward velocity of  $v_{\text{obj}} = v_{\text{maxF}}$ , and braking of both vehicles. From this, a required sensor range of  $d_{\text{req,minR}} \geq 20.88 \text{ m}$  can be calculated. Finally, a worst case for the perception distance to the side is given by crossing an intersection at a maximum allowed intersection crossing velocity of  $v_{\text{obj}} = v_{\text{maxI}}$

$$d_{\text{req,minFS}} = d_{\text{req,minRS}} \geq v_{\text{obj}} \cdot (t_{\text{B,lag}} + t_{\text{R,obj}}) + \frac{v_{\text{obj}}^2}{2 \cdot D_{\text{min}}} + d_{\text{tol}} \quad (\text{Equation 3})$$

We end up with a required sensor perception range of  $d_{\text{req,minFS}} = d_{\text{req,minRS}} \geq 19 \text{ m}$ . The required sensor perception area to the rear side is actually largest if the vehicle leaves the parking spot backwards. However, since the required sensor perception area to the front is mandatory in many specific situations, the required sensor perception area to the rear side  $d_{\text{req,minRS}}$  can be significantly reduced if only reverse parking and forward leaving of the parking bay is allowed. Considering a parking spot length of  $L_{\text{P,min}} = 5 \text{ m}$  [26], we can approximate  $d_{\text{req,minRS}} \geq L_{\text{P,min}} = 5 \text{ m}$ . Objects that lie within the ego-vehicle's required sensor perception area and are covered, have to be detected by top-mounted sensors of the infrastructure. The elaborated safety zone should adjust its size according to the present velocities in the sensor perception area. The overall required horizontal FoV of  $180^\circ$  in the front and to the rear is required to detect moving objects in the frontal/ rear vehicle area. Elaborated functional safety requirements are shown in Table 3.



**Table 2.**  
**Pre-defined Constraints for Automated Valet Parking [28]**

ID	Description	Value
C01	Maximum allowed velocities: in forward $v_{\max,f}$ , in reverse $v_{\max,r}$ , at intersections $v_{\max,i}$	$v_{\max F} = 30 \text{ km/h}$ $v_{\max R} = 10 \text{ km/h}$ $v_{\max I} = 10 \text{ km/h}$
C02	Worst-case expected time delays: system response time from the plausibility check until initiating the brakes $t_{R,ad}$ , driver reaction time $t_{R,md}$ , lag time of the brake $t_{B,lag}$ given by the response time of the brake $t_{R,b}$ and the time until buildup of deceleration $t_{B,b}$	$t_{R,ad} = 0.3 \text{ s}$ $t_{R,md} = 1.5 \text{ s}$ $t_{B,lag} \approx t_{R,b} + \frac{t_{B,b}}{2}$ $t_{B,lag} = 0.2 \text{ s}$
C03	Minimum expected deceleration $D_{\min} = \mu_{\min} \cdot g$ for object- and ego-vehicle	$D_{\min} = 8 \frac{\text{m}^2}{\text{s}}$
C04	Safety margin $d_{\text{tol}}$	$d_{\text{tol}} = 0.5 \text{ m}$

1) Breuer and Bill, 2008

**Table 3.**  
**Derivation of FSR3.1: “The system shall detect objects in its sensor perception area.”**

ID	Functional Safety Requirement
FSR3.1.1	The system shall detect the object’s state variables sufficiently accurate.
FSR3.1.1.1	The system shall localize the object’s pose $p_{\text{obj}}$ . The error for size determination and object localization shall be less than $W_{\text{err,obj}}$ .
FSR3.1.1.1.1	The system shall detect objects in a $180^\circ$ front and rear horizontal and sufficiently high vertical field of view.
FSR3.1.1.1.2	The system shall detect the object’s pose $p_{\text{obj}}$ in its minimum required sensor range $d_{\text{req,minF}}$ , $d_{\text{req,minFS}}$ , $d_{\text{req,minR}}$ , and $d_{\text{req,minRS}}$ .
FSR3.1.1.2	The system shall determine the object’s dimensions length $l_{\text{obj}}$ , width $w_{\text{obj}}$ , height $h_{\text{obj}}$ in its minimum required sensor range. The error for size determination and object localization shall be less than $W_{\text{err,obj}}$ .
FSR3.1.1.3	The system shall determine the object’s velocity $v_{\text{obj}}$ in its minimum required sensor range.
FSR3.1.1.4	The system shall detect objects under all possible environment conditions in the PAM area.
FSR3.1.1.5	The system shall diagnose broken/ covered or misplaced sensors.
FSR3.1.1.6	The system shall detect objects that are covered from the vehicle’s view in its minimum required sensor perception area.
FSR3.1.2	The system shall have an ASIL-dependent false positive and false negative rate.
FSR3.1.3	The system’s object classification shall not lead to harmful situational interpretation.

## B. Plan

The navigation to a specified destination starts with mission planning. The vehicle’s position and the destination’s position are required for mission planning. Based on the current and the destination’s position, today’s graph-based search algorithms for road networks determine a route. The computed route shall be composed of up-to-date, accessible, connected road segments that shall be driven in compliance with traffic regulations. The functional safety requirements are equally valid for the lane assignment. Maneuvers such as lane changes are required to reach the destination. The maneuver and the corresponding trajectory shall be feasible, collision-free, and calculated within hard real-time constraints. Thereby, hard real-time is defined as “a missing system response deadline leads to a collision”. Start and end of the maneuver have to be defined depending on the maneuver and environmental constraints. Derived functional safety requirements are presented in Table 4.

**Table 4.**  
**Derivation of FSR3.2: “The system shall not plan a harmful trajectory.”**

ID	Functional Safety Requirement
FSR3.2.1	The system shall plan a safe mission.
FSR3.2.1.1	The system shall localize its pose $p_{obj}$ . The error for size determination and localization shall be less than $W_{err,ego}$ .
FSR3.2.1.2	The system shall localize the destination’s position. The error for size determination and localization shall be less than $W_{err,obj}$ .
FSR3.2.2	The system shall plan routes on up-to-date, accessible, connected road segments in compliance with traffic regulations.
FSR3.2.3	The system shall assign maneuvers on up-to-date, accessible drivable area in compliance with traffic regulations.
FSR3.2.4	The system shall compute a feasible, collision-free maneuver within hard real-time constraints (= missing deadline leads to a collision).
FSR3.2.5	The system shall plan a collision-free trajectory.

### C. Act

Act-failures are not further broken down since an investigation is already done in [13] and state of the art. For the sake of completeness, functional safety requirements are illustrated exemplary in Table 5.

**Table 5.**  
**Derivation of FSR3.3: “The vehicle shall prevent unintended control actions.”**

ID	Functional Safety Requirement
FSR3.3.1	The system shall detect corrupted or uncalibrated actuators and breakdown of necessary vehicle components.
FSR3.3.2	The system shall prevent unintended steering.
FSR3.3.3	The system shall prevent unintended shifting.
FSR3.3.4	The system shall prevent unintended accelerating.
FSR3.3.5	The system shall prevent unintended braking.

Finally, a safety engineer has to control whether a functional safety requirement is not yet covered by another safety goal and should inherit the corresponding safety goal’s Automotive Safety Integrity Level (ASIL). The functional safety requirements for the remaining safety goals are shown in Table 6. in the appendix.

### CONCLUSION AND OUTLOOK

The state of the art has revealed challenges for automated driving in terms of functional safety. Beside malfunctions, the safety of the intended functionality has to be considered. The derivation of safety requirements for complex automated driving functions leads to the completeness issue. An approach is proposed to derive functional safety requirements in compliance with ISO 26262 according to a deductive fault tree-based methodology for automated driving functions. Functional safety requirements can be derived systematically to target the completeness issue qualitatively. The technique is applied on elaborated safety goals for automated valet parking. Functional safety requirements are derived for all elaborated safety goals. A minimum required sensor perception area could be specified for AVP in which the object’s parameters such as pose, dimensions, velocity, existence and class are required to be known. The maximum accepted total error of size determination and object localization could be identified. In future work, functional safety requirements should be assigned to functional blocks of the valet parking system architecture. Thereby, the distribution of functionalities between the automated vehicle and the parking area management system will be targeted and additional test cases will be derived for functional safety requirements to validate the safety concept of automated valet parking.

## ACKNOWLEDGEMENT

This project has received funding from the ECSEL Joint Undertaking under grant agreement No 692455. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Denmark, Germany, Finland, Czech Republic, Italy, Spain, Portugal, Poland, Ireland, Belgium, France, Netherlands, United Kingdom, Slovakia, Norway.

## REFERENCES

- [1] World Health Organization, "Global status report on road safety 2015," World Health Organization, 2015.
- [2] S. Singh, "Critical reasons for crashes investigated in the national motor vehicle crash causation survey," No. DOT HS 812 115, 2015.
- [3] W. Wachenfeld and H. Winner, "The Release of Autonomous Vehicles," in *Autonomous Driving: Technical, Legal and Social Aspects*, M. Maurer, J. C. Gerdes, B. Lenz, and H. Winner, Eds.: Springer, 2016, pp. 425–449.
- [4] International Organization for Standardization, "ISO 26262: Road vehicles - Functional Safety," Geneva, Switzerland, 2011.
- [5] International Electrotechnical Commission, "Functional safety of electrical/electronic/programmable electronic safety related systems," IEC 61508, 2000.
- [6] SAE, "Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles," Society of Automotive
- [7] V. Schönemann and H. Winner et al., "Scenario-based Functional Safety for Automated Driving on the Example of Valet Parking," in *IEEE Future Information and Communication Conference*, Singapore, 2018.
- [8] H. Winner, M. Graupner and W. Wachenfeldt, "How to Address the Approval Trap for Autonomous Vehicles (Keynote)," in *IEEE 18th International Conference on Intelligent Transportation Systems (ITSC)*, Sep. 2015.
- [9] R. Alexander, N. Herbert, and T. Kelly, "Deriving safety requirements for autonomous systems," in *4th SEAS DTC Technical Conference*, 2009.
- [10] M. Hall-May, "Ensuring Safety of Systems of Systems—A Policy-based Approach," PhD Thesis, University of York, 2007.
- [11] H. Ross, "Functional Safety for Road Vehicles: New Challenges and Solutions for E-mobility and Automated Driving," Springer Verlag, pp. 115 – 119, 2016.
- [12] H. Lambert, "Use of fault tree analysis for automotive reliability and safety analysis," Lawrence Livermore National Lab., CA (US), 2003.
- [13] T. Stolte, G. Bagschik and M. Maurer, "Safety goals and functional safety requirements for actuation systems of automated vehicles," *19th IEEE Intelligent Transportation Systems (ITSC)*, 2016.
- [14] German Aerospace Center (DLR), "PEGASUS RESEARCH PROJECT," [Online] Available: <http://pegasus-projekt.info/en/home>, accessed: March 28th 2018.
- [15] C. Amersbach and H. Winner, "Functional Decomposition - An Approach to Reduce the Approval Effort for Highly Automated Driving," in *8. Tagung Fahrerassistenz*, 22.-23. November, München, 2017.
- [16] A. Reschka, Safety Concept for Autonomous Vehicles, In *Autonomous Driving – Technical, Legal and Social Aspects*, pp. 473–496, Springer Nature, 2016
- [17] Automotive World, 2018. Daimler and Bosch jointly premiere automated valet parking in China. From: [www.automotiveworld.com/news-releases/daimlerand-bosch-jointly-premiere-automated-valet-parking-in-china/](http://www.automotiveworld.com/news-releases/daimlerand-bosch-jointly-premiere-automated-valet-parking-in-china/). Accessed: November 2018
- [18] M. Chirca, R. Chapuis, and R. Lenain, "Autonomous Valet Parking System Architecture," *IEEE International Conference on Intelligent Transportation Systems (ITSC)*, 2015.
- [19] U. Schwesinger, M. Bürki, J. Timpner, S. Rottmann, L. Wolf, ... & L. Heng. Automated valet parking and charging for e-mobility. In *Intelligent Vehicles Symposium (IV)*, pp. 157-164, 2016.
- [20] J. Hertzberg, K. Lingemann and A. Nüchter, "Mobile Roboter: Eine Einführung aus Sicht der Informatik," Springer-Verlag, 2012.
- [21] K. Dietmayer, "Predicting of machine perception for automated driving," in *Autonomous Driving: Technical, Legal and Social Aspects*, M. Maurer, J. C. Gerdes, B. Lenz, and H. Winner, Eds.: Springer, 2016, pp. 407-424.
- [22] F. Lotz, „Entwicklung einer Referenzarchitektur für die assistierte und automatisierte Fahrzeugführung mit Fahrereinbindung“, PhD thesis, Technische Universität Darmstadt, Darmstadt, Germany, 2017, pp. 85-87
- [23] A. Cacilo et al. "Hochautomatisiertes Fahren auf Autobahnen–Industriepolitische Schlussfolgerungen" Stuttgart: Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO , 2015.

- [24] International Council on Clean Transportation, "European Vehicle Market Statistics Pocketbook 2017/18." (2017).
- [25] Arbeitsgruppe Straßenentwurf, "Richtlinien für die Anlage von Straßen (RAS), Teil Querschnitte (RAS-Q 96)," Forschungsgesellschaft für Straßen und Verkehrswesen, Bonn.(a)(b)(c)(d), 1996.
- [26] Bundesministerium der Justiz und für Verbraucherschutz, „Anordnung über den Bau und Betrieb von Garagen (GarBBAnO),“ 1990.
- [27] Bundesministerium der Justiz und für Verbraucherschutz, "Straßenverkehrs-Zulassungs-Ordnung (StVZO), " 2012.
- [28] V. Schönemann, M. Duschek, H. Winner, "Maneuver-based adaptive Safety Zone for infrastructure-supported Automated Valet Parking," 5th International Conference on Vehicle Technology and Intelligent Transport Systems (in publication), 2019.

## APPENDIX

**Table 6.**  
***Derivation of functional safety requirements for derived safety goals***

ID	Safety Goal (SG)/ Functional Safety Requirement (FSR)	SG
SG01	Unintended activation of the valet parking function outside of the PAM-controlled parking area shall be prevented.	SG01
FSR1.1	The system shall detect if the automated vehicle's position is located within the handover zone.	
FSR1.2	The system shall detect if the automated vehicle is in standstill.	
FSR1.3	The system shall have the ability to activate and deactivate the valet parking function.	
FSR1.4	The system shall not activate the valet parking function without user permission.	
SG02	The integrity of the communication between the PAM and the vehicle shall be ensured.	SG02
FSR2.1	The system shall control transmitted safety relevant information for authentication, identification, error correcting, and manipulation. Transmitted data shall be encrypted.	
FSR2.1.1	The system shall add to transmitted safety relevant information a check sum, a signature, a time stamp, and an identifier. Transmitted data shall be encrypted.	
FSR2.1	The system shall receive safety-relevant information in time.	
SG04	The vehicle shall not start moving during embarkment and disembarkment.	SG04
FSR4.1	The system shall detect the embarkment and disembarkment of passengers with its sensors.	
FSR4.1.1	The system shall detect persons in the handover and handback zones.	
FSR4.1.2	The system shall detect if doors are closed.	
SG06	The system shall notify a human supervisor in case of a collision or fire.	SG06
FSR6.1	The system shall detect collisions.	
FSR6.2	The system shall detect fire in the parking garage.	
FSR6.2	The system shall stop the valet parking service by applying an emergency brake of automated vehicles in case of a fire.	
FSR6.3	The system shall notify a human supervisor via a Human Machine Interface.	
SG07	The system shall ensure that the vehicle stays within the (statically defined) drivable area during AVP.	SG07
FSR7.1	The system shall detect if a digital map of the parking garage was transferred.	
FSR7.2	The system shall place the automated vehicle's trajectories within the drivable area.	
FSR7.3	The maximum distance error of the automated vehicle's lateral control with respect to the lane center shall not exceed $W_{err,ego}$ .	
SG08	The valet parking function shall be disabled if people are inside the vehicle.	SG08
FSR8.1	The system shall detect whether people are inside the vehicle.	

# OCCUPANT PROTECTION FOR AD CARS – THE PARADIGM SHIFT IN CRASH SAFETY?

**Lotta Jakobsson**  
**Katarina Bohman**  
**Bo Svanberg**  
**Trent Victor**

Volvo Cars  
Sweden

Paper Number 19-0281

## ABSTRACT

When moving towards unsupervised autonomous driving (AD) and the customer expectations of those vehicles, the approach, tools and methods used today in occupant protection assessment are likely not sufficient. Single sitting postures, limited sizes of occupants and crash test set-ups used today will not cover the situations arising. Fundamental changes in evaluation approach and underlying assumptions are foreseen, similar to a paradigm shift.

The objective of this paper is to elaborate on and concretize the research needed, specifically targeting the question: How do we assess the protection of the heterogeneous passenger population in future vehicle crashes enabling occupant protection in unsupervised AD, providing the extended customer benefits of those cars? This paper summarizes relevant state-of-art research in the area and identifies topics for further research focusing on methods and tools for occupant protection assessment.

Future unsupervised AD cars, in addition to future manually driven cars, are likely to be exposed to crashes. Hence, the occupants' need to be protected is obvious, as today. The paradigm shift is driven by and relates to the mindset on car usage and occupant requests. It calls for new ways of addressing crashworthiness evaluation, emphasizing the large effort in research and knowledge creation needed, as well as a new setup in procedures and responsibilities of stakeholders involved. It likely requires addressing expanded crash set-ups, taking the whole event into account (including pre-crash maneuvers), in addition to a larger population of occupants, and a larger range of seat positions, seating configurations and sitting postures. A human-centric approach is proposed as the way forward. Being an alternative to a technology-driven approach (e.g. the SAE levels of automation), the human-centric approach sets the human needs and abilities in focus, and designs technology around them.

Substantial data on sitting postures and behavior in cars today needs to be collected and analyzed, to enhance the interpretation of existing real world data and to form the knowledge foundation towards the future challenges. Furthermore, user studies of future expectations are desired, especially in the light of changes in mobility trends. Simplified crash test dummy designs will not be sufficient. There is a need of continuous development of today's human body models facilitating the expansion in sitting postures and sizes, enhanced injury predictability and capable of simulating pre-crash kinematics. This includes generation of validation data and biomechanics research on injury mechanisms as well as material data such as adipose tissues. Pediatric occupant tools need special attention, in addition to investigating and cooperating around the protection of children in future cars.

In order not to be a stopper for enabling the customer benefits in the development of autonomous drive, the occupant protection challenges need to be addressed. This paper discusses some different aspects of this, however being a paradigm shift, a common discussion and cooperation among stakeholders is needed to cover the whole spectra of aspects.

## INTRODUCTION

Passenger car occupant protection today is evaluated through a limited number of crash tests. Although extensive, a limited number of situations are evaluated through the safety standards, such as the FMVSS and UN ECE. In most cases, the standard specifies a certain crash scenario using a single specific occupant size, in one sitting posture. Child restraints are mainly considered add-on devices, certified using a generic rig. In addition, the consumer test programs (eg. performed by IIHS and EuroNCAP) add to the tests for which most cars are evaluated in. In addition, some additional real-world situations form the platform for occupant protection. However, when difficult to protect, the passengers will be informed and/or restricted in usage, through the user manual or similar. Examples of this are compulsory seat belt use, and information on limitations in protection if the seat is substantially reclined.

When moving towards unsupervised autonomous driving (AD) and the customer expectations with those self-driving cars, the approach, tools and methods used today are likely not sufficient. Single sitting postures, limited sizes of occupants and crash test set-ups used today will not cover the situations arising for occupant protection evaluations.

The objective of this paper is to elaborate on and concretize the research needed, specifically targeting the question: How do we assess the protection of the heterogeneous passenger population in future vehicle crashes enabling occupant protection in unsupervised AD, providing the extended customer benefits of those cars?

## THE PARADIGM SHIFT IN CRASH SAFETY?

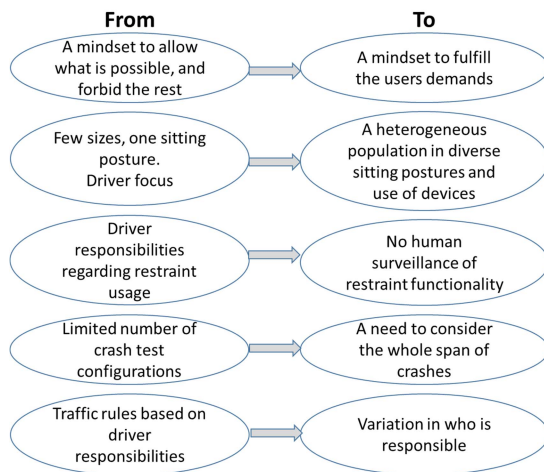
As shown in several studies, the extended customer benefits of future cars include other activities and seating configurations as of today. Extended ways of using the car are foreseen. A qualitative study in Sweden, Jorlöv et al. (2017) showed user expectations of seating configuration facing each other, when travelling together with friends and families for a longer trip. In the shorter trip scenario, the users were less in desire to rotate the seat, but instead aspiring to recline the seat into a more relaxed position enabling relax, sleep, surf the internet, work, or read. Similar findings were found when the study was repeated in Shanghai, China (Östling and Larsson, 2019).

Using online survey with 1,000 respondents in Germany, Fraedrich et al. (2016) investigated use-case-oriented mindsets on several topics for different types of automated concepts, For trips in the city and with shopping and luggage haulage, 'Parking Pilot' was seen as helpful while 'Highway Pilot' was deemed most positive on longer trips and journeys. Both of these allow a driver to disengage from the driving task, but the driver needs to be prepared to take over whenever requested. While, among the steering-wheel free concepts, the so called 'Fully Automated Vehicle' was perceived as being more useful than the 'Vehicle on Demand' (e.g. "robotaxi"), likely related to that a larger share of the respondents could not really picture what that concept was. Long distance trips, longer journeys and cross country trips were the trip types most stated as being helpful for the so called 'Fully Automated Vehicle'.

Hence, new ways of using the cars could include long trips, where the car replaces the train or even the plane. Examples of this was shown with this business model of using the car as a comfortable experience for replacing short-haul flights, such as the Volvo 360c concept (Volvo Cars, 2018). This concept can transform from a comfortable seat, possible to recline in different degrees, into a sleeping compartment, providing an alternative to the flight. The concept is capable of taking you to the meeting in the other city during the night, from door to door; arriving more relaxed than after a flight travel. Some other variants of interior concept models were shown within the Volvo 360c concept. One of them being a business case of an office on wheels, e.g. replacing the need for an expensive office in an attractive city location, enabling use of pick-up time, in addition to use the parked car as the meeting place. The set-up of such a car would include face-to-face seating, table and devices needed for meetings. When addressing the user's demands in these examples, occupant protection challenges includes activities and a range of sitting postures, including lying down.

The other end of new ways of using the cars is exemplified by the 'robotaxi'/'robocab', enabling transportation of passengers during shorter trips. On one hand, the sitting postures and activities might not deviate substantially from today's cars, with the addition of increasing degree of rearward facing. On the other hand, those vehicles will likely pick-up new passengers frequently, and there will be protection challenges accommodating the variety of passengers, including children, in addition to the lack of dedicated on-board human support and supervision.

Introducing new types of vehicles will add to the variations in traffic. It will likely be a combination of mixed traffic, including AD, driver assistance and manually driven cars, and fully autonomous traffic, both having their challenges. Simply, it will provide a larger variety of cars that need to be addressed from a crashworthiness perspective, on top of adding the complexity in the rules/ guidelines on responsibility set-up.



**Figure 1. Examples of aspects in the paradigm shift**

As illustrated in Figure 1, we need to move towards a mindset of addressing the demands of the user, from a reality today of allowing what is possible, and to forbid the rest. An example of this is when reclining the seatback to get a more relaxed position. Although it is possible to recline most front seats today, it is requested in most cars' user manuals to have the seat in an upright position, according to the certified position.

Applying such mindset of addressing customer demands, also includes that everyone should be equally protected, in their chosen sitting posture and activity. Today, the capabilities of the occupant tools are limited, restricting the inclusion in a regulative perspective. There is a need for increased focus on passengers of all sizes and ages, expanding the scope of today with few occupant sizes, one sitting posture and a driver focus.

Today, there is a driver having an overall responsibility (or at least a possibility to have) to ensure usage of restraints. It could be the seat belt or child restraints usage, or simply ensure that the passengers are seated within dedicated space. In the future non-driver environment, this is a challenge that needs to be taken care of.

The limited number of crash test set-ups that the vehicles are certified for today, will likely not be sufficient in the context of tomorrow. As a result of the advancements in occupant protection over the years, more unique cases are needed to be addressed. In addition, the rapid implementation of collision mitigation technologies is seen. Hence, an important topic is the need to handle the large span of crashes, in addition to that the crash will be dependent by the collision mitigation technology, or the autonomous drive systems. Today, the influence of an autonomous pre-crash intervention (e.g. braking or steering) is usually not taken into consideration in the crash testing for evaluating crashworthiness, while they in real world situations could contribute to the occupant protection by reducing speed. From a real-world perspective, today as well as in the future, enabling the automated pre-crash maneuvers to be a part of the design of the crashworthiness evaluation is desired.

As also listed in Figure 1, the role of the driver today to obey the traffic rules plays an important part of the traffic system. In future cars without dedicated drivers, the aspects of this role need to be included in the context as well.

Summing this up, fundamental changes in evaluation approach and underlying assumptions are foreseen, similar to a paradigm shift.

The paradigm shift can be summarized by the following main points:

- The mindset
- The population
- New seating configurations, seat positions and sitting postures
- Responsibilities; who takes over the driver's role in occupant protection?
- The span of crashes and whole crash events to understand and handle

In order not to be a stopper for enabling the customer benefits in the development of autonomous drive, the occupant protection challenges need to be addressed. This paper discusses some different aspects of this, however being a paradigm shift, a common discussion and cooperation among stakeholders is needed to cover the whole spectra of aspects.

## HUMAN-CENTRIC SAFETY

The development towards autonomous drive has been ongoing for more than a decade, starting with driver support systems in car-following situations, followed by autobrake functionality including when turning in front of an oncoming vehicle in intersections (Ljung Aust et al., 2015). Assisting the driver when inattentive or distracted, the auto brake and/or auto steer functionalities will add to the proportion of crashes which are preceded by a maneuver. Hence, moving towards higher degree of automation, a large share of the crashes that occur are likely to have exerted the occupants to a pre-crash kinematics exposure (e.g. from deceleration), caused either by the driver or the technology.

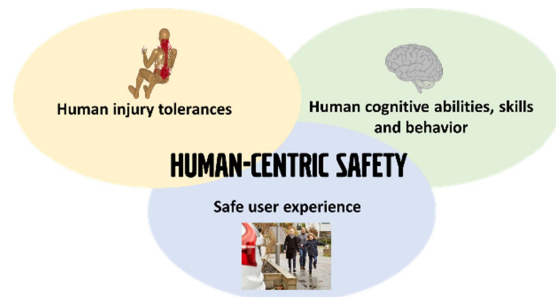
From an occupant protection point of view, it does not make much difference whether a human driver is driving the car, or the machine. Except, for the driver for whom the steering wheel would be included in the protection systems, and the differences in his/her pre-crash kinematics. What really influences the occupant protection needs are the business cases for which the vehicles are designed for (e.g. those described in the 360c concept above); adding customer values influencing the use of the car, including possible sitting postures and seating configurations.

From a human-centric point of view, the SAE levels of automation (SAE J3016) do not provide a relevant framework. This is quite obvious with respect to occupant protection. In addition, even from a driver's role perspective it does not provide sufficient structure. A human-centric approach calls for a need to clarify the driver's role, reducing the confusion on whether the automation is driver assistance which requires driver engagement and responsibility or whether the automation is designed for the operator to safely do something else while relieved from the driving task (unsupervised AD). Driver assistance systems only partly support the driving task (e.g. headway control with some degree of steering assistance), and the driver is still required to supervise the driving and intervene at sensing or actuation limits (e.g. conflict situations). In contrast, unsupervised AD enables either (1) periods of drive-free time where the driver assumes a temporary role of a passenger for a period of time or (2) full trips where the user delegates full control and responsibility to the vehicle (e.g. 'robotaxis'). Until unsupervised AD exists and the driver can switch roles to become a passenger, automation is assistance and the driver is not free to disengage from the driving task to freely do non-driving related activities. The driver must clearly understand when

automation provides a role switching from a driver role to a passenger/operator role.

Thus, different types of automation are associated with and designed for different expectations on the driver or passengers. For example systems could be designed to allow all occupants to sleep, or could be designed to expect a driver to monitor and act when automation encounters its limitations. Clearly, knowledge regarding human limitations is key to setting constraints. Safe, human-centric automation sets the human needs and abilities in focus, and designs technology around this. Safe, human-centric types of automation is to be seen as an alternative to the technology-driven approach, which the SAE levels of automation represents.

Human-centric safety relies on three parts, as illustrated in Figure 2. The three parts are based on areas in which human limitations can help create a platform of knowledge and implementation. 'Human cognitive abilities, skills and behavior' and 'Safe user experience' are the two complements to the more established 'Human injury tolerances'. The latter will be further addressed in this paper.



*Figure 2. Human-centric safety at Volvo Cars*

Human injury tolerances are the foundation in occupant protection. Biomechanics and fundamental principles of protection are the guiding essentials and the paradigm aspects (as presented in prior chapter) and type of automation is a crucial context.

## FOCUS AREAS FOR HUMAN INJURY TOLERANCES

Future unsupervised AD cars, in addition to future manually driven cars, are likely to be exposed to crashes. Hence, the occupants' need to be protected is obvious, as today. As described in previous chapter, the current situation for occupant protection calls for fundamental changes in evaluation approach, underlying assumptions and role of different



stakeholders. This includes new research and application of this research.

Following a summary of *Biomechanical Principles*, this chapter provides a description of the major challenges within knowledge needed to encompass the wide spectra of future cars. The challenges include the *Complete Crash Event*, *Occupant Sitting Postures at Impact* and *Occupant Protection Principles* described in a human-centric perspective.

### Biomechanical Principles

The fundamental biomechanical principles for impact trauma apply. The most important are summarized as follows:

- Restrain strong body parts
- Early coupling
- Distribute load
- Minimize relative motion between body parts
- Reduce contact forces to interior

Strong body parts are pelvis, shoulder, thorax and femur, including axial direction through the lower extremities, including the feet. Protection should be achieved by adapting the force distribution over various body regions by controlling and adapting kinematics and restraint forces. The three-point seat belt is an example of interaction with strong body regions, see Figure 3.

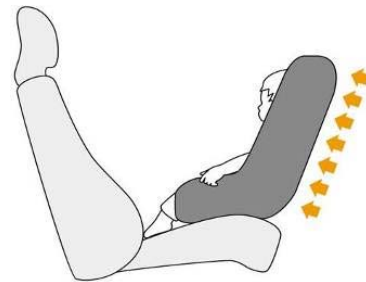


**Figure 3. Example of interacting with strong body parts. The three point seat belt should be positioned over the pelvis and across the chest and shoulder.**

As emphasized by (Kent and Forman, 2015), early coupling of the occupant is beneficial. This means achieving occupant deceleration similar to the vehicle deceleration, in contrary to an unrestrained occupant that does not benefit from the vehicle deceleration

and will thus experience higher forces when contacting. This occupant/vehicle coupling can be referred to as “ride down of the vehicle deceleration”. By the use of the whole time of the crash and to distribute the load during the whole event, the internal loadings will be less. The distance include both interior space and vehicle crush zone, in addition to the contribution of crash mitigation time. It is essential to maintain the coupling during the complete crash event (also including a pre-crash maneuver), to ensure control of the occupant kinematics and force control.

Distributed loads are essential to minimize deformation to the body tissues and reduce loads between body parts. As an example, the spine is sensitive to shear forces if applied locally, but can withstand high forces if distributed over a larger area (Crandall et al., 1997, Kent et al., 2001). By distributing the load over e.g. the whole ribcage, or by supporting the head and torso together, as for astronauts when launched in space, or the principles of a rearward facing child seat (Aldman, 1964, Figure 4), needed protection is achieved.



**Figure 4. A child in a rearward facing seat, illustrating the protection principle of distributed loads, in case of a frontal impact.**

The principle of minimizing relative motion between body parts is essential. Unbalanced head and neck kinematics may result in neck injuries, including whiplash injuries (Siegmund et al., 2009). Unbalanced pelvis and upper torso kinematics may contribute to submarining (Adomeit and Heger, 1975). It is vital to control kinematics and restraint forces to manage the relative motion between body parts.

If the distances are not enough for a smooth “ride down of the vehicle deceleration”, the forces when the occupant impacts the interior surface should be controlled. Padding and airbags are means to control the stiffness of interior surfaces. The challenge is higher when short distance between the occupant and the interior, such as for an occupant today in a side impact. To control contacts include means to help protect the occupant, e.g. knee contact with the

interior, assisting in the early coupling. Car body strength is an enabler to help keep the intruding structure (magnitude and velocity) into the vehicle compartment low, and thereby the loading to the occupant.

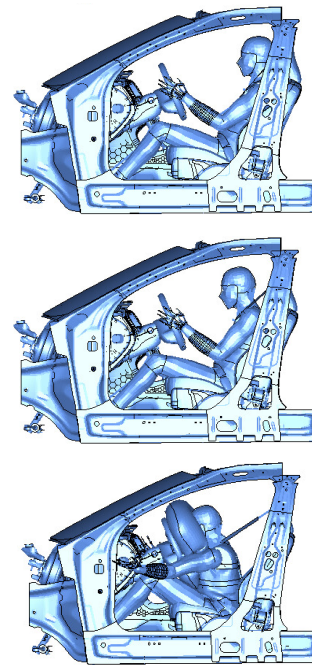
### Complete Crash Event

In most of the crashes, the AD car will likely perform a maneuver prior to the crash targeting avoidance or mitigation. Already today, occupants are exposed to braking and steering prior to a crash, and technology influencing the crash configuration is available. However, in the standardized crash testing today, the cars are not exposed to pre-crash maneuvers, and the crash test dummies used are limited in their capabilities. As example, the crash test dummies designed for frontal impact tests are not capable of capturing biofidelic kinematics nor injury mechanisms in side impacts. None of them are designed for biofidelic kinematics in braking or steering movements.

There are two main concerns in this area. Firstly, it is relevant to include the influence of pre-crash kinematics into the occupant protection evaluation. In that way, the collision mitigation technology can be evaluated as part of the occupant protection. A simple example is how an autobrake in car-following situations can serve the purpose of reducing the occupant impact exposure in the same way as a well-designed energy absorption of the front structure. Occupant tools are needed that are capable of humanlike kinematics throughout a complete crash event, including the preceding event. Secondly, it is relevant to develop methods and tools that are omnidirectional in kinematics and injury prediction capabilities, i.e. possible to use independent of direction of impact. This will enable the possibility to design collision mitigation technologies that influence the crash configuration as a part of the occupant protection. An example of this is that for an intersection autobrake system, the activation algorithms can be further developed together with the interior restraint systems and car body design.

Today, the most capable tools to address these concerns are human body models (HBM). As compared to crash test dummies, HBMs have biofidelic sensitivity to different loading directions and differences in acceleration levels and can represent different occupant sizes, gender, and anthropometry. In addition, if muscle tonus is implemented in the models, so called Active HBMs, they have the potential to predict the occupant response in pre-crash and emergency events (Östh et al. 2015). An example of an active HBM capable of

occupant simulation comprising a maneuver and crash event was used in studies on braking and/or lane-change followed by frontal impacts (Östmann and Jakobsson, 2016, Saito et al, 2016, Pipkorn and Wass, 2017, Östh, 2018). Figure 5 is an illustration of the model and the sequences, taken from the study by Östmann and Jakobsson (2016).



**Figure 5. Illustration of an active HBM capable of simulating a brake event prior to a crash event. Top: initial position, Middle: at time of impact, Bottom: at most forward head position**

Methods to evaluate complete crash events need to be in focus for future occupant protection assessment. The methods and tools should be capable of including maneuvers and simulating occupant movements prior to the crash, in addition to being capable of injury prediction, independent of direction of impact.

### Occupant Sitting Postures at Impact

In real world crashes, the occupants' sitting postures at impact are influenced by the selected sitting posture and the sitting posture as a result of the vehicle motion prior to the crash. This was described by Stockman (2016) and Jakobsson et al. (2017), focusing children in the rear seat. Driving studies with children showed that children choose a range of common user positions, which includes upright sitting posture, as well as forward leaning positions, including bending their necks forward when using

e.g. electronic hand-held devices (Osvalder et al., 2013, Andersson et al., 2010, Jakobsson et al., 2011, Arbogast et al., 2016, Cross et al., 2017). This is referred to as voluntary sitting postures, driven by comfort and the activities they engage into. Studies with children exposed to steering and braking maneuvers illustrate examples of non-voluntary sitting postures, moving the occupants forward or sidewise, even moving out of the shoulder belt (Stockman et al., 2013, Bohman et al., 2011b, Baker et al., 2017, Baker et al., 2018). It was hypothesized that the influence of the sitting posture at time of impact could explain why children sustained head impact related injuries, although they were correctly restrained according to the dataset analyzed (Bohman et al., 2011a). Based on this work, Jakobsson et al. (2017) emphasized that it is essential to monitor occupant postures and kinematics for enhanced understanding of protection needs at time of impact.

There is limited knowledge on voluntary sitting postures of front seat adult passengers, with only a few studies available on the topic. Zhang et al. (2004) made a survey with 560 participants. They identified 29 sitting postures for adult passengers and estimated the frequency of those. Upright selected posture was the most common (45%), followed by leaning inboards (8%) and leaning outboards towards b-pillar (8%). In an observational study by Bingley et al. (2005), front seat occupants were observed from the outside of the car. Passenger head centerline to vehicle centerline was collected, in addition to use of seatbelts, hand positions and activities.

Studies on front seat passenger kinematics in evasive maneuvers have been performed with the primary purpose of creating validation corridors for active human body models (Ólafsdóttir et al., 2013, Ghaffari et al., 2018). The studies provide evidence on non-voluntary movements in braking and lane-change maneuvers. Although not comparable in set-up, the adult front seat passengers seemed more restricted in sidewise movements, as compared to the child rear seat passengers, likely due to more side support by the seat in the front seat, and probably more likely to support themselves with the feet than the children were .

Sitting posture influences injury outcome in case of a crash, in vehicles today. McMurry et al. (2018) analyzed data from CIREN and NASS-CDS, and found an elevated injury risk for occupants registered in the data as in an out-of-positions, e.g. reclined position, as compared to the occupants registered as in-position. Real world case studies have shown the limitations of protection in reclined sitting postures in existing cars, causing submarining resulting in

injuries to the abdomen as well as cervical spine (Jeffery and Cook 1991, Rehm and Goldman 2001, Dissanaik et al. 2008). Investigating thoraco-lumbar spine injury mechanisms, it was seen that a forward bended occupant posture, due to kinematics in run-off road events, influenced the occurrence of spine injuries at the sudden stop (Jakobsson et al., 2006).

Using multibody human body models, Bose et al. (2010) investigated influence of sitting posture on injury outcome in frontal impacts, as one of four occupant parameters. They found several of the eight sitting postures evaluated to increase the risk of injury. Another study, using finite element human body models, showed that reclined sitting postures with state-of-art restraint system increase the risk of submarining (Lin et al. 2018).

Substantial data on sitting postures and behavior in cars today needs to be collected and analyzed, to form the knowledge foundation for the future challenges. Furthermore, user studies of future needs and expectations should be conducted, especially in the light of changes in mobility trends

### **Occupant Protection Principles**

Traditionally, occupant protection principles have been related to principle direction of force (PDOF) of the crash and with the seats facing forward of the direction of travel. In future seating configuration, we may see seats rotated in various degrees, taking any direction up to turned rearward facing relative to the travel direction. Hence, it is more logical and constructive to relate the protection principles to the direction of force for which the occupant will be exposed to. This means taking into account both PDOF of the vehicle and the seating configuration. Therefore, we will refer to e.g. “forward”, “rearward”, “lateral”, “oblique” movement of the occupant, irrespectively what direction the occupant and the seat is facing in the car. This is an example of human-centric approach, referring to the human instead of the car or crash.

No matter direction of occupant movement, the protection should to be designed around the occupant, e.g. both the seat belt as well as the seat itself. Future technical solutions are likely different from today’s in order to work in new seating configuration. New seating configurations may include other direction of travel than today, as well as traditional support surfaces such as the instrument panels may not be available. The purpose of the description of the occupant protection principles in this chapter is to describe and exemplify the human-

centric approach, which should be valid, irrespectively of the boundary conditions.

Restraining the occupant in a pure forward movement (sagittal-anterior, such as a forward facing occupant in a frontal impact), the hipbone (pelvis) is essential to catch – allowing for controlled forward motion of the upper body. The conventional three point seat belts work in line with these principles. An essential part is the lap belt anchorage placement below the hips, as stated already when introduced in 1959 (Bohlin, 1964 and 1981). The seat structure is also a fundamental part of the protection. Airbags could be used to reduce relative motions between body parts and to distribute the load, but they may be designed differently than in today's vehicles. Load paths using the knees or feet could be effective means, especially when the occupant is reclined, helping to restrain the forward motion of the pelvis. It will be more challenging when using conventional restraints since it is more difficult to restrain a pelvis when it is rotated rearwards from its initial position. The real world case studies reported on injured passengers exposed to frontal impacts when substantially reclined confirm the challenges of today's technologies (Jeffery and Cook, 1991, Rehm and Goldman, 2001, Dissanaik et al. 2008).

Restraining the occupant in a pure rearward movement, has been a successful way of reducing injuries to the youngest children. By distributing the load of upper torso, neck and head over the whole the seat back (Figure 4), risk of injury is reduced. It is essential that the occupant remains supported by the seat back and head restraint during the whole crash, and does not slip off the seat back or head restraint, in order to control the relative motion between the head and torso.

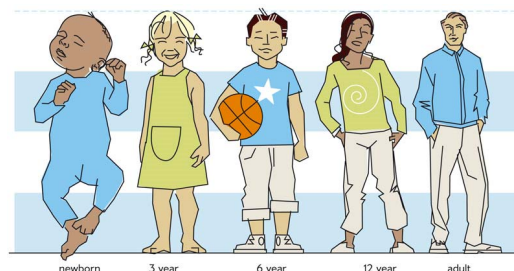
Protecting the occupant in a pure lateral movement and all oblique combinations follows the fundamental biomechanical principles, as presented above. However, depending on the seating configuration and the surrounding interior structure, it will be more or less challenging. Likely, these situations are driving the most challenging needs of developments of tools, methods and new restraint strategies.

Studies have already provided insights into the challenge of maintaining the occupant in its protection as the occupant movement becomes oblique (Kitagawa et al. 2017). Already in today's vehicles, oblique frontal impacts, as well as far-side side impacts, for forward facing occupants are demanding in terms of controlling the kinematics of the upper torso and head. The way forward is to base the protection on the biomechanical principles, including an early coupling of the occupant,

restraining the strong body parts and distribute the loads. Likely, this means that the seat belt plays the fundamental role of protection but may need to be supported by other technical solutions in order to control the loading to the occupant and the kinematics of the occupant.

**Specific concerns for children:** Two major areas of concerns are special for children, otherwise the basic principles of occupant protection are valid, and independent of size and age. The two areas are neck vulnerability for the infants and toddlers, and pelvic bone size and shape for children up to puberty.

The infants and toddlers are especially vulnerable for relative motion between the head and the upper body. The special concern for this group is due to a combination of relatively large head size/weight (see Figure 6) and an immature neck with more horizontal vertebra which grow stronger when bone is replacing cartilage. It is therefore essential that the forces are distributed over a larger part of body, which can be achieved by riding in a seat with the back towards the travel direction (illustrated in Figure 4), also having side supports close to the body for lateral support.



**Figure 6. Body proportions for different ages**

For children with relatively smaller pelvic body, using an adult designed seat belt, usually need to be adjusted in height to benefit from the same principles in the forward movement as explained above. However, from a principle perspective there are no major difference, although the shorter limbs and body regions call for comfort adjustments to accommodate a comfortable ride in the protected mode. As an example, if the seat cushion is too long for the child's legs to be comfortably bended, he/she will likely slouch forward whereby the intended interaction with the seat belt is missed.

## DISCUSSION

The paper suggests that fundamental changes in evaluation approach and underlying assumptions are foreseen, similar to a paradigm shift. The paradigm shift is driven by and relates to the mindset on car

usage and occupant requests. It calls for new ways of addressing crashworthiness evaluation, emphasizing the huge effort in research and knowledge creation needed, as well as a new set-ups in procedures and responsibilities of stakeholders involved. It likely requires addressing expanded crash test set-ups, taking the whole event into account, in addition to a larger population of occupants, and a larger range of seat positions and sitting postures.

This is not the first time the crashworthiness challenges in unsupervised AD are addressed. In 2016, NHTSA published a Federal Automated Vehicles Policy as agency guidance to speed the delivery of an initial regulatory framework and best practices to guide manufacturers and other entities in the safe design, development, testing, and deployment of highly automated vehicles (NHTSA, 2016). Occupant protection, as part of crashworthiness, was addressed as one of 15 safety assessment topics. They stated that manufactures and other entities should exercise and demonstrate due care to provide countermeasures that will fully protect all occupants given any planned seating or interior configurations, and the tools to be used need not be limited to physical testing but also could include virtual tests with vehicle and human body models.

In Europe the focus on AD challenges is also high. Thatcham states that the rapid development of AD may force regulators to consider alternative and faster regulatory approaches than today, highlighting the need of fully redundant systems for robust automated driving solutions and how to prevent systems sold as 'Automated' when they require driver intervention to be safe (Thatcham, 2017). Euro NCAP describes in their road map 2025 a focus on the assessment of automated driving systems and driver/vehicle interaction (Euro NCAP, 2017). However, at this point neither Thatcham nor EuroNCAP address how occupant protection in AD cars should be assessed.

Safe Kids Worldwide organized a Blue Ribbon panel on children in autonomous vehicles, since they identified there is a great focus on adults and autonomous vehicles but there is lack of understanding the unique needs of children in this context. (Safe Kids Worldwide, 2018). They summarize five areas of actions encompassing safety standards, usability testing, inclusive design, appropriate supervision and marketed standards, emphasizing that children should be included in all phases. The report concludes that it is time to act straightaway, as it is necessary to build the knowledge of the needs of the children and the

families now, enabling them to be addressed in the ongoing rapid development of the technology.

Future unsupervised AD cars are likely to be exposed to crashes. The AD cars will be mixed with human-driven cars. Hence, the occupants' need to be protected is obvious. This paper suggests a human-centric approach as the way forward to address fundamental changes in evaluation approach, underlying assumptions and role of different stakeholders. This includes new research and application of this research. A human-centric approach applied to occupant protection is based on human injury thresholds. It addresses the needs of the occupants based on who they are, how they are sitting and what forces they are exerted to, according to the human reference system. It is also about a mindset, of changing from e.g. forward facing occupant in frontal impact; to understanding the occupant's sitting posture at impact, as a result of the whole crash event, and referring the protection principles to the human instead of the interior setting of the car or the impact type.

Based on the state-of-art tools and methods today, substantial knowledge gaps are evident, which we need to address through collective research in several areas. This paper highlights three main areas important for occupant protection assessments; the whole crash event, the sitting postures at impact and challenges regarding protection principles applied for relevant real world situations.

Occupant protection in cars is continuously improving. The large steps in injury reduction taken in the past, exemplified by introduction of e.g. seat belts, airbags, advanced front vehicle structures and side impact protection structure, are likely to be less frequent in the future. Instead, as result of the efficient work, the remaining priorities are more unique cases, in which tools and methods replicating a larger variety of crash and occupant characteristic are necessary. In addition, the rapid implementation of collision mitigation technologies calls for methods and tools including the pre-crash phase into the evaluation. Hence, methods and tools to evaluate complete crash events need to be in focus, considering maneuvers and occupant kinematics prior to the crash, in addition to all directions of impact.

Today, passenger cars are mainly designed to protect upright sitting occupants, who are centralized in their seat. At least, this is the way the crash test dummies are designed to be used. To change this and to form the knowledge foundation towards the future challenges, research in this area is needed both to interpret the real world data today, i.e. what are the

ranges of postures that are reflected by the data in the databases, as well as to understand future priorities.

Different activities will result in different sitting postures, for example a comfortable resting position will be different from a working position. It should be acknowledged, that changing sitting posture is part of our natural way of gaining comfort. To enable protection, the different postures need to be understood, and if not possible to protect based on available technology, ways of guiding the occupant into a preferred posture based on comfort should be in focus. Hence, data on sitting postures are also essential to understand the preferences of humans and how to address their preferences with respect to protection in the best way.

Substantial data, especially on passengers, needs to be collected during standard car drives, in addition to evasive maneuvers, quantifying differences between individuals as well as situations. Manual analysis of naturalistic driving studies is time consuming. Development of more automatic analysis methods has recently been initiated (Reed et al., 2018), and should be further enhanced capturing details on sitting postures as well as restraint positions.

Furthermore, user studies of future needs and expectations should be conducted, especially in the light of changes in mobility trends. Staged studies investigating seating configurations and sitting postures in relation to future perceived needs when moving towards higher degree of automation will help guide the development of functionalities not available in traffic today. Jorlöv et al. (2017) and Östling and Larsson (2019) are examples of such studies on seating configurations and activities.

Being the most capable tools to address the whole crash event and inherently designed with human properties, HBMs including muscle activation are today the most promising tools. Already today it can be used for combination of pre-crash events and impacts in different directions. This is needed when moving towards including the crash mitigation technologies being a part of the occupant protection. Just as important as being capable of recreating human kinematics in different types of maneuvers, is the ability to compare injury prediction responses resulting from different directions and contact points of a body region, resulting from a change in impact configuration due to the collision mitigation technology. Further, there is a need to include similar research for child occupant tools and to develop relevant physical tools (crash test dummies) as complement enabling hardware validation.

Substantial research is required to support the development of the occupant tools needed in the future. The research includes foundation for validation, development of relevant injury prediction, in addition to understand and take into account individual differences of all aspects.

New morphing techniques of HBM opens up the possibility of developing the families of HBM that can represent the population to a much wider extent, than the limited sizes of crash test dummies and HBMs currently available. There is need of research to determine what that population should look like, and if different families are needed for the difference in crashes and seating configuration. Knowledge is needed to understand who is vulnerable in the specific situation, but also to complement with other representatives of the population to ensure the wide range of occupants will be protected. The families include children as well. The biofidelic validation of existing pediatric tools (crash test dummies and HBMs) is lagging behind the work ongoing for adult tools, due to lack of data.

The morphed family needs to be validated, since it is not enough to morph the occupant to a relevant shape and size. The need of validation data include kinematics and muscle responses in maneuvers in addition to biomechanical data providing validation corridors for occupant movement directions and interactions. Especially there is a lack of validation data for occupants in a non-upright seat position.

NHTSA recently started a research program, including generation of validation data in reclined seat positions. Pure forward occupant movements and pure rearward occupant movements (simulating rear facing occupant in a frontal impact) are within the scope (Reed, 2019). In addition to the reclined postures, the inclusion of high severity rearward occupant movement is new. The latter providing a good complement to the available extensive rear-end impact research at lower severity. In addition, and just as important, validation data in lateral and oblique directions is urgently needed.

Applying the protection principles on new seating configurations and seat positions is challenging and it will require more advanced tools. In the development of new types of restraints, the tools are needed to help predict occupant interaction in a variety of sitting postures and occupant sizes. Hence, detailed models and biomechanical data is required, especially for the load bearing body parts. Restraint interaction with the pelvis is essential as this is a basic structure to use as load path. Interaction with the shoulder will likely continue to be an essential part of the protection system, ensuring the occupant remains restrained,

especially in oblique occupant movements. The load to lumbar spine may be increasing depending on how the load path in reclined sitting positions can be solved, and it is essential to have tools that can predict loads to the spine. Another challenge is valid representation of soft tissues, which today is very limited in any of the tools used for occupant protection. One example is the importance of adipose tissues influencing the position of the restraints, as well as the time of restraint interaction to the skeleton. Reed et al. (2012 and 2013) showed how the lap belt will be positioned more forward of the pelvis bones if the occupant has high body mass index (BMI) compared to occupants with normal BMI.

For children, smart adaption of protection is a focus area with increasing importance in the future. Today the children's needs are addressed by adding child restraint systems into the vehicle. The majority of these solutions are aftermarket solutions, while only a few cars offer built-in solutions, such as booster seats (Jakobsson et al., 2007). In line with the increased shared mobility, it is essential that the solutions for child occupant protection are convenient, easy to use and provide adequate safety in case of a crash. Jakobsson et al. (2017) summarized that from a real-world safety perspective, the vehicle and child restraint should be designed together targeting a range of acceptable common user positions; sitting postures preferably guided by comfort and positive means. Such designs will ensure robust function of the protection systems for these young occupants, and advance the development of countermeasures that protect children in real-world crashes, also including dynamic events prior to a crash. Again, a human-centric approach understanding the users' specific needs, is likely the most successful way.

We foresee a paradigm shift in occupant protection. It is partly driven by the unsupervised AD, especially concerning change in mindset of enabling an expanded user request, exemplified by sitting postures and activities in the cars. It is also driven by the fact that less people are injured in cars today, and therefore improved methods and tools are needed to address the remaining cases. The paradigm shift will impact the assessment tools and underlying knowledge for occupant protection, as elaborated on in this study. It will require synchronized cooperation among stakeholders to collect and create the needed real world data, validation data and tools. In addition we need to raise our view and perspective in the area. Specifically, it requires a consensus that we together need to take this step on development of assessment methods, as well as taking on the discussion of the whole picture, exemplified by issues like who will

take care of the occupant protection relevant tasks as the driver has today.

## REFERENCES

- Adomeit D, Heger A., Motion sequence criteria and design proposals for restraint devices in order to avoid unfavorable biomechanic conditions and submarining, *19<sup>th</sup> Stapp Car Crash Conf*, SAE-751146, 1975:3150--9
- Andersson M, Bohman K, Osvalder A-L. Effect of booster seat design on children's choice of seating positions during naturalistic riding. *54<sup>th</sup> AAAM Annual Conference, Annals of Adv in Automot Med*, 54, 2010:171-80
- Aldman B. A protective seat for children – Experiments with a safety seat for children between one and six, *8<sup>th</sup> Stapp Car Crash Conf.*, SAE-640855, 1964:320-328
- Arbogast KB, Kim J, Loeb H, Kuo Johnny, Koppel S, Bohman K, Charlton J, Naturalistic driving study of rear seat child occupants: Quantification of head position using a Kinect™ sensor. *Traffic Inj. Prev.* 17(1), 2016: 168-74
- Baker G, Stockman I, Bohman K, Jakobsson L, Svensson M, Osvalder A-L, Wimmerstedt M. Kinematics and shoulder belt engagement of children on belt-positioning boosters during emergency braking events. *IRCOBI Conference*, Antwerp, Belgium, 2017
- Baker G, Stockman I, Bohman K, Jakobsson L, Osvalder A-L, Svensson M, Wimmerstedt M. Kinematics and shoulder belt engagement of children on belt-position boosters during evasive steering maneuvers. *Traffic Inj. Prev.* 19:sup1, 2018
- Bingley L, Richard M, Gabrielle C. Determination of real world occupant postures by photo studies to aid smart restraint development. *19<sup>th</sup> Int. Tech. Conf. Enhanced Safety Vehicle, ESV*, Paper No. 2005-0319, Washington DC, USA, 2005
- Bohlin NI. Studies of three-point restraint harness systems in full-scale barrier crashes and sled runs. *8<sup>th</sup> Stapp Car Crash Conf*, SAE-640854, 1964:258-319
- Bohlin NI. Refinements of restraint system design – A primary contribution to seat belt effectiveness in Sweden, *International Symposium on Occupant Restraint, AAAM*, Toronto, Ontario, Canada, June 1-3, 1981
- Bohman K, Arbogast K, Boström O. Head injury causation scenarios for belted, rear-seated children in frontal impact, *Traffic Inj. Prev.* 12(1), 2011a:62-70
- Bohman K, Stockman I, Jakobsson L, Osvalder AL, Bostrom O, Arbogast KB. Kinematics and shoulder belt position of child rear seat passengers during vehicle maneuvers. *55<sup>th</sup> AAAM Annual Conference, Annals of Adv in Automot Med*, 55, 2011b:15-26.
- Bose D, Crandall JR, Untaroiu CD, Maslen EH. Influence of pre-collision occupant parameters on injury outcome in a frontal collision. *Accid. Anal. Prev.* 42, 2010
- Crandall J, Bass CR, Pikey WD, Miller HJ, Sikorski J, Wilkins M. Thoracic response and injury with belt, driver side airbag and force limited belt restraint systems, *Int J Crashworthiness*, 2(1) 1997:119-32

- Cross S, Charlton J, Koppel S. How do child occupants really behave during motor vehicle travel, *15th International Conference on Protection of Children in Cars*, Munich, Germany, 2017
- Dissanaike S, Kaufman R, Mack CD, Mock C. The effect of reclined seats on mortality in motor vehicle collisions, *J Trauma*, 64(3), 2008
- Euro NCAP, EuroNCAP 2025 Roadmap, EuroNCAP, June 2017. <https://cdn.euroncap.com/media/30700/euroncap-roadmap-2025-v4.pdf> (Downloaded 20190219)
- Fraedrich E, Cyganski R, Wolf I, Lenz B. User perspectives on autonomous driving. A Use-Case-Driven Study in Germany. *Arbeitsberichte, Heft 187, Geographisches Institut, Humboldt-Universität zu Berlin, Germany*, ISSN 0947 – 0360, 2016
- Ghaffari G, Brolin K, Bråse D, Pipkorn B, Svanberg B, Jakobsson L, Davidsson J. Passenger kinematics in lane change and lane change with braking manoeuvres using two belt configurations: standard and reversible pre-tensioner. *IRCOBI Conference*, IRC-18-80, Athens, Greece, 2018
- Jakobsson L, Bergman T, Johansson L. Identifying thoracic and lumbar spinal injuries in car accidents. *IRCOBI Conference*, Madrid, Spain, 2006
- Jakobsson L, Wiberg H, Isaksson-Hellman I, Gustafsson J. Rear seat safety for the growing child – A new 2-stage integrated booster cushion. *20th Int. Tech. Conf. Enhanced Safety Vehicle, ESV*, Paper No. 07-0322, Lyon, France, 2007
- Jakobsson L, Bohman K, Stockman I, Andersson M, Osvalder AL. Older Children's Sitting Postures when Riding in the Rear Seat. *IRCOBI Conference*, Krakow, Poland, 2011
- Jakobsson L, Bohman K, Svensson M, Wimmerstedt M. Rear seat safety for children aged 4-12: Identifying the real-world needs towards development of countermeasures, *25th Int. Tech. Conf. Enhanced Safety Vehicle, ESV*, Paper no. 17-0088, Detroit, USA, 2017
- Jeffery RS, Cook PL. Seat belts and reclining seats, *Injury: the British Journal of Accident Surgery* 22(5), 1991
- Jorlöv S, Bohman K, Larsson A. Seating positions and activities in highly automated cars – A qualitative study of future automated driving scenarios. *IRCOBI Conference*, Antwerp, Belgium, 2017
- Kent R, Forman J. Restraint biomechanics, *In: Yoganandan N. Accidental Injury*, Springer, 2015:116-118
- Kent RW, Crandall JR, Bolton J, Prasad P, Nusholtz G, Mertz H. The influence of superficial soft tissues and restraint condition on thoracic skeletal injury prediction. *Stapp Car Crash Journal*, 45, SAE-2001-22-008, 2001
- Kitagawa Y, Hayashi S, Yamada K, Gotoh M. Occupant kinematics in simulated autonomous driving vehicle collisions: Influence of seating position, direction and angle, *Stapp Car Crash Journal*, 61, 2017:101-155
- Lin H, Gepner B, Wu T, Forman J, Panzer M. Effect of Seatback recline on occupant model response in frontal crashes, *IRCOBI Conference*, Athens, Greece, 2018
- Ljung Aust M, Jakobsson L, Lindman M, Coelingh E. Collision avoidance systems - Advancements and efficiency, *SAE World Congress*, SAE- 2015-01-1406, 2015
- NHTSA. Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety, *NHTSA, U.S. Department of Transportation (DOT)*, USA, 2016 <https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016/> (downloaded 2019-03-03)
- McMurry TL, Poplin GS, Shaw G, Panzer MB. Crash safety concerns for out-of-position occupant postures: A look toward safety in highly automated vehicles. *Traffic Inj. Prev.*, 19(6), 2018:582--7.
- Ólafsdóttir JM, Östh J, Davidsson J, Brolin K. Passenger kinematics and muscle responses in autonomous braking events with standard and reversible pre-tensioned restraints, *IRCOBI Conference*, Sweden, 2013
- Osvalder AL, Hansson I, Stockman I, Carlsson A, Bohman K, Jakobsson L. Older children's sitting postures, behaviour and comfort experience during ride – A comparison between an integrated booster cushion and a high-back booster, *IRCOBI Conference*, Gothenburg, Sweden, 2013
- Pipkorn B, Wass J (2017). Pre-crash triggered pretensioning of the seat belt for improved safety. *25th Int. Tech. Conf. Enhanced Safety Vehicle, ESV*, Paper no. 17-0104, Detroit, USA, 2017
- Reed M, Ebert-Hamilton S, Rupp J. Effects of obesity on seat belt fit. *Traffic Inj. Prev.*, 13(4), 2012:364-72.
- Reed MP, Ebert SM, Hallman JJ. Effects of driver characteristics on seat belt fit. *Stapp Car Crash Journal*, 57, 2013:43-57.
- Reed MP, Park B-K, Ebert S, Hallman JJ, Sherony R. Marker-less tracking of head motion in abrupt vehicle maneuvers, *IRCOBI Conference*, Athens, Greece, 2018
- Reed M. Personal communication, March 5, 2019
- Rehm CG, Goldman K. Seat belt and car seat in a reclined position: A dangerous combination, *J Trauma*, 51(6), 2001
- Safe Kids Worldwide. Children in Autonomous vehicles, Blue Ribbon Panel. *Safe Kids Worldwide*, USA, 2018. [https://www.safekids.org/sites/default/files/children\\_in\\_av-brp-report-2018.pdf](https://www.safekids.org/sites/default/files/children_in_av-brp-report-2018.pdf) (Downloaded 20190219)
- Saito H, Matsushita T, Pipkorn B, Boström O Evaluation of frontal impact restraint system in integrated safety scenario using Human Body Model with PID controlled active muscles, *IRCOBI Conference*, IRC-16-35, Malaga, Spain, 2016
- Siegmund GP, Winkelstein BA, Ivancic PC, Svensson MY, Vasavada A. The anatomy and biomechanics of acute and chronic whiplash injury. *Traffic Inj. Prev.* 10(2), 2009
- Stockman I, Bohman K, Jakobsson L, Brolin K. Kinematics of child volunteers and child anthropomorphic test devices during emergency braking events in real car environment, *Traffic Inj. Prev.*, 14(1), 2013: 92-102
- Stockman I. Safety for children in cars – Focus on three point seatbelts in emergency events. *Doctoral Thesis*, Department of Applied Mechanics, Chalmers University of Technology, ISBN: 978-91-7597-468-2, 2016



- Thatcham, Regulating Automated Driving, *Thatcham Research*, <https://news.thatcham.org/documents/regulating-automated-driving-a-uk-insurer-view-69167>, UK, Aug 2017
- Volvo Cars, Volvo Cars' new 360c autonomous concept: reimagining the work-life balance and the future of cities, *Press Release by Volvo Car Group*, 2018 <https://www.media.volvocars.com/global/en-gb/media/pressreleases/237020/volvo-cars-new-360c-autonomous-concept-reimagining-the-work-life-balance-and-the-future-of-cities> (Downloaded 20190219)
- Zhang L, Chen L, Vertiz A, Balci R. Survey of front passenger posture usage in passenger vehicles. *SAE 2004 World Congress & Exhibition*, SAE-2004-01-0845, Detroit, USA, 2004
- Östh J, Marín Ólafsdóttir J, Brolin K, Davidsson J, Pipkorn B, Jakobsson L, Törnvall F, Lindkvist M. Muscle Activation Strategies in Human body Models for the Development of integrated Safety, *24th Int. Tech. Conf. Enhanced Safety Vehicle, ESV*, Paper no. 15-0345, Gothenburg, Sweden, 2015
- Östh J. Implementation and Application of Human Body Models for Vehicle Development. *7th International Symposium: Human Modeling and Simulation in Automotive Engineering, carhs*, Berlin, Germany, Oct. 18 - 19, 2018
- Östling M, Larsson A. Occupant activities and sitting positions in automated vehicles in China and Sweden, *26th Int. Tech. Conf. Enhanced Safety Vehicle, ESV*, Paper no. 19-0083, Eindhoven, Belgium, 2019
- Östmann M, Jakobsson L. An Examination of Pre-crash Braking Influence on Occupant Crash Response using an Active Human Body Model; *IRCOBI Conference*, IRC-16-37, Malaga, Spain, 2016

# **Research of Minimize Steering Grasping to Take over Driver from System in Advance Safety System**

**Shotaro Odate**

**Naohiro Sakamoto**

Honda R&D Co., Ltd Automobile R&D Center

Paper Number 19-0039

## **ABSTRACT**

Advances being made today in electronic technology are evolving the processes that make vehicles more intelligent, in addition to realizing safer and more comfortable driving. Lane departure prevention systems are also becoming practical due to millimeter-wave radar and onboard forward observation cameras. The U.S. Department of Transportation has implemented a National Automotive Sampling System Crashworthiness Data System (NASS/CDS) for North America that found 10,743 accidents in 2016 involved departure from the road. There were 12,043 fatalities in these accidents. Lane departure prevention systems are expected to make a major contribution to reducing accidents of this kind. Advances are also being made in the development of systems that will enable autonomous driving, and the system to ensure safe and comfortable vehicle operation is being developed.

These systems embody great potential for reducing the number of accidents caused by road departure. However, the validity of the systems is largely dependent on the level of acceptance by drivers. System validity will be determined by when they provide driving assistance, how much relaxation will be permissible on the driver's side, given that the driver needs to maintain contact with the steering wheel, and the extent of assistance provided by the system.

This paper will discuss research on the minimum necessary contact and contact strength with the steering wheel on the part of the driver when the autonomous system is in operation. Using a six-axis driving simulator employing an actual vehicle, the research conducted tests involving 22 test subjects, and studied the relationship between the status of the driver's contact in terms of steering angle speed and steering angular velocity and vehicle behavior when the system failed. The authors analyzed the influence on avoidance behaviors depending on the state in which the steering is held or not grasped when a person performs avoidance behavior.

When the steering torque activates, such as in a curve, the reaction will be faster if drivers touch the hand. In the case of a straight road with no steering torque activating, the result of the difference in reaction time depending on whether they are gazing at the front, regardless of grasping or non-grasping, has been clarified from this research.

## **INTRODUCTION**

The advances being made in electronic technology today are causing evolution in the processes of making vehicles more intelligent. This is realizing greater safety and comfort in driving. In addition, millimeter-wave radar and forward-mounted cameras for observing the area around the vehicle are making lane departure prevention systems feasible. The US Department of Transportation has implemented a National Automotive Sampling System Crashworthiness Data System (NASS/CDS) that found 10,743 accidents in 2016 involving departure from the road [1]. These accidents involved 12,043 fatalities. It is expected that lane departure prevention and autonomous traveling system recognizing the lane's white line by the camera and performing autonomous operation will greatly contribute to this type of accident reduction (Figure A). Advances are also being made in the development of systems that will enable further automated autonomous driving, and the system to ensure safe and comfortable vehicle operation is being developed [2]. The evolution of this kind of advanced safety system, however, is raising concerns that drivers may feel excessively confident in the safety systems so that they take their hands off the steering wheel and stop paying attention while the systems are providing driving assistance [3]. Furthermore, In the event of a malfunction in a part of the safety system, it is necessary to immediately return the responsibility of the vehicle to the driver, but there is a possibility that the driver may not be able to respond adequately. For this reason, sensors to detect steering wheel operation by the driver are becoming increasingly important. The authors employed a six-axis driving simulator located at the Automobile R&D Center of Honda R&D Co., Ltd., to investigate the situation when an advanced safety system experiences a failure during operation so that responsibility is passed from the system to the driver. The extent of driver hand contact with the steering wheel that is needed in order to enable the driver to operate the vehicle correctly after such circumstances have occurred was clarified, and the least amount of grasp needed on the steering wheel was investigated.

### ***System features***

Figure B shows the layout and configuration of the steering wheel system developed for this research. The static capacitance sensor is used to determine whether or not the driver is grasping the steering wheel. Human hands have capacitance like that of a capacitor. By detecting this capacitance, the system can determine whether or not the driver has a hand or hands on the steering wheel (Figure B).

### **Methods**

As far as the authors have ascertained, the driver modeling literature indicates that there are numerous factors involved in driving but sufficient attention in computer simulation [4,5]. There are almost no examples of simulations using complete models, but the existing models are able to be modified by incorporating insights from psychophysical and physiological research. In addition, the advancements that have been realized up to the present are in sensor technologies. Therefore onboard electronics make it possible to develop workable models [6,7].

### **Test subject**

Twenty-two people who have driving licenses participated in the simulation tests. The test subjects ranged in age from their 20s to their 60s. In order to enable investigation of the question of whether there is a relationship between contact of the driver's hand with the steering wheel and the driver's grip strength, each driver's grip strength was measured (Table 1). The data acquired also included vehicle speed, steering angle, amount of braking, amount of acceleration, yaw rate, and steering torque (Figure E).

### ***Data weighting***

In order to eliminate the deviation of the measured data, we assumed that the reaction time would be earlier if the grip strength of the subject was high, and weighted the measured data using the normal distribution of Japanese grip strength.

Table 2. Normal distribution of Japanese grip strength [8].

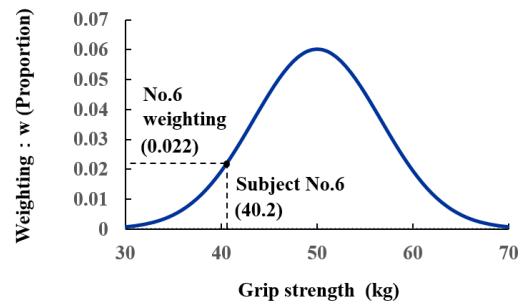
N=72,157

Age	Grip strength (kg)			
	Male		Female	
	Average	Standard deviation	Average	Standard deviation
20-24	48.92	6.83	29.09	4.67
25-29	49.17	6.95	29.51	4.74
30-34	50.33	6.83	30.23	4.56
35-39	50.01	6.64	30.58	4.49
40-44	49.21	6.33	30.47	4.65
45-49	48.07	6.26	29.74	4.74
50-54	46.72	6.05	28.21	4.38
55-59	44.72	6.23	27.12	4.18
60-64	42.24	6.14	25.65	4.14
65-69	38.44	5.84	24.04	4.46
70-74	36.2	5.67	22.8	4.3
75-79	33.53	6.14	21.22	4.32

Assuming that the distribution is a normal distribution in table 2, weighting the individual's grip strength from the grip strength data of the whole country and add it to the result. As a calculation example, calculate with subject No. 6 as an example in the table 1.

Where, W is the weighting data, f is the function of normal distribution. These are then substituted in the defined equation:

$$\begin{aligned}
 W &= f(\text{Ave}, \text{Normal deviation}, \text{Grip strength}) \\
 &= f(50.01, 6.64, 40.2) \\
 &= 0.022
 \end{aligned}$$



Where, i is the subject, n is the number of subjects,  $g_i$  is the grip strength of the subjects,  $W(g_i)$  is the weighting,  $RT_i$  is the reaction time. RT is the result.

$$RT = \frac{\sum_i^n (W(g_i)) \times RT_i}{\sum_i^n W(g_i)}$$

### Simulation apparatus

Data was collected using a full motion simulator located at Honda's Tochigi Automobile R&D Center, an apparatus capable of conducting advanced simulations. This simulator surrounds an actual vehicle with a dome-shaped screen, and allows measurements to be conducted while a projector reproduces video images around the vehicle. In order to realize an environment in which the driver can believe that they are actually operating the vehicle, the system is able to move on six axes to reproduce vehicle behavior. The vehicle employed in the measurements was a 2013 model

year Honda legend (powertrain : Hybrid). Test subjects' manual contact with the steering wheel, the steering angle, and steering torque were measured (Figure F). The measured data was obtained using the vehicle's CAN. The vehicle's meters were modified, and warnings were provided to drivers via a liquid crystal panel, to help ensure that they were easy to understand (Figure G). These modified meters alerted drivers with takeover warnings in visual and audio form (Figure H).

### ***Procedure***

After having their grip strength measured, test subjects were provided with preliminary explanations and a discussion of informed consent, followed by a presentation explaining test procedure. The test subjects completed a five-minute practice drive on a high-speed road used for test driving consisting of a straight section, a junction, and a curve. A light volume of traffic was also present on the road in order to allow the test subjects to get used to the simulator environment, but no events involving the safety system occurred during the practice drives. Following the practice drive, the test subjects ran through the test course using five patterns of manual contact with the steering wheel (contact with one finger, two fingers, three fingers, one hand, and no hands), and measurements were conducted of the extent to which the test subjects were able to operate the steering wheel when the request to take over operation came from the system. Although the method of holding the steering wheel is designated, even at the time of one finger, since the evasive behavior after that is avoided in a manner easy for the subject to perform, it is considered that there is no influence. In order to simulate distracted driving, the same tests were conducted with the navigation system in operation. Considering the possibility that drivers would become used to the requests to take over vehicle operation if they always came at the same time, measurements were conducted with requests made randomly, with and without any event having occurred. Each drive continued for approximately 30 minutes. The requests to take over control of the steering wheel are randomised in time with no reference to any external events. Test subjects were instructed to drive normally, observing the speed limits (Figure 8). The vehicle is traveling on a Highway at 100 (km/h), and enters a junction in order to take a new route. The vehicle reduces its speed to 60 (km/h) in order to negotiate the curve. As the vehicle is rounding the curve, automated driving systems suddenly fail and steering control is lost. the driver performs an emergency avoidance maneuver (Figure I).The vehicle is following a preceding vehicle at 100 (km/h) on a highway. The speed of the preceding vehicle suddenly drops, and the distance between the vehicles is reduced. At the same time, automated driving systems suddenly fail, and accelerator and brake control are lost. The driver conducts an emergency avoidance maneuver. In order to regulate the method used to avoid danger, the drivers were instructed in advance to use the steering wheel for this maneuver (Figure J). Even when the operating the navigation system, the same test cases were carried out as in the case of straight running and curved driving (Figure K).

### **Result**

- When driving behind a vehicle ahead, delays were not observed in the reaction time from the termination of autonomous driving until avoidance was initiated, even when the driver's hands were off the wheel, except when the driver was operating the navigation system. Other than that, no differences were seen, including when the hands were not grasping the wheel when driver's hands were in the lap (Figure 1).
- When driving behind a vehicle ahead, the steering angle velocity in steering wheel operation following the termination of autonomous driving tended to be greater when the driver's hands were off the steering wheel than when the hands were touching the steering wheel. When the hands were off the steering wheel, whether they were in the driver's lap or operating the navigation system did not affect the result. In either case, the steering angle velocity grew greater in the same way. When the driver's hands were in contact with the steering wheel, the steering angle velocity exhibited the same tendency regardless of whether the driver was grasping the steering wheel, pinching the wheel with the fingers, or touching the wheel (Figure B).
- The reaction time from termination of autonomous driving until avoidance was initiated when driving through a curve was faster when the driver was touching the steering wheel than when the driver's hands were off the steering wheel. The reaction time grew even faster when the grasp was in the form of pinching the wheel with three fingers or grasping the wheel with one hand (Figure 3).
- When grasping the wheel with one hand or having one finger in contact with the wheel, the reaction curve described a small circle and avoidance was accomplished with minimal steering wheel operation. When the driver was not grasping the steering wheel, that circle grew larger and the driver would operate the steering wheel more than needed for avoidance (Figure 4,5,6).

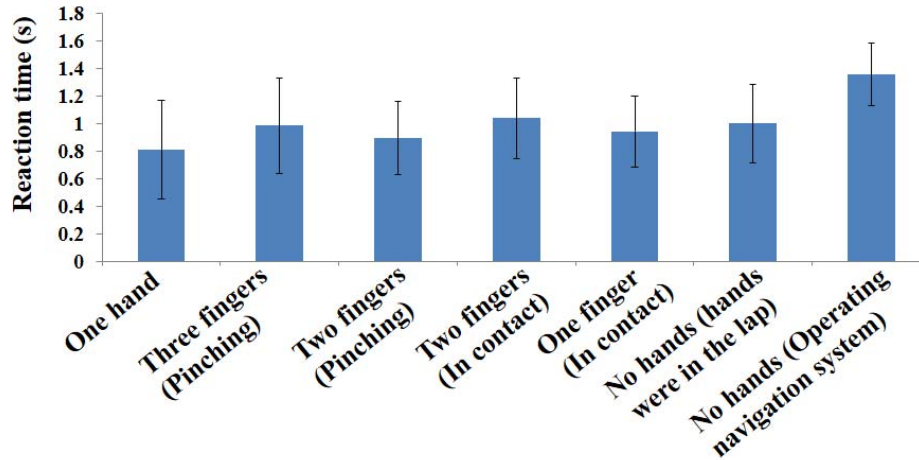


Figure 1. Reaction time from completion of automatic operation to avoidance start

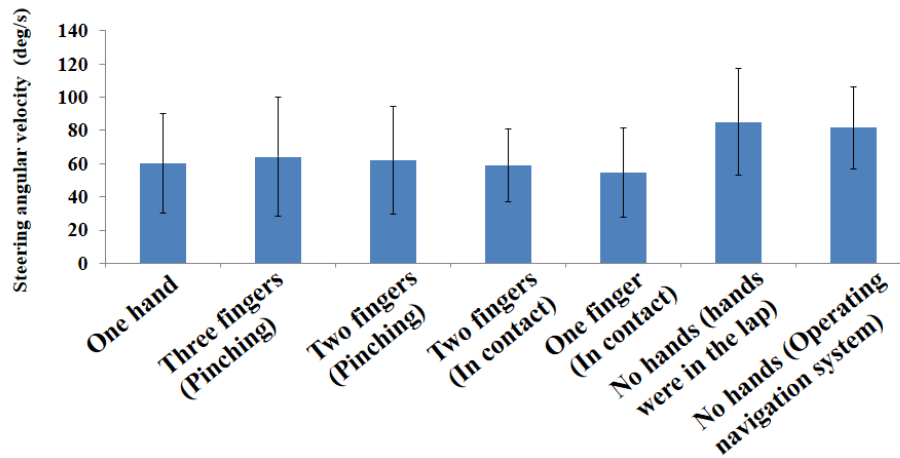


Figure 2. Steering operation during follow-up driving

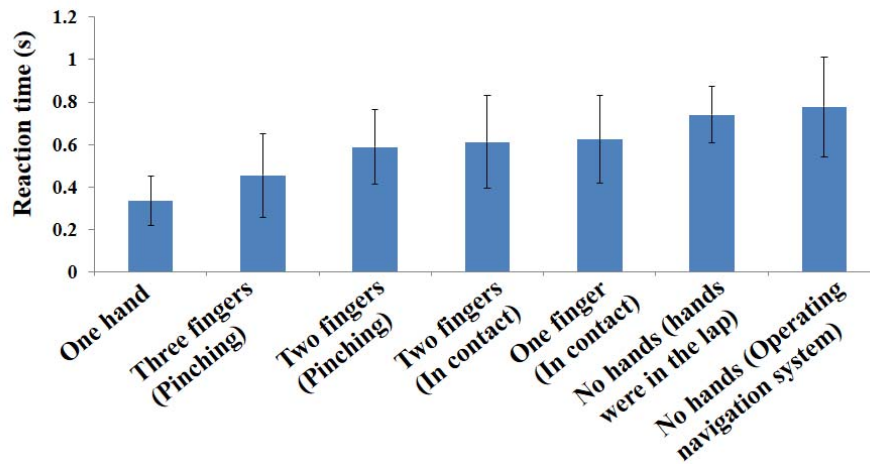


Figure 3. Time from completion of automatic operation in curves to start of avoidance

In order to judge the steering operation amount of the driver, the relation between the steering angle and the steering angular velocity was measured. When the reaction time is early, since the steering operation amount is accurately performed quickly, both the steering angle and the steering angular velocity become small, and the curve also draws a small circle. Also, when the reaction time is slow, the steering operation amount increases and the steering angle and the steering angular velocity show large values, so the curve becomes large.

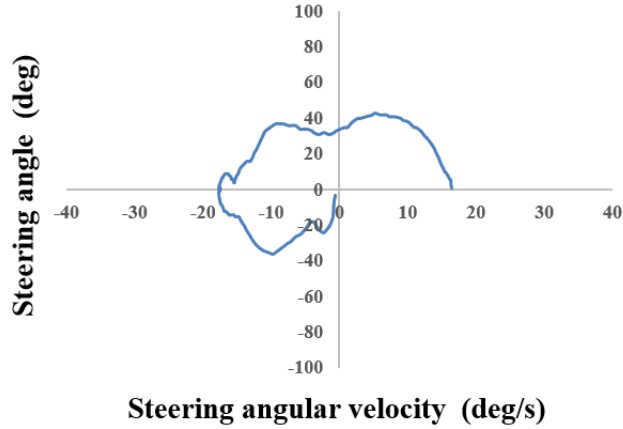


Figure 4. Steering operation when holding with one hand

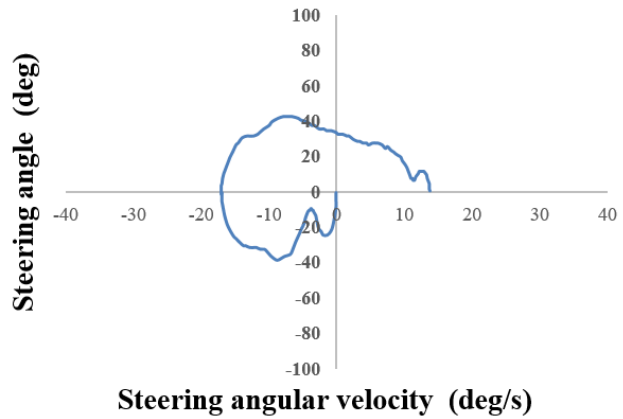


Figure 5. Steering operation at one finger

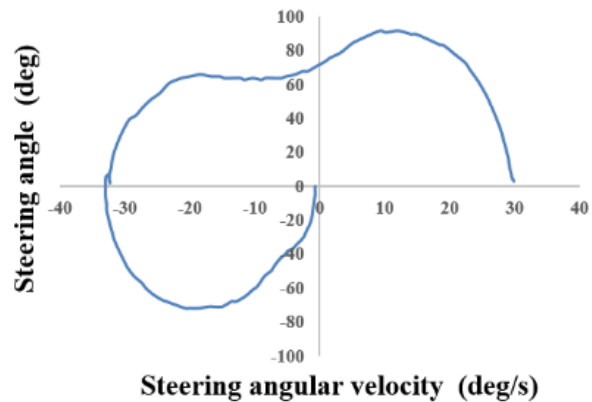


Figure 6. Non-gripping (state where hands are placed on knees)

## Discussion

- The reaction time following the termination of autonomous driving when driving through a curve is thought to be faster when the driver's hand is in contact with the steering wheel because the steering wheel reaction force that occurs when autonomous driving cuts out can be felt by the tactile sense, and this enabled faster reaction than to sound or light.
- When driving behind a vehicle ahead, the reaction time from termination of autonomous driving until avoidance was initiated was the same whether the driver's hands were off the steering wheel or simply resting on the driver's lap with the driver looking to the front, and when the driver was in contact with the steering wheel and similarly looking to the front. However, when the driver was operating the navigation system, not only was the driver's hand touching it, but the driver's gaze was also directed toward the navigation system or control panel. This is thought to be the cause of the delay in reaction to the vehicle ahead.
- When driving behind a vehicle ahead and the status of steering wheel operation was suddenly changed from having the driver's hands off the steering wheel to operating the steering wheel, there was a visible tendency for steering wheel operation to become rough or uneven (the steering speed became faster). If the driver had even just a single finger in contact with the steering wheel, then the steering wheel was operated in the same way as when grasping the steering wheel with one hand. This suggested that having even slight contact with the steering wheel means that there is some readiness in the driver's consciousness to engage in operation.
- When the driver's hands were off the steering wheel, resumption of steering for avoidance sometimes involved sudden operation of the wheel. Therefore it appears advisable to provide a period of several seconds for the driver to have contact with the steering wheel before autonomous driving is terminated. However, the testing reported here did not include testing of how many seconds in advance would be desirable or what kind of human machine interface (HMI) should be used to notify the driver. The authors hope to pursue research from that perspective in the future.

## Conclusion

Simulation tests were conducted in order to study the effect of the drivers' manual contact with the steering wheel. The following results were obtained ;

- (1) The reaction time from termination of autonomous driving until avoidance was initiated when driving through a curve tended to be faster when the driver was in contact with the steering wheel than when the driver was not grasping it. Also, a trend toward even faster reaction times was observed when the driver was grasping the steering wheel by pinching the wheel with three fingers or grasping the wheel with one hand.
- (2) The reaction time from termination of autonomous driving until avoidance was initiated when driving behind a vehicle ahead showed delays only when operating the navigation system, even when the driver's hands were off the steering wheel. Otherwise no difference was observed, including when the driver was not grasping the steering wheel (hands resting in the driver's lap).
- (3) Steering wheel operation from termination of autonomous driving until avoidance was initiated when driving behind a vehicle ahead tended toward greater steering angle velocity when the driver's hands were off the steering wheel than when they were in contact with the steering wheel. When the driver's hands were off the steering wheel, the result was not affected whether the hands were in the driver's lap or operating the navigation system. In either case, the steering angle velocity grew greater in the same way. Also, when the driver was touching the steering wheel, the steering angle velocity tended to exhibit the same tendency whether the driver was grasping the steering wheel, pinching it with the fingers, or in contact with it.

## References

- [1] <https://crashstats.nhtsa.dot.gov>
- [2] Young, R., "Revised Odds Ratio Estimates of Secondary Tasks: A Re-Analysis of the 100-Car Naturalistic Driving Study Data," SAE Technical Paper 2015-01-1387, 2015, doi:10.4271/2015-01-1387
- [3] Gaspar, J., Brown, T., Schwarz, C., Chrysler, S. et al., "Driver Behavior in Forward Collision and Lane Departure Scenarios," SAE Technical Paper 2016-01-1455, 2016, doi:10.4271/2016-01-1455.
- [4] Kamiji, K. and Akaba, H., "RESEARCH OF AN ADVANCED SEAT BELT SYSTEM," ESV 2003 Paper No. 480



- [5] Ito, D., Ejima, S., Sukegawa, Y., Antona, J., Ito, H. and Komeno, F., “ASSESSMENT OF A PRE-CRASH SEATBELT TECHNOLOGY IN FRONTAL IMPACTS BY USING A NEW CRASH TEST SLED SYSTEM WITH CONTROLLABLE PRE-IMPACT BRAKING;” ESV 2013 Paper Number 13-0274
- [6] Rooij, L., Pauwelussen, J., Camp, O. and Jansse, R., “DRIVER HEAD DISPLACEMENT DURING (AUTOMATIC) VEHICLE BRAKING TESTS WITH VARYING LEVELS OF DISTRACTION;” ESV 2013 Paper Number 13-0403
- [7] Infantes, E., Schaub, S., Kramer, S., Langner, T., Eggers, A., Caspar, M.E., Unselt, T. and Lemmen, P./ “EVALUATION OF OCCUPANT PROTECTION DURING THE CRASH PHASE CONSIDERING PRE-CRASH SAFETY SYSTEMS – RESULTS FROM THE EC-FUNDED PROJECT ASSESS;” ESV 2013 Paper number 13-0419
- [8] Physical fitness and exercise capacity investigation, Japanese Ministry of education in 2000 year

**APPENDIX: TABLES AND FIGURES**

*Table 1. Subject details*

No.	Age	Gender	Grip strength (Right) : kgf	Grip strength (Left) : kgf	No.	Age	Gender	Grip strength (Right) : kgf	Grip strength (Left) : kgf
1	Late 30s	Male	52	54.1	12	Late 20s	Male	45.9	52.1
2	Early 30s	Male	49	49	13	Early 30s	Male	47.4	43.8
3	Early 20s	Male	47.2	53.1	14	Early 30s	Male	48.1	44.1
4	Late 20s	Male	52.3	44	15	Early 60s	Male	35.6	29.3
5	Early 30s	Male	42	36	16	Early 30s	Male	48.2	40.6
6	Late 30s	Male	40.2	35.5	17	Late 30s	Female	26.9	27
7	Late 30s	Male	43.9	38.7	18	Early 30s	Male	48.7	42.6
8	Early 50s	Male	51.2	41.7	19	Early 30s	Male	59	52.8
9	Late 30s	Male	37.9	38.1	20	Late 50s	Male	48.6	54.9
10	Late 20s	Male	36.5	32.8	21	Late 20s	Male	37.5	33.9
11	Early 30s	Male	34.3	35.4	22	Early 30s	Female	33.6	32



*Figure A. Image of the advanced safety system recognizes the white line on the road*

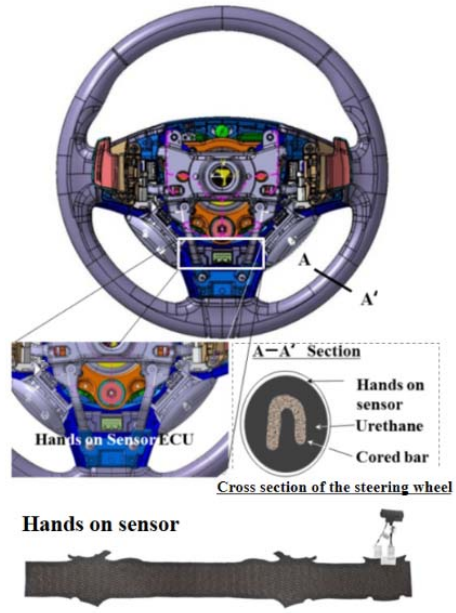


Figure B. Layout of Hands on sensor ECU

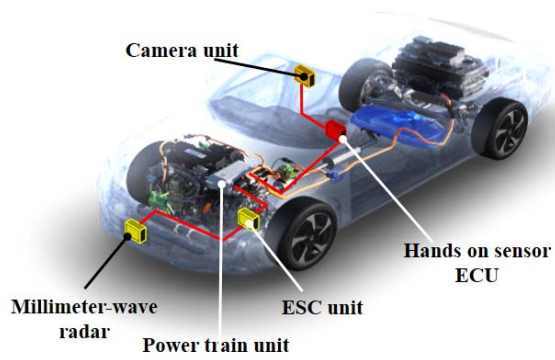


Figure C. Concept diagram of the system operation

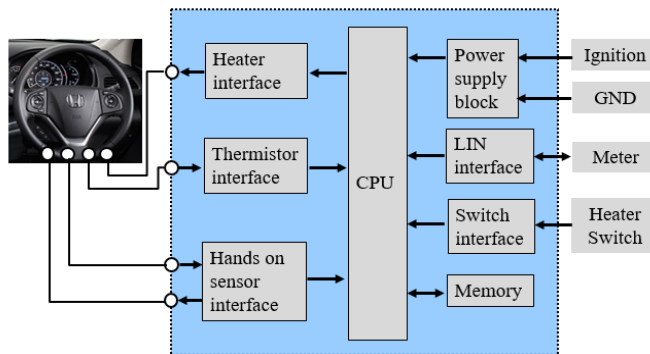


Figure D. System configuration diagram of hands-on sensor

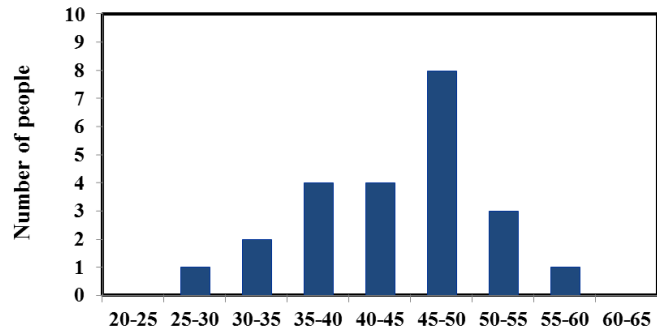


Figure E. Subject distributions



Figure F. Simulation equipment for this study

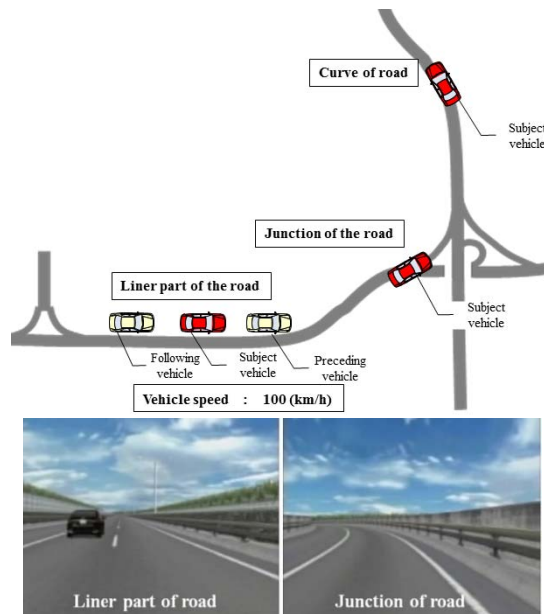


Figure G. Course of simulation



Figure H. Status of assumed steering grasping (The environmental conditions are measured at a temperature of 25 ° C and a humidity of 50%).



Figure I. Simulation with curve

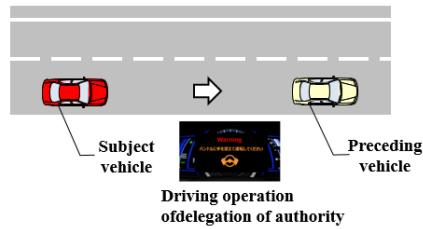


Figure J. Simulation on straight road



Figure K. The driver is manipulating the navigation

# Research on skillful drivers' merging behaviors and statistical analysis of traffic lane flow for an investigation of automatic merging assessment method

**Eiji, Nunobiki**  
**Kota, Harada**  
**Yoichi, Kondo**  
**Koei, Minami**  
 Toyota Motor Corporation  
 Japan

Paper Number 19-0207

## ABSTRACT

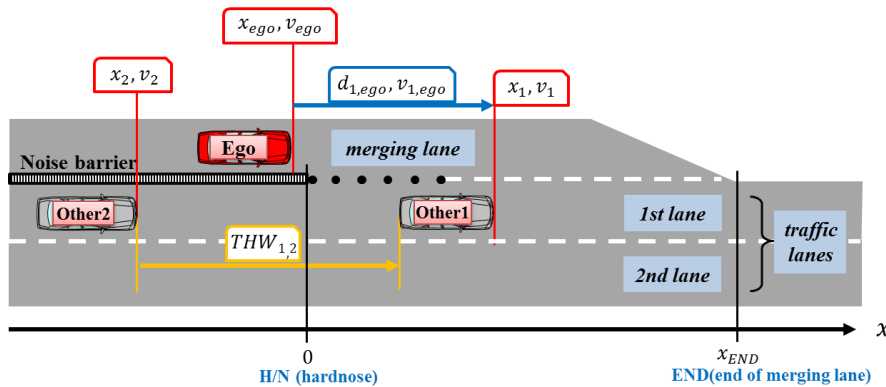
AM (Automatic Merging) is a driving support system which helps drivers to merge into a traffic lane. It is required to set its performance assessment method to see whether it meets people's driving style of each country or region. In this paper, we propose methodologies to set suitable assessment method of AM (target performances and test conditions) which can be applied in each country or region. As for target performances, suitable ones are set by studying Japanese skillful drivers' merging behaviors on highway and on test track. As for test conditions, a new method is proposed to calculate the possibility that a merging vehicle encounters a difficult situation by analyzing traffic camera and cloud data, which allows us to set reasonable test conditions as "X%ile difficulty" of real environment. These methodologies can be applied not only in Japan but also in other countries or regions.

## INTRODUCTION

Demand for AD (automated driving) is increasing rapidly. AM (Automatic Merging) is one of the most complex functions of AD. It helps drivers to merge into a traffic lane, and it is the essential function to achieve automated driving from entrance to exit of highway. Various kinds of researches on function of AM have been reported [1] [2] [3]. Then performance of AM should also be considered in order to provide reliable and comfortable AM. However, its performance assessment method hasn't been generalized yet. Additionally, it should be applied to each country or region because traffic conditions varies among them and AM interacts with other vehicles more than the other ADAS functions do. In this paper, we propose methodologies to provide an assessment method (target performances and test conditions) of AM which can be applied in each country or region. In chapter 1, AM target performances are set as "equal to skillful drivers" by modeling their merging behaviors. In chapter 2, reasonable AM test conditions are set by analyzing the traffic flow of 1st lane (the lane being merged) of real environment.

## Definitions

Figure 1 shows the definitions of terms and variables. Explanations of each term/variable are listed in Table 1.



*Figure 1. Definitions of terms and variables*

**Table 1. Definitions of terms and variables**

Term/ Variable	Definition
1st lane	The nearest traffic lane to the merging lane.
END	End of merging lane.
H/N	Hardnose. In this paper, it is assumed that the ego-vehicle driver cannot see other vehicles on traffic lanes until he/she passes this point.
$x_{ego}, x_1, x_2, x_{END}$	Position on x-axis of each vehicle or point.
$v_{ego}, v_1, v_2, v_{END}$	Velocity of each vehicle or point.
$d_{A,B}$	Relative distance between each vehicle or point. <i>e.g.</i> $d_{END,ego} = x_{END} - x_{ego}$
$THW_{A,B}$	Time headway between each vehicle. <i>e.g.</i> $THW_{ego,2} = (x_{ego} - x_2) / v_2$

**1. Target performance setting by studying skillful drivers’ merging behaviors**

Our basic idea of target performance (T/P) is “equal to skillful drivers.” Table 2 shows the list of the target performances of AM. The classification is composed of “reliability” and “comfort.” “Reliability” means whether the driver can trust AM without feeling uneasy. “Comfort” means whether the driver can feel comfortable. The viewpoints are listed by discussing with skillful drivers based on each classification. Then KPIs (Key Performance Indicators) corresponding to each viewpoint were proposed. Based on these KPIs, all of the target performances were set by analyzing skillful drivers’ behaviors on highway or highway-modeled test track. In this paper, “margin to other vehicles on 1st lane (static)” and “which space to merge” are explained as examples.

**Table 2 List of target performance for AM**

Classification	Viewpoint		KPI	Study method
Reliability	<i>Margin to other vehicles on 1st lane</i>	(Static)	Restricted area for other vehicles [m] (& THW[s])	Study of skillful drivers’ behaviors on highway
		(Dynamic)	Minimum TTC to the other vehicles [s]	
	Margin to the lane end edge	(Static)	Restricted area for end edge[m]	
		(Dynamic)	Minimum TTC to the lane end edge[s]	
Comfort	<i>Which space to merge (in front of / behind other vehicle)</i>		Judgment formula composed of $d_{1,ego}, v_{1,ego}, v_{ego}, x_{END}$	Study of skillful drivers’ behaviors on highway-modeled test track
	Longitudinal motion		Long. acceleration [m/s <sup>2</sup> ]	Study of skillful drivers’ behaviors on highway
			Long. jerk [m/s <sup>3</sup> ]	
	Lateral motion		Lat. acceleration [m/s <sup>2</sup> ]	
		Lat. jerk [m/s <sup>3</sup> ]		

**1-1. T/P example 1: Margin to other vehicles on 1st lane (static)**

Concept & Data collection

This target performance provides “how close the ego-vehicle can be to other vehicles on traffic lanes.” Our aim is to make the target performance as “equal to skillful drivers.” Then a public road test was carried out to acquire the data of skillful drivers’ behaviors. The test vehicle was equipped with external sensors such as lidar for all directions. The test was carried out mainly on Shutoko (urban highway in Tokyo) which is one of the busiest highways in Japan. Three skillful drivers who have Toyota’s advanced licenses drove the vehicle. They drove not trying to make passengers feel uneasy or uncomfortable. It is because skillful drivers can drive either aggressively or smoothly, and obviously AM should follow the latter way. Additionally, we tried to record if the driver or the passengers (who are also skillful drivers) judged the merging behavior was not ideal, but eventually it never occurred. The test was carried out for three days, and 102 merging cases were collected. In this paper, 22 cases of stop & go traffic jam situation are excluded because the driver’s strategy would be different from that of non-traffic jam situation.

Analysis & Result

We set the target performance as the “minimum margin area” of the skillful drivers’ merging behaviors. As a first step, we analyzed the skillful drivers’ each merging case. Each case was extracted from when the ego-

vehicle passed a hardnose to when it passed end of merging lane. See Figure 2 as an example. In this case, ego-vehicle merged from right to left while 4 other vehicles were driving on the traffic lanes (Figure 2a). Red points in Figure 2b shows the trajectory of the lidar points. Then these points were extended to longitudinal and lateral direction to obtain the edge of the other vehicles (Figure 2c). The obtained white area is the area where the ego-vehicle's driver didn't allow the other vehicles to enter in this case. As a second step, a heatmap of other vehicles' existence possibility was obtained by superimposing each case and dividing it by the number of merging cases (Figure 3). Note that each case is flipped horizontally because there was no significant difference between cases of merging to left and to right. Figure 3a shows the result with lateral position and longitudinal position axis, and Figure 3b shows the result with lateral position and THW axis. Note that negative THW means that to the following vehicle, and there is no THW in the side area of ego-vehicle. The area surrounded by red line is the area where the other vehicles never entered. This is the target performance of AM as "restricted area for other vehicles to enter." In addition, we also conducted a study with the same method in Michigan. The result is also shown in Figure 3 as the areas surrounded by white dotted lines. Here we can see the difference between two regions. This shows that suitable target performances would be different among regions or countries.

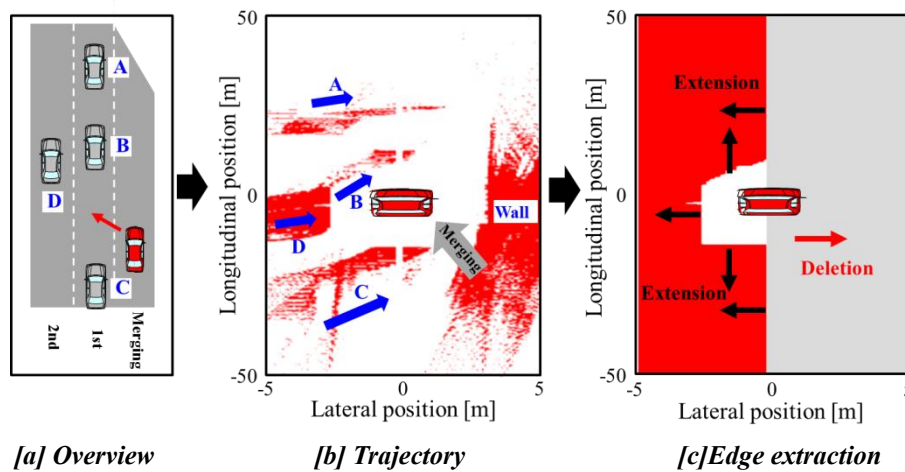


Figure 2. Analysis method of restricted area (1 case example)

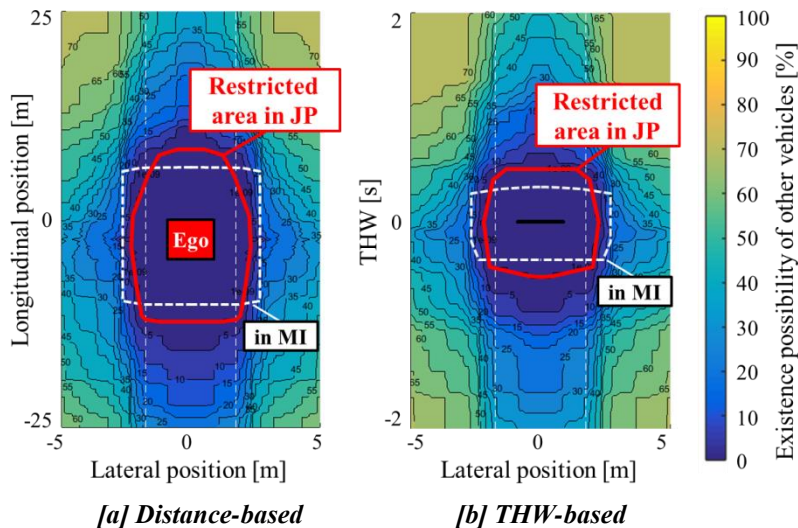


Figure 3. Restricted area for other vehicles

## 1-2. T/P example 2: "Which space to merge"

### Concept & Data collection

This target performance provides "which space should the ego-vehicle merge, in front or behind of a vehicle on 1st lane" when driver recognizes the vehicle on 1st lane at H/N position. The purpose is to avoid uneasy or strange feeling caused by AM's judgment different from drivers' own. Then skillful drivers' behaviors were

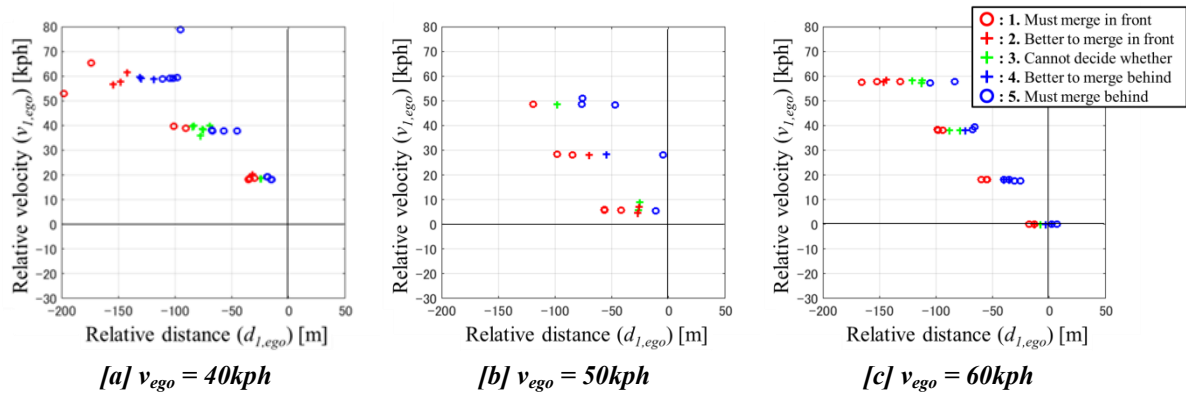
studied with controlled conditions of one other vehicle. The test was conducted on a test track for test efficiently. Tests were conducted with varied conditions as shown in Table 3. The test track was modeled as a typical merging lane of interurban highway in Japan. Initial  $v_{ego}$ ,  $v_1$  and  $d_{1,ego}$  means those of when the ego-vehicle passes H/N. As for velocity, in this paper, we focused on the condition that the ego-vehicle's velocity is lower than or equal to the other vehicle's because it is the most common situation in Japan. Then the drivers scored from 1 to 5 in each test case to describe their judgment as defined in Table 4. For example, the driver scored "1" when he/she judged that ego-vehicle must merge in front of the other vehicle. All of the drivers' scoring are shown in Figure 4.

**Table 3. Test conditions for the study**

Length of merging lane ( $x_{END}$ )[m]	Speed limit assumption of 1st lane [kph]	Initial $v_{ego}$ [kph]	Initial $v_1$ [kph]	Initial $d_{1,ego}$ [m]	Total number of test cases
220	100	40 to 60	60 to 120	-180 to 10	92

**Table 4. Definition of scoring**

Evaluation score	Definition
1	Must merge in front
2	Better to merge in front
3	Cannot decide whether
4	Better to merge behind
5	Must merge behind



**Figure 4. Judgment of skillful drivers**

### Analysis & Result

We set the target performance as "ego-vehicle must merge in front/behind if the skillful drivers judge it as must." Here, the target performance based on driver's judgment models is proposed as below.

- (i) Must merge behind if Equation 1 is satisfied. (*Merge behind model*)

$$F_b = w_{b1}d_{1,ego} + w_{b2}v_{1,ego} + w_{b3}v_{ego} + w_{b4}x_{END} \frac{v_{1,ego}}{v_{ego}} + C_b > 0 \quad [\text{Equation 1}]$$

- (ii) Must merge in front if Equation 2 is satisfied. (*Merge in front model*)

$$F_f = w_{f1}d_{1,ego} + w_{f2}v_{1,ego} + w_{f3}v_{ego} + w_{f4}x_{END} \frac{v_{1,ego}}{v_{ego}} + C_f < 0 \quad [\text{Equation 2}]$$

- (iii) No requirement if neither of them is satisfied.

Here,  $d_{1,ego}$ ,  $v_{1,ego}$ ,  $v_{ego}$ ,  $x_{END}$  are the variables defined in Table 1, and  $w_*$  is the weight of each variables. To identify the parameters of each model, Support Vector Machine (SVM) [4] is adopted. Parameters of *Merge in front model* are identified by dividing the score "1" from "2, 3, 4, 5" and those of *Merge behind model* are identified by dividing the score "5" from "1, 2, 3, 4" respectively. Then the suitable parameters for each model were obtained. Figure 5 shows the fitting result of the each model. The blue-colored area means "must merge behind", the red-colored area means "must merge in front", and the non-colored area means "no requirement."



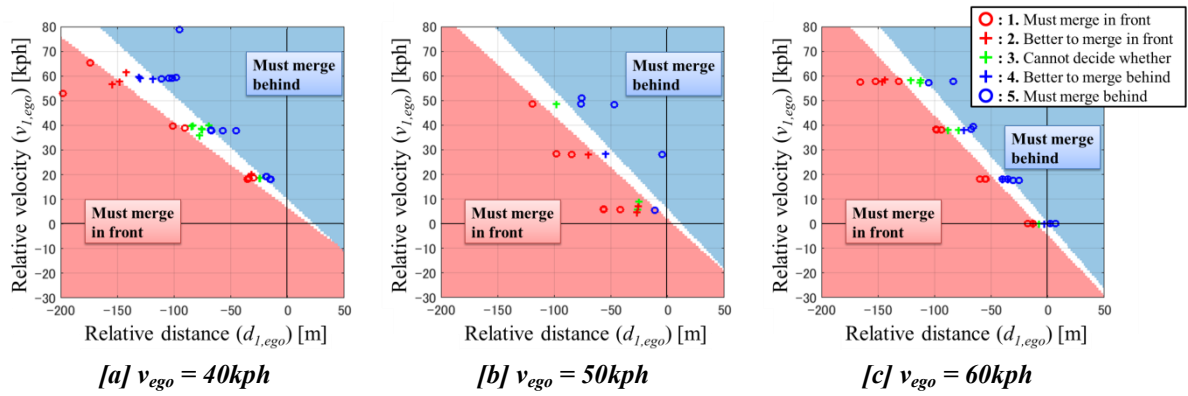


Figure 5. Fitting result of each model

To evaluate the accuracy of the obtained model, three accuracy indexes: precision, recall, and F-measure are calculated. These values of *Merge in front model* and *Merge behind model* are shown in Figure 6a. The model accuracy is high considering that human judgment is sometimes inconsistent even under the same condition. Additionally, these values of *Merge in front model* are lower than those of *Merge behind model*. It implies that it is more difficult for human to judge consistently as “merge in front” than as “merge behind” because the 1st lane vehicle is further away.

The same methodology was also applied to urban-highway-modeled merging test which has a shorter length of merging lane (140m). Then the similar fitting result was obtained, and the fitting accuracy was as high as that of interurban-highway-modeled merging test (Figure 6b).

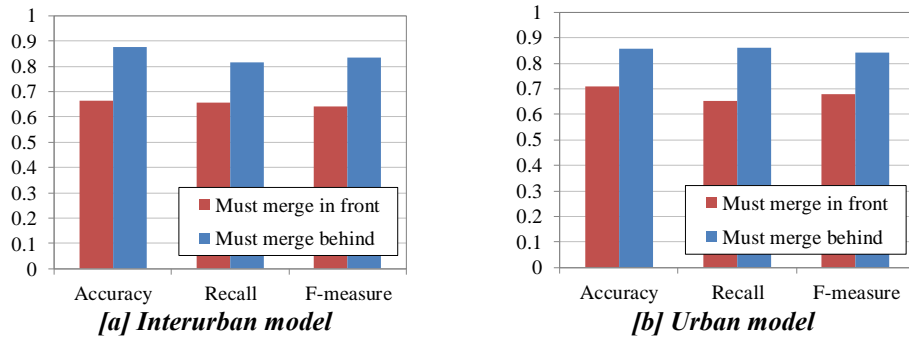


Figure 6. Fitting accuracy of each model

## 2. Test condition setting by studying 1st lane traffic flow

The conditions of 1st lane vehicles play a key role in AM evaluation. For example, it is obviously more difficult to merge when there are the other vehicles on 1st lane with close distance than when there is no other vehicle. Then reasonable and rather difficult test conditions should be set for effective evaluation of AM. In this chapter, we aim to set suitable ones by studying 1st lane traffic flow of real environment.

First of all, we have to consider what difficult conditions are. There would be two types of traffic situation: traffic jam and non-traffic jam. In this paper, we focus on the difficulty of non-traffic jam situation. Then, we assume that it would be difficult for drivers to merge in the conditions below:

- (C1) There is a 1st lane vehicle in a position where the ego-vehicle driver cannot judge which space to merge immediately. (Then the driver would have to drive long distance to merge.)
- (C2) There is another vehicle near the vehicle described in C1.

Figure 7 shows an image of these conditions.

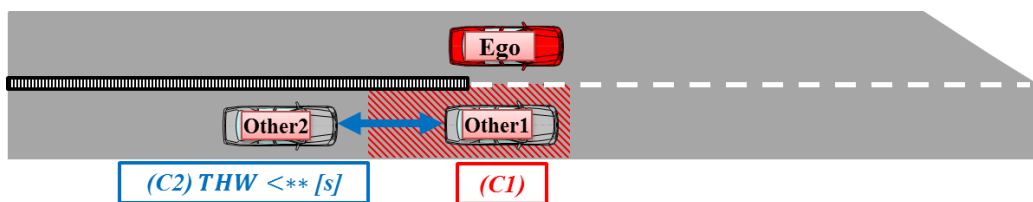


Figure 7. Difficult conditions for merging

With this assumption, a possibility to encounter such a difficult situation can be calculated. We call it “difficult possibility ( $P_{dif}$ ).” It is calculated by following equation.

$$P_{dif} = P(C1 \cap C2) \quad [\text{Equation 3}]$$

As for the condition  $C1$ , it can be modeled as no requirement area of “which space to merge” (described as white areas in Figure 5) because drivers within this area have to drive further. Furthermore, it would be also difficult for AM because it should switch its judgment within this area. Then, it is important to clarify how often these conditions ( $C1$  and  $C2$ ) appear in the real highway. Then traffic camera data was analyzed for this purpose because it allows us to obtain the traffic flow on 1st lane quite directly without losing statistical information. Two interchanges (Higashi-Ikebukuro and Kasugai) are chosen to study the traffic flow of urban and interurban highway (Figure 8). Table 5 and Figure 9 show the overview of traffic camera data. Note that the traffic jam situation (1st lane velocity < 30kph) was excluded in this paper.

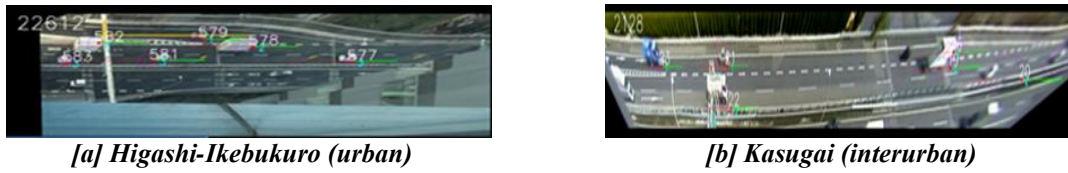


Figure 8. Traffic camera image

Table 5. Traffic camera data overview

No.	Interchange	Highway	Speed limit on 1st lane [kph]	Shooting time [hour]	Number of vehicles on 1st lane	Average number of vehicles [Num. / hour]
1	Higashi-Ikebukuro	Shutoko (urban)	60	10.4	7758	746.0
2	Kasugai	Tomei (interurban)	100	11.1	5375	484.2

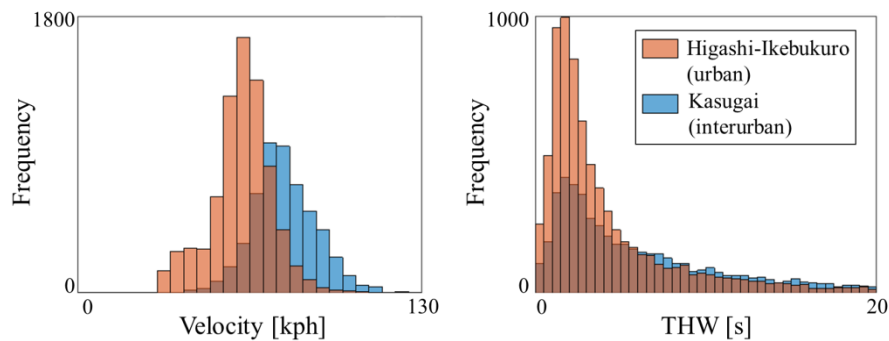


Figure 9. Traffic camera data overview

With these data,  $P_{dif}$  can be calculated by following equation with the assumption that the data distribution of sampled period is equal to that of the population.

$$P_{dif} = \frac{t(C1 \cap C2)}{t_{total\_cam}} \quad [\text{Equation 4}]$$

Here,  $t(C^*)$  is the accumulated time when the condition  $C^*$  is satisfied, and  $t_{total\_cam}$  is the total time of traffic camera data. To calculate  $t(C1 \cap C2)$  with Equation 1 and 2, it is assumed that ego-vehicles appear at every moment at the hardnose with initial velocity. The initial velocity should be set as AM’s setting considering that the purpose is to set reasonable test conditions. Here, it is supposed that AM’s initial velocity is 50kph at Higashi-Ikebukuro and 60kph at Kasugai, for example. Figure 10 shows the result of  $P_{dif}$  calculation. The horizontal red line shows  $P(C1)$ . The blue line shows the cumulative distribution of  $P_{dif}$  as a function of  $THW_{2,1}$  (as  $C2$ ). With this result, reasonable AM test conditions can be set by setting reasonable value of  $P_{dif}$ . For

example, if we assume that AM test condition should be set as difficult as “ $P_{dif} = 1\%$ ” of real environment, corresponding  $THW_{2,1}$  is 1.07[s] for Higashi-Ikebukuro (urban highway), and 1.54[s] for Kasugai (interurban highway). The set  $THW_{2,1}$  is shorter at Higashi-Ikebukuro than at Kasugai even with the same  $P_{dif}$  because the 1st lane traffic is heavier in Higashi-Ikebukuro than in Kasugai. (In other words, it is more frequent to encounter a difficult situation in Higashi-Ikebukuro than in Kasugai.)

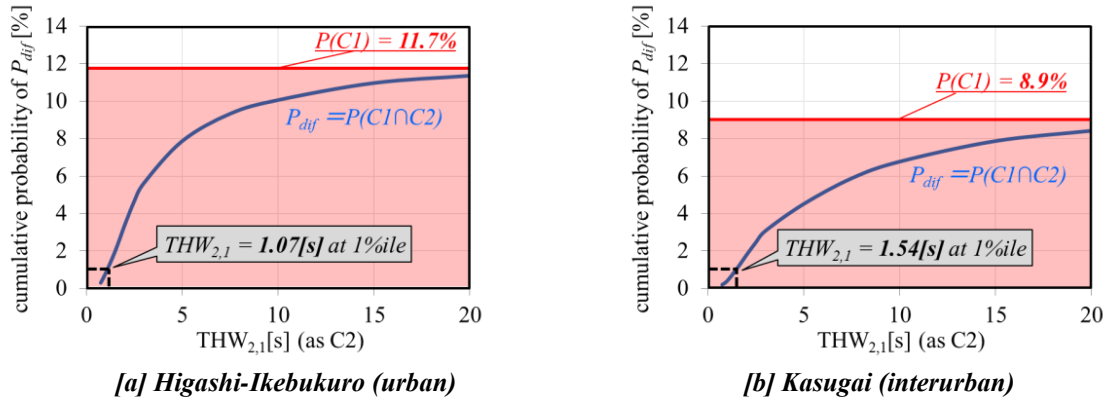


Figure 10. Result of difficult possibility calculation

With this method, it would be possible to make reasonable test conditions corresponding to every merging lane of real environment. However, it is unfeasible to collect traffic data of every merging lane by methods such as traffic camera. Then we kept studying to seek an alternative method as following.

$\hat{P}_{dif}$  is defined by the following equation.

$$\hat{P}_{dif} = P(C1) * P(C2) \quad \text{[Equation 5]}$$

Figure 11 shows the comparison between  $P_{dif}$  and  $\hat{P}_{dif}$  of each interchange. Their values match well, which means it is possible to suppose that conditions  $C1$  and  $C2$  are almost independent of each other when velocity is higher than 30kph.

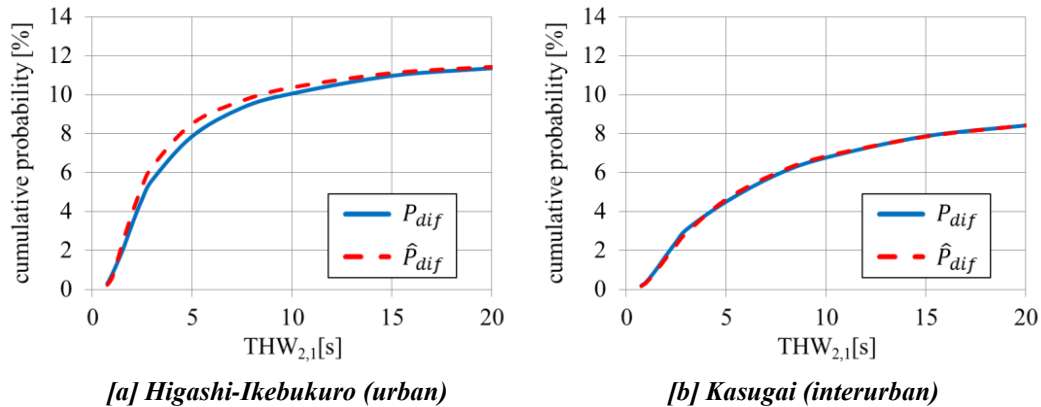
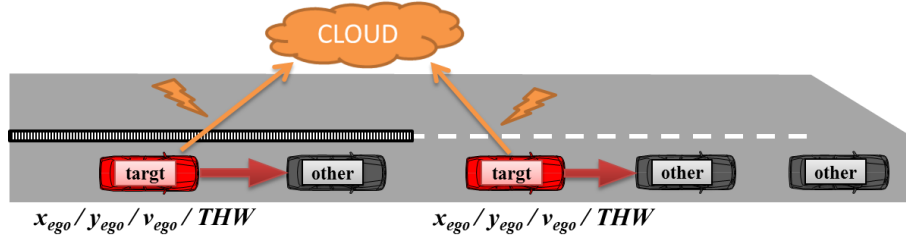


Figure 11. Comparison of  $P_{dif}$  and  $\hat{P}_{dif}$

The following equation is obtained from this result.

$$P_{dif} \cong \hat{P}_{dif} \quad \text{[Equation 6]}$$

Then, we assume a data sampling method that some of vehicles can send  $v_{ego}$  and  $THW$  to data cloud (Figure 12). Note that, unlike traffic camera data analysis, it is impossible to obtain the data of all vehicles on 1st lane through the sampled period.



**Figure 12. Data collection by cloud**

With this kind of method,  $P(C1)$  and  $P(C2)$  can be also calculated as following equations with assumption that  $v_{ego}$  and  $THW$  distributions of sampled vehicles are equal to those of the population.

$$P(C1) = \frac{t_{sample}(C1)}{t_{total\_sample}} * \frac{N_{AVE\_population}}{N_{AVE\_sample}} \quad [\text{Equation 7}]$$

$$P(C2) = \frac{t_{sample}(C2)}{t_{total\_sample}} \quad [\text{Equation 8}]$$

Here,  $t_{sample}(C^*)$  is accumulated time when the condition  $C^*$  is satisfied by sampled vehicles,  $t_{total\_sample}$  is total time of data-sampled period,  $N_{AVE\_population}$  is number per unit time of vehicles of the population, and  $N_{AVE\_sample}$  is that of sampled vehicles. Note that  $N_{AVE\_population}$  can be obtained from public database of each region or country. For example, those data of major road junctions in Japan are open to public by MLIT of Japan [5]. Finally, it is possible to calculate  $P_{dif}$  of each merging lane of real environment by Equations 5-8 with this kind of data collection method.

## CONCLUSION

New methodologies are proposed to determine “target performances” and “test conditions” for Automatic Merging (AM). As for target performances, skillful drivers’ merging behaviors were studied and modeled as what AM should follow. It was found that one of the target performances is different between in Japan and in Michigan. As for test conditions, a new method is proposed to calculate the possibility that a merging vehicle encounters a difficult situation by analyzing traffic camera and cloud data, which allows us to set reasonable test conditions as “X%ile difficulty” of real environment. In addition, another analysis method using cloud data is also proposed as a substitute for traffic camera analysis. These methodologies proposed in this paper would help us to set suitable target performances and test conditions for each country or region.

## REFERENCES

- [1] P. Kachroo and Zhijun Li. “Vehicle merging control design for an automated highway system.” *Proceedings of Conference on Intelligent Transportation Systems* (1997): 224- 229.
- [2] Xiao-Yun Lu and K.J. Hedrick . “ Longitudinal control algorithm for automated vehicle merging.” *Proceedings of the 39th IEEE Conference on Decision and Control* (2000). 450- 455 vol.1.
- [3] H. Liu, W. Zhuang, G. Yin, Z. Tang and L. Xu. “Strategy for heterogeneous vehicular platoons merging in automated highway system.” *Chinese Control And Decision Conference* (2018): 2736- 2740.
- [4] U. Fayyad. ”A tutorial on support vector machines for pattern recognition.” *Data Mining and knowledge diccovery*, (1998): 2, 121- 167.
- [5] Ministry of Land, Infrastructure, Transport and Tourism, “Road Traffic Census 2015”, <http://www.mlit.go.jp/road/census/h27/>