CAMP

Automated Vehicle Research Consortium

Mercedes-Benz
Research & Development North America, Inc.

GM

TOYOTA

VOLKSWAGEN
GROUP OF AMERICA

Ford

NISSAN

Intelligent Transportation Systems

Automated Vehicle Research for Enhanced Safety

Final Report

Submitted to the United States Department of Transportation
National Highway Traffic Safety Administration (NHTSA)

March 2016

In Response to Cooperative Agreement Number
DTNH22-05-H-01277

Notice

This publication is distributed by the U.S. Department of Transportation in the interest of information exchange. The opinions, findings, and conclusions expressed in this publication are those of the authors and not necessarily those of the U.S. Department of Transportation. The United States Government assumes no liability for its contents or use thereof.

If trade or manufacturers’ names or products are mentioned, it is because they are considered essential to the object of the publication and should not be construed as an endorsement. The United States Government does not endorse products or manufacturers.

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.

4. Title and Subtitle

Automated Vehicle Research for Enhanced Safety
Final Report

5. Report Date
March 2016

6. Performing Organization Code

7. Authors
Tellis, L., Engelman, G., Christensen, A., Cunningham, A., Debouk, R., Egawa, K., Green, C., Kawashima, C., Nicols, G., Prokhorov, D., Wendling, B., Yako, S., and Kiger, S.

8. Performing Organization Report No.

9. Performing Organization Name and Address
Crash Avoidance Metrics Partnership on behalf of the
Automated Vehicle Research Consortium
27220 Haggerty Road, Suite D-1
Farmington Hills, MI 48331

10. Work Unit No. (TRAIS)

11. Contract or Grant No.
DTFH6114H00002

12. Sponsoring Agency Name and Address

National Highway Traffic Safety Administration
1200 New Jersey Avenue, SE
West Building
Washington, DC 20590

13. Type of Report and Period Covered
Final Report
September 30, 2015 – June 30, 2015

14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

The work described in this report was conducted by the Crash Avoidance Metrics Partnership (CAMP) Automated Vehicle Research Consortium (Ford Motor Company, General Motors, Nissan, Mercedes-Benz, Toyota, and Volkswagen Group of America). The project was sponsored by the National Highway Traffic Safety Administration (NHTSA) through Cooperative Agreement No. DTNH22-05-H-01277, Project Order 0009. The overall objective of the project was to develop detailed functional descriptions for on-road driving automation levels and identify potential objective test methods that could be used as a framework for evaluating emerging and future driving automation features. A key contribution of the report is the clarification of the scope and definitions of driving automation levels. All driving automation functionality that can be engaged by a driver such that the functions operate simultaneously are considered. Functions that only intervene for specific events (e.g., a potential loss of stability, lane departure, or collision) and do not provide sustained vehicle motion control between and across events, do not change the role of the driver and as such are not driving automation. This report introduces safety principles based on a comprehensive safety analysis of driving automation Levels 2 through 5. The safety principles developed apply to driving automation systems and features that reside under a given level. We hope that this work will be used as a reference for any continued work to develop objective tests for driving automation systems as this technology space matures.

17. Key Word	18. Distribution Statement

19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 184	22. Price

Executive Summary

This report describes the work completed by the Crash Avoidance Metrics Partnership (CAMP) Automated Vehicle Research (AVR) Consortium in the project titled "Automated Vehicle Research for Enhanced Safety" (i.e., the AVR Project).

The overall objective of the project was to develop detailed functional descriptions for on-road driving automation levels and identify potential objective test methods that could be used as a framework for evaluating emerging and future driving automation features. Participating companies in the AVR Consortium are Ford Motor Company, General Motors, Nissan, Mercedes-Benz, Toyota, and Volkswagen Group of America. The project is sponsored by the National Highway Traffic Safety Administration (NHTSA) through Cooperative Agreement No. DTNH22-05-H-01277, Project Order 0009.

Task 1

Task 1 was the project management task for the project. The goal of this task was to provide project oversight to ensure that the project achieved its objectives within the timeframe and resources allocated for the effort.

Task 2

Within Task 2, a research consortium, operating under the Crash Avoidance Metrics Partnership (CAMP) structure, was formed to execute this project. Throughout the project this task provided coordination with NHTSA regarding program execution and changes to the work plan that may be required as new information is developed within the project.

Task 3

The objectives of Task 3 were to define functional descriptions for proposed driving automation levels, delineate a methodology and/or set of identifiable characteristics that allow classification of new automation features into the appropriate levels, and describe sets of automation functions that fit within the automation levels.

The project derived five factors for consideration in defining automation levels. At the time of this work, several automation level definitions were under consideration within organizations worldwide: NHTSA's Preliminary Statement of Policy Concerning Automated Vehicles (NHTSA 2013), SAE J3016:2014 and the German Federal Highway Research Institute (Bundesanstalt für Straßenwesen, or BASt). After examining each, the SAE J3016 automation levels appeared to offer the greatest alignment to the five factors for consideration. The project elaborated on the SAE levels by further differentiating both the driver versus system roles in completing the Dynamic Driving Task (DDT) at lower levels of driving automation, and also further detailed the functional characteristics of each automation level. The outcome of this effort was the development of a minimum set of automation functions for each automation level identified in this report. It is important to note that higher levels of driving automation include those functional capabilities found at lower levels of automation, and that each increasing level of automation includes functions that reduce the driver's role in completing the DDT and/or DDT fallback.

Lastly, a methodology that allows classification of new and existing automation features into the appropriate SAE J3016 levels was described. In order to illustrate the application of the classification methodology, a set of exemplar automation features was identified and descriptions were sought for each of the characteristics that differentiate automation levels. The features were subsequently classified into automation levels.

We note that, in order to enable correct feature classification according to the methodology developed in this report, a description of the proper usage of each automation feature in question would need to be obtained from the manufacturer (who designed, developed and tested such feature).

Task 4

The objectives of Task 4 were to develop an exemplar list of driving automation features that the AVR Consortium concludes are likely to be marketed by vehicle manufacturers in the future. The list included features that are near-term (0-4 years), mid-term (5-9 years), and long-term (10+ years) in terms of potential deployment. The list was based only on publicly available information and leveraged work from NHTSA to the extent possible. The driving automation features listed were then compared and contrasted based on the minimum sensing/processing control functionality and Human-Machine Interface (HMI) required for each feature.

Task 6

The objective of Task 6 was to develop a set of solution-neutral, top-level Safety Principles (SPs) for the partial automation (Level 2) through full automation (Level 5) driving automation levels differentiated in Task 3. These SPs were to be generated from a hazard analysis, with the expectation that the SPs would effectively and succinctly address the identified hazards.

The project utilized a hazard analysis strategy based on System-Theoretic Process Analysis (STPA). In the execution of this process, the project defined *accident* as a loss that results from an undesired and unplanned event and causes human injury or property damage, and focused on vehicle collisions as the primary accident (loss) under consideration. The project defined *hazard* as a system state that, together with a worst-case set of external disturbances, may lead to a loss, and identified four primary hazards for analysis. The project developed a high-level control structure for each of the driving automation levels defined in Task 3, and considered how errant control actions within the structure may result in a vehicle collision. Safety constraints were developed to prevent each Undesired Control Action (UCA) from resulting in a hazard. The project then summarized the developed safety constraints and constructed a minimum set of SPs for each driving automation level.

Lastly, matrices were developed to map the alignment of the SPs to the driving automation levels differentiated in Task 3 and to categorize the SPs as to whether they apply to the driver/operator, the driving automation system, or the base vehicle. As higher driving automation is developed, a greater number of SPs will apply to the driving automation system.

Tasks 5 and 7

Building on the automation levels differentiated in Task 3, work in Tasks 5 and 7 provides a method for determining objective Safety Principle assessments to demonstrate that a driving automation system meets the Task 6 SPs for its manufacturer-designated automation level. Given that driving automation systems are not standardized in terms of scope or performance, this approach relies on a Classification and Operational Description filled out by the manufacturer to highlight feature operation, automation level, attendant SPs and use cases appropriate for testing. The report focuses on Level 2 driving automation systems designed for parking, low-speed Traffic Jam Assist (TJA) and High Speed Automated Cruise (HSAC). Given that these systems are not widely deployed and are the subject of significant industry competition, and that system concepts vary widely, the report was not able to provide test conditions and actual data that apply across all manufacturers. However, three hypothetical examples from two fictitious automakers (Acme and GloCo) were provided to highlight the nature of the Classification and Operational Description fact finding, given that it depends on self-reporting; the nuances of testing divergent designs; and the challenges associated with test conditions and operational domain limitations.

Task 8

Through the execution of Tasks 1 through 7 the AVR Project team identified several areas of synergy between the AVR project deliverables and other NHTSA projects. Through the execution of Task 6, the AVR team identified several areas of human factors research.

Task 9

The final task of the AVR Consortium involved combining the results from the interim reports generated from Technical Task(s) 3, 4, 5, 6, and 7 into a cohesive final report. This report is the product of that effort.

Acknowledgements

The authors wish to thank Frank Barickman, National Highway Traffic Safety Administration, for his advice and guidance during this project.

In addition, the authors also wish to thank Bill Taylor and Jim Winkelman, kVA, for their significant contributions to Section 4 of this report.

Table of Contents

Executive Summary i

Acknowledgements i

List of Acronyms viii

1 Introduction 10

2 Develop Detailed Functional Descriptions of Levels of Automation 14

2.1 Rationale for Driving Automation Levels 14

2.2 Rationale for Specific Levels of Driving Automation 19

2.3 Application of Driving Automation Levels 23

2.4 Detailed Discussion of Driving Automation Levels 23

2.5 Identification of Minimum Automation Functions by Driving Automation Level 28

2.6 Methodology for Classifying Features to Driving Automation Levels and Example Classifications 31

2.6.1 Methodology for Classifying Features 31

2.6.2 Example Classification of Driving Automation Features Using Methodology 32

2.7 Summary - Functional Descriptions of Levels of Automation 38

3 Determine Concept Roadmaps for Future Driving Automation Features 40

3.1 Driving Automation Features 40

3.1.1 Near-term Features 40

3.1.2 Mid-term Features 41

3.1.3 Long-term Features 41

3.2 Similarities and Differences between Driving Automation Features 42

3.2.1 HMI Similarities and Differences 48

3.2.2 Sensing and Processing Similarities and Differences 50

3.2.3 Control Functionality Similarities and Differences 51

3.3 Summary - Concept Roadmaps for Future Driving Automation Features 51

4 Top-Level Safety Principles for Levels of Automation 53

4.1 Introduction to System-Theoretic Process Analysis (STPA) for Hazard Analysis 53

4.2 Accidents and Hazards Under Consideration 54

4.2.1 Losses (Accidents) ... 54
4.2.2 Hazards ... 54
4.3 Generic Control Structure for Driving Automation ... 56
4.4 Application of Safety Analysis by Level of Driving Automation ... 57
4.5 Level 2 Driving Automation ... 58
4.5.1 High-Level Control Structure for Level 2 Driving Automation ... 58
4.5.2 Safety Principles (SPs) for Level 2 Driving Automation ... 59
4.5.3 Key Findings ... 61
4.6 Level 3 Driving Automation ... 62
4.6.1 High-level Control Structure for Level 3 Driving Automation ... 62
4.6.2 Safety Principles (SPs) for Level 3 Driving Automation ... 63
4.6.3 Key Findings ... 65
4.7 Level 4 Driving Automation ... 66
4.7.1 High-level Control Structure for Level 4 Driving Automation ... 66
4.7.2 Safety Principles (SPs) for Level 4 Driving Automation ... 67
4.7.3 Key Findings ... 68
4.8 Level 5 Driving Automation ... 69
4.8.1 High-Level Control Structure for Level 5 Driving Automation ... 69
4.8.2 Safety Principles (SPs) for Level 5 Driving Automation ... 70
4.8.3 Key Findings ... 71
4.9 Summary of Safety Principles (SPs) ... 71
4.10 Summary - Top-Level Safety Principles for Levels of Automation ... 74
5 Development of Use Cases and Preliminary Objective Test Methods .. 77
5.1 Testing Goals for Level 2 and Level 3 Driving Automation Systems ... 77
5.1.1 Lower Level Driving Automation System Testing ... 78
5.1.2 Higher Level Driving Automation System Testing ... 79
5.2 Classification and Operational Description and Safety Principle Assessment Procedure ... 80
5.2.1 Goal of the Classification and Operational Description and Safety Principle Assessment Procedure ... 80
5.2.2 Driving Automation Level Determination ... 81
5.2.3 Testing Relevant to Level-Specific SPs ... 83
5.3 Preliminary Test Concepts for Selected Automation Features ... 86

5.3.1 Level 2 Parking Assist Feature 86
5.3.2 Level 2 Traffic Jam Assist Feature 87
5.3.3 Level 2 High Speed Automated Cruise Feature 88
5.4 Challenges in Testing Driving Automation Systems 89
5.5 Open Issues Related to Testing 90
5.5.1 Testing Issues with Level 2 Systems and Above 90
5.5.2 Other Features Not Considered 91
5.6 Summary - Development of Use Cases and Preliminary Objective Test Methods 91
6 Project Summary 93
7 References 95
Appendix A: Matrices of Undesired Control Actions 97
A.1 UCA Matrix for Level 2 Driving Automation 97
A.2 UCA Matrix for Level 3 Driving Automation 101
A.3 UCA Matrix for Level 4 Driving Automation 111
A.4 UCA Matrix for Level 5 Driving Automation 116
Appendix B: Blank Classification and Operational Description 118
Appendix C: Blank Driving Automation System Level 2 Safety Principle Assessment 124
Appendix D: GloCo Parking Assist Driving Automation System Classification and Operational Description 126
Appendix E: GloCo Parking Assist Driving Automation System Safety Principle Assessment 132
Appendix F: Acme Parking Assist Driving Automation System Classification and Operational Description 136
Appendix G: Acme Parking Assist Driving Automation System Safety Principle Assessment 142
Appendix H: GloCo Traffic Jam Assist Driving Automation System Classification and Operational Description 144
Appendix I: GloCo Traffic Jam Assist (TJA) Driving Automation System Safety Principle Assessment 150
Appendix J: Acme Traffic Jam Assist Driving Automation System Classification and Operational Description 153
Appendix K: Acme Traffic Jam Assist (TJA) Driving Automation System Safety Principle Assessment 160

Appendix L: GloCo High Speed Adaptive Cruise Driving Automation System Classification and Operational Description 162

Appendix M: GloCo High Speed Adaptive Cruise Driving Automation System Safety Principle Assessment 168

Appendix N: Acme High Speed Adaptive Cruise Driving Automation System Classification and Operational Description..170

Appendix O: Acme High Speed Adaptive Cruise Driving Automation System Safety Principle Assessment 177

Appendix P: Reccomendations for Follow On Proposal: Safety Principles on the Driver - Human Factors Research 179

Glossary of Selected Terms..183

List of Figures

Figure 1: Human Operation of a Traditional Vehicle – the Dynamic Driving Task 16
Figure 2: The Introduction of Machine Automation to the DDT 17
Figure 3: The Changing Role of the Driver 27
Figure 4: Flow Chart Illustrating the Methodology for Classifying Automation Features to Levels of Automation 32
Figure 5: Principle Actors in the DDT 56
Figure 6: Control Structure for Level 2 Driving Automation 59
Figure 7: Control Structure for Level 3 Driving Automation 63
Figure 8: Control Structure for Level 4 Driving Automation 67
Figure 9: Control Structure for Level 5 Driving Automation 70

List of Tables

Table 1: Distribution of Functions by SAE/BASt Driving Automation Level 22
Table 2: Exemplar Driving Automation Features 35
Table 3: Mapping Automation Features into Driving Automation Levels 37
Table 4: Minimum HMI, Control, Sensing and Processing Functionality for Driving Automation Level 1-5 Exemplar Features 43
Table 5: Summary of Safety Principles 72
Table 6: Driving Automation System Level 2 83
Table 7: Driving Automation System Level 3 83
Table 8: Driving Automation System Level 4 85
Table 9: Driving Automation System Level 5 86

List of Acronyms

AASHTO	American Association of State Highway and Transportation Officials
ACAS	Automotive Collision Avoidance System
ACC	Adaptive Cruise Control
ACEA	European Automobile Manufacturers Association (Association des Constructeurs Européens d'Automobiles)
AHDA	Automated Highway Driving Assistant
AVR	Automated Vehicle Research
BASt	Federal Highway Research Institute of the Republic of Germany (Bundesanstalt für Straßenwesen)
C-ACC	Cooperative Adaptive Cruise Control
CAMP	Crash Avoidance Metrics Partnership
CAN	Controller Area Network
CC	Cruise Control
DDT	Dynamic Driving Task
DOT	Department of Transportation
ESC	Electronic Stability Control
FARS	Fatality Analysis Reporting System
FHWA	Federal Highway Administration
FMVSS	Federal Motor Vehicle Safety Standards
FOT	Field Operational Test
GPS	Global Positioning System
HAZOP	Hazard and Operability Analysis
HMI	Human-Machine Interface
HSAC	High Speed Automated Cruise
LCC	Lane Centering Control
LKA	Lane Keeping Assist
MHz	Megahertz
MIT	Massachusetts Institute of Technology
N/A	Not Applicable
NASS	National Automotive Sampling System

NCAP	New Car Assessment Program
NHTSA	National Highway Traffic Safety Administration
ODD	Operational Design Domain
OEDR	Object and Event Detection and Response
OEM	Original Equipment Manufacturer
OICA	International Organization of Motor Vehicle Manufacturers (Organisation Internationale des Constructeurs d'Automobiles)
POV	Principle Other Vehicle
SAE	SAE International
SoP	Statement of Policy
SP	Safety Principle
STPA	System Theoretic Process Analysis
TJA	Traffic Jam Assist
UCA	Undesired Control Action
USDOT	United States Department of Transportation
V2V	Vehicle-to-Vehicle
VDA	German Automobile Industry Association (Verband Der Automobilindustrie)

1 Introduction

The objectives of the Automated Vehicle Research (AVR) Project were accomplished in cooperation and consultation with the U.S. Department of Transportation (USDOT) National Highway Traffic Safety Administration (NHTSA):

- Develop detailed functional descriptions for levels of driving automation
- Develop a methodology for binning driving automation features to their appropriate automation level using systematic methods
- Develop a list of potential driving automation features that may be emerging on vehicles in the future
- Develop high-level safety principles that apply to the driving automation levels, and thus to the driving automation features that bin to a particular level
- Develop preliminary test methods for Level 2 driving automation

To accomplish these objectives the AVR Project performed the eight tasks below.

Task 1: Technical Project Management
The goal of this task was to provide project oversight to ensure that the project achieved its objectives within the timeframe and resources allocated for the effort. Included in the scope of the project management activities were technical and administrative leadership over all work within the project.

Task 2: Planning and Coordination
The primary objectives of this task were:

- Form a research consortium, operating under the Crash Avoidance Metrics Partnership (CAMP) structure, to execute this project
- Work with the Consortium to finalize a work plan for Tasks 3 through 9
- Provide ongoing coordination with NHTSA regarding program execution and changes to the work plan that may be required as new information is developed within the project

Six Original Equipment Manufacturers (OEMs) were chosen to execute the project:

- Ford Motor Company
- General Motors
- Mercedes Benz
- Nissan
- Toyota
- Volkswagen Group of America

Ford Motor Company was the lead company for the project.

The remaining sections of the AVR Final Report are organized to reflect the sequence of the AVR tasks performed.

Task 3: Functional Descriptions of Proposed Levels of Automation

The objectives of Task 3 were to define functional descriptions for proposed driving automation levels, delineate a methodology and/or set of identifiable characteristics that allow classification of current and new automation features into the appropriate levels, and describe sets of automation functions that fit within the driving automation levels.

The project derived five factors for consideration in defining driving automation levels. At the time this task was begun, several driving automation level definitions were under consideration within organizations worldwide: NHTSA's Preliminary Statement of Policy Concerning Automated Vehicles (NHTSA 2013), SAE J3016:2014 and the German Federal Highway Research Institute (Bundesanstalt für Straßenwesen, or BASt). The outcome of this effort was a set of driving automation levels that were harmonized with SAE J3016 and BASt levels. Additionally, a minimum set of automation functions for each automation level were also identified in Task 3.

Lastly, a methodology that allows classification of new and existing driving automation features into the appropriate levels was described. In order to illustrate the application of the classification methodology, a set of exemplar driving automation features was defined and generic descriptions were prepared for each of the characteristics that differentiate driving automation levels. The features were subsequently classified into driving automation levels.

Task 4: Concept Roadmaps for Future Automated Feature Applications

The objectives of Task 4 were to develop an exemplar list of standard driving automation features that the AVR Consortium believes are likely to be marketed by vehicle manufacturers in the future. The list included applications that are near term (0-4 years), mid-term (5-9 years), and long-term (10+ years) in terms of potential deployment. The list was based only on publicly available information and leveraged work from NHTSA to the extent possible. The list of driving automation features were then compared and contrasted based on the minimum sensing/processing, control functionality and Human-Machine Interface (HMI) required for each feature.

Task 6: Top-Level Safety Principles for Levels of Automation (intentionally conducted ahead of Task 5)

The objectives of Task 6 were to develop a set of solution-neutral, top-level SPs for the partial- through full-automation driving automation levels defined in Task 3. These SPs were generated from a hazard analysis, with the expectation that the SPs would effectively and succinctly address the identified hazards.

The project utilized a hazard analysis strategy based on Systems Theoretic Process Analysis (STPA). In the execution of this process, the project defined *accident* as a loss that results from an undesired and unplanned event and causes human injury or property damage, and focused on vehicle collisions as the primary accident (loss) under consideration. The project defined *hazard* as a system state that together with a worst-case set of external disturbances may lead to a loss, and identified four primary hazards for analysis. The project developed a high-level control structure for each of the driving automation levels defined in Task 3, and considered how errant control actions within the structure may result in a vehicle collision. Safety constraints were developed to prevent each Undesired Control Action (UCA) from resulting in a hazard. The project then summarized the safety constraints developed and constructed a minimum set of safety principles for each driving automation level.

Lastly, matrices were developed to map the alignment of the safety principles to the driving automation levels defined in Task 3 and categorize the safety principles as to whether they apply to the driver/operator, the driving automation system, or the base vehicle. As higher driving automation is developed, a greater number of safety principles will apply to the driving automation system.

Tasks 5 and 7: Development of Objective Safety Principle Assessment Procedures

In Tasks 5 and 7 a Classification and Operational Description for collecting data regarding specific design features from developers was proposed. Further, the team proposed having the developer of the driving automation feature identify the level of driving automation, the accompanying safety principles, and recommended assessment procedures for the individual product. While not providing the traditional fixed requirement and test procedures common to the FMVSS, it is believed this approach provides several key benefits as NHTSA moves toward regulation of these technologies:

- Self-reporting of the system level and intent by the developer
- A framework to establish minimum owner's manual content for customer communication
- A framework to adapt to the rapidly changing technical and competitive environment around driving automation systems
- A framework for NHTSA to learn and see trends relevant to its mission

Tasks 5 and 7 highlighted the systems of most near-term interest to NHTSA as communicated to the AVR Project team, but also left technical details unresolved in the testing of higher level Automated Driving Systems. Fundamentally, Level 2 and lower systems are used by a human driver who still has a role in completing the dynamic driving task in real time. As such the safety principles and the testing for L1 and L2 features revolve around the ability of the driver to take over complete control from the driving automation system at any time and for any reason. Higher level automation (Levels 3, 4, and 5) is distinguished by the system itself formally handling the complete Dynamic Driving Task (DDT). The safety principles and testing of these Automated Driving Systems are therefore very different and focused on performance of the system within its operational design domain. The investigation into the performance requirements of higher levels of driving automation is not presented in this report and could be the subject of future research.

Task 8: Other Critical Tasks

Through the execution of Tasks 1 through 7 the AVR Project team identified several areas of synergy between the AVR project deliverables and other NHTSA projects. Through the execution of Task 6, the AVR team identified several areas of human factors research. The recommendations from the AVR Consortium can be found in Appendix P.

Task 9: AVR Final Report

The final task of the AVR Consortium involved combining the results from the interim reports generated from Technical Task(s) 3, 4, 5, 6, and 7 into a cohesive final report. This report is the product of that effort.

2 Develop Detailed Functional Descriptions of Levels of Automation

2.1 Rationale for Driving Automation Levels

The historical roles of drivers, vehicle manufacturers, federal and state regulators, and law enforcement agencies in maintaining automotive safety is well understood. However, the increasing deployment of driving automation features will begin to alter those roles as various comfort, convenience, efficiency, productivity and mobility features are implemented. Maintaining safety throughout this transition is the highest priority. The AVR Consortium believes that initial automated driving features will likely focus on customer convenience, however indirect safety benefits may be demonstrated in the future. This will depend on several factors, including automation function, the domain in which the automated driving features are designed to operate, and the degree of fleet penetration. Because driving automation systems have not yet been widely deployed and are still evolving while undergoing rapid and competitive development, there is a risk of stifling innovation should standards or requirements for such systems be prematurely defined or imposed. Yet in order to support safety in the development and deployment of driving automation features, it is important to consider and communicate the way in which the role of the driver will change, particularly in this transition period, to avoid issues like abuse and overreliance on technology, among others. because the human inclination is to trust a technology that appears to work properly, perhaps even more than the manufacturer of the technology intended.

The task of driving can be divided into three types of activities necessary to operate a vehicle (Michon, 1985):

- Operational behaviors such as longitudinal and lateral control as well as object and event detection, classification and response execution
- Tactical behaviors such as speed selection, lane selection, object and event response selection, and maneuver planning
- Strategic behaviors including destination planning and route planning

The operational behaviors of longitudinal and lateral vehicle motion control refer to the mostly automatic actions that experienced human drivers use to control vehicle speed (using the accelerator and brake pedals) and vehicle position within the driving environment (using the steering wheel). Object and Event Detection and Response (OEDR) refers to the perception by the driver of any circumstance that is situationally-relevant to the immediate driving task, as well as the appropriate driver response to such circumstance.

Within the overall task of driving, the operational and tactical behaviors relate directly to the dynamic aspects of driving and are thus grouped into what is referred to as the Dynamic Driving Task, or DDT (SAE J3016:2014). An examination of changes in the driver's role in the DDT can provide a basis for categorizing driving automation systems. Together, lateral vehicle motion control, longitudinal vehicle motion control, and OEDR make up the three primary subtasks of the DDT (along with secondary tactical subtasks, such as determining when to change lanes or signaling). A brief explanation of the DDT and other selected terms is presented in the Glossary at the end of the report.

When discussing categorization of driving automation into levels, it is important to clarify the difference between the capabilities for which these level categories are intended and those for which they are not intended. Driving automation systems are designed to provide sustained operation of part or all of the DDT allocated to the system for extended periods of time (i.e., both between and across external driving events that necessitate its response), thus changing the driver's role. Depending on the level in question, the driver's continued involvement may include such things as engaging the driving automation system and resuming control when prompted to do so. A driving automation feature example would be Adaptive Cruise Control (ACC) which responds to external events (slower vehicle ahead), adjusts speed accordingly (between events) and then resumes the set speed when the lead vehicle exits the lane.

Other types of automation that do not perform part or all of the DDT on a sustained basis are not considered driving automation. Some active safety systems may provide temporary or event-based support to the driver by intervening in critical situations, but they do not provide sustained operation of part or all of the DDT, and the driver's role in performing the DDT does not change during their activation. For example, a system such as Electronic Stability Control (ESC) provides only temporary support to the driver for short periods of time by intervening in specified situations, thus enhancing the driver's performance rather than altering their role. Conventional Cruise Control (CC), while performing sustained closed-loop control of vehicle speed, does not react to any external driving events or objects and therefore, does not alter the role of the driver in the performance of the DDT. Driving automation systems differ fundamentally from other types of automation systems applied to vehicles in their intent, extent and/or duration, because they alter the role of the driver in performance of the DDT.

Traditionally, the design of the machine or automobile has focused around responding to driver inputs in a predictable and prescribed way with high reliability. The use of the machine and the commands issued to the machine are a role entirely performed by the driver based upon his or her perception, experience and desired outcomes. Figure 1 depicts the combined HMI that constitutes the traditional DDT for human operation of a vehicle without a driving automation system.

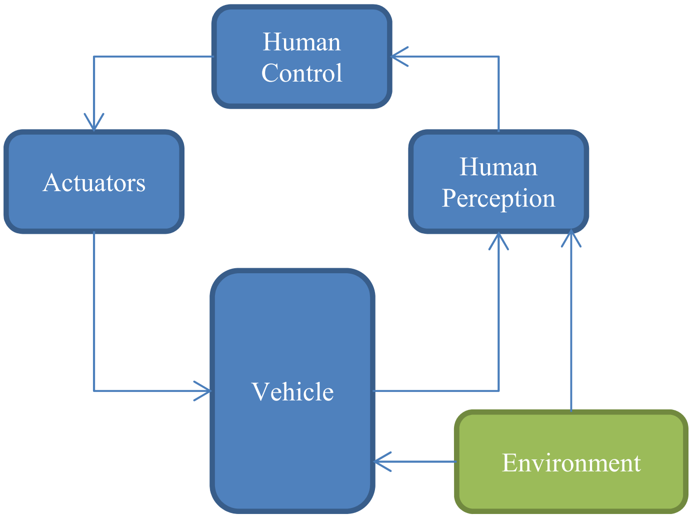


Figure 1: Human Operation of a Traditional Vehicle – the Dynamic Driving Task

Automation of elements of the DDT is not new to the automotive industry. However, successful automation to date has focused on rather specific functions designed to assist the driver while he or she otherwise maintains overall authority for use and motion control of the vehicle. These assist functions improve the interface between the driver and the vehicle in such a way as to provide better control or more convenient operation but do not substantially alter the role of the driver in performing the DDT. Consider ACC as an example. The driver must turn the feature on and select a desired speed. Once turned on, this driving automation system will maintain that speed until it detects a slower-moving vehicle in its pathway, at which point it will automatically adjust the vehicle speed to maintain a fixed distance to the lead vehicle. The automation system is not assessing the traffic or weather, nor making an attempt to assess the safe speed for the current road conditions. The automation system is also not considering whether to change lanes and go around a slower-moving lead vehicle, or how to avoid suddenly-appearing hazards, such as a close-cutting vehicle, or a large pot hole. Rather, these latter functions are performed by the driver, even while an ACC system is active. In this sense, safety performance is an outcome of the combination of the attributes of the design of the ACC system and the driver's proper use of it. Safety performance, as measured through accident statistics, is a function of the man-machine combination executing all facets of the DDT correctly and in unison, and is not solely a function of the design of the machine.

The invention of new driving automation capabilities that enable additional portions of the driving task to be reallocated from the driver to the vehicle could potentially alter the traditional driver-vehicle relationship. Consider Figure 2 where both the human driver and the machine may have the ability to control the vehicle.

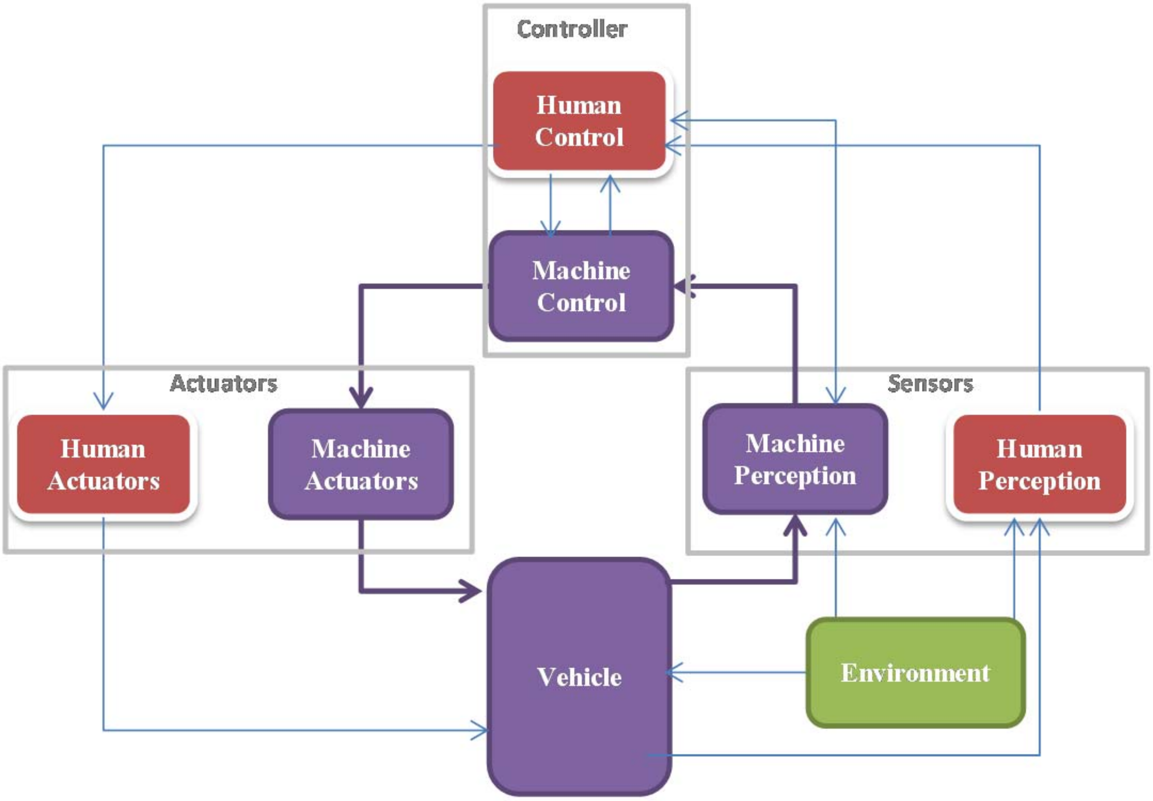


Figure 2: The Introduction of Machine Automation to the DDT

The various subtasks that comprise DDT performance have not necessarily been altered in number or scope, but, with the addition of driving automation capability, they may now be expected to be performed by either the human driver, the driving automation system or both. It is this design allocation of the various subtasks that make up the DDT to either the machine or the human driver that initially motivates the discussion of categories or "levels" of automation. Engineers, designers, and policy makers, including regulators, benefit by having a methodology to clearly and functionally categorize degrees of automation of the DDT in order to assist in communications between these stakeholder groups. However, it is also important for the driver to understand their role in the proper usage of a driving automation system in order for the driver-vehicle system to function as intended. The coordination of the driver and the driving automation system in the execution of the DDT, when elements of it are distributed between man and machine, are key to the safe operation of the vehicle.

For example, consider an automated parallel parking feature such as that currently equipped on some production vehicles. Some executions require the driver to engage the system to look for a parking space on a particular side of the vehicle. Upon scanning an available parking space, the system provides either a confirmation of the ability to park or a denial for the automation if no suitable physical space is found. If a physical space is found and the driver confirms the desire to park, the system will automate the lateral control subtask of the DDT to enter the space while the driver performs the longitudinal control as well as the OEDR subtask of the DDT. In making the decision to allow the vehicle to park, the driver is also judging the performance of the automation and ultimately maintaining total control of the vehicle. If the machine-executed steering might lead to a collision, the driver is expected to stop the automated parking maneuver, and at all times has the vehicle control authority to do so. The system is assisting the driver in executing a steering maneuver, just as ACC assists the driver in maintaining a desired speed and headway, but the driver has the role and authority to take actions to avoid collisions. The elements of Figure 2 are preserved, but the functions expected of the driver and system are different than parallel parking executed according to Figure 1.

Now consider a new parking feature which, in addition to automating lateral control, also automates longitudinal control during the parking maneuver. This type of automation of the motion control function of the vehicle is well within the scope of existing technology; in fact, the system may be capable of actuating the longitudinal motion with a precision beyond the driver's capability. But what of the task of deciding if the vehicle sensors have adequately mapped the physical space? Recall in the previous example, the human driver was performing two roles: to control the longitudinal motion of the vehicle and to decide if longitudinal motion was appropriate, namely, the OEDR portion of the DDT. A system that automated the longitudinal control only, but relied on the driver to maintain the task of determining if the automation was appropriate, would be different from a system that automated both the longitudinal control and lateral control subtasks, but not the complete OEDR. In the latter case, in order to operate the vehicle safely and successfully, the driver is expected to understand the limits of the automation, namely, its incomplete capability to detect and avoid all situationally-relevant objects and events in the pathway of the vehicle, and to complement that capability by completing the DDT.

As driving automation technology begins to alter the allocation of DDT subtasks between the driver and driving automation system, two fundamental points emerge:

- Proper use of the technology requires the driver to perform all aspects of the DDT that are not performed by the driving automation system
- The driving automation system manufacturer should consider all aspects of the DDT and design it such that the system and the driver individually or together perform all of the DDT

This paper defines categorical divisions (or "Levels") for driving automation and the accompanying assignment of roles for the driver and driving automation system in order to provide a common understanding of the capabilities and limitations of specific driving automation systems among stakeholders. These levels are based on the functional capabilities of the automation and their impact on driver roles and expected uses. The following five factors guided this effort to define levels of automation:

- The levels should seek to remove ambiguity from both the driver's and manufacturer's standpoint by focusing on the functional attributes of driving automation that clearly characterize the relative roles of the driver/operator and the driving automation system in performing the DDT
- The levels should ensure a unique classification of any system

- The levels should be defined such that engineering direction regarding relevant requirements and test procedures can be assessed at the time a design proposal is generated, and not just after development is completed
- The levels should be simple enough that they convey meaning and define expected usage for the driver as well as the system designer
- The levels should allow the classification of current and forecasted automation features independent of the technology chosen to achieve the automation

2.2 Rationale for Specific Levels of Driving Automation

In addition to the levels defined within the NHTSA's Preliminary Statement of Policy Concerning Automated Vehicles (NHTSA, 2013), several automation level definitions are under consideration within organizations worldwide. These include SAE J3016: JAN2014 and BASt. Other organizations have rendered opinions on the existing levels, such as the International Association of Automotive Associations (French acronym, OICA), the European Automobile Manufacturers Association (French acronym, ACEA) iMobility Forum, and the German automotive manufacturers association (German acronym, VDA). Since SAE J3016 was published in January 2014, OICA, ACEA and VDA have all explicitly endorsed it.[1] Moreover, VDA has begun the process of working with BASt to revise its levels to align (in English) with J3016, including the addition of a sixth level to represent "full automation."

The SAE J3016 driving automation levels appear to offer the greatest alignment to the project findings, as detailed below, and the aforementioned five factors for consideration in defining automation levels. In addition, the SAE levels provide a clear and logical framework for categorizing the types of driving automation features actually being developed and described in publications.

The following discussion provides rationale for, and further details of, certain aspects of the levels.

As discussed in the prior section, the driving automation system and the driver must individually or together perform all subtasks of the DDT on a sustained basis (i.e., between and across external driving events). A given driving automation system may be capable of performing part or all of the DDT in some or all driving conditions, modes, and/or geographical locations, but either the driver or the automation system must provide fallback capability in the event that the automation system reaches the limits of its operational design domain, or an automation system or vehicle failure occurs.

The least amount of driving automation (Level 1) has only the functional capability to perform (in part or in whole) either longitudinal or lateral control on a sustained basis relative to external objects or events, so the driver must continue to perform the remainder of the DDT. Systems of this type, such as ACC, which provides both braking and acceleration as well as some OEDR, have been widely deployed, and drivers' proper

[1] OICA: Informal document No. WP.29-162-20, 162th WP.29 session, 11-14 March 2014, agenda item 20. ACEA: iMobility Forum: "Workshop WG Automation – Deployment Paths," July 5, 2014. VDA: "Automated driving - motivation and need for action," Berlin, December 24, 2013.

use of the systems has been confirmed through extensive research and production experience. Thus, with less capable driving automation where only part of the DDT can be automated, the functional capability to perform (in part or in whole) either longitudinal or lateral control within a limited operational design domain is the relevant distinction to determining the level of the automation.

With somewhat more capable driving automation (Level 2), the system performs both sustained longitudinal and lateral control to external objects and events simultaneously within its operational design domain, but cannot perform the complete OEDR subtask, and thus the driver must perform the remainder of the OEDR subtask. In this case, the driver's "supervisory" role may not be as natural for drivers, and may be associated with "complacency" (Salinger et al., in publication; Llaneras et al., 2013). Complacency has been defined, for example, as, "…when…[an operator] over-relies on and excessively trusts the automation, and subsequently fails to exercise his or her vigilance and/or supervisory duties" (Parasuraman, 1997), and, "Self-satisfaction which may result in non-vigilance based on an unjustified assumption of satisfactory system state" (Billings, et al., 1976). As appropriate, manufacturers and suppliers of driving automation features that provide simultaneous longitudinal and lateral vehicle motion control may choose to apply countermeasures to address complacency and assist drivers in properly using the feature.

At Level 3, driving automation features can perform the complete DDT within their operational design domain, providing appropriate responses to relevant objects and events, but require the driver to take over in the event that the vehicle is about to exit its operational design domain, or when certain types of failures occur. As a result of this conditionality, the driver (or operator) must be available and able on short notice to take over the performance of the DDT from the driving automation system under conditions that exceed its operational capability.

At Level 4, driving automation features are able to perform the complete DDT within the system's operational design domain, and to automatically bring the vehicle to a "minimal risk condition" (SAE, 2014) without reliance on the driver in the event that the system is no longer operating within its design domain ("conditionality"), or the system and/or vehicle experiences a failure, and no driver intervenes (this is commonly referred to as "fallback" capability). Thus, "conditionality" and "fallback" capability are the characteristics that separate higher levels of automation.

At the highest level of driving automation (Level 5), the system is capable of performing the complete DDT and automatically bringing the vehicle to a "minimal risk condition" under all on-road driving conditions in which the operator is legally permitted to operate a vehicle. In short, relative to a Level 4 driving automation system, a Level 5 system is not limited to a prescribed operational design domain.

Thus, the automation levels are differentiated according to the following functional characteristics (which are further defined within SAE J3016 as well as German BASt documents)

- Primary subtasks of the DDT
    - Lateral control subtask
    - Longitudinal control subtask

  - OEDR subtask
- Functional capabilities
  - Fallback capability
  - Operational design domain

Using these functional characteristics, and considering that higher degrees of automation exceed and include lesser automation capabilities, it is possible to define step-wise levels of increasing driving automation that provide a framework for creation of a driving automation classification method. Table 1 provides a visual overview of the SAE/BASt levels and illustrates the distribution of functions by automation level to either the driver or the automation system. A detailed description of each level in the taxonomy will follow in subsection 2.4.

Table 1: Distribution of Functions by SAE/BASt Driving Automation Level

Automation Level Name	Automation Level Narrative Description	Dynamic Driving Sub-Tasks		Functional Capability	
		Sustained Lateral and/or Longitudinal Control to External Objects or Events	**Completes the Object & Event Detection and Response (OEDR) Subtask**	**Fallback Performance of Dynamic Driving Task**	**Operational Design Domain (ODD) Capabilities**
Driver performs all or part of the dynamic driving task (DDT) and general system functional capabilities					
0 **No Automation**	The full-time performance by the driver of all aspects of the DDT, even when augmented by other systems	Driver	Driver	Driver	None of the DDT is automated
1 **Driver Assistance**	The execution by a system of either sustained lateral **OR** sustained longitudinal control with the expectation that the driver performs the remainder of the DDT	Driver and system	Driver	Driver	ODD limited
2 **Partial Automation**	The execution by one or more systems of both sustained lateral **AND** sustained longitudinal control with the expectation that the driver performs the remainder of the DDT	System	Driver	Driver	ODD limited
3 **Conditional Automation**	The ODD-limited performance by a system of all aspects of the DDT, providing appropriate responses to relevant objects and events, but relying on the human driver to provide fallback performance capability when prompted by the automation system (i.e., when about to exit its ODD or a relevant failure has occurred in the driving automation system), or when certain vehicle failures occur	System	System	Driver	ODD limited
4 **High Automation**	The ODD-limited performance by a system of all aspects of the DDT, providing appropriate responses to relevant objects and events, even if a driver does not respond appropriately to a request to resume performance of the DDT	System	System	System	ODD limited
5 **Full Automation**	The full-time performance by a system of all aspects of the DDT, providing appropriate responses to relevant objects and events, under all on-road driving conditions legally available to a driver	System	System	System	No ODD limit
Higher driving automation systems perform the complete DDT, providing appropriate responses to relevant objects and events, and greater functional capability					

2.3 Application of Driving Automation Levels

Levels apply to the set of all driving automation system functions classifiable under this taxonomy that a driver can engage simultaneously. They apply independently of Operational Design Domain (ODD), or of which system (or feature or application) is said to be delivering the function.

The ODD of a driving automation system refers to the specific operating conditions under which it is designed to function, and outside of which it is designed not to function. These may include geographic, roadway, environmental, traffic, speed, and/or temporal conditional limitations. For example, a level 4 driving automation system (feature) may be designed to operate a vehicle only within a geographically-defined (i.e., geo-fenced) military base, only under 25 mph, and only in daylight. An ODD may also be described in terms of driving or operating modes that prescribe a specific type of driving scenario with characteristic dynamic driving task requirements (e.g., expressway merging, high-speed cruising, low-speed traffic jam, etc.). For example, a given driving automation system feature may be designed to operate a vehicle only on fully access-controlled freeways and in low-speed traffic, high-speed traffic, or in both of these driving/operating modes.

A vehicle may be equipped with one or more driving automation features that serve specific use cases and which may be used in combination. As such, a given driving automation system may be able to provide different levels of driving automation capability for the driver, as engaged by the human driver. For example, a driving automation system that provides Level 1 lane centering capability, as well as a Level 1 ACC capability, delivers Level 2 capability when both Level 1 features are engaged simultaneously. The driver therefore experiences a driving automation operating state that changes as none, one, or more driving automation functions are engaged or disengaged. The driving automation levels, while functionally defined, describe the roles of the driver and the automation system for a given level of driving automation capability. Driving automation levels do not apply to a vehicle as a whole, because many vehicles equipped with a driving automation system will also be capable of and often operate at Level 0 (non-automated driving), so it is a misnomer to refer to such a vehicle as "an automated vehicle." Further, terms such as complete "autonomy," "autonomous" or "self-driving" may be confusing and not useful in a technical context even at Level 5, because even such a driving automation system does not completely automate the entire *vehicle* (i.e., including features unrelated to driving), nor determine for the user where it ought to go and whether to stop anywhere on the way.

2.4 Detailed Discussion of Driving Automation Levels

Level 0: No Driving Automation – Vehicle systems and features in this level do not automate (in part or in whole) any of the dynamic driving subtasks on a sustained basis to external objects or events, and as such, are not driving automation. The driver of a vehicle without a driving automation system must perform the complete DDT, providing appropriate responses to relevant objects and events in all operating domains, and must achieve a minimal risk condition in the event of a relevant vehicle failure. Alert systems that support the driver's OEDR performance (e.g., forward collision warning, lane departure warning, blind spot warning), and systems that intervene momentarily in affecting lateral and/or longitudinal control of the vehicle to prevent or mitigate collision (e.g., crash imminent braking systems, electronic stability control, anti-lock brake systems, dynamic brake support) are included in Level 0, as they do not automate part or all of the DDT on a sustained basis to external objects or events.

> **Note**
>
> Systems classified here as a Level 0 system, i.e. not a driving automation system, could still be classified under another taxonomy, for example as an active safety system or driver assistance taxonomy.

Level 1: Driver Assistance – Driving automation system features in this level automate on a sustained basis either the lateral control subtask of the DDT, or the longitudinal control subtask of the same, but not both simultaneously. In order to perform either the lateral or longitudinal control subtask on a sustained basis (i.e., both between and across relevant external driving events), a Level 1 automation system must also perform part, but not all, of the OEDR subtask associated with that aspect of vehicle control (i.e., lateral or longitudinal vehicle control automation in Level 1 entails sustained control to external objects and events). The driver of a vehicle equipped with an active Level 1 driving automation system must perform the full remainder of the DDT, and must achieve a minimal risk condition in the event of a relevant automation system or vehicle failure.

Level 2: Partial Automation – Driving automation system features in this level automate on a sustained basis both the lateral and longitudinal control subtasks of the DDT simultaneously. In conjunction with performance of the lateral and longitudinal control subtasks, a Level 2 automation system performs part, but not all, of the OEDR subtask. That is, the driver of a vehicle equipped with an active Level 2 driving automation system must still perform the full remainder of the DDT (i.e., complete the remainder of the OEDR subtask) and recognize the system's ODD limits, as well as achieve a minimal risk condition in the event of a relevant automation system or vehicle failure. Note that this OEDR completion role of the driver requires the driver to devote the same level of *active* monitoring, or attention, to the external driving environment, as they would need to devote in the absence of any driving automation. In this way, the driver *supervises* the performance of the driving automation in the external environment.

> **Note**
>
> Level 2 driving automation systems may present unique human factors considerations therefore it is helpful to differentiate systems which when used in combination can become Level 2 from those that cannot. Thus the distinction between Level 1 and Level 0 becomes of particular interest by delineating systems that alter the driver's role in performing the dynamic driving task (Level 1) from those that do not (Level 0).
>
> We note that at this point in the hierarchy of levels, a critical distinction is made between driving automation at Levels 1 and 2 and driving automation at Levels 3-5, namely, Levels 1 and 2 encompass features that automate part, but not all, of the DDT, whereas Levels 3-5 encompass

> features that automate the entire DDT, whether on a part-time basis (limited ODD) or full-time basis (unlimited ODD). Because automation systems in Levels 3-5 are capable of performing the complete DDT, they are referred to in this report as “higher” driving automation systems, while Levels 1 and 2 are referred to as “lower” driving automation systems. Vehicles equipped with higher driving automation systems are commonly referred to as “autonomous” or “self-driving” vehicles in state government and media publications. This technical document does not use the terms “autonomous” or “self-driving” because these terms may incorrectly imply that a driving automation system is capable of independently changing the rules by which it operates, and because, as stated above, driving automation levels do not apply to whole vehicles.

Level 3: Conditional Automation – Higher driving automation system features in Level 3 automate the complete DDT on a sustained basis within a limited ODD, providing appropriate responses to relevant objects and events. However, they do not automatically achieve a minimal risk condition in the event of a failure or by exceeding the feature’s ODD (i.e., they do not provide automated fallback performance capability). That is, Level 3 driving automation features are capable of performing the complete DDT under limited conditions, outside of which the driver must perform or complete the DDT.

In the event that the driving automation system is about to leave its ODD *or* experiences a relevant driving automation system failure, it will warn the driver of the need to resume performance of the DDT far enough in advance to permit an orderly transfer of control. If the driver fails to respond in time to a such a takeover warning, the automation system may not be able to achieve a minimal risk condition in all cases, which may create a safety risk. In addition, the driver’s fallback role includes detecting base vehicle failures.

The driver’s role while using a Level 3 driving automation feature includes being sufficiently alert and physically in position to be able to recognize and act appropriately either to automation system-initiated takeover requests, or to base vehicle failures unrelated to the automation system. Supervision of the automation system operation or the driving environment is *not* part of the driver’s role while a Level 3 system is operating. This differentiation is best understood in terms of visual attention: the driver’s visual attention is not required to be focused on the external driving environment (e.g., roadway) *at all* during Level 3 operation, nor is it the driver’s role to evaluate the performance of the driving automation system. This is because the driver does not have the role of performing the OEDR subtask of the DDT, nor of detecting automation failures or evaluating automation performance. The driver’s role is limited to perceiving (through visual, auditory, haptic and/or kinesthetic senses) a takeover request issued by the driving automation system, or a vehicle failure that requires immediate attention (e.g., a flat tire, broken axle, or serious engine failure), and respond by taking over the DDT.

While drivers may glance (visually attend) to the external environment or to automation displays during Level 3 operation, it is the role of the driving automation system to *get the driver’s attention* for a takeover request. The driver is otherwise expected to have his or her attention focused on non-driving tasks during Level 3 driving automation system activation. This is the critical difference in the driver’s role, and in associated functional requirements between Level 2 and Level 3 driving automation. By contrast, during Level

2 driving automation, the driver must complete the DDT by continuing to pay attention to the driving task and actively supervising the driving automation system's performance and must take over control when needed (e.g., due to a developing circumstance outside the vehicle, changes in performance of the automation, or an imminent exiting of the system's operational design domain). In Level 3, the driving automation system has the role to monitor its own performance and the external environment, and to respond to all relevant objects and events. It must also determine whether it is operating within its design domain and issue a takeover request to the driver in preparation for exiting the automation ODD. Thus in Level 3 automation, the driver has only the role to notice and respond to a driving automation system takeover request, and can confidently perform non-driving tasks (unless and until there is a takeover request) that would otherwise be incompatible with driving.

Due to changes in the focus of the driver's attention prior to and following a driving automation system request for takeover, there are important human factors considerations to address in the design of these systems and alerts. These human factors topics related to the driver fallback role are outside the scope of the present project and are being addressed in other NHTSA research efforts (e.g., the Human Factors Evaluation of Level 2 and Level 3 Automated Driving Concepts Project).

Level 4: High Automation – Driving automation system features in this level automate the complete DDT within a limited ODD. In the event that the system is about to transition out of its ODD *or* if a relevant failure in the system and/or base vehicle occurs, the automation system may alert the driver (or remote operations center) of the need to resume performance of the DDT far enough in advance to permit an orderly and safe transfer. If the driver (or remote operations center) fails to respond in time to such a takeover warning, the system will automatically achieve a minimal risk condition. (Note that the difference between Level 3 and Level 4 driving automation systems is that the latter will reliably achieve a minimal risk condition without driver support, whereas the former will not reliably do so.)

Level 5: Full Automation – A driving automation system in this level automates the complete DDT in all designated or prepared surface operational domains in which a human driver can prudently drive. A Level 5 driving automation system will automatically achieve a minimal risk condition in the event of a driving automation or base vehicle failure.

To conceptually show the changing role of the driver, a graphical representation is shown in the figures below. The performance of the DDT encompasses the interaction of the driver, vehicle, environment, and automation system. The progression of increasing automation shows how the driver's role changes in relation to the DDT and ultimately when the driver's role is no longer part of the DDT performance.

In vehicles without driving automation, the driver performs the complete DDT (i.e., controlling the vehicle and responding to the environment) as shown in Figure 3a. With the introduction of a lower automation system, the driver and the automation together complete the DDT (Figure 3b). If the driving automation system is capable of performing the complete DDT, but otherwise relies on the driver to take over when requested to do so by the driving automation system (i.e., Level 3), the driver's role is outside of the

DDT. The driver's only role is to respond to automation system takeover requests and to respond if needed to certain vehicle failures, such as engine failure, flat tire or broken suspension component (Figure 3c). Finally, when the automation system can perform the entire DDT, as well as provide automated fallback by achieving minimal risk condition in the event of all foreseeable automation/vehicle issues (Figure 3d), the driver is no longer required to perform any part of the DDT or fallback either within the driving automation feature's ODD (Level 4), or at all (Level 5).

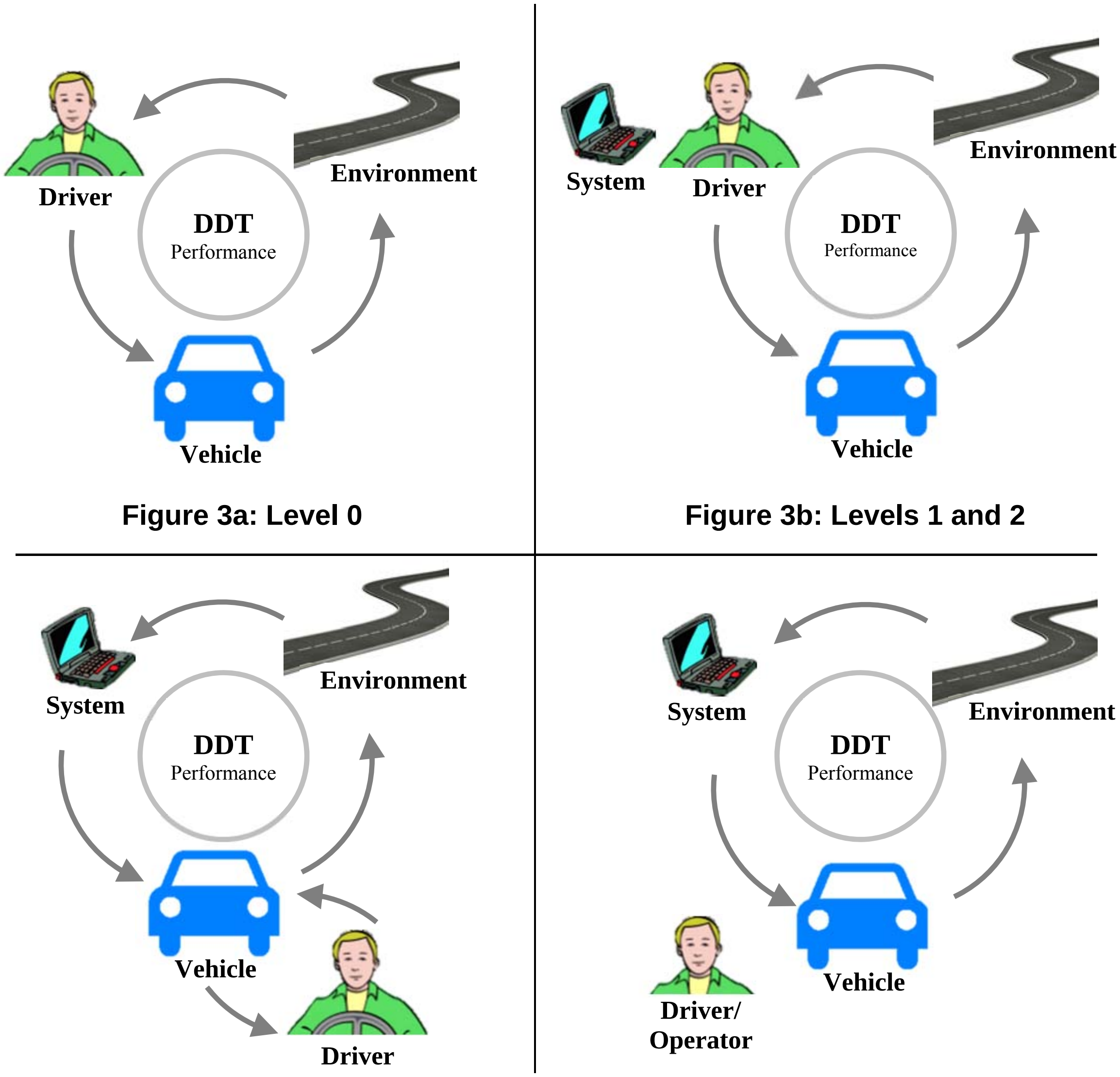


Figure 3a: Level 0

Figure 3b: Levels 1 and 2

Figure 3c: Level 3

Figure 3d: Levels 4 and 5

Figure 3: The Changing Role of the Driver

2.5 Identification of Minimum Automation Functions by Driving Automation Level

In this section, the minimum set of automation functions for each level of driving automation is presented. Minimum sets are presented in part because high levels of automation include the functional capabilities of lower levels of automation. Thus, as previously noted, levels apply to the set of all driving automation system functions classifiable under this taxonomy that a driver can engage simultaneously. Also, as discussed previously, while a portion of the OEDR subtask is performed by a given driving automation system, such a system does not qualify as higher automation unless the complete DDT is performed by it, including the complete OEDR subtask. Similarly, driving automation is not qualified as Level 4 unless it is also able to achieve a minimal risk condition whenever and wherever a transition is warranted. Finally, most driving automation features will operate only with a limited ODD. Driving automation systems only qualify as Level 5 automation if they are capable of operating in all legal on-road driving conditions (i.e., without a manufacturer-specified ODD).

Level 0: No part of the DDT is automated on a sustained basis.

Level 1: The driving automation system performs one "operational" motion-control subtask of the DDT on a sustained basis

- Longitudinal vehicle motion control to objects or events OR
- Lateral vehicle motion control to objects or events

The driver's role is to perform the remainder of the DDT by performing the other dimension of control (either lateral or longitudinal), completing the OEDR subtask of the DDT, and performing other tactical subtasks (Section 2.1).

Level 2: The driving automation system performs both motion-control subtasks of the DDT simultaneously and on a sustained basis:

- Longitudinal vehicle motion control to objects or events AND
- Lateral vehicle motion control to objects or events

The driver's role is to complete the object and event detection and response subtask of the DDT. The driver must also perform certain tactical subtasks of the DDT.

Level 3: The system performs the complete DDT on a sustained basis, providing the appropriate responses to relevant objects and events and including all of the following functions:

- Longitudinal vehicle motion control
- Lateral vehicle motion control
- Complete performance of OEDR

Level 3 automation is limited in its ODD and is capable of detecting when its ODD limits are about to be exceeded and alerting the driver of the need to takeover performance of the DDT.

Level 3 automation must also perform the tactical subtasks of the DDT within its ODD. There is no minimum set of functions applicable to all Level 3 automation, because the functions will vary depending on the specific feature and its ODD.

Tactical subtasks performed by a Level 3 system, depending on the specific feature and operational design domain, could include:

- Speed selection
- Lane selection
- Maneuver planning and execution, e.g., parking-related motions (turning, deceleration, potentially gear selection), lane changes, intersection turns, signaling

All or a subset of these functions may be included in a specific Level 3 driving automation system implementation. This depends entirely on the driving modes and/or conditions supported by a given driving automation feature.

Situations may arise in which a particular Level 3 driving automation feature may no longer be able to operate normally. In such cases, a take-over request is issued by the system to the driver. This occurs before the Level 3 automation system drives out of its ODD (e.g., no longer on freeway), or if there is a relevant failure in the automation system. In such cases, a Level 3 driving automation system must recognize these events and alert the driver of the need to resume performance of the DDT. It is then the driver's role to respond appropriately to the system-generated alert by resuming performance of the DDT. In the case of a relevant base vehicle failure (e.g., engine failure, flat tire, broken suspension component), the driver has the role to notice the failure and take over control of the vehicle, even if not alerted to do so by the Level 3 driving automation system.

Level 4: The system performs the complete DDT on a sustained basis, providing the appropriate responses to relevant objects and events and including all of the following functions:

- Longitudinal vehicle motion control
- Lateral vehicle motion control
- Complete performance of OEDR

Level 4 automation is limited in its ODD and is capable of detecting when these limits are about to be exceeded; in that event the system may alert the driver (or remote operations center) of the need to takeover performance of the DDT, but will otherwise automatically fallback to a minimal risk condition.

Level 4 automation must also perform the tactical subtasks of the DDT within its ODD. There is no minimum set of functions applicable to all Level 4 automation, because the functions will vary depending on the specific feature.

Tactical subtasks performed by a Level 4 system, depending on the specific feature and ODD, could include:

- Speed selection

- Lane selection
- Maneuver planning and execution, e.g., parking-related motions (include turning, deceleration, potentially gear selection), lane changes, intersection turns, signaling

A subset or all of these functions may be included in a specific driving automation system implementation, depending on the ODD supported by it.

The driver is not required to perform any part of the DDT once Level 4 automation has been engaged. When a Level 4 automation system has been engaged, but then is no longer able to operate normally, it must be capable of recognizing this without the driver's help and automatically bringing the vehicle to a minimal risk condition. However, as a practical matter, because a given Level 4 driving automation system may be designed to operate only in specific modes during a trip where a human driver otherwise performs the DDT, a driver may prefer to respond to a takeover request before the automated fallback to minimal risk condition takes place in order to complete the trip. Conversely, because Level 4 driving automation systems are capable of performing the complete DDT, as well as providing automated fallback to minimal risk condition in any event, this is the first level of higher automation that is capable of operating a vehicle within its ODD without the presence of a human driver prepared to take over the DDT if needed.

Level 5: The driving automation system performs the complete DDT on a sustained basis in all legal driving modes and conditions (i.e., is not subject to operation design domain limitations). It performs all of the functions from this list:

- Longitudinal motion control
- Lateral motion control
- Complete performance of OEDR

Level 5 automation performs all tactical subtasks of the DDT as well. The minimum set of tactical subtasks includes:

- Speed selection
- Lane selection
- Maneuver planning and execution, e.g., parking-related motions (include turning, deceleration, potentially gear selection), lane changes, intersection turns, signaling

A driver is not required for DDT or fallback performance during Level 5 automation, although it should be noted that nothing precludes the possibility of designing a vehicle that is capable of multiple levels of driving automation, up to and including both Level 0 and Level 5.

2.6 Methodology for Classifying Features to Driving Automation Levels and Example Classifications

2.6.1 Methodology for Classifying Features

As shown previously in Table 1, there are four important characteristics that differentiate the levels of automation:

- The sustained performance of the lateral and/or longitudinal subtasks of the DDT
- The performance of the OEDR subtask of the DDT
- The fallback/minimal risk condition capability
- The applicability of ODD limitations

Given these characteristics of driving automation features and automation levels, a methodology can be proposed to allow an OEM to properly assign a new automation feature to an appropriate automation level. A series of sequential questions are as follows:

1. Does the feature perform sustained control of lateral <u>or</u> longitudinal vehicle motion to external objects or events in lieu of the driver?
   a. No: ***Level 0***
   b. Yes: Proceed to Question 2
2. Does the feature perform both sustained longitudinal <u>and</u> sustained lateral control to external objects or events in lieu of the driver?
   a. No: ***Level 1***
   b. Yes: Proceed to Question 3
3. Does the feature require supervision by the driver during its normal operation?
   a. Yes: ***Level 2***
   b. No: Proceed to Question 4
4. Does the feature rely on the driver to take over if it is not operating normally?
   a. Yes: ***Level 3***
   b. No: Proceed to Question 5
5. Does the feature have a limited scope of operation?
   a. Yes: ***Level 4***
   b. No: ***Level 5***

Figure 4 shows a flow-chart which distills the methodology for classifying automation features to levels of automation introduced in the previous subsections of this document. The encircled numbers shown in the figure are the automation levels, resulting from following the Y(es) or N(o) paths when answering the specified questions sequentially from top to bottom.

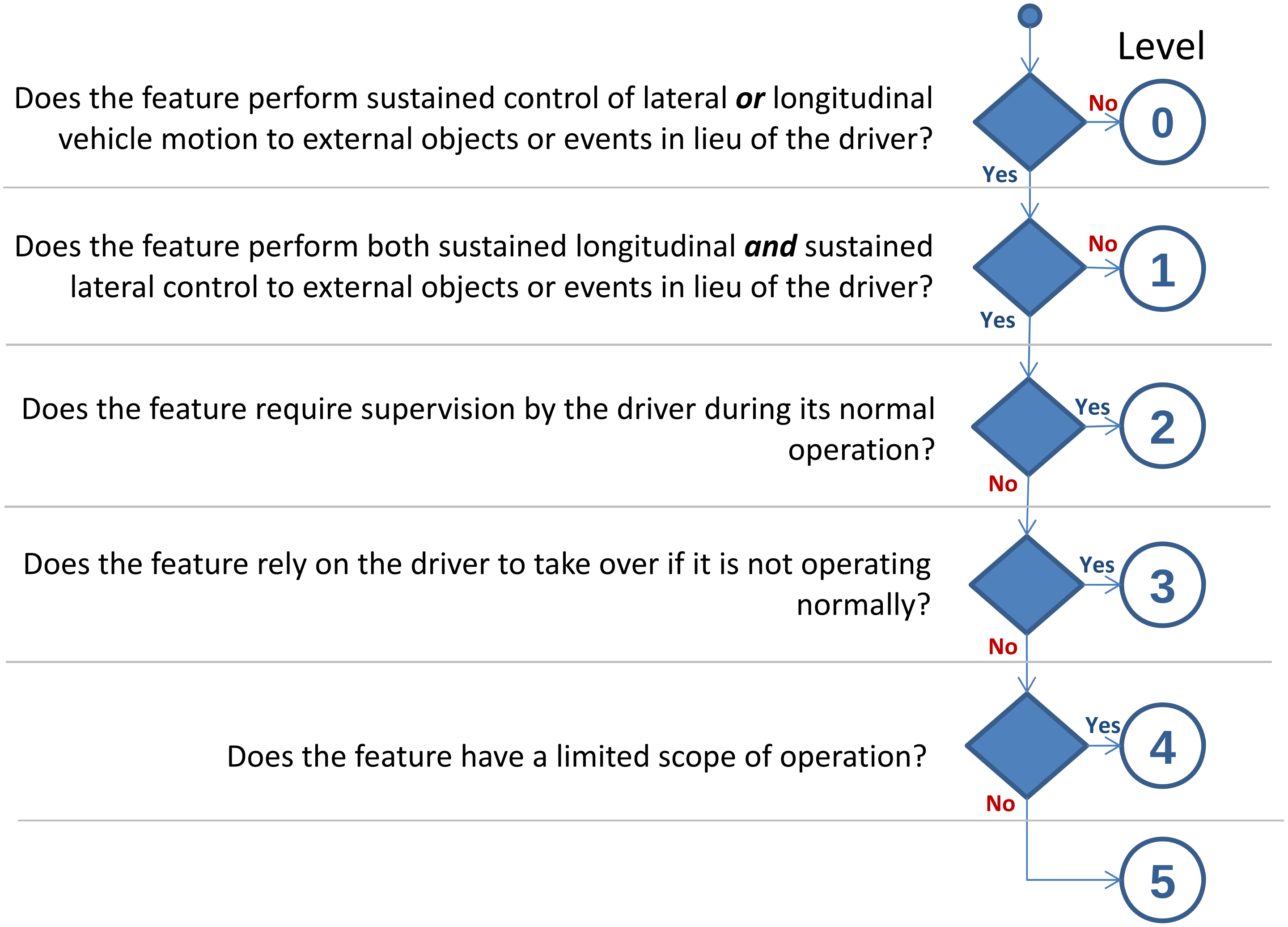

Level
Does the feature perform sustained control of lateral *or* longitudinal vehicle motion to external objects or events in lieu of the driver?
No
0
Yes
Does the feature perform both sustained longitudinal *and* sustained lateral control to external objects or events in lieu of the driver?
No
1
Yes
Does the feature require supervision by the driver during its normal operation?
Yes
2
No
Does the feature rely on the driver to take over if it is not operating normally?
Yes
3
No
Does the feature have a limited scope of operation?
Yes
4
No
5

Figure 4: Flow Chart Illustrating the Methodology for Classifying Automation Features to Levels of Automation

2.6.2 Example Classification of Driving Automation Features Using Methodology

2.6.2.1 Overview of Driving Automation Features

The following list of driving automation features is provided to illustrate the use of the classification methodology. The descriptions are reproduced from the corresponding references, whenever available. The next two sections of the report, respectively, provide an example of a single automation feature classified to a level using the methodology and the summary results of mapping a larger list of features to automation levels.

- Level 1, Adaptive Cruise Control (ACC): While engaged, it performs longitudinal control within a limited driving domain (e.g., speed range, acceleration and deceleration/coast capability, environmental conditions). ACC performs distance (headway) control to some detected objects in addition to its speed control capabilities. As with conventional cruise control, driver supervision is required (see also Section 2.6.1). This system is Level 1 because it performs sustained longitudinal vehicle motion control, but does not also perform simultaneous sustained lateral vehicle motion control.

- Level 1, Cooperative Adaptive Cruise Control (C-ACC): Same as ACC except the ACC-equipped vehicle and other vehicles in front of it are equipped with Vehicle-to-Vehicle (V2V) communication capabilities so as to inform each other of their current speed and other operationally relevant parameters (Nowakowski et al., 2010). This system is Level 1 because it performs sustained longitudinal vehicle motion control, but does not also perform simultaneous sustained lateral vehicle motion control.
- Level 2, Super Cruise: “Super Cruise is capable of semi-automated driving including hands-off lane following, braking and speed control under certain driving conditions. The system is designed to ease the driver’s workload on freeways only, in bumper-to-bumper traffic and on long road trips; however, the driver’s attention is still required” (General Motors, 2013). This system is Level 2 because it performs both sustained lateral (automated lane centering) and sustained longitudinal (automated braking and acceleration) vehicle motion control, and the driver must continue to supervise in real time the system’s performance in light of the traffic environment while engaged.
- Level 2, Traffic Jam Assistant: “The traffic jam assistant helps you in monotonous situations on the motorway. In dense traffic at speeds of up to 60 km/h, the system allows you to move easily along with the traffic and stay relaxed. It automatically maintains the desired distance from the vehicle ahead and regulates the car’s speed right down to standstill − as well as providing active steering support, too. This helps you stay on track, providing you keep at least one hand on the steering wheel” (BMW AG, 2013). This system is Level 2 because it performs both sustained lateral (automated lane centering) and sustained longitudinal (automated braking and acceleration) vehicle motion control, and the driver must continue to supervise in real time the system’s performance in light of the traffic environment while engaged.
- Level 2, Highway Driving Assist: “Toyota’s Automated Highway Driving Assistant: The first part of the system is the Cooperative-adaptive cruise control, essentially a next-gen automated cruise control. The system uses 700 MHz band vehicle-to-vehicle ITS communications to gather acceleration/ deceleration data from the vehicles ahead and maintain a safe, uniform following distance. The second part of AHDA is Lane Trace Control, which Toyota described to us as a more advanced form of its Lane Keeping Assist system. Current-generation lane systems simply provide a warning or minimal amount of steering feedback when the vehicle begins to stray from the lane, but Toyota’s Lane Trace adjusts the steering angle, torque and braking in order to maintain a driving line within the lane” (Weiss, 2013). This system is Level 2 because it performs both sustained lateral (automated lane centering) and sustained longitudinal (automated braking and acceleration) vehicle

motion control, and the driver must continue to supervise in real time the system's performance in light of the traffic environment while engaged.

- Level 4, Automatic Parking: "The Audi technology works through a mobile app. A driver exits the car at the entrance to a parking garage, then simply touches the app on a mobile device so the driverless car can scour the garage for an open space. It then parks itself. When the driver returns, he or she simply selects the app again and like valet parking, the car returns to the entrance" (Mearian, 2013). This system is Level 4 because it is able to perform the complete dynamic driving task (DDT), as well as the DDT fallback, within its ODD, and with no driver inputs during feature engagement.
- Level 4, Closed Circuit/Campus Automatic Shuttle/Delivery Vehicle: A driving automation feature that operates a vehicle along a fixed route and/or within a prescribed closed campus environment, such as a military base or college campus. The system may have other ODD limitations, such as lighting and/or weather conditions. The passenger (or goods) can enter and exit the vehicle at a set of stops (i.e., point-to-point). The system is not required to have an on-board driver control interface to operate within its specified ODD. This system is Level 4 because it is able to perform the complete DDT, as well as the DDT fallback, within its ODD, and with no driver inputs while in normal operation.
- Level 5, Robotic Taxi: A driving automation feature that operates a vehicle under all legal on-road conditions such that it can pick up passengers (or goods), then drive them to the place of their choosing (i.e., point-to-multi-point). The system is not required to have an on-board driver or driver control interface. The system does not have limited domains of operation; it can operate within any legal road system and under any environmental conditions that human-driven vehicles can operate.

2.6.2.2 Example Classification of Automation Feature

Consider Toyota's Automated Highway Driving Assistant as an example of classifying a feature to an automation level. According to the flow chart in Figure 4 (Section 2.1), the first question is whether the feature is capable of sustained control of either lateral or longitudinal motion to external objects or events in lieu of the driver. The answer is yes, therefore, the logic flow proceeds to the next question. The answer to the second question is again yes; according to the feature's description it can control the vehicle both laterally and longitudinally on a sustained basis to external objects and events in lieu of the driver. The next question is whether the feature requires a driver's supervision during its normal operation. While the feature description as provided above is not complete, Toyota's current view is that human supervision is necessary; the answer is therefore yes and the feature is thus classified as Level 2.

2.6.2.3 Mapping of Automation Features to Automation Levels

Table 2 illustrates example features derived from the automation features listed above, as well as additional information available to the AVR Project team. A generic description based on the information above is provided for each feature in the table. Driving automation feature descriptions are also provided to illustrate the nature of the variation and to facilitate classification of the feature to an automation level. The feature descriptions needed to categorize the levels are shown in the columns on the right side of the table.

Table 2: Exemplar Driving Automation Features

		Descriptions required to categorize levels			
		Sustained Control	Sensing and Response Capability (Driver's supervisory role)	Only required if driver does not have supervisory role	
Feature	**Description**			Fallback	Operational conditions
Adaptive Cruise Control (ACC)	While engaged, it performs longitudinal control within a limited driving domain (e.g., speed range, acceleration and deceleration/coast capability, environmental conditions). ACC may perform distance (headway) control to some detected objects (again within its limited domain) in addition to its speed control capabilities. As with conventional cruise control, driver supervision is required (see also Section 2.6.1).	Sustained Longitudinal control	Driver must supervise	▒	▒
Cooperative Adaptive Cruise Control (C-ACC)	Same as ACC except the ACC-equipped vehicle and other vehicles in front of it are equipped with Vehicle-to-Vehicle (V2V) communication capabilities so as to inform each other of their current speed and other parameters (Nowakowski et al., 2010).	Sustained Longitudinal control	Driver must supervise	▒	▒

GM Super Cruise	"Super Cruise is capable of semi-automated driving including hands-off lane following, braking and speed control under certain driving conditions. The system is designed to ease the driver's workload on freeways only, in bumper-to-bumper traffic and on long road trips; however, the driver's attention is still required" (General Motors, 2013).	Sustained Lateral and Longitudinal control	Driver must supervise		
Traffic Jam Assistant	"The traffic jam assistant helps you in monotonous situations on the motorway. In dense traffic at speeds of up to 40 km/h, the system allows you to move easily along with the traffic and stay relaxed. It automatically maintains the desired distance from the vehicle ahead and regulates the car's speed right down to standstill – as well as providing active steering support, too. This helps you stay on track, providing you keep at least one hand on the steering wheel" (BMW AG, 2013).	Sustained Lateral and Longitudinal control	Driver must supervise		
Toyota Highway Driving Assistant	"Toyota's Automated Highway Driving Assistant: The first part of the system is the Cooperative-adaptive cruise control, essentially a next-gen automated cruise control. The system uses 700 MHz band vehicle-to-vehicle ITS communications to gather acceleration/ deceleration data from the vehicles ahead and maintain a safe, uniform following distance. The second part of AHDA is Lane Trace Control, which Toyota described to us as a more advanced form of its Lane Keeping Assist system. Current-generation lane systems simply provide a warning or minimal amount of steering feedback when the vehicle begins to stray from the lane, but Toyota's Lane Trace adjusts the steering angle, torque and braking in order to maintain a driving line within the lane" (Weiss, 2013).	Sustained Lateral and longitudinal control	Driver must supervise		
Audi Parking System	"The Audi technology works through a mobile app. A driver exits the car at the entrance to a parking garage, then simply touches the app on a mobile device so the driverless car can scour the garage for an open space. It then parks itself. When the driver returns, he or she simply selects the app again and like valet parking, the car returns to the entrance" (Mearian, 2013).	Sustained Lateral and Longitudinal control	No driver required, therefore no supervisory requirements	Driver is not required	Low speed, parking lot only
Closed Circuit Automatic Shuttle/Delivery Vehicle	A vehicle that drives along a fixed route (i.e., a particular form of limited driving domain, limited to a specific route; the system may have other domain limitations such as weather conditions). The passenger (or goods) can enter and exit the vehicle at a set of stops (i.e., point-to-point). The system is not required to have an on-board driver control interface to operate within specified operational conditions.	Sustained Lateral and Longitudinal control	No driver required, therefore no supervisory requirements	No driver required	Fixed route
Robotic Taxi	A vehicle that can pick up passengers (or goods), then drive them to the place of their choosing (i.e., point-to-multi-point). The system is not required to have an on-board driver control interface to operate within specified operational conditions. The system does not have limited domains of operation, it can operate within any legal road system and under any environmental conditions deemed acceptable by road system authorities (i.e., when roads are open). This hypothetical vehicle is claimed to be one of the future products of Google's self-driving car program (see, e.g., Fitzsimmons, 2013).	Sustained Lateral and Longitudinal control	No driver required, therefore no supervisory requirements	No driver required	Any publicly available roads

Table 3 illustrates the application of the developed methodology to map the features from Table 2 onto the automation levels. The methodology question from Figure 4 is shown in the first row. The feature's automation level results from answering "Yes" or "No" to the appropriate question. The arrows indicate whether to move to the next question (right-arrow) or to stop at the resulting level (up-arrow). Comments are also provided regarding assumptions made based on the feature description, whenever necessary.

Table 3: Mapping Automation Features into Driving Automation Levels

Driving Automation Methodology Question	Sustained Lateral **OR** Longitudinal control?	Sustained Lateral **AND** Longitudinal Control?	Driver supervision required?	Driver required outside normal operation?	Limited scope of operation?	
Driving Automation characteristic	Control to external objects or events		Sensing and response	Fallback	Operational conditions	
Response to methodology question confirms level or proceeds to next question	Yes, move to next question		No, move to next question			
	No, stop at this level		Yes, stop at this level			
Driving Automation Level	**0**	**1**	**2**	**3**	**4**	**5**
Electronic Stability Control (ESC)	No ↑					
Conventional Cruise Control	No ↑					
Adaptive Cruise Control (ACC)	Yes →	No ↑				
ACC with Lane Keeping (steering support)	Yes →	No ↑				
ACC with Lane Centering	Yes →	Yes →	Yes ↑			
Highway Pilot	Yes →	Yes →	No →	Yes ↑		

Automated Parking System	Yes →	Yes →	No →	No →	Yes ↑	
Robotic Taxi	Yes →	Yes →	No →	No →	No →	↑

Readers should be cautioned that, for the given feature, it is very important to have sufficient information in the description to be able to answer the methodology questions unambiguously. A complete description of the automation feature in question needs to be furnished by the OEM (who designed, developed, tested, and verified performance of the feature) in order to enable the correct and unambiguous feature classification by following the methodology developed in this report. The OEM who designed, developed and tested the feature to be classified is best qualified to furnish such detailed information about a given driving automation system.

2.7 Summary - Functional Descriptions of Levels of Automation

The introduction of higher driving automation capability (Levels 3-5) has the potential to alter the traditional driver-vehicle relationship. Because driving automation systems have not yet been widely deployed and are evolving while undergoing rapid and competitive development, there could be a significant risk of stifling innovation, should standards or requirements on such systems be prematurely defined or imposed. However, in order to facilitate a uniform understanding of the capabilities and limitations of specific driving automation systems, and to demonstrate a clear distinction in the role of the driver versus the role of the automation system in performing the DDT and fallback actions, it is beneficial to define categorical divisions for driving automation based on the functional capabilities of the driving automation and while also accounting for the role of the driver (if any) in performing the DDT and/or providing fallback performance when the system is unable to do so. Section 2.1 of this report presents five factors for consideration in defining automation levels. Those factors focus on removing ambiguity from both the driver's and manufacturer's standpoints relative to the safe execution of the DDT and fallback actions.

While there are several different automation level definitions available at the time of this writing, it is recommended that the definition set used should be largely based on the SAE J3016 (2014), which are harmonized with the BASt levels. The SAE J3016 automation levels offer the greatest alignment to the aforementioned five factors for consideration in defining automation levels. In addition, the SAE J3016 automation levels, including supporting terms and definitions, focus on:

- The functional capability of the automation system (and the subsequent role of the driver versus the role of the driving automation system) in performing the complete DDT, providing the appropriate responses to relevant objects and events
- The fallback capability of the automation system (i.e., ability to automatically achieve a minimal risk condition when necessary)
- ODD limits (if any)

Higher levels of driving automation include those functional capabilities found at the lower levels of automation, and that each increasing level of automation includes functions that reduce the driver's role in completing the DDT and providing fallback as needed.

Lastly, a methodology that classifies new driving automation features into the appropriate levels is proposed based on the automation capabilities provided by the feature. The proposed methodology considers whether vehicle motion control is sustained to external objects or events, the degree of the environmental sensing and response capability, the allocation of fallback performance to the driver or the system, and the feature's operational design domain. Given this information about a driving automation feature, it is possible to objectively classify such features to a driving automation level by following the approach outlined in Section 2.6. However, a detailed understanding of the driving automation system design and verified performance capability is needed to make this classification definitively.

3 Determine Concept Roadmaps for Future Driving Automation Features

3.1 Driving Automation Features

The following is an exemplar list of driving automation features that may be deployed in the future. The estimated time-to-deployment for the features described below has been classified into near-term, mid-term, and long-term categories of potential deployment. This feature list was created solely from publicly available information and, as such, should not be used as a mechanism to gain insight into any particular OEM's product development plans for driving automation.

3.1.1 Near-term Features

- Level 1, Adaptive Cruise Control (ACC): While engaged, it performs sustained longitudinal vehicle motion control within a limited driving domain (e.g., speed range, acceleration and deceleration/coast capability, environmental conditions). ACC performs distance (headway) control to some detected objects (again within its limited domain), in addition to its speed control capabilities. Driver supervision of system performance and the driving environment is required while engaged.

- Level 1, ACC with Lane Keep Assist: ACC without sustained lateral vehicle motion control (which only intervenes when nearing lane markings). Driver supervision of system performance and the driving environment is required while engaged.

- Level 2, Adaptive Cruise Control with Lane Centering: ACC with sustained lateral vehicle motion control active simultaneously. ACC with lateral control limited to specific driving domains (e.g., road types, lane curvatures, environmental conditions, lane, and/or object detection capabilities). Driver supervision of system performance and the driving environment is required while engaged.

- Level 1, Automatic Parking Type A: Provides sustained lateral vehicle motion control while parallel parking or parking in garages, within limited parking domains (e.g., presence of other vehicles or objects, curbs, road surfaces and grades, environmental conditions). When the driver sets the designated parking location, the system controls lateral vehicle motion while the driver controls longitudinal motion. Driver supervision of system performance and the driving environment is required while engaged.

- Level 2, Automatic Parking Type B: After the driver sets the designated parking location, system provides both sustained lateral vehicle motion control and sustained longitudinal vehicle motion control simultaneously within limited parking domains. Driver supervision of system performance and the driving environment is required while engaged, and the driver may be either in the driver's seat or outside the vehicle using a remote control.

3.1.2 Mid-term Features

- Level 2 Highway Pilot A: ACC with sustained lateral control within limited driving domains. Driver supervision of system performance and the driving environment is required while engaged.

- Level 3 Automatic Parking C: Driver activates parking feature and system begins searching for an available spot or proceeds to a known parking spot within limited parking domains. The driver does not need to supervise system performance and the driving environment while engaged. However, the driver is required to be in a position to resume control if the system cannot find an available parking spot or if the driving automation system determines its limitations are exceeded by the parking maneuver.

3.1.3 Long-term Features

- Level 4 Automatic Parking Type D: Driver activates parking feature and system begins searching for an available spot, or proceeds to a known parking spot within limited parking domains. While activated, the driving automation system has the capability to perform the complete DDT. Dedicated parking domains for this type of feature may allow earlier introduction. The driver does not need to supervise system performance or the driving environment. However, the vehicle may not complete the parking if the system cannot find an available parking spot or if the system determines its limitations are exceeded by the parking maneuver. In such cases, the system will automatically fallback to a minimal risk condition. The driver may desire to take control of the vehicle in order to get it parked in a desired location.

- Level 3 Highway Pilot Type B: When activated, the driving automation system has the capability to perform the complete DDT. The system is only available in limited driving domains (e.g., road types, speeds). The driver is not required to supervise driving automation system performance or the driving environment during normal system operation. However, the driver must be available to respond to the system's request to take over when necessary.

- Level 4 Highway Pilot Type C: When activated, the system has the capability to perform the complete DDT. The system is only available in limited driving domains (e.g., road types, speeds). The driver is not required to monitor driving automation system performance or the driving environment during normal system operation. The system is capable of falling back to a minimal risk condition. In that event, the vehicle may not complete the trip unless the driver resumes performance of the DDT in order to do so.

- Level 4 Automated Closed Campus Shuttle: A driving automation feature that operates a vehicle along a fixed route and/or within a prescribed closed campus environment, such as a military base or college campus. The system may have other operational design domain limitations, such as lighting and/or weather conditions. The passenger (or goods) can enter and exit the vehicle at a set of stops (i.e., point-to-point). The system is not required to have an on-board driver control interface to operate within its specified ODD.

- Level 5 Robotic Taxi: A driving automation feature that operates a vehicle under all legal on-road conditions such that it can pick up passengers (or goods), then drive them to the place of their choosing (i.e., point-to-multi-point). The system is not required to have an on-board driver or driver control interface. The system does not have limited domains of operation; it can operate within any legal road system and under any environmental conditions that human-driven vehicles can operate.

3.2 Similarities and Differences between Driving Automation Features

Table 4 represents the minimum Driver Vehicle Interface (DVI/HMI), control, sensing and processing functionality for features classified under driving automation Levels 1-5.

Table 4: Minimum HMI, Control, Sensing and Processing Functionality for Driving Automation Level 1-5 Exemplar Features

Feature	Estimated Time Frame for Deployment	Internal Reference Level of Automation	Primary Operational Areas	Minimum HMI	Control Functionality	Sensor and Processing		
						Minimum Requirements when Engaged	Minimum Requirements during Fallback	Minimum Requirements Outside of Conditions
Adaptive Cruise Control (ACC)	Near	1	Highway	Driver control to engage/ disengage Driver can override longitudinal control (accelerator and brake) anytime	Sustained longitudinal automated control	Some automated object and event detection within the design of the system	No	No
ACC with Lane Keep Assist	Near	1	Highway	Driver control to engage/ disengage Driver can override lateral assist and longitudinal control (steering, accelerator and brake) anytime	Sustained longitudinal automated control While there may be some intervention-type lateral control provided there is not sustained control	Some automated object and event detection within the design of the system	No	No
Automatic Parking Type A	Near	1	Parking	Driver control to engage/ disengage Driver can override lateral control (steering) anytime	Sustained lateral automated control	Some automated object and event detection within the design of the system	No	No
ACC with Lane Centering	Near	2	Highway	Driver control to engage/ disengage Driver can override longitudinal control (accelerator and	Sustained longitudinal automated control Sustained lateral automated control	Some automated object and event detection within the design of the system	No	No

Feature	Estimated Time Frame for Deployment	Internal Reference Level of Automation	Primary Operational Areas	Minimum HMI	Control Functionality	Sensor and Processing		
						Minimum Requirements when Engaged	Minimum Requirements during Fallback	Minimum Requirements Outside of Conditions
				brake) anytime Driver can override lateral control (steering) anytime				
Automatic Parking Type B	Near	2	Parking	Driver control to engage/ disengage Driver can override lateral control (e.g., brake to a stop) anytime Driver can override longitudinal control (e.g., brake to a stop) anytime	Sustained longitudinal automated control Sustained lateral automated control	Some automated object and event detection within the design of the system	No	No
Cooperative Adaptive Cruise Control (C-ACC)	Mid	1	Highway	Driver control to engage/ disengage Driver can override longitudinal control (accelerator and brake) anytime	Sustained longitudinal automated control	Some automated object and event detection within the design of the system	No	No
Highway Pilot Type A	Mid	2	Highway	Driver control to engage/ disengage Driver can override longitudinal control (accelerator and brake) anytime Driver can override lateral control (steering) anytime	Sustained longitudinal automated control Sustained lateral automated control	Some automated object and event detection	No	No

Feature	Estimated Time Frame for Deployment	Internal Reference Level of Automation	Primary Operational Areas	Minimum HMI	Control Functionality	Sensor and Processing		
						Minimum Requirements when Engaged	Minimum Requirements during Fallback	Minimum Requirements Outside of Conditions
Automatic Parking Type C	Mid	3	Parking	Indication of system engagement Driver control to engage/ disengage Alert: System initiated takeover request to driver Driver can take longitudinal control (accelerator and brake) when requested Driver can take lateral control (steering) when requested	Sustained longitudinal automated control Sustained lateral automated control	All automated object and event detection within the design of the system	Yes	No
Highway Pilot Type B	Long	3	Highway	Driver control to engage/ disengage Indication of system engagement Alert: system initiated takeover request to driver Driver can take longitudinal control (accelerator and brake) when requested	Sustained longitudinal automated control Sustained lateral automated control	All automated object and event detection within the design of the system	No	No

Feature	Estimated Time Frame for Deployment	Internal Reference Level of Automation	Primary Operational Areas	Minimum HMI	Control Functionality	Sensor and Processing		
						Minimum Requirements when Engaged	Minimum Requirements during Fallback	Minimum Requirements Outside of Conditions
				Driver can take lateral control (steering) when requested The feature may or may not allow override at any time				
Automatic Parking Type D	Long	4	Parking	Indication of system engagement Driver control to engage/ disengage	Sustained longitudinal automated control Sustained lateral automated control	All automated object and event detection within the design of the system	Yes	No
Highway Pilot Type C	Long	4	Highway	Driver control to engage/ disengage Indication of system engagement Alert: System initiated takeover request to driver Driver can take longitudinal control (accelerator and brake) when requested Driver can take lateral control (steering) when requested	Sustained longitudinal automated control Sustained lateral automated control	All automated object and event detection within the design of the system	Yes	No

Feature	Estimated Time Frame for Deployment	Internal Reference Level of Automation	Primary Operational Areas	Minimum HMI	Control Functionality	Sensor and Processing		
						Minimum Requirements when Engaged	Minimum Requirements during Fallback	Minimum Requirements Outside of Conditions
Automated Closed Campus Shuttle	Long	4	Urban	Indication of system engagement Operator control to engage/ disengage	Sustained longitudinal control Sustained lateral control	All automated object and event detection within the design of the system	Yes	No
Robotic Taxi	Long	5	Urban	Indication of system engagement Operator control to engage/ disengage	Sustained longitudinal control Sustained lateral control	All automated object and event detection	Yes	Yes

3.2.1 HMI Similarities and Differences

3.2.1.1 Overview

HMI refers to information passed from the operator to the driving automation system and from the system to the operator. Specific information passed from the operator to the automation system includes requests for the automation system to engage or disengage altogether (e.g., through a control action such as pressing a button or the brake pedal) and requests from the operator to take control of one or more of the aspects of driving, such as longitudinal control or lateral control (e.g., by pressing a button or turning the steering wheel). Specific information passed from the automation system to the operator includes whether the automation system is currently engaged. This may include further information about which DDT subtasks the automation system is currently performing (e.g., through a visual display such as an instrument panel cluster or center mounted display), and, may also include requests for the driver to take over operation of one or more of the DDT subtasks (e.g., through an alert of some kind, including one or more visual, auditory, and haptic components, depending on the expected available operator sensory modalities).

Certain minimum HMI capabilities are required for the driving automation system and the driver to operate together as designed, according to the minimal function set provided by the system, and the driver's role in proper usage of it, and thus are described herein.

3.2.1.2 Engagement and Disengagement

All driving automation systems provide a means for engagement and disengagement requests to the automation system to be made by the driver or operator. With the exception of Level 5 Full Automation (i.e., not limited in driving domain capability, such as the Robotic Taxi), all driving automation systems may be programmed not to honor engagement requests due to the vehicle being outside of the driving automation system's domain of operation. For example, ACC may not honor an engagement request when the vehicle is travelling very slowly. Some higher driving automation features (Levels 4 and 5) may not immediately honor disengagement requests from a driver or operator due to their need to abide by their domains of operation and the particular driving situation. In particular, driving automation systems whose domain of operation does not include mixed fleet conditions (i.e., it can only operate with other vehicles that have a higher driving automation system engaged) would not immediately honor disengagement requests until the system could manage leaving such a driving domain. This could be true of a specific execution of Highway Pilot Type B or Automatic Parking Type C, for example.

Higher driving automation systems (Levels 3-5, including Highway Pilot Type B, Closed Campus Shuttle, Automatic Parking Type C, and Robotic Taxi) should all provide indications of engagement in order that the driver is informed about what role (if any) he or she has at any given time in performing the DDT or fallback actions. Again, any automation system could provide such an indication (as a quality execution), but it is only minimally required for higher driving automation systems.

3.2.1.3 Taking Control

The ability for the driver to take control varies substantially among the features. Lower driving automation systems (Levels 1-2, including ACC, Highway Pilot Type A, Automatic Parking Type A and B, and others) provide the driver the ability to take control of whichever dimension(s) of vehicle motion control are automated, lateral and/or longitudinal. This capability is provided at all times when the driving automation system is engaged, because the driver's proper usage of the system includes a supervisory role where the driver is expected to monitor driving automation performance and the external driving environment, and to respond appropriately to situationally-relevant objects and events. For some parking features where the driver may be outside of the vehicle (Automatic Parking Type B), this capability may amount to only an ability to brake the vehicle to a stop through a remote control, because this is the only appropriate response required during the parking. However the driver can then re-enter the vehicle and maneuver it to its final position manually, without using the driving automation system. For the majority of lower driving automation systems, however, the driver can take control through utilization of the primary vehicle controls (i.e., steering wheel, brake and accelerator pedal), although other means (e.g., button press such as using the 'increase speed' button to accelerate manually while Cruise Control is engaged) may also be available.

Level 3 driving automation systems (such as Highway Pilot Type B) are not capable of handling every abnormal driving situation, or of operating outside of their operational design domain, and therefore must request the driver to take over DDT performance in these cases. When this occurs, the driver is provided the capability to take control. Level 3 systems may allow drivers to take over portions of the DDT when the system is otherwise engaged. However, as mentioned previously with regard to disengagement requests, some higher driving automation systems may delay a driver's takeover request in certain situations, such as when the takeover request occurs in the middle of a very tight turn or during a collision avoidance maneuver.

Level 4 driving automation systems such as Closed Campus Shuttle may or may not allow a driver or operator to take over control of the system while it is engaged, depending on operating prevailing conditions. For example, a Level 4 system operating in a restricted domain that only allows other vehicles which have higher driving automation systems engaged may not honor takeover attempts from the driver while the system is engaged in such a driving domain if doing so would risk a collision. Examples of this could include Highway Pilot Type B operating in restricted highway lanes or Automatic Parking Type C operating in a restricted-access parking garage (i.e., no pedestrians; only vehicles equipped with the Automatic Parking Type C feature). Level 4 systems cannot operate in all driving domains (otherwise they would be Level 5), so any such system which finds itself outside of its ODD would need to provide either the means for a driver to take control or be capable of automatically achieving a minimal risk condition in the event of a relevant failure. Thus, there is no minimum requirement for some of these systems to maintain driver take over capability.

Level 5 driving automation systems such as the Robotic Taxi do not necessarily have any capability for an operator to take control. Even if such a capability is provided, a request from an operator to take over would not be permitted in certain restricted driving domains as previously discussed. Once again, there is no minimum requirement for such systems to have a driver present that is able to take over DDT performance.

3.2.1.4 Take-over Alert

Level 3 driving automation systems such as Highway Pilot Type B have a unique additional HMI capability, namely, an alert to the driver to take over control. Again, this is to complete the DDT and balance the limited capabilities of such systems in that they cannot always perform automated fallback actions to maneuver the vehicle to the minimal risk condition. Proper usage of such a system would require that the driver take over in this situation. Alert displays are a specific subset of display types and the automation function. Because the driver is not required to actively supervise the performance of this type of driving automation system or the external environment during its engagement, driver visual attention may not be available for system displays (humans' primary sense is visual, which in this instance may be devoted to a non-driving task). Non-visual displays are often utilized for alerts (although typically in conjunction with visual displays for clarity) as a method for affecting driver attention, including audible and/or haptic alert displays, although other human sensory systems could be utilized.

3.2.2 Sensing and Processing Similarities and Differences

As driving automation applications continue to evolve and increase in their functionality, the capability of vehicle-based sensors will also continue to evolve and the similarities and differences found in those increasingly automated features, as it relates to these sensors, will also increase. Consider Table 4 and the outline for sensor requirements where three categories are contained:

- Minimum requirements when engaged
- Minimum requirements during fallback
- Minimum requirements outside of conditions

Vehicle-based sensor sets for features that occur between Levels 1-3 do not demand minimum requirements for fallback performance. The operator is considered to have control and to serve as the fallback solution. Likewise, there are not minimal requirements outside of the feature's operating conditions. Levels 1, 2, and 3 can be further differentiated so that in Levels 1-2 the driving automation system is unable to perform the complete DDT, whereas Level 3 systems are able to perform the complete DDT within the domain for which it is designed. Accordingly, vehicle-based sensors are not capable of performing the complete OEDR subtask of the DDT because driving automation systems within these levels are designed only to augment human driving. In Level 3 applications, the driving automation system feature must be capable of performing the complete OEDR subtask while operating within its design domain, thus performing the entire DDT while the system is engaged. The system must also be able to provide a minimal level of fallback mitigation during a brief transition period between when the system issues a request for the driver to resume performance of the DDT and the time when the driver resumes control. However, the system is not required to provide fully-automated fallback (i.e., minimal risk) capability, as this is still the role of the driver for a Level 3 system. It is also important to note that for a Level 3 feature, when considering sensor redundancy, the operator is still considered as the final fallback for the driving automation system. As the complexity further increases for Level 4 systems, where the driver or operator is not required to provide fallback performance in the event of failure or if the driving automation system exceeds its design domain, the sensors are required to provide the necessary information for the system to respond appropriately to driving events. Therefore, in a Level 4 system, the sensors must be adequate to enable the system to perform the entire DDT, including the complete OEDR subtask, and provide automated fallback (i.e., minimal risk) capability as needed. In the most complex environment, Level 5 sensors are not domain limited. Accordingly, Level 5 sensors must fulfill all requirements of Level 4 systems in all legal, on-road driving domains.

3.2.3 Control Functionality Similarities and Differences

Control functions are defined at a high level based on previously described levels of automation in order to remain technology and implementation neutral. Sections 2.5 and 2.6 emphasized the importance of sustained longitudinal and/or sustained lateral control in terms of motion control functionality in the automation levels. For example, sustained control is defined as being able to perform a lateral and/or longitudinal control subtask of the DDT between and across events, controlled to the external environment, as opposed to momentary system interventions to a given event, and is a requirement for Level 1 and higher driving automation systems. Limited longitudinal and/or lateral control is different in that it can only augment the driver's operational input, and, as such, is not considered driving automation and is classified as Level 0.

In terms of minimum motion control functionality, the same control requirements (limited, sustained, longitudinal, lateral) are used, along with the OEDR subtask of the DDT for determining similarities and differences between automation features. Table 4 illustrates various features and the corresponding minimum control functionality required to be able to assign the feature to the specified level of driving automation.

The common control elements for Levels 2, 3, 4 and 5 are shown in Table 4. These are sustained automated longitudinal control and sustained automated lateral control, which are needed at a minimum in order to perform the longitudinal and lateral DDT subtasks in place of the driver.

3.3 Summary - Concept Roadmaps for Future Driving Automation Features

The AVR Consortium was tasked with building upon the work described in Section 2 to develop a list of driving automation features that are likely to be marketed by vehicle manufacturers in the foreseeable future. A primary outcome of this work is the identification of similarities and differences between the driving automation features (in terms of the minimum sensing and processing, control functionality, and minimum HMI design requirements) for each identified feature.

Section 3.1 of this report provides an exemplar list of driving automation features, delineated by the estimated number of years to production deployment. It is important to note that this feature list was created solely from publicly available information and, as such, should not be used as a mechanism to gain insight into any particular OEM's product development plans for driving automation.

In Section 3.2, the similarities and differences between the exemplar list of driving automation features is provided in terms of the minimum sensing/processing, minimum control functionality and minimum HMI design requirements. From a sensing/processing perspective, all features classified under lower automation Levels 0-2 are similar in their inability to perform the complete OEDR subtask of the DDT. Higher automation Levels 3-5 are similar in that they must all perform the complete OEDR for the specified application, as an integral part of completing the entire DDT while the system is engaged. However, a distinguishing characteristic among features classified under higher driving automation Levels 3-5 is whether the system has the ability to automatically bring the vehicle to a minimal risk condition without driver action in the event that the system is no longer operating in the conditions for which it is designed, or the system and/or vehicle experiences a relevant failure, and no driver intervenes (i.e., the "fallback" capability of the system). An additional distinguishing factor among higher driving automation Level 3-5 features is in the design domain (e.g., expressway, low-speed traffic jam, parking, closed campus, etc.) in which complete performance of the DDT is expected. In the case of Level 5, the design domain is unlimited for legal, designated or on-road use.

Identifying similarities and differences in the exemplar list of driving automation features in terms of control functionality is a simple matter once the features are classified by level. As stated in Section 3.2, features classified under driving automation Level 0 do not exhibit sustained longitudinal or lateral control (i.e., driving) functionality, and, thus, are different from all features classified under driving automation Levels 1-5.

From an HMI perspective, all features listed under the exemplar list are similar in their need to provide a means for engagement and disengagement requests to the automation system by the driver or operator. However, the ability for the driver to take control varies substantially among the features. For the majority of lower driving automation systems (i.e., Levels 1-2), the driver can take control through utilization of the primary vehicle controls. This is also true for Level 3 systems, where a driver may need to exercise his or her fallback role. Level 4 and 5 systems may restrict drivers from taking over portions of the DDT when the system is engaged while operating in a restricted domain that only includes other vehicles which have higher driving automation systems engaged (e.g., a Level 4 driving automation systems designed to pilot a vehicle at high speeds in close-coupled "convoys" with other similarly equipped vehicles would not immediately restore the DDT to a human driver upon request, because to do so would pose a hazard for the other vehicles in the convoy; instead, the system would safely exit the convoy before honoring the operator's takeover request). Lastly, Level 3 driving automation systems have a unique additional HMI requirement to alert the driver to take over control, while Level 1, 2, 4, and 5 systems do not have such a requirement.

The value of classifying the features to the appropriate driving automation level using the methodology defined within Section 2.6.1 should not be underestimated. Using the subtasks of the DDT and the functional capability defined for each automation level as the guiding principle allowed similarities and differences between the features to be identified.

4 Top-Level Safety Principles for Levels of Automation

4.1 Introduction to System-Theoretic Process Analysis (STPA) for Hazard Analysis

System-Theoretic Process Analysis (STPA), developed by Nancy Leveson at the Massachusetts Institute of Technology (MIT), is a relatively new hazard analysis technique based on systems thinking and accident causation. As described in *Engineering a Safer World* (Leveson, 2012), the hazard analysis technique offered by STPA focuses on accident scenarios that "encompass the entire accident process (e.g., mechanical, socio-technical), not just the electromechanical components." With this in mind, the causes of accidents identified by STPA extend beyond failures or unreliability; accident causes identified by STPA extend into societal, regulatory, and cultural factors as well.

Like traditional hazard analysis techniques such as Hazard and Operability Analysis (HAZOP), STPA uses "guidewords" to assist in the analysis of hazards. The advantages of this approach are commensurate with those found in HAZOP analysis in general. In particular, STPA is easily learned and performed, the analysis does not require a significant amount of technical expertise for application, and the analysis focuses on system elements within the control system and hazards associated with inadequate control within those elements.

STPA was chosen as the hazard analysis technique for identifying and developing safety principles (SPs) for the levels of driving automation under consideration because it offered the flexibility for analyzing the undesired control actions (UCAs) that can lead to hazards based on a functional control diagram, and did not necessitate that a physical design was available at the time of analysis.

In addition, using STPA allowed the AVR Consortium to analyze the four methods of inadequate control:

- Control not provided or not followed
- Control action leads to a hazard
- Control action is provided too late, too early, or out of sequence
- Control action is stopped too soon or applied too long.

These four methods were analyzed in the abstract for each driving automation level, which could then be cascaded to features whose characteristics align with a particular driving automation level.

The primary steps in the STPA process are as follows:

- Determine the type of accidents (losses) to be considered in this analysis
- Identify the hazards
- Develop the System Boundaries / Functional Control Structure under analysis

- Identify the UCAs in the control structure under analysis that could lead to the hazards under consideration
- Determine how each identified UCA could occur within the Functional Control Structure
- Specify the Top-level SPs for eliminating the UCAs under consideration

The reader is encouraged to refer to *Engineering a Safer World* for more information regarding STPA and its application.

4.2 Accidents and Hazards Under Consideration

4.2.1 Losses (Accidents)

Existing literature on the STPA process defines accident as "an undesired and unplanned event that results in a loss, including a loss of human life or human injury, property damage, environmental pollution, mission loss, financial loss, etc." This definition is somewhat at odds with the traditional terminology in the automotive industry, where "accident" carries a specific connotation of collision between a vehicle and another object.

To employ the concepts of STPA, the concept of an "accident" was replaced with that of a "loss." In this analysis, a loss is defined as follows:

Loss: an undesired and unplanned event that causes human injury or property damage.

It is important to note that some losses may be simply unavoidable and may be outside the scope of what this exercise can address. For example, if a heavy object is dropped from an overpass onto a vehicle, it may not be feasible for a human driver or a vehicle with driving automation features to avoid it, no matter their capability or driving ability. Any environmental or societal impact of accidents is covered by the existing definition.

A single loss is identified for automated driving, as follows:

Loss # 1: *Vehicle Collision with a Threatening Object.*

This primary loss includes a variety of situations to be avoided, including collision with other vehicles, collision with humans, collision with objects in the roadway, and collision with objects outside the roadway.

4.2.2 Hazards

Existing literature on the STPA process defines a hazard as *"a system state or set of conditions that together with a worst-case set of environmental conditions will lead to an accident (loss)."* This definition is generally sound for the work carried out here, but with the clarification that the "environment" should be interpreted broadly to include any disturbances to the vehicle's surroundings, and not only meteorological factors such as wind, rain or snow. The definition employed in this work is as follows:

***Hazard:** A system state that together with a worst-case set of external disturbances may lead to a loss.*

In this definition, “system state” is taken to include the vehicle, the driver or operator and his or her state, and interactions between them. The concept of a hazard does not depend upon the assignment of the role with respect to hazard avoidance actions, which may accrue to the driver, the driving automation system or a combination of the two. Further, “external disturbances” may include surrounding vehicles, infrastructure, roadway, weather, and other factors.

STPA also notes that “the system and safety analysis … needs to consider the humans in systems.” In this analysis, we include both human and machine actions needed to complete the DDT, and address the interaction between them, if applicable.

The hazards identified for driving automation systems are as follows:

Hazard #1: The vehicle leaves the roadway. The general presumption that a roadway is the proper location for safe vehicle operation is fundamental to this analysis. It is noted that specific exceptions to this general condition may be necessary in some limited cases; for example pulling off the roadway in a controlled manner if required as a fallback maneuver or emergency response to an on-roadway event.

Hazard #2: The vehicle loses traction or stability. Safe driving depends on maintaining vehicle traction and stability. If the tires lose traction with the roadway, then many nominal control actions are limited in their effectiveness, or become entirely ineffective at controlling the vehicle. Note that while loss of traction may occur through several dynamic driving maneuvers, it can also occur when road surfaces are slippery due to rain, snow, ice, etc. Vehicle conditions such as excessive tire tread wear also contribute.

While it is unclear whether this hazard is contributory to other hazards or represents a fundamental hazard distinct from the others, in many cases loss of traction or stability leads to the hazard of departing the roadway and/or coming too close to other objects. However, the need to maintain vehicle traction and stability can be considered fundamental enough to warrant its own distinct hazard.

Hazard #3: The vehicle comes “too close” to threatening objects in the roadway. This hazard is the most difficult to interpret, as it includes many variants which are situation-dependent. It includes well-known automotive hazards such as following too close to a vehicle in front, or swerving into an adjacent lane occupied by another vehicle. When considering pedestrians, the definition of “too close” becomes much more conservative. Yet where there are existing traffic laws, rules, and norms, it may be perfectly appropriate to be very near a human (e.g., passing a cyclist on a city street).

To develop this hazard the team applied the concept of a continuously adapting “cocoon” around the vehicle, representing the space envelope into which threatening objects may not enter without incurring a hazard.

Hazard #4: Violating traffic laws, rules, and norms pertaining to the DDT. This hazard covers a variety of potential situations where the vehicle might incur an accident (loss) due to violating the driving behavior standards that are applied to typical licensed drivers. The immediate concern is violations of traffic laws associated with the performance of the DDT. A driving automation system that runs stop signs, far exceeds posted speed limits, or violates other traffic laws, could incur hazards as a result of such behavior. This hazard includes some behaviors that may be difficult to classify into laws; or that may vary from region to region. For example, in some conditions it may be a normative behavior to maintain speeds with the surrounding traffic, even if such speeds exceed the posted speed limit. These conflicts may exist in performance of the DDT, even within the definition of the hazard. As mentioned, laws or norms may vary from state to state.

Driving laws, rules, and norms are meant to provide directives and guidance to a driver on how to prevent or avoid other hazards. In cases of conflict between this hazard and the other hazards, it is recognized that this hazard is avoided at a lower priority than the other hazards. For example, if it is necessary to change lanes quickly to avoid striking a threatening object, such action should be taken even if sudden lane change violates a traffic rule.

In closing it is important to note, manufacturers define the proper use of features. If drivers or operators use these features outside of their intended design, it is either "misuse" (i.e., an unintentional improper use) or "abuse" (i.e., an intentional improper use), depending on whether he or she understood the proper use of the feature, and can be a causal factor for hazards as defined above. Key human factors considerations are to understand the propensity for a driver or operator to properly use versus unintentionally misuse or intentionally abuse a feature, and how that use occurs.

4.3 Generic Control Structure for Driving Automation

In order to understand how hazards are handled for driving automation systems, it is necessary to first describe the control structure. At a high level of abstraction, the system can be modeled as the interplay of three principal actors: the vehicle, the driver/operator and the driving automation system as in Figure 5.

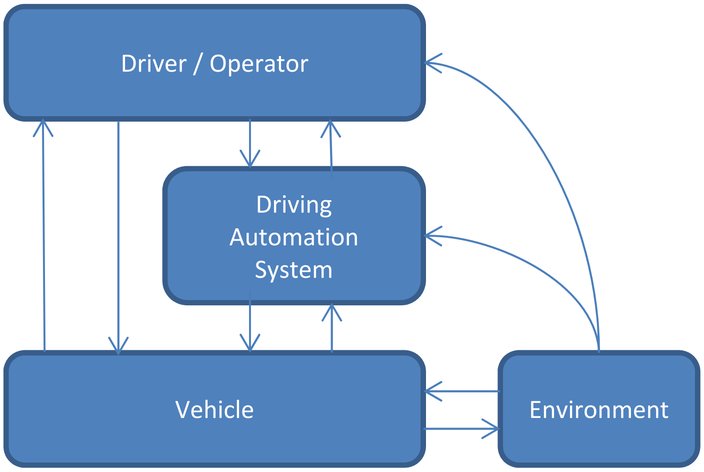


Figure 5: Principle Actors in the DDT

These are functional divisions and not necessarily components that can be identified in a traditional parts list. In this model, the vehicle is the object that is under the control of the driver and/or the automation. The *vehicle* is every part of the automobile not directly involved in the control of the DDT. Components such as tires, tie rods, seats, airbags, the steering column, windows, etc. comprise the *vehicle*. Driver support functions (e.g., Stability Control, Crash Imminent Braking) are not defined as driving automation systems because they are event-based or limited in authority and do not perform elements of the DDT on a sustained basis. The *driving automation system* comprises those components added to the vehicle to enable performance of the DDT. This may include such things as radar or cameras, digital controllers and computers, auxiliary steering motors, and auxiliary braking circuits. While these components are also installed in the vehicle and could be considered part of the vehicle, they serve primarily to enable performance of the DDT in a manner similar to a human driver and are functionally distinct from the object under control (the vehicle). As such, within this model it is not possible to classify each component of an automobile as exclusively ‘belonging’ to one of these three actors, and doing so would also be at odds with the functional systems approach used in this analysis. For example, a Controller Area Network (CAN) bus may transmit messages associated with any of these actors. Similarly, an Electric Power Steering System may provide torque to the steering mechanism at the request of the *driver* or the *driving automation system*.

The interplay between the actors in this model, regardless of the specific components involved, is the key functional concept used in defining the levels of automation, as well as the applicable SPs, which must be adhered to in order to avoid the hazards. Either the *driver* or the *driving automation system* must respond appropriately to all relevant objects and events in the driving environment (e.g., other vehicles, road conditions, fixed obstacles) by maneuvering the *vehicle* in order to avoid hazards. Similarly the *driver* and *driving automation system* should not contradict each other such that an appropriate response to a potential hazard becomes impossible.

The role of the *driver* and *driving automation system* in controlling the *vehicle* by performing the DDT and fallback as needed, along with the determination of final authority in arbitrating conflicting commands, are the fundamental building blocks of the levels of automation.

4.4 Application of Safety Analysis by Level of Driving Automation

The SPs developed in this portion of the project are intended to be applied according to the level of driving automation that may be experienced. While an individual feature or system, as engaged, could be analyzed with respect to the principles; as discussed in Section 2.4, it is also appropriate to evaluate the combinations of driving automation systems or features that can be engaged simultaneously and that determine a given level of driving automation.

4.5 Level 2 Driving Automation

4.5.1 High-Level Control Structure for Level 2 Driving Automation

The control structure diagram for Level 2 driving automation is shown in Figure 6. In order to model the change in roles, a color scheme has been implemented to represent corresponding changes in the locus of control. Green lines and green elements have the role to avoid hazards during automated operation, and provide appropriate responses to relevant situations and events. Since errors propagate throughout the diagram, green functions and signals may contain UCAs, but the design must resolve them at the root cause of the error.

Red lines and red elements are limited in their vehicle control capability within the applicable driving automation level and as such are not critical in providing appropriate responses in relevant situations and events. UCAs may arise from red functions or signals and they may in fact propagate through the system, but the design must ensure that this propagation ends prior to adversely affecting DDT performance. It should be noted that red does not imply that a signal or function is incorrect. Rather it signifies the limited role and the design attributes of those elements in the operational concept of the driving automation.

To understand Level 2 automation, it is helpful to start with a comparison between the machine sensors and the human sensors. The “red” designation on the machine sensors in this case indicates that the automation sensors may not be capable of reliably providing complete information regarding the surrounding environment or the vehicle itself. By contrast, the “human sensors” (or more colloquially the eyes, ears, and other perceptions of the human driver) have the role to avoid or prevent hazards at Level 2.

This distinction propagates through the control structure. The human driver, having the primary role in the control loop, and receiving information from his or her “human sensors,” makes the final control determinations to prevent hazards. At this level the driving automation system, using information provided via the machine sensors shown in red, are limited at Level 2 from making final control decisions in the event of a hazard.

Note that the driver commands pass to the vehicle along two paths. One is the human actuation to the machine controller, which reflects the modern reality that most driver inputs to the vehicle (e.g., via brake pedal, steering wheel, or accelerator pedal) are sensed by electronic sensors that feed into control electronics to ultimately implement the DDT. The line “Human Actuation to Machine Controller” reflects this sensed driver input. This driver input would need to be arbitrated with the driving automation system input, and a decision made on which to use if they conflict.

Separately, there is in some cases a “Driver Direct Action,” wherein the driver’s direct actuation is fed directly into the mechanical control system (e.g., the steering wheel transmits steering force to the rack.) This direct human input is fed into a “Final Arbitration” element, reflecting mechanical systems (e.g., the brake master cylinder or steering column) that ultimately arbitrate between the force inputs of the driver and the driving automation system.

In the Level 2 automation case, the final control actions are allocated to the driver, because the driving automation system may be limited in its capability to observe and control all potential hazards. The control structure is "closed" by the green loop connecting the sensing to the final arbitration through the human driver.

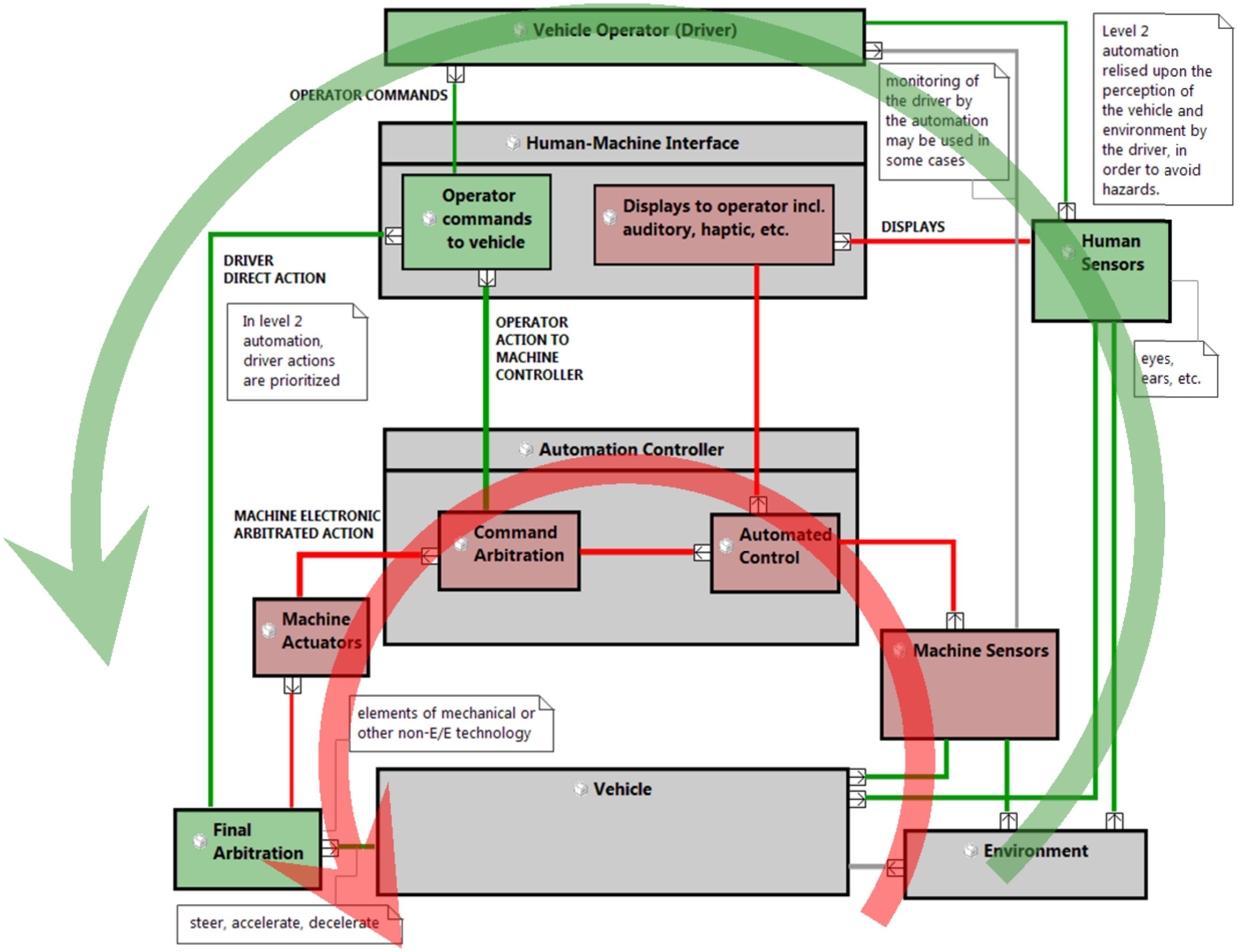

Vehicle Operator (Driver)
OPERATOR COMMANDS
monitoring of the driver by the automation may be used in some cases
Level 2 automation relised upon the perception of the vehicle and environment by the driver, in order to avoid hazards.
Human-Machine Interface
Operator commands to vehicle
Displays to operator incl. auditory, haptic, etc.
DISPLAYS
Human Sensors
DRIVER DIRECT ACTION
In level 2 automation, driver actions are prioritized
OPERATOR ACTION TO MACHINE CONTROLLER
eyes, ears, etc.
Automation Controller
MACHINE ELECTRONIC ARBITRATED ACTION
Command Arbitration
Automated Control
Machine Actuators
Machine Sensors
elements of mechanical or other non-E/E technology
Vehicle
Final Arbitration
Environment
steer, accelerate, decelerate

Figure 6: Control Structure for Level 2 Driving Automation

4.5.2 Safety Principles (SPs) for Level 2 Driving Automation

Following the STPA process, UCAs were generated from the control structure. Also following the STPA process, safety constraints were developed for each UCA. Tables outlining the UCA and safety constraint development are provided in Appendix A.

The safety constraints were highly repetitive in the analysis. Thus, the analysis method led to the collapsing of the list of safety constraints into more general "SPs."

With this in mind, the following SPs were developed for Level 2 Driving Automation:

(SP 2.1) For Level 2 driving automation, avoidance of hazards depends on the vehicle driver properly using the vehicle and automation, which includes:

i. Ensuring vehicle operational readiness before engaging driving automation features

ii. Completing the OEDR subtask in order to complete the DDT, by providing the appropriate responses to all relevant objects and events, in cases when the driving automation does not provide the appropriate response to avoid hazards

Note on SP 2.1: This principle is based largely on the definition of Level 2 driving automation, and is an assignment to the driver of the safe completion of the DDT in case of any question. The driver must understand these concepts in an L2 system:

- *It is their role to detect and respond appropriately to all situationally-relevant objects and events (OEDR) where the automation does not provide the appropriate response to avoid hazards*
- *That the automation is designed such that driver attempts to take full control will be honored, and the vehicle will respond (see SP 2.3)*

Some research (Llaneras et al., 2013) has indicated that drivers may not always perform the OEDR in some Level 2 systems as studied; additionally, concerns have been raised in some forums that drivers may misunderstand their role in the level, or misunderstand what level of automation they are using.

While purposeful abuse of systems is out of scope of this analysis, misunderstanding and associated misuse could be a causal factor in UCAs associated with this SP.

As such, human factors research could be conducted to investigate:

- *To what extent these concepts are already present as driver mental models (intuitive) in L2 executions*
- *HMI elements that could create affordances to support these driver mental models*
- *Educational approaches (e.g., training, owner's manual text, advertising) to support the driver's understanding of these concepts in L2 systems*
- *Methodologies to evaluate the driver's understanding of these concepts in the context of a Level 2 automation equipped vehicle*

The following safety principles, SP 2.2 and SP 2.3, are related to potential UCAs that might prohibit the driver from fulfilling this role, if the following principles are disregarded.

(SP 2.2) The driving automation system shall be integrated with the vehicle in a manner that does not inhibit the driver's ability to perform the DDT, which includes:

i. Control of the vehicle, lateral and longitudinal

ii. OEDR

Note on SP 2.2: This principle would require, for example, that the vehicle windows provide a clear view of the surrounding environment, as well as the provision of mechanisms (e.g., pedals, steering wheel) for the driver to control the vehicle.

(SP 2.3) The driving automation system shall prioritize predefined driver inputs for full control over driving automation commands.

Note on SP 2.3: The definition of "predefined driver inputs" will be established by the system design.

4.5.3 Key Findings

A Level 2 driving automation system is intended to complement but not substitute for the human driver in performing the dynamic driving task. The Level 2 driving automation system, when enabled, may provide indirect safety benefits that in the future may be measurable. However, in Level 2, overall safety will always be a result of the driver understanding and performing their role in relation to that of the driving automation system. The definition of the driver's role in a Level 2 driving automation system leads to the principle (SP 2.1.ii) that a driver's OEDR behaviors should be complete without regard to whether the system is attempting to respond to any detected objects. A human factors analysis may show that the overall performance of the driver and the system could be significantly enhanced if the driver knows that the system is engaged. Therefore, human factors research could be conducted to optimize the HMI support of Level 2 systems to optimize driver's awareness of the system state.

Designed input provided by the driver shall always be prioritized and the driving automation system must not inhibit the driver's ability to perceive or react to observable hazards. The human driver is the primary arbitrator due to the driving automation system's limited capability.

Each driving automation system manufacturer will seek to develop controls that allow the driver to request and take full control when necessary. In this capacity, it is the driver's role to understand proper control inputs for the system that they are operating. The manufacturer's design and integration may be proprietary and unique but should still meet the principles for a Level 2 driving automation system. Prior to engaging the system, it is the role of the driver to verify the operational readiness of the driving automation system and vehicle. Meaning, the driver is responsible for ensuring the vehicle is properly maintained and in a condition to be used appropriately, and must also understand that modifying or changing any form, fit, or function of the driving automation system may alter the vehicle's end performance.

Increased software and hardware functional capabilities as a result of advanced automation may provide increased performance capabilities for crash avoidance technologies. With this, crash avoidance technologies (not considered as driving automation) may find increased capabilities in vehicles that have Level 2 driving automation systems.

4.6 Level 3 Driving Automation

4.6.1 High-level Control Structure for Level 3 Driving Automation

The control structure diagram for Level 3 driving automation is shown in Figure 7. As in the previous diagram, green lines and green elements have the role to avoid hazards during driving automation operation, and provide appropriate responses to relevant situations and events. However, in the Level 3 control structure diagram, purple lines are used to reflect interactions, and purple elements depict those components that during automation are NOT charged with performing the primary tasks of control, but instead are charged with implementing specific selected functions to ensure automated driving safety.

A short review of the Level 3 control structure diagram shows several important differences from Level 2. In particular, the machine sensors and machine controller are now tasked to accomplish the DDT within the ODD. Therefore the primary role in avoiding hazards during Level 3 operation is relegated to the driving automation system, and not the human driver.

The human driver's role is now limited to a specific sub-set of overall functions. The driver must respond to the feedback displays and indications given by the system, when it requests the driver take action to resume the DDT. The driver must also be able to detect and respond to vehicle failures, which may not be detectable by the driving automation system.

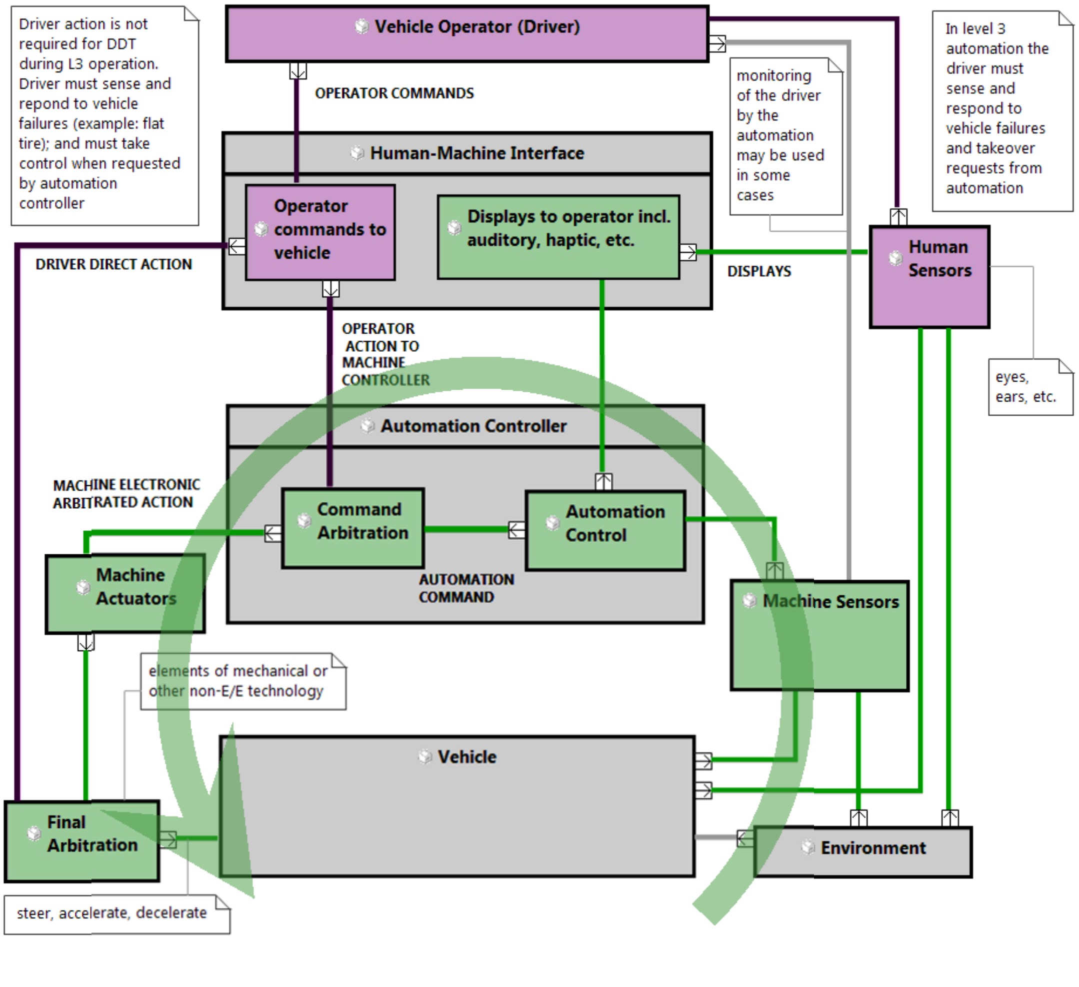

Driver action is not required for DDT during L3 operation. Driver must sense and repond to vehicle failures (example: flat tire); and must take control when requested by automation controller
Vehicle Operator (Driver)
OPERATOR COMMANDS
monitoring of the driver by the automation may be used in some cases
In level 3 automation the driver must sense and respond to vehicle failures and takeover requests from automation
Human-Machine Interface
Operator commands to vehicle
Displays to operator incl. auditory, haptic, etc.
DRIVER DIRECT ACTION
DISPLAYS
Human Sensors
OPERATOR ACTION TO MACHINE CONTROLLER
eyes, ears, etc.
Automation Controller
MACHINE ELECTRONIC ARBITRATED ACTION
Command Arbitration
Automation Control
AUTOMATION COMMAND
Machine Actuators
Machine Sensors
elements of mechanical or other non-E/E technology
Vehicle
Final Arbitration
Environment
steer, accelerate, decelerate

Figure 7: Control Structure for Level 3 Driving Automation

4.6.2 Safety Principles (SPs) for Level 3 Driving Automation

The following SPs were developed for Level 3 Driving Automation:

(SP 3.1) The driver shall ensure vehicle operational readiness before engaging driving automation features.

(SP 3.2) The driving automation system shall be integrated with the vehicle in a manner that does not inhibit the driver's ability to perform the DDT, which includes:

i. Control of the vehicle, lateral and longitudinal

ii. OEDR

(SP 3.3) The driving automation system shall prioritize predefined driver inputs for full control over driving automation commands.

Note on SP 3.3: The definition of "predefined driver inputs" will be established by the system design.

(SP 3.4) The driving automation system must not engage unless activated by the driver. After initially being activated, the automation can automatically resume if appropriate and within the same drive cycle. As a default, automation is not activated at the beginning of each drive cycle.

(SP 3.5) The driving automation system shall provide persistent indication to the driver that signifies when a vehicle is operating in high automation state, i.e., at Level 3 or higher.

(SP 3.6) The driving automation system shall provide indication to the driver upon any request to transition from Level 3 to a lower level (2, 1, or 0).

Note on SP 3.5 and SP 3.6: The indicators should be such that the driver can take over control when required and perform the DDT at the lower level. These two principles are meant to be achieved with independent indications. They are intended in response to an identified class of UCAs where the driver and driving automation system each believe the other is in control, leading in essence to no one controlling the vehicle. The transition out of Level 3 automation, into lower levels where the driver is recognized as the primary loop to complete the DDT, necessitates these transition indication concepts.

(SP 3.7) When activated, the driving automation system shall perform the DDT within its application-specific ODD, including providing the appropriate responses to relevant objects and events. This includes but is not limited to:

i. Continuous assessment of operation within actual versus operational design domain

ii. Inhibit operation when operational design domain is not achieved

(SP 3.8) The driving automation system shall be designed in such a way that a failure in the driving automation system does not lead to an immediate loss of the longitudinal and/or lateral control in order to allow the driver to respond as prescribed by SP 3.10 (iii).

When the driving automation system is engaged it shall operate in ~~s~~uch a way that, if a vehicle failure occurs that impacts longitudinal and/or lateral vehicle dynamics, systems shall continue to stabilize the vehicle's path within the given physical and technical limits in order to allow the driver to react as prescribed by SP 3.10 (i).

(SP 3.9) Before exiting the ODD, upon occurrence of a driving automation system failure that prevents performance of the DDT, the driving automation system shall request the driver to take control.

i. Verified driver control inputs shall cause transition from Level 3 into a lower level of automation.

ii. The driving automation system shall maintain an operating condition that affords a controlled transition to driver control, regardless of whether the transition is prompted by fault within the driving automation system, or prompted by violation of the intended ODD.

Note on SP 3.9-ii: Determining a "controlled transition" is a human factors consideration, which may vary by feature, location, speed, operational conditions, etc. An example of intended ODD might be environmental conditions that exclude snow and ice. A fault within the automation may be a hardware failure in a sensing system.

(SP 3.10) The driver must understand the following:

i. The driver's role is to determine if there has been a vehicle failure that may impact the safe operation of the vehicle, and to take over control of the vehicle when such a failure occurs.

Note on SP 3.10-i: This role of the driver is related to vehicle failures, and not to failures of the driving automation system.

ii. In response to a driver request to take over performance of the DDT, the primary response from the driving automation system is to transition out of Level 3 automation and into a lower driving automation level.

Note on SP 3.10-ii: There is a potential exception of accelerating out of the maximum speed capability of the steering automation.

iii. When the driving automation system is requesting the driver to take control of the vehicle, the driver's role is to respond by taking control.

Note on SP 3.10-iii: This principle implies that the vehicle operator's role is to assume control in the case that the automation requests it. Safe and proper operation depends on this understanding by the operator.

iv. After requesting the driver to take control, the driving automation system will remain in control for a limited time period.

4.6.3 Key Findings

Level 3 driving automation systems introduce the capability for the automation to perform the complete DDT within its ODD. This capability fundamentally alters the traditional role of the driver and therefore places additional SPs on the driver and the driving automation system.

The most significant principle placed on a Level 3 driving automation system is that when it is engaged, the DDT is performed solely by the driving automation system within a limited ODD (e.g., geographical location, environmental condition, speed, etc.). While operating within its ODD, the driving automation system must provide an appropriate response to all relevant objects and must both detect and avoid the potential hazards defined in Section 4.2.2. Such performance relies on sensing technology to perceive a variable external environment. Due to inherent limitations of technology, and an infinitely variable external environment, an outcome cannot be assured. While avoidance of design flaws is necessary to avoid systematic errors, unforeseeable variance in the environment may also contribute to non-systematic errors. Therefore, it is important to consider both when developing features. Due to the DDT performance requirements for a Level 3 driving automation system, there may be significant dependencies on the maintenance of the vehicle, including a need to utilize OEM parts and procedures for maintenance, repair, and customer alterations.

The automation must also "preview" its ODD and ensure that the transfer of the DDT back to the driver can be completed before the vehicle exits its ODD. However, when outside of this operating domain or in the event of an automation or vehicle failure, the DDT must be completed by the driver; therefore the primary principle for a driver in Level 3 is that they retain the role of "fallback" in relation to the driving automation system. For the driver to understand their role, clear indication of both the automation mode and the need for transitioning out of automation become a safety principle of the system. Also, since "fallback" to the driver is necessary in the case of a vehicle failure, the principle remains that the automation will allow the driver a means to take full control of the vehicle at any time.

Several of the Level 3 principles raise human factors considerations such as the driver's need to understand their role of "fallback" and their performance transitioning into and out of that role. Studies of those human factors considerations are out-of-scope of this task and should be addressed in future research.

4.7 Level 4 Driving Automation

4.7.1 High-level Control Structure for Level 4 Driving Automation

The control structure diagram for Level 4 driving automation is shown in Figure 8. As in previous diagrams, the green lines and green elements depict the performance of primary functions in the control of vehicle motion during automated operation, and are charged with providing appropriate responses in relevant situations and events. Red lines and red elements indicate secondary functions in the control of the vehicle within the automation level and as such are not critical to avoiding hazards. In Level 4 driving automation, note that hazards can be mitigated entirely by the driving automation system, without active participation by the vehicle operator.

The machine sensors, machine controller, and actuation are all primary elements. Because Level 4 driving automation includes suitable fallback mechanisms even in case of a vehicle failure, the vehicle can prevent hazards during operation without human intervention. As shown in Figure 8, the human driver is not charged with mitigating hazards at Level 4.

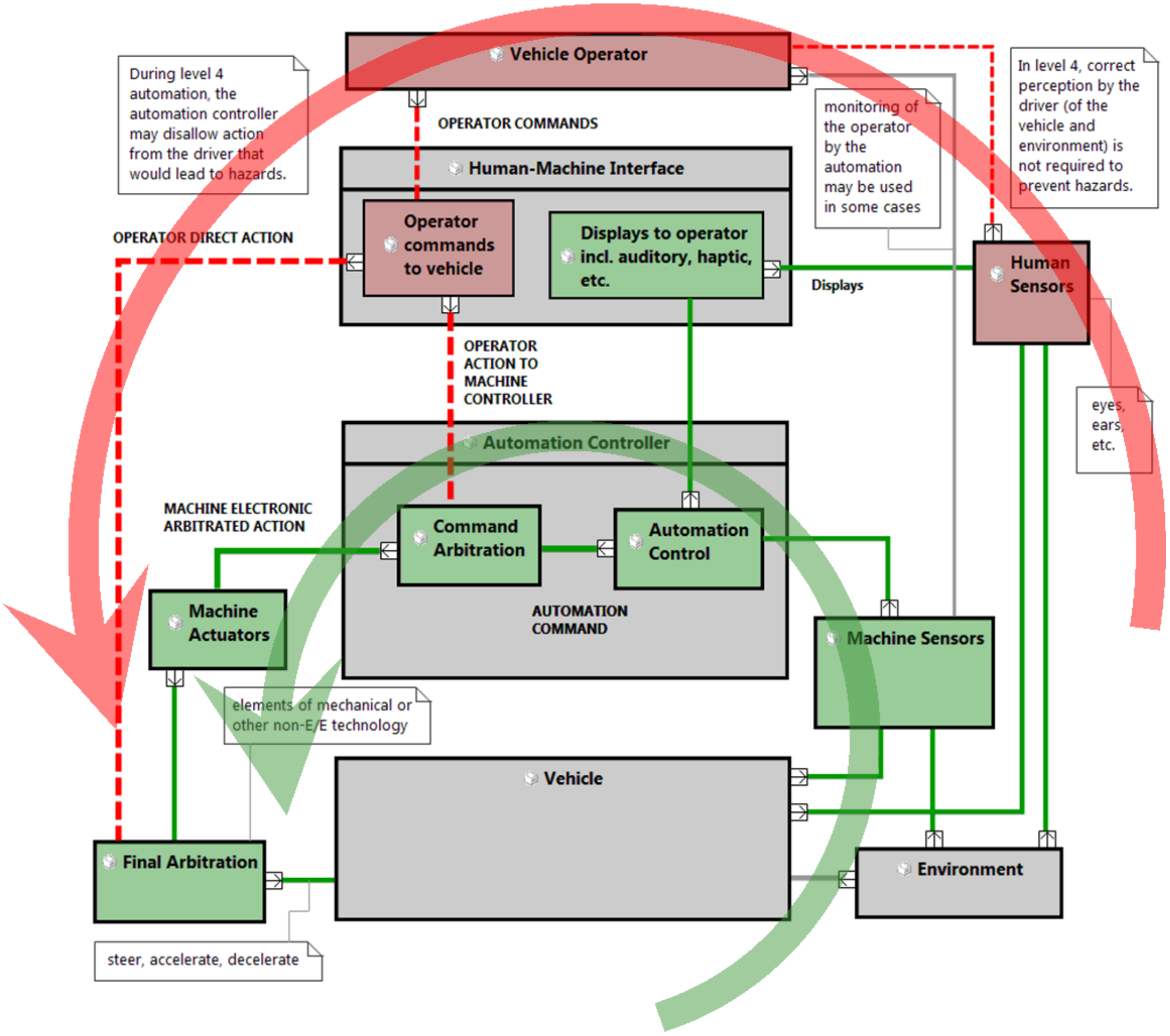

Vehicle Operator
OPERATOR COMMANDS
During level 4 automation, the automation controller may disallow action from the driver that would lead to hazards.
monitoring of the operator by the automation may be used in some cases
In level 4, correct perception by the driver (of the vehicle and environment) is not required to prevent hazards.
Human-Machine Interface
Operator commands to vehicle
Displays to operator incl. auditory, haptic, etc.
OPERATOR DIRECT ACTION
Displays
Human Sensors
OPERATOR ACTION TO MACHINE CONTROLLER
eyes, ears, etc.
Automation Controller
MACHINE ELECTRONIC ARBITRATED ACTION
Command Arbitration
Automation Control
AUTOMATION COMMAND
Machine Actuators
Machine Sensors
elements of mechanical or other non-E/E technology
Vehicle
Final Arbitration
Environment
steer, accelerate, decelerate

Figure 8: Control Structure for Level 4 Driving Automation

4.7.2 Safety Principles (SPs) for Level 4 Driving Automation

The following SPs were developed for Level 4 driving automation. Note that at Level 4, principles no longer refer to the "driver," but instead to the term "operator." The operator may be a driver in a traditional sense, or may be another overseeing entity such as a remote dispatcher, maintenance facilitator, or owner/user. The operator is defined as distinct from the driving automation system, although either one may perform the DDT depending on the system design and situation.

(SP 4.1) The vehicle operator shall ensure vehicle operational readiness before engaging the driving automation system.

(SP 4.2) When activated, the driving automation system shall perform the DDT and fallback as needed within its application-specific ODD, providing the appropriate responses to relevant objects and events. This includes but is not limited to:

i. Continuous assessment of operation within actual versus operational design domain

ii. Prohibiting entry into automated driving when the operational domain is not achieved

iii. Ability to achieve minimal risk condition if necessary due to any one of the following:

a) Operator failure to respond appropriately to pending exit of the ODD

b) A failure that prevents performance of the complete DDT

(SP 4.3) The driving automation system may delay its response to operator take-over requests, and/or operator requests to stop driving automation when necessary to avoid causing a hazard.

(SP 4.4) The driving automation system must not engage unless activated by the operator.

4.7.3 Key Findings

Level 4, as with Level 3, is capable of completing the DDT within the ODD and also can achieve a minimal risk condition as part of the Level 4 driving automation system fallback strategy. This level allows the operator to engage the system when the ODD is achieved, at which point the operator no longer needs to supervise the vehicle, because the system can achieve a minimal risk condition while operating within its ODD.

Operator requests to take over part or all of the DDT may not be immediately granted as the system may be operating in domains where human control is not allowed or could cause an undesired hazard/control action. For example, in high-speed platoons with short following gaps there is likely to be a specific protocol that must be followed to safely leave the platoon, or to exit a dedicated lane/corridor where vehicles without specific Level 4 or 5 driving automation system capabilities are not allowed. This may result in a driver being unable to take over the DDT from the driving automation system until the vehicle has exited from the dedicated Level 4 or 5 lane or corridor.

Due to the DDT performance requirements for a Level 4 driving automation system, there may be significant dependencies on the maintenance of the vehicle, including a need to utilize OEM parts and procedures for maintenance, repair, and customer alterations.

Within the ODD, the fallback strategy must be robust enough that in the event the operator does not respond to a take-over request, the driving automation system will complete a single, or series of, maneuver(s) to achieve a minimal risk condition. Note: This is a functional design feature of a vehicle with a Level 4 system, and not different level of automation to which the driving automation system resorts under failure conditions.

It is important to note that on vehicles with a driving automation system that is capable of Level 4 operation but where lower levels of automation are also possible, the applicable principles must be applied for transitioning into those lower levels from the higher level. These are not Level 4 principles per se, but must be accommodated when developing a vehicle that may operate at Level 4 or at a lower level. For example, the following principles would apply to a Level 4 vehicle that had the capability of operating at lower level:

- (from SP 2.2) On vehicles where lower levels of automation (or Level 0 / no automation) are possible, the driving automation system shall be integrated with the vehicle in a manner that does not inhibit the driver's ability to fully perform the DDT
- (from SP 3.5) On vehicles where lower levels of automation (or Level 0 / no automation) are possible, automation shall provide persistent indication to the driver whenever the vehicle is operating in high automation state (e.g., at Level 3 or higher)
- (from SP 3.6) On vehicles where lower levels of automation (or Level 0 / no automation) are possible, the driving automation system shall provide indication to the driver upon any transition from a high automation state (e.g., Level 3 or higher) to a lower level (2, 1, or 0), such that the driver/operator is enabled to achieve effective driver performance at the lower level

In reviewing these principles, it appears that there may be human factors considerations where both Level 3 and Level 4 capability coexist in the same vehicle. Level 3 requires the driver to understand that a predefined driver control input will generally cause the driving automation system to transition immediately into a lower automation mode; whereas Level 4 automation may delay a response to operator input if a foreseeable hazard is likely to occur. These are very different responses to driver inputs that raise human factors considerations for vehicles containing both Level 3 and Level 4 automation capability.

Note that Level 4 driving automation systems may also include the capability for an operator to request takeover of the DDT from the driving automation system at any time. Such a request may be issued for purely personal reasons (e.g., the operator feels like driving), or for more event-based reasons (e.g., the operator or a passenger experiences a medical emergency that necessitates rushing to the nearest hospital). This latter example is a case of a hazard that occurs at the level of driving strategy (versus operational or tactical levels of driving) and is thus not part of the DDT.

4.8 Level 5 Driving Automation

4.8.1 High-Level Control Structure for Level 5 Driving Automation

The control structure diagram for Level 5 driving automation is shown in Figure 9. Note that the diagram for Level 5 is very similar to Level 4, reflecting similarities between the two levels. As was evident in the Level 4 case, Level 5 driving depends on a primary set of automation elements to prevent hazards, while not relying on the correctness of the vehicle operator's inputs to avoid hazards. Note that in both Level 4 and Level 5 driving automation, hazards associated with strategic topics (i.e., non-DDT-related), such as where the vehicle should travel at a given time, or if and when the riders may exit, are viewed as outside the scope of this analysis.

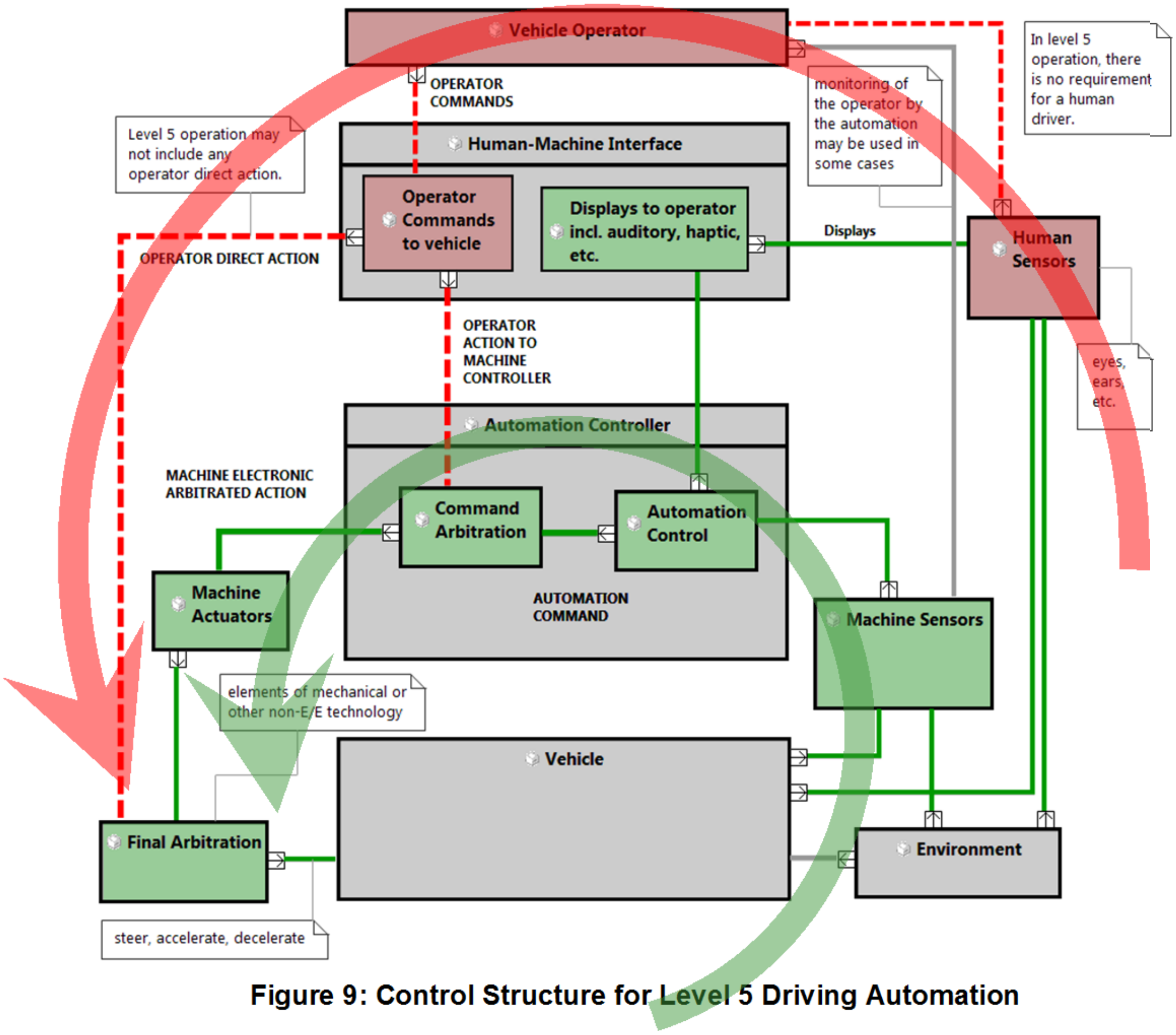

Vehicle Operator
OPERATOR COMMANDS
In level 5 operation, there is no requirement for a human driver.
monitoring of the operator by the automation may be used in some cases
Level 5 operation may not include any operator direct action.
Human-Machine Interface
Operator Commands to vehicle
Displays to operator incl. auditory, haptic, etc.
Displays
OPERATOR DIRECT ACTION
Human Sensors
OPERATOR ACTION TO MACHINE CONTROLLER
eyes, ears, etc.
Automation Controller
MACHINE ELECTRONIC ARBITRATED ACTION
Command Arbitration
Automation Control
Machine Actuators
AUTOMATION COMMAND
Machine Sensors
elements of mechanical or other non-E/E technology
Vehicle
Final Arbitration
Environment
steer, accelerate, decelerate

Figure 9: Control Structure for Level 5 Driving Automation

4.8.2 Safety Principles (SPs) for Level 5 Driving Automation

The following SPs were developed for Level 5 Driving Automation:

(SP 5.1) The vehicle operator shall ensure vehicle operational readiness before engaging driving automation.

(SP 5.2) The vehicle system overall (including the driving automation system and its integration) shall be designed such that the driving automation system is capable of performing the DDT and fallback as needed, including:

i. Providing appropriate responses to relevant objects and events

ii. Ability to achieve a minimal risk condition if necessary due to a failure that prevents performance of the complete DDT

(SP 5.3) The driving automation system may delay response to operator requests to take over, and/or operator requests to stop driving automation when necessary to avoid causing a hazard.

(SP 5.4) The driving automation system must not engage unless activated by the operator.

4.8.3 Key Findings

Level 5 represents the leap to fully automated driving where equipped vehicles are capable of delivering passengers or products to their desired destination without human input. Level 5 operates without design domain limitations. As such, it represents a significant disconnect between the user/passenger and the vehicle that may fundamentally change the current perception of road transportation. Level 5 driving automation systems offer the ability to virtually eliminate driver/operator error in performance of the DDT as a cause of vehicle accidents and therefore may result in direct safety benefits. Given that the complete vehicle motion control authority rests with the driving automation system, passenger requests for changes in strategic priorities (e.g., the programming of new destinations or waypoints) will only be implemented when, based upon assessment by the driving automation system, conditions are deemed safe enough to affect the change.

Due to the DDT performance requirements for a Level 5 driving automation system, there may be significant dependencies on the maintenance of the vehicle, including a need to utilize OEM parts and procedures for maintenance, repair, and customer alterations.

A Level 5 driving automation system may have the capability to transition down to a lower level upon operator request provided that no hazards will occur during the transition. A vehicle operating at these lower levels will be required to meet all applicable SPs associated with the applicable operational level.

4.9 Summary of Safety Principles (SPs)

Table 5 presents a summary of the SPs introduced in Sections 4.5 through 4.8 of this report. The SPs are organized by driving automation level and the ‘actor’ to which the principle applies (i.e., the driver/operator, vehicle systems, or driving automation system). The table provides a concise summary of the SPs showing how some principles are common across driving automation levels while others only apply to particular driving automation levels. While this table is intended to provide a high level summary of the SPs, it should only be used in conjunction with the report text to accurately describe the developed SPs.

Table 5: Summary of Safety Principles

Safety Principle Related to:	When Driving Automation System is Engaged at			
	Level 2	Level 3	Level 4	Level 5
Driver / Operator	Assures operational readiness (SP 2.1 i)	← (SP 3.1)	← (SP 4.1)	← (SP 5.1)
	Relied upon to avoid hazards, by completing the OEDR subtask of the DDT (SP 2.1 ii)			
		Determines if vehicle failure occurs and takes over DDT (SP 3.10 i)		
		Understands that a driver request to take over performance of the DDT will cause a transition to lower level automation (SP 3.10 ii)		
		Performs the DDT when requested by the driving automation system (SP 3.10 iii)		
		Understands that after the driving automation system request to take over the DDT, automation will only remain in control for a limited time (SP 3.10 iv)		

Safety Principle Related to:	**When Driving Automation System is Engaged at**			
	Level 2	**Level 3**	**Level 4**	**Level 5**
Vehicle Systems	Designed such that the driver is capable of performing the complete DDT (lateral / longitudinal control and OEDR) (SP 2.2)	← (SP 3.2)	Note: Include if vehicle is capable of lower level automation	Note: Include if vehicle is capable of lower level automation
Driving Automation System	Prioritize predefined driver inputs for full control over driving automation commands (SP 2.3)	← (SP 3.3)		
		Cannot engage unless activated by driver/operator (SP 3.4)	← (SP 4.5)	← (SP 5.5)
		Provides persistent indication to driver of operation in high automation state (SP 3.5)	Note: Include if vehicle is capable of lower level automation	Note: Include if vehicle is capable of lower level automation
		Provides indication to driver of request to transition to lower level automation (SP 3.6)	Note: Include if vehicle is capable of lower level automation	Note: Include if vehicle is capable of lower level automation
		Performs the complete DDT within its operational design domain (SP 3.7 i)	← (SP 4.2 i)	Performs the DDT in all domains (SP 5.2 i)
		Prohibit entry into automated driving when operational design domain is not achieved (SP 3.7 ii)	← (SP 4.2 ii)	

Safety Principle Related to:	When Driving Automation System is Engaged at			
	Level 2	Level 3	Level 4	Level 5
Driving Automation System		A failure in the driving automation system shall not lead to an immediate loss of the longitudinal and/or lateral control, and when engaged it shall operate in such a way that systems shall continue to stabilize the vehicle's path within the given physical and technical limits in the presence of a vehicle failure (SP 3.8)		
		Before exiting the operational design domain or upon occurrence of a driving automation system failure that prevents performance of the DDT, system shall transfer DDT to the driver (SP 3.9)	Able to achieve minimal risk condition when necessary (SP 4.2 iii)	← (SP 5.2 ii)
		Verified driver control inputs shall cause transition to lower level automation (SP 3.9 i)	May delay its response to request by operator to take over/stop driving automation when necessary to avoid causing a hazard (SP 4.3)	← (SP 5.3)
		Maintain operational condition that affords a controlled transition to driver (SP 3.9 ii)		

4.10 Summary - Top-Level Safety Principles for Levels of Automation

The objective of this phase of the project was to develop by driving automation level, a solution-neutral set of SPs that are based on the potential hazards associated with automation.

Section 4.1 of this report provides an introduction to the particular hazard analysis technique used to identify and develop SPs for the levels of driving automation under consideration. The hazard analysis technique used in this effort was based on the System-Theoretic Process Analysis (Leveson, 2012). The use of STPA in this analysis should not be interpreted as a general preference for this method over all other available methods of hazard analysis. The STPA methodology was used because it is familiar to most of the CAMP AVR members and offered a great amount of flexibility for analyzing the UCAs associated with the interaction of the driver and the driving automation system that can lead to hazards. Usage of STPA also did not necessitate the availability of a physical design at the time of analysis.

In Section 4.2, the hazards and losses to be considered in the development of SPs per driving automation level were defined. The identified hazards were based on the defined loss of experiencing a crash with a threatening object on or just off the roadway. To this end, four generalized hazards were developed: leaving the roadway; losing traction / stability; coming too close to an object in the roadway; and violating traffic laws, rules or norms pertaining to the DDT.

In Section 4.3, the generic control structure for driving automation Levels 2 through 5 was defined with three principle ‘actors’: the driver, the driving automation system, and the base vehicle. As stated in Section 4.3, the role of the driver and driving automation system in controlling the vehicle by performing the DDT and fallback as needed, along with the determination of final authority in arbitrating conflicting commands, are the fundamental building blocks of the levels of automation.

In Sections 4.5 through 4.8, the SPs for each driving automation level were defined. The SPs were developed by:

1) **Developing the system boundaries / functional control structure under analysis**. In this step, the functional control structures for the driving automation Levels 2 through 5 were developed to determine which conditions should be considered as a contributing element to the existence of the hazard.

2) **Identifying the UCAs in the control structure under analysis that could lead to the hazards under consideration.** This work focused on identifying the UCAs that could occur because:

    a. A control action required to avoid the defined hazards was not provided or followed

    b. UCAs are provided / allowed based on the functional control structure

    c. A required control action is provided too early or too late

    d. A required control action is stopped too soon or applied too long

3) **Determining how each identified UCA could occur within the functional control structure.**

4) **Specifying the top-level SPs for driving automation Levels 2 through 5.** Using the control structures and UCAs as a guide, safety constraints were developed. The safety constraints were then collapsed into fewer, more general SPs for driving automation Levels 2 through 5 to eliminate the UCAs under

consideration. These SPs were allocated to the driver/operator, the vehicle, and/or the driving automation system, as appropriate, and are transferable to features that reside under each automation level.

Section 4.9 provides a table summarizing the SPs introduced in Sections 4.5 through 4.8 of this report, organized by driving automation level and the 'actor' to which the principle applies (i.e., the driver/operator, vehicle systems, or driving automation system).

The outcomes from this effort were used as a foundation for the development of use cases and preliminary objective test methods, described in the next section of the report. The goal of this work is the development of preliminary objective tests used to primarily verify adherence to the Level 2 SPs.

Task 8 of the AVR project is intended to identify synergies in NHTSA's internal and external research projects for vehicles with driving automation features related to human factors, cybersecurity, electronics reliability, and public policy. Throughout this document, a variety of human factors considerations have been discussed (e.g., several of the Level 3 principles raise human factors considerations such as the driver's need to understand their role of "fallback" and their performance transitioning into and out of that role).

Through Task 8, these (and other human factors) considerations will be communicated as appropriate.

5 Development of Use Cases and Preliminary Objective Test Methods

5.1 Testing Goals for Level 2 and Level 3 Driving Automation Systems

Testing goals for driving automation systems are complex and widely diverse. Where traditional safety testing and certification have been refined to achieve the required testing goals in the form of standardized requirements and test procedures, the field of driving automation is evolving and therefore not so easily molded into a standard regimen. Automotive systems, both passive and active, are verified to ensure that they meet specific performance or functionality criteria. The goals of such tests are dependent on the type of system and are expressed in objective standards that represent reasonable state-of-the-art system capabilities and establish minimum performance requirement(s). For functional tests, standards can range from minimum miles per gallon for environmental impact, or route optimization for enhanced mobility, to crash avoidance/worthiness for safety gains. As systems mature in performance and functionality, standards are often modified to reflect enhanced levels of system performance and functionality.

In the area of automotive safety, NHTSA Federal Motor Vehicle Safety Standards (FMVSS) specifications establish test scenarios that (1) address a real-world crash problem, (2) are supported by information that demonstrates an expected or actual safety benefit while minimizing the risks of negative unintended consequences, (3) are able to be tested by objective performance tests and procedures that are reproducible and repeatable, and (4) are practicable and feasible. Initially, crash types are identified through the study of real-world crash statistics and records that can be quantified by vehicle dynamics, impact location, severity, road type, presence of other traffic, and other factors that characterize crash types of interest. Databases such as the Fatality Analysis Reporting System (FARS)[2] and the National Automotive Sampling System (NASS)[3] are typically used to identify crash types that have a significant influence on roadway safety in the U.S. Once the crash type is determined, a selection of the most frequent and/or most severe crash scenarios are characterized to understand the potential or actual benefits associated with the crash type. If the potential or actual benefits calculation relative to the cost associated with deployment of the technology is positive, then a representative, objective and reproducible test scenario could be pursued.

To make a test scenario objective and repeatable across manufacturers, stringent testing tolerances and practices must be defined so that the test procedures ensure the vehicles are exposed to the same test parameters, and that these remain representative of real-world crash scenarios. Key testing parameters include, but are not limited to, vehicle speed, approach distance, yaw rate, acceleration/deceleration, proximity (lateral and longitude) to a potential crash partner, physical attributes of other vehicles/objects,

[2] http://www.nhtsa.gov/FARS

[3] http://www.nhtsa.gov/NASS

weather conditions, vehicle type, roadway type, and driver inputs. To establish an objective and reproducible test, requirements with tolerances must be placed on each testing parameter. These requirements must also be defined such that they do not create a scenario in which they evoke or instruct driver control inputs to the vehicle or driving automation system responses that do not reflect actual vehicle operation encountered in the real-world. Such unrealistic requirements may otherwise create inappropriate test environments that are not experienced in a non-manufactured environment, or that specify an environment in which a specific driving automation system could not actually operate.

Test requirements that apply across all manufacturers to achieve some minimum level of performance or functionality generally do not focus on how it is achieved (i.e., what technology is utilized to meet the requirements, or how the system performs outside of a prescribed scenario). Additionally, in absence of real-world crash data, system performance requirements are limited to those that are developed to address functional safety hazards that have been defined for the driving automation system's operational design domain.

5.1.1 Lower Level Driving Automation System Testing

For Level 2 systems, largely due to the supervisory role of the driver, the driver's ability to resume performance of a portion or the complete DDT when the system is presented with a hazard that it is not designed to manage, can be assessed. In this case, the driver requires the ability to override the driving automation system or terminate its operation and complete the DDT at any time while the driving automation system is engaged. To achieve this, manufacturers may have different design elements to enable the override or termination function, and to ensure that the driver's ability to complete the DDT is not compromised. This results in tests that are specific to the driving automation system feature being evaluated.

The system's operational design domain will directly influence what HMI features and driver inputs are needed for the driving automation feature to function. For example, a Level 2 partial automation parking feature requires the driver to override or terminate automated operation if the vehicle encounters a hazard during the parking maneuver. A partial automation parking feature from a specific manufacturer and model may require the driver to be inside the vehicle activating a control to carry out the parking maneuver sequence. Another version of such a parking automation feature from the same or different manufacturer may allow a driver to exit the vehicle and to activate the system via a dedicated feature on a remote control device or smartphone while remaining within a specified range of the vehicle and maintaining line-of-sight to it. In the first case, the driver completes the OEDR subtask of the DDT from within the vehicle and, if a hazard is perceived, takes over steering and/or braking control causing the automation to discontinue. In the second case, if the driver exercising the remote control device sees that something or someone has entered the pathway of the vehicle, s/he releases the control, thus bringing the vehicle to a stop. Also, if the driver exercising the remote control device is not within the design-specific range of the vehicle, the automation will either not engage or discontinue operation as the driver moves out of range and the vehicle will either remain stationary or brake to a stop until the driver re-enters the vehicle and resumes the DDT. Both of these example approaches achieve the same goal of partially automated parking (Level 2), but each uses a different design concept to address the SPs derived from the hazards, which are assigned according to that automation level. The latter example has more ODD limits to address the same set of SPs that apply to both partial automation parking features. Conditions that are embedded in the design concept require that SP assessment procedures be developed for specific driving automation features so that the SPs can be tested for the applicable ODD.

Feature performance in terms of the driving automation system ODD, vehicle dynamics limits, and driver interface while operating in specific modes are optimized for driver acceptance and response performance, and are tailored to the overall HMI concept for specific vehicle makes and models. While maintaining this design freedom, the driving automation system driver interface must nonetheless ensure that SPs are achieved while in operation. For example, while a parking automation feature is operating, the feature may bring the vehicle to a complete stop and fully turn the steering wheel to its full stop, prior to resuming forward motion. Other automated parking feature implementations may gradually turn the wheel while proceeding into the parking space or even execute multiple fore and aft maneuvers to enter the same parking space. All three implementations are equally acceptable, provided the applicable SPs are achieved while the feature is engaged and operating. At the same time, the overall driving automation system ODD, vehicle dynamics limits, and driver interface may have considerable effects on driver satisfaction and usage of the feature, which are not subject to standardized performance testing.

5.1.2 Higher Level Driving Automation System Testing

Testing of lower levels (Levels 1 and 2) of driving automation systems compared to the higher levels (Levels 3 through 5) of driving automation systems differs significantly. In the lower levels, where the driver is responsible to complete the OEDR, the driving automation system must demonstrate that override and feature termination capabilities remain functional at all times and that the system does not prevent the driver from completing the OEDR. Higher level driving automation systems are responsible for performing the complete DDT (including complete OEDR) and no longer require a driver to supervise the driving automation system performance. This generates a set of new SPs that include operational performance of the system and depending on the ODD and level, fallback performance as well as different system override and termination capabilities.

The driving automation system must respond appropriately to all relevant objects and events in the driving environment (e.g., other vehicles, road conditions, fixed obstacles) by maneuvering the *vehicle* in order to avoid hazards. In this way the system design satisfies the associated SPs. The set of scenarios representing potential hazards that must be managed by the driving automation system within certain domains is potentially unlimited.

Some ODDs, such as for a Level 4 closed campus shuttle, may have a limited set of scenarios that must be managed due to the physical limitations, design of the domain or associated policies that prevent a set of objects or events, such as pedestrians or unknown objects in the roadway, from being encountered. Other systems will operate in less restricted domains (e.g., typical public roads) that will not have such advantages. Objects and events that may be encountered will have widely ranging physical characteristics which must be responded to appropriately by an engaged driving automation system. Examples of objects and events include: pedestrians emerging from behind parked cars, rolling trashcans, running animals, potholes, mailboxes, vehicle accidents and road construction. The exposure, appearance and physical proximity to objects and events cannot always be predicted, and require a response appropriate to the object or event.

The random nature of encounters with objects and the occurrence of events challenges standardized testing of driving automation systems. This is because standardized testing demands a finite set of relevant test scenarios associated with an acceptable test burden to reproducibly assess system performance across manufacturers. Scenario relevance must be assessed for each system implementation, variances in which may render a particular scenario irrelevant due to the limited ODD. The test burden, in terms of the number and complexity of trials, must also be reasonably limited with practical test facilities in a safe test environment. This can potentially be achieved through selecting a subset of scenarios with objects and events that best represent the broad array of scenarios that the system may be expected to encounter within its ODD.

5.2 Classification and Operational Description and Safety Principle Assessment Procedure

5.2.1 Goal of the Classification and Operational Description and Safety Principle Assessment Procedure

With the complexity and diversity of the ODDs being developed for vehicles with driving automation systems, in-vehicle conditions and vehicle status must be achieved to enable, disable, or override system functionality. To test a system, customized information regarding the design of a particular implementation is required because a given set of standardized test conditions would not match diverse ODDs. In determining an approach for accomplishing these objectives, there is merit in adopting a general method for gathering system ODD requirements.

The method proposed incorporates a Classification and Operational Description to supplement detailed SP assessment procedure instructions. The description contains basic information regarding an overall vehicle and specific vehicle systems. For purposes of this method, driving automation systems are specific vehicle systems.

For vehicles equipped with driving automation systems, the approach is envisioned to involve the following information:

- Vehicle make, model, and model year
- Description of driving automation system as provided in the vehicle’s owner manual
- Determination of the driving automation system’s automation level
- Identification of SPs relevant to that level
- Proposed SP assessment procedures

Because SPs for each automation level entail driver knowledge of driving automation system operation, the most apparent way to describe operation to drivers is through owner's manual. Descriptions will vary with different systems, developers, and automation levels. Therefore, providing such owner's manual information would support the related SPs.

Although as discussed earlier in this report, a given automation system may provide multiple features that operate at different levels, for the purposes of the method described here, each driving automation system will have a single corresponding automation level. Also, each system will be designed to perform under criteria established by its developer. Although systems provided by different developers may appear to perform a similar task, their capabilities and operational design domains may be different. As a result, only the developer is able to appropriately determine the automation level of its system. To help explain a developer's determination of automation level, the Classification and Operational Description poses a series of questions based on the work in Section 2. Answers to the questions yield the automation level of a system.

Each system's driving automation level will have a set of corresponding SPs. Since the driving automation level of a system is determined by the developer, the developer has knowledge about how the system satisfies related SPs and is best positioned to provide SP assessment procedures to evaluate the system implementation.

Examples of SP assessment procedure concepts for three potential driving automation systems are described in Sections 5.3.1, 5.3.2, and 5.3.3. The three potential systems are:

- Level 2 Parking Assist
- Level 2 Traffic Jam Assist (TJA)
- Level 2 High Speed Automated Cruise (HSAC)

The generic Classification and Operational Description is presented in Appendix B while the non-specific outline of procedures is shown in Appendix C. In Appendices D through O, hypothetical Classification and Operational Descriptions and SP assessment procedures of two fictitious manufacturers are shown for each of the three potential systems.

5.2.2 Driving Automation Level Determination

In order for a driver to properly understand his or her role when operating a vehicle equipped with driving automation features, the role of the driver and the role of driving automation system must be clearly specified. An industry-common classification was developed to distinguish automation features by levels in Section 2. Each driving automation level is defined according to the automation function and the roles that are required of the driver and the driving automation system when the system is engaged. A detailed description of the levels of automation can be found in Section 2.

Section 2 of the Classification and Operational Description is intended to allow a developer to properly classify a driving automation feature into the appropriate level of driving automation. The classification method consists of a series of yes/no questions related to the functional capabilities of the driving automation feature. The answer to each question will either result in an automation level classification or require additional questions to determine the appropriate driving automation level. Below are a brief explanation of each question and interpretations of the responses.

Question 1: Does the feature perform sustained control of lateral or longitudinal vehicle motion to external objects or events in lieu of the driver?

The term "sustained" implies that the control provided by the feature is of a duration and authority that allows the driver to cede control (either lateral or longitudinal) to the automation system (i.e., "hands-off" ***or*** "feet-off") – i.e., it provides sustained control between and across external objects or events.

If Q1 is answered "no," the feature is not considered automation and is Level 0

If Q1 is answered "yes," proceed to Question 2

Question 2: Does the feature perform sustained control of lateral and longitudinal vehicle motion to external objects or events in lieu of the driver?

Question 2 is answered "yes" only when the feature can provide both sustained lateral and longitudinal control simultaneously (i.e., "hands-off" ***and*** "feet-off)

If Q2 is answered "no," the feature is considered automation Level 1

If Q2 is answered "yes," proceed to Question 3

Question 3: Does the feature require supervision by the driver during its normal operation?

Supervision of the automation feature is defined such that the driver is required to oversee the feature's control operation by comparing the control actions to the objects and/or events occurring in the environment. If necessary, the driver must immediately take control whenever the system is not reacting appropriately.

If Q3 is answered "no," proceed to Question 4

If Q3 is answered "yes," the feature is considered automation Level 2

Question 4: Does the feature rely on the driver to take over if it is not operating normally?

This can also be referred to as "fallback" whereby the system may require the driver to re-take control in situations of leaving the ODD or if there is a failure in either the automation or a vehicle system that could affect the automation system's ability to operate as designed. An example would be a scenario where the system may be about to leave its ODD (e.g., exit an expressway) and would request the driver to take control.

If Q4 is answered "no," proceed to Question 5

If Q4 is answered "yes," the feature is considered automation Level 3

Question 5: Does the feature have a limited scope of operation?

If the system is limited by design as to its domain of operation (e.g., speed, geographical location, road type) then this question would be answered "yes."

If Q5 is answered "no," the feature is considered automation Level 5

If Q5 is answered "yes," the feature is considered automation Level 4

5.2.3 Testing Relevant to Level-Specific SPs

After a developer has classified the driving automation system, it is appropriate to identify the related SPs for relevant testing. The SPs, identified in Section 4, are worded to differentiate clearly the role of the driver versus the role of the driving automation system.

Tables 6 through 9 each represent a driving automation system level and relevant SPs in the left column and the proposed test criteria in the right column. Test criteria can be demonstrated by a combination of static tests (e.g., owner's manual content review or system control features) and dynamic tests (e.g., confirmation of driver override and response to associated hazards).

Table 6: Driving Automation System Level 2

Safety Principle Criteria	Nature of Testing	Fulfilment
Safety Principle 2.1 For Level 2 driving automation, avoidance of hazards depends on the vehicle driver properly using the vehicle and automation, which includes: i. Driver ensuring the vehicle operational readiness before engaging driving automation features	OEM describes requirements for vehicle operational readiness	Reference to Owner's Manual
ii. Driver completing the Object and Event Detection Response (OEDR) subtask in order to complete the DDT, by providing the appropriate responses to all relevant objects and events, in cases when the driving automation does not provide the appropriate response to avoid hazards.	OEM describes the proper use of the feature which includes the driver's role in the object and event detection and response	Reference to Owner's Manual
Safety Principle 2.2 The driving automation system shall be integrated with the vehicle in a manner that does not inhibit the driver's ability to perform the DDT, which includes: i. Control of the vehicle, lateral and longitudinal	OEM to verify driver can have means of controlling longitudinal and lateral motion of the vehicle when feature is engaged	Reference to Owner's Manual
ii. OEDR	OEM to verify driver's role in the object and event detection and response while feature is engaged	Reference to Owner's Manual
Safety Principle 2.3 i. The driving automation system shall prioritize predefined driver inputs for full control over driving automation commands.	OEM describes mechanism(s) for driver defined inputs	OEM proposed Safety Principle assessment procedure

Table 7: Driving Automation System Level 3

Safety Principle Criteria	Nature of Testing	Fulfilment
Safety Principle 3.1 i. The driver shall ensure operational readiness before engaging driving automation feature	OEM describes requirements for vehicle operational readiness	Reference to Owner's Manual
Safety Principle 3.2 The driving automation system shall be integrated with the vehicle in a manner that does not inhibit the driver's ability to perform the DDT, which includes: i. Control of the vehicle, lateral and longitudinal	OEM to verify driver can have means of controlling longitudinal and lateral motion of the vehicle when feature is engaged	Reference to Owner's Manual

Safety Principle Criteria	Nature of Testing	Fulfilment
ii. OEDR	OEM to verify driver's role in the object and event detection and response while feature is engaged	Reference to Owner's Manual
Safety Principle 3.3 i. The driving automation system shall prioritize predefined driver inputs for full control over driving automation commands.	OEM describes mechanism(s) for driver defined inputs	OEM proposed Safety Principle assessment procedure
Safety Principle 3.4 i. The driving automation system must not engage unless activated by the driver. After initially being activated, the automation can automatically resume if appropriate and within the same drive cycle. As a default, automation is not activated at the beginning of each drive cycle.	OEM describes mechanism(s) for feature engagement criteria and feature engagement process	OEM proposed Safety Principle assessment procedure
Safety Principle 3.5 i. The driving automation system shall provide persistent indication to the driver that signifies when a vehicle is operating in high automation state, i.e., at Level 3 or higher.	OEM describes HMI indication for high automation state modes	OEM proposed Safety Principle assessment procedure
Safety Principle 3.6 i. The driving automation system shall provide indication to the driver upon any request to transition from Level 3 to a lower level (2, 1, or 0).	OEM describes HMI indication(s) for any high automation level mode transition to a lower automation level (2, 1, or 0) mode.	OEM proposed Safety Principle assessment procedure
Safety Principle 3.7 When activated, the driving automation system shall perform the DDT within its application-specific operational design domain, **including providing the appropriate responses to relev**ant objects and events. This includes but is not limited to: i. Continuous assessment of operation within actual vs. operational design domain	OEM describes driving automation system operational design domain, assessment of the design domain, and DDT execution.	OEM internal confidential test results
ii. Inhibit operation when operational design domain is not achieved	OEM describes driving automation system operational design domain, assessment of the design domain, and operational inhibit mechanism(s).	OEM internal confidential test results
Safety Principle 3.8 i. The driving automation system shall be designed in such a way that a failure in the driving automation system does not lead to an immediate loss of the longitudinal and/or lateral control in order to allow the driver to respond as prescribed by SP 3.10 (iii).	OEM to define mechanism(s) for driver to respond and resume the DDT in the event of driving automation system failures.	OEM internal confidential test results
ii. When the driving automation system is engaged it shall operate in such a way that, if a vehicle failure occurs that impacts longitudinal and/or lateral vehicle dynamics, systems shall continue to stabilize the vehicle's path within the given physical and technical limits in order to allow the driver to react as prescribed by SP 3.10 (i).	OEM to define mechanism(s) for driver to respond and resume the DDT in the event of vehicle failures.	OEM internal confidential test results
Safety Principle 3.9 Before exiting the operational design domain, upon occurrence of a driving automation system failure that prevents performance of the DDT, the driving automation system shall request the driver to take control i. Verified driver control inputs shall cause transition from Level 3 into a lower level of automation.	OEM to define driving automation system HMI driver take over request method. OEM to define mechanism(s) for driver defined inputs for driving automation system transition to a lower level of automation.	OEM internal confidential test results

Safety Principle Criteria	Nature of Testing	Fulfilment
ii. The driving automation system shall maintain an operating condition that affords a controlled transition to driver control, regardless of whether the transition is prompted by fault within the driving automation system, or prompted by violation of the intended operational design domain.	OEM to define controlled transition operating condition	OEM internal confidential test results
Safety Principle 3.10 The driver must understand the following: i. The driver's role is to determine if there has been a vehicle failure that may impact the safe operation of the vehicle, and to take over control of the vehicle when such a failure occurs.	OEM to define vehicle type failures and driver's role during abnormal operation	Reference to Owner's Manual
ii. In response to a driver request to take over performance of the DDT, the primary response from the driving automation system is to transition out of Level 3 automation and into a lower driving automation level.	OEM to define mechanism(s) for driver defined inputs for driving automation system transition to a lower level of automation.	Reference to Owner's Manual
iii. When the driving automation system is requesting the driver to take control of the vehicle, the driver's role is to respond by taking over control.	OEM to define driver's role during abnormal operation and driver's defined input mechanisms for full control	Reference to Owner's Manual
iv. After requesting the driver to take control, the driving automation system will remain in control for a limited time period.	OEM to define driving automation system transition performance limitations	Reference to Owner's Manual

Table 8: Driving Automation System Level 4

Safety Principle Criteria	Nature of Testing	Fulfilment
Safety Principle 4.1 i. The vehicle operator shall ensure vehicle operational readiness before engaging the driving automation system.	OEM describes requirements for vehicle operational readiness	Reference to Owner's Manual
Safety Principle 4.2 When activated, the driving automation system shall perform the DDT and fallback as needed within its application-specific operational design domain, providing the appropriate responses to relevant objects and events. This includes but is not limited to: i. Continuous assessment of operation within actual vs. operational design domain	OEM describes driving automation system operational design domain, assessment of the design domain, and DDT execution.	OEM internal confidential test results
ii. Prohibiting entry into automated driving when the operational domain is not achieved	OEM describes driving automation system operational design domain, assessment of the design domain, and operational inhibit mechanism(s).	OEM internal confidential test results
iii. Ability to achieve minimal risk condition if necessary due to any one of the following: a. Operator failure to respond appropriately to pending exit of operational design domain b. A failure that prevents performance of the complete DDT	OEM describes minimal risk conditions and mechanism(s) for achieving it.	OEM internal confidential test results
Safety Principle 4.3 i. The driving automation system may delay its response to operator take-over requests, and/or operator requests to stop driving automation when necessary to avoid causing a hazard.	OEM describes capabilities and limitations of driver take over requests.	Reference to Owner's Manual
Safety Principle 4.4 i. The driving automation system must not engage unless activated by the operator.	OEM describes robustness of engagement mechanism.	OEM internal confidential test results

Table 9: Driving Automation System Level 5

Safety Principle Criteria	Nature of Testing	Fulfilment
Safety Principle 5.1 i. The vehicle operator shall ensure vehicle operational readiness before engaging driving automation.	OEM describes requirements for vehicle operational readiness	Reference to Owner's Manual
Safety Principle 5.2 The vehicle system overall (including the driving automation system and its integration) shall be designed such that the driving automation system is capable of performing the DDT and fallback as needed, including: i. Providing appropriate responses to relevant objects and events	OEM describes driving automation system DDT execution.	OEM internal confidential test results
ii. Ability to achieve a minimal risk condition if necessary due to a failure that prevents performance of the complete DDT	OEM describes minimal risk conditions and mechanism(s) for achieving it.	OEM internal confidential test results
Safety Principle 5.3 i. The driving automation system may delay response to operator requests to take over, and/or operator requests to stop driving automation when necessary to avoid causing a hazard.	OEM describes capabilities and limitations of driver take over requests.	Reference to Owner's Manual
Safety Principle 5.4 i. The driving automation system must not engage unless activated by the operator.	OEM describes robustness of engagement mechanism.	OEM internal confidential test results

5.3 Preliminary Test Concepts for Selected Automation Features

5.3.1 Level 2 Parking Assist Feature

Parking assist systems have been introduced in the market for several years with increasing system capability. Previous systems generally automated only the lateral portion of the parking maneuver while the driver, following prompts from the vehicle, continued to control fore-aft motion and perform a portion of or the complete OEDR. However, the latest systems have begun to completely automate both lateral and longitudinal control and would be defined as Level 2 driving automation systems where the driver is still required to complete the OEDR subtask of the DDT while the system is engaged. The ODD, OEDR capability and completion of specific maneuvers may be unique for each feature, yet each must address all associated SPs.

For example, System A may perform parallel parking with an available parking space defined by one vehicle each forward and rearward of the open parking space and will not initiate or complete the parking sequence of maneuvers unless the two vehicles are present. System B may only maneuver into perpendicular spaces using camera sensors to identify parking boundaries defined by parking lot pavement markings and will not initiate or complete the parking sequence of maneuvers unless the markings can be identified. Both systems are clearly automated parking aids, but due to their different maneuver capabilities, ODD requirements and sensors, developing a common set of test procedures beyond the SPs that both systems must be able to achieve is not possible. Appendices D through G present hypothetical Classification and Operational

Descriptions and recommended SP assessment procedures for the two fictitious Parking Assist manufacturers.

5.3.2 Level 2 Traffic Jam Assist Feature

5.3.2.1 Feature Overview

In this section, a feature consisting of the same marketing name and driving automation system classification type from two different vehicle manufacturers will be evaluated. The two hypothetical companies market a feature called Traffic Jam Assist (TJA) which provides longitudinal and lateral control at low speeds to alleviate mundane driving tasks from the driver. This feature is often constructed from another well-known feature, ACC, as the base feature, but with the addition of sustained lateral control. It enables both continuous longitudinal and lateral support for the driver when operating within its defined domain. At least one aspect of the ODD may be apparent from the feature name, TJA which would assume it is for high density stop and go traffic on highway type roadways. If equipped, the lateral control performance is limited to specific driving domains and environmental conditions. Additionally, it will always require driver supervision while engaged. An engaged Level 2 driving automation system may not react to all objects and events and it is the role of the driver to supervise system performance and take control whenever necessary.

Appendices H through K present hypothetical Classification and Operational Descriptions and recommended SP assessment procedures for the two fictitious TJA system manufacturers.

5.3.2.2 Test Specification Domain Challenges

Manufacturers must provide instructional guidelines on how to operate their driving automation features which may cover user interface instructions and environmental and operating condition requirements. Each manufacturer may elect to be as descriptive as necessary when explaining the ODD so that a user may experience the nominal performance and benefit of the feature’s intended use. However, manufacturers are not required to include a level of detail that would potentially divulge proprietary information. A set of unique operating instructions and domain-specific requirements are necessary to operate and evaluate the driving automation system feature yet, if these are not known to the user/evaluator, the feature may not be executed and evaluated as expected.

In the low-speed driving automation feature, TJA, separate manufacturers released requirements on user interaction and ODDs that differ. In addition to these different domain requirements, each company had determined a different driving automation system classification level.

The company GloCo followed the automation level classification questionnaire and provided a Level 2 result. The accompanying Classification and Operational Descriptions, specified that the feature is domain-limited to highway roads only and requires a Global Positioning System (GPS) and cellular access for validity. The feature also requires asphalt road type with two lanes in the same direction, solid white dashed visible lane markings and shoulder designated areas on both sides. GloCo’s TJA feature does require a lead vehicle but mentions only that it must be at a steady 25 mph to engage.

For Acme's TJA feature, classified as a Level 1, the ODD is less restrictive. The only common domain factors are the solid white dashed lane markings and a lead vehicle at a steady 25 mph speed. Acme's feature is not limited to an asphalt road type and does not require GPS or cellular access. It does not specify two lanes in the same direction with shoulder areas available on both sides. However, it does have a specific operational condition for a lead vehicle positioned for a minimum of five seconds before the feature can be engaged. This clearly is important to know beforehand when attempting to engage the feature and is likely a lead cause to the differing driving automation levels for these two different systems.

Subsequently, there are now two vehicle manufacturers releasing a driving automation system feature with the same name but requiring specific and different ODDs as well as different roles from respective vehicle operators. The test environment is not generic enough to create and repeat for each company to demonstrate their driving automation system level classification and adherence to the SPs. The verification effort requires a custom-made test location per vehicle manufacturer.

5.3.3 Level 2 High Speed Automated Cruise Feature

5.3.3.1 Feature Overview

A driving automation system feature expected to be available relatively soon to the public can be labeled as High Speed Automated Cruise (HSAC). HSAC can be considered a combination of two technologies as a single feature: ACC and Lane Centering Control (LCC).

Currently available on the market, ACC allows a vehicle equipped with the technology to sustain longitudinal control (accelerate and decelerate), within the technology's limits, to maintain headway to a preceding vehicle on a roadway. Longitudinal control is performed without driver utilization of the accelerator pedal. ACC employs a sensor system (e.g., radar, camera, laser) to detect the travel of a preceding vehicle.

Predicted to be available on the market imminently, LCC allows a vehicle equipped with the technology to sustain lateral control (position in a lane), within the technology's limits, in response to recognition of lane boundary markings. LCC employs a sensor system (e.g., camera) to detect lane boundary markings.

HSAC is intended to provide a driver with the means to travel on highways at typical speeds without the need for continual, direct driver control of the accelerator pedal and steering wheel. However, an important point is that driver supervision of the vehicle operation is required while a Level 2 HSAC feature is engaged.

5.3.3.2 Test Specification Domain Challenges

Appendices L through O present hypothetical Classification and Operational Descriptions and recommended SP assessment procedures of two fictitious HSAC system manufacturers. Comparing information from the two manufacturers is another demonstration of how two separate systems performing apparently similar functions have quite different ODDs. These different ODDs again emphasize how a single SP assessment procedure is unable to accommodate multiple system designs.

In completing the Automation Level Classification questionnaire, both fictitious companies arrived at a Level 2 result. However in comparing ODDs of the two systems, we observe noticeable differences.

GloCo's system functions in the range of speeds between 65 and 85 mph. Acme's system functions in the range of speeds between 45 and 60 mph. Although both systems could be used on freeways, use of Acme's system would be constrained to travel at lower speeds than posted when the speed limit is greater than 60 mph. The GloCo system is more likely to travel at freeway speed limits as its range essentially captures all typical United States freeway speed limits. An important point is that there is no overlap in the speeds at which the two systems operate. At a minimum, SP assessment procedures for the two systems would need to be performed at two different speeds.

In considering the surrounding traffic environment, once more there are differences in how the two systems operate. GloCo's system can operate when it detects vehicles in the same lane in which it is traveling. However, it does not operate when it detects vehicles in lanes adjacent to the lane in which it is traveling. For Acme's system, the condition is directly opposite to GloCo's. Acme's system can operate when it detects vehicles in lanes adjacent to the lane in which it is traveling. However, it does not operate when it detects a vehicle in the same lane in which it is traveling.

These simple examples reflect potential different approaches employed in designing HSAC systems. The approaches result in mutually exclusive ODDs between the two systems. Even though the two systems perform a similar function, the mutually exclusive ODDs preclude development of a single assessment procedure to confirm adherence to associated SPs. This situation leads to the necessity of recommended manufacturer SP assessment procedures explained earlier in this report.

5.4 Challenges in Testing Driving Automation Systems

Key challenges in developing tests for driving automation systems stem from their nature as convenience features. While very advanced, future versions of these features may have implied or associated safety benefits, the driving automation systems of the near and mid-term future are designed to increase the comfort of drivers by gradually taking over their duties. As a result, developers choose under which conditions (i.e., in which domains) the features may be available based on technology capability, feasibility, or potential marketing value. Feature domains also may vary not just between features from a manufacturer and between manufacturers, but also across regions and over time.

However as discussed in Section 5.3, the appropriate customer feature usage would need to be clearly communicated and the associated HMI would need to provide the support for the unique application. As described in Section 5.3, some automated parking features may be for parallel parking, some for perpendicular. Some traffic jam features may only operate on highways, others only on secondary roads. Some of these features may require surrounding traffic, others may require none. These differences can further be accompanied by differences in compatible weather conditions, speeds, and other road conditions.

With domain differences come differences in use cases and therefore test conditions. Thus a customized test condition may be necessary for every feature. As the technology capability evolves the domain differences will also continue to evolve. As developers progress the innovation in this area with regards to functionality and HMI, there will be differences in how features are operated. Again, the SP assessment procedure will need to be customized to each feature's concept of operation.

The technologies for driving automation systems are also evolving, leading to differences and challenges in setting up necessary test conditions. For example, some technologies may require certain GPS or map information. Others may attempt to visually recognize certain road or other traffic features. With the sophisticated nature of these systems, some features may only become available in the presence of a complex mixture of conditions. It may impose significant logistical challenges to arrange the test conditions for a feature to become available.

5.5 Open Issues Related to Testing

A number of open issues still exist concerning the testing of driving automation systems. While driving automation systems may indirectly provide safety benefits which may be demonstrated in the future, as noted in Section 5.4, driving automation systems for the near- and mid-term future are principally designed to improve comfort and convenience without introducing new safety dis-benefits. The vast majority of near- and mid-term future driving automation systems may not avoid all hazards during complex situations; however, these systems will work to transition driving roles from the system back to the driver once complex driving situations are detected. To ensure these near-term systems appropriately allow for the driver to reengage their role in the DDT, testing of driving automation systems should focus on the top-level SPs described in Section 4. Such tests would demonstrate that the appropriate SPs have been addressed within the system design. Therefore, it is not sufficient or appropriate to downgrade the level classification of the system just because the system does not meet the recommended SPs for a given level. Likewise, if a system outperforms the SPs of a given level, an outside entity cannot conclude that the system level classification should be upgraded. As explained in Section 2.6.2.3, it is the role of the developer to determine the intended level of the system and the role of testing is to demonstrate the SPs have been addressed.

5.5.1 Testing Issues with Level 2 Systems and Above

There are an abundance of challenges facing the testing of driving automation systems in Level 2 alone. The number and complexity of issues gradually increase in higher driving automation system levels. Principally, testing systems within the intended domain of a system will prove to be a great challenge and a key differentiator between low and high automation.

Given the great range of unique offerings that each manufacturer will choose to offer for driving automation systems and the continual technology evolution, highly standardized testing cannot be achieved. Advanced automation systems will likely be constrained to a given domain, including geographical parameters that may require highly detailed mapping data. As such, it may not be possible to conduct physical testing of a driving automation system in a geographical location outside of the intended driving domain as prescribed by the system designer or vehicle manufacturer.

5.5.2 Other Features Not Considered

As SPs were only derived for systems that cede full motion control to the driver, i.e., Level 2 systems and above, intervening systems (e.g., electronic stability control) are also not included in the range of systems to be tested. While emergency intervention systems may provide control in the case of a crash-imminent situation, such systems do not provide sustained control of the vehicle ceded by the driver and thereby do not change the driver's role in driving. Therefore, such systems were not included in the taxonomy of systems to be tested in this report.

If detailed performance requirements are to be considered for varying levels of driving automation systems, several key issues will need to be addressed and defined. Presently, fault tolerance times (i.e., the required time to detect a fault in the system) appropriate environmental perception performance levels for systems, and the required takeover time by the driver of the vehicle are not yet researched or well understood across the industry. Without first understanding and defining key human factors thresholds, detailed performance requirements will not be able to be derived and applied to test procedures.

5.6 Summary - Development of Use Cases and Preliminary Objective Test Methods

Testing of driving automation systems is a complex and widely diverse subject. While traditional safety testing and certification has been refined to be in the form of standardized requirements and test procedures, the field of driver automation is still evolving and therefore it is unclear if the traditional standards regimen will be easily molded to cover this new area. At its root, this is because driver automation systems are comfort and convenience systems designed to enhance the customer experience rather than address a particular crash modality. Technical solutions aimed at addressing the mobility needs of various customer demographics are inherently more diverse than crash modes which transcend vehicle types and customer demographics.

The rapid changes in technology as well as the diverse demands for mobility have created an evolving engineering field that is highly competitive. Many of the ideas considered in features discussed earlier in Section 3 are being worked on internally and discussed in marketing conversations in the media, but they are not real products in the field. Their timing and capabilities are not publicly known. As such, it is impossible to speculate on proactive standardized tests to address these future systems. The AVR Project team has responded by choosing to define SPs agnostic of individual feature capabilities. This strategy presents a unique challenge to formulating requirements with test procedures.

To handle this concern, the AVR Project team proposed a Classification and Operational Description for collecting data regarding specific design features from developers. Further, the team proposed having the developer identify the level of automation, the accompanying SPs, and recommended SP assessment procedures for the individual product. This is considered the best possible approach to handling testing of current systems but more importantly future automation systems that have yet to be announced or released. This report includes the recommendation for a Classification and Operational Description form and content as well as sample descriptions and SP assessment procedures for automated parking, TJA and HSAC features from two hypothetical vehicle manufacturers. These examples illustrate the diversity in feature definitions, customer interactions, and the manufacturers' presentation of the feature to customers. While not providing the traditional fixed requirement and test procedures common to passive or active safety, it is believed this approach provides several key benefits:

- Self-reporting of the system level and intent by the developer
- A framework to establish minimum owner's manual content for customer communication
- A framework to adapt to the rapidly changing technical and competitive environment around driving automation systems
- A framework for NHTSA to learn and see trends relevant to their mission about the true nature of the capabilities of different offerings

By focusing on Level 2 systems only, this report highlights the systems of most near-term interest to NHTSA as communicated to the AVR Project team, but it also leaves technical details unresolved in the testing of higher level automated driving systems. Fundamentally, Level 2 and lower systems are still driven by a driver who is responsible for the DDT. As such, the SPs and the testing revolve around the ability of the driver to take control of the driving automation system at all times for any reason. Higher level automation (Levels 3, 4, and 5) is distinguished by the system itself formally handling the DDT. The SPs and testing of these automated driving systems are therefore very different and focused on performance of the system within the ODD. The investigation into the performance requirements of higher levels of automation is not presented in this report and could be the subject of future research.

6 Project Summary

In order to support safety in the development and deployment of driving automation systems, it is important to consider and communicate the way in which the fundamental roles of the driver will change. In this report, the AVR consortium sought to add clarity in this rapidly growing technology space with the confirmation of the SAE J3016 driving automation levels and the further embellishment of them to clarify the role of the driver and the role of the driving automation system in performing the dynamic driving task at all levels of driving automation.

A key contribution of the report is the clarification of the scope of driving automation levels. All functionality that can be engaged by a driver in a vehicle simultaneously should be considered. Functions that only intervene for specific events (e.g., a potential loss of stability, lane departure, or collision) and do not provide sustained vehicle motion control between and across events, do not change the role of the driver and as such are not driving automation.

Perhaps the largest contribution this report makes to the technology area is the introduction of safety principles based on a comprehensive safety analysis of driving automation Levels 2 through 5. The safety principles developed apply to driving automation systems and features that reside under a given level.

The safety principles developed for Level 2 driving automation systems provide the minimum set of safety principles that should be considered, with the intent that Level 2 driving automation systems serve to complement, but not substitute for, the human driver in performing the dynamic driving task (DDT). Overall safety for Level 2 systems will always be a result of the driver understanding and performing their role in relation to that of the driving automation system.

Level 3 driving automation systems introduce the capability for the automation to perform the complete DDT within its operational design domain. This capability fundamentally alters the traditional role of the driver and therefore places additional safety principles on the driver and the driving automation system. The safety principles developed for Level 3 driving automation place the responsibility on the driving automation system to alert the driver when he/she must resume part / all of the DDT. Several of the Level 3 principles raise human factors considerations, such as the driver’s need to understand their role of “fallback” and their performance transitioning into and out of that role. While these human factors considerations were out-of-scope for this project, the members of the AVR consortium believe these considerations should be addressed in future research.

Level 4 and 5 driving automation systems have safety principles that facilitate a safe exchange between the driving automation system and the operator when the operator requests to take over parts or all of the DDT. Operator requests to take over part or all of the DDT may not be immediately granted as the system may be operating in domains where human control is not allowed or could cause an undesired hazard/control action. Due to the DDT performance requirements for Level 4 and Level 5 driving automation systems, there may be significant dependencies on the maintenance of the vehicle, including a need to utilize OEM parts and procedures for maintenance, repair, and customer alterations.

This project also provided a framework for developing objective tests that allow the safety principles to be evaluated on driving automation systems/features, based on the level in which they reside. The consortium offered for consideration an exemplar assessment sheet that can be used to capture a driving automation systems’ adherence to a particular safety principle. It is the hope of the consortium that this work will be used as a reference for any continued work to develop objective tests for driving automation systems as this technology space matures.

7 References

Billings, C. E., Lauber, J. K., Funkhouser, H., Lyman, G., and Huff, E. M. (1976). *NASA Aviation Safety Reporting System* (Tech. Rep. TM-X-3445). Moffett Field, CA: NASA Ames Research Center.

BMW AG. (2013). Traffic Jam Assistant. Retrieved March 24, 2014 from http://www.bmw.com/com/en/newvehicles/x/x5/2013/showroom/driver_assistance/traffic_jam_assistant.html#t=l

Fitzsimmons, M. (2013). Google may be crafting its own self-driving cars, tinkering with robo-taxis. In techradar. Retrieved on March 24, 2014 from http://www.techradar.com/news/car-tech/google-may-be-designing-its-own-self-driving-cars-tinkering-with-robo-taxis-1175511

General Motors Corporation. (2005). *Automotive Collision Avoidance System Field Operational Test (ACAS FOT) Final Program Report* (Report No. DOT HS 809 886). Washington, DC: National Highway Traffic Safety Administration.

General Motors. (2013). 'Super Cruise' Takes on Real-World Traffic Scenarios, Cadillac's semi-automated vehicle technology undergoes further testing. Retrieved March 24, 2014 from http://media.gm.com/media/us/en/gm/news.detail.html/content/Pages/news/us/en/2013/Apr/0429-cadillac-super-cruise.html

Llaneras, R. E., Salinger, J. and Green, C. A., (2013). Human Factors Issues Associated with Limited Ability Autonomous Driving Systems: Drivers' Allocation of Visual Attention to the Forward Roadway. In *Proceedings of the 7th International Driving Symposium on Human Factors in Driver Assessment, Training, and Vehicle Design.* Paper presented at Driving Assessment 2013, Bolton Landing, New York (pp. 92-98). Iowa City, IA: University of Iowa Public Policy Center.

Mearian, L. (2013). Audi tech automatically finds vacant parking spot, sans driver. In *Computerworld.* Retrieved March 24, 2014 from http://www.computerworld.com/s/article/9242138/Audi_tech_automatically_finds_a_vacant_parking_spot_sans_driver_

Michon, J. A., (1985). A Critical Review of Driver Behavior Models: What Do We Know, What Should We Do? In L. Evans and R. C. Schwing (Eds.), *Human Behavior and Traffic Safety* (pp. 485-520). New York, NY: Plenum Press.

National Highway Traffic Safety Administration, (2013). "*Preliminary Statement of Policy Concerning Automated Vehicles*." Washington, DC: Author. Retrieved March 18, 2014 from http://www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf.

Nowakowski, C., Shladover, S., Cody, D., Fanping, B., O'Connell, J., Spring, J., Dickey, S., and Nelson, D. (2010). *Cooperative Adaptive Cruise Control: Testing Drivers' Choices of Following Distances* (California PATH Research Report No. UCB-ITS-PRR-2010-39. Berkeley, CA: University of California, California PATH Program. Retrieved

March 24, 2014 from http://www.path.berkeley.edu/PATH/Publications/PDF/PRR/2010/PRR-2010-39.pdf

Parasuraman, R.; Riley, V. (1997). "Humans and Automation: Use, Misuse, Disuse, Abuse." Human Factors 39: 230–253.

SAE International On-Road Automated Vehicle Standards Committee, (2014). SAE Information Report: (J3016) *"Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving System."* Warrendale, PA: SAE International.

Salinger, J., Green, C., Reid, B., Widmann, G. R., Prieto, R., Llaneras, E., Chen, Y., Koskie, S., Rajput, V. S., Tian, R., Bolourchi, F., and Prabhuswamy, S. (In Publication). *"Human Factors for Limited Ability Autonomous Driving Systems (HF4LAADS), FHWA Cooperative Agreement # DTFH61-08-R-00006, Deliverable 8 – Final Report* ." Washington, DC: Federal Highway Administration.

Toyota Motor Corporation. (2014). Technology that Supports Parking. Retrieved March 24, 2014 from http://www.toyota-global.com/innovation/safety_technology/safety_technology/parking/

Weiss, C. C. (2013). Toyota details its Automated Highway Driving Assist system. Gizmag. Retrieved on March 24, 2014 from http://www.gizmag.com/toyota-automated-highway-driving/29378/

Appendix A: Matrices of Undesired Control Actions

A.1 UCA Matrix for Level 2 Driving Automation

Undesired Control Actions (UCAs)	Safety Constraints	Potential Safety Principles (SPs)	Notes on Causal Factors and Situations
Vehicle not controllable when control needed during automation, due to vehicle not safely equipped or maintained	Operator must assure maintenance / operational readiness	Operator must assure operational readiness of the vehicle.	Mis-equipped vehicle e.g., with slicks in snow, poorly maintained brakes, mis-inflated tires, etc.
Driving automation system incorrectly controls DDT (or controls it too early / too late, or fails to control it)	Driving automation system incorrectly controlling the DDT shall not lead to a hazard --> driver must take control to prevent hazards	For Level 2 automation, avoidance of hazards is dependent on the driver performing the OEDR subtask and completing the DDT. (Note: The driver's capability is controlled and enforced by existing structures such as driver licensing, traffic laws and norms, etc.) Driving automation system shall enable driver to take full control of the vehicle at any time.	Machine controller is incorrect and tries to incorrectly control the vehicle. Causal factors may include incorrect algorithm, sensor failure or sensor not capable of detecting surroundings, etc. These causal factors are anticipated in Level 2. Level 2 controller (red) is a secondary element for all hazard avoidance
Driver provides incorrect control when control not needed, when human OEDR is not engaged due to lack of attention or understanding	Human OEDR shall be engaged	For Level 2 automation, avoidance of hazards is dependent on the driver performing the OEDR subtask and completing the DDT.	Human factors issues such as inattention, distraction, etc. Example: driver not paying attention steps on accelerator and collides with leading vehicle during lane centering + adaptive cruise operation
Driver provides incorrect control when control not needed, when human OEDR is not engaged due to inability to perceive environment	Human OEDR shall be engaged; and driver shall be able to perceive environment.	For Level 2 automation, avoidance of hazards is dependent on the driver performing the OEDR subtask and completing the DDT. The driver's capability is controlled and enforced by existing structures such as driver licensing, traffic laws and norms, etc. Vehicle design must allow driver to perceive environment.	Example: driver’s view of leading vehicle is obstructed; driver applies accelerator and collides with leading vehicle during lane centering + adaptive cruise operation

Undesired Control Actions	Safety Constraints	Potential Safety Principles (SPs)	Notes on Causal Factors and
Driver provides incorrect control when control not needed, when human OEDR is slow	Human OEDR shall be engaged and timely	For Level 2 automation, avoidance of hazards is dependent on the driver performing the OEDR subtask and completing the DDT. The driver's capability is controlled and enforced by existing structures such as driver licensing, traffic laws and norms, etc.	Example: driver is distracted by situation in the car; driver applies accelerator and collides with leading vehicle during lane centering + adaptive cruise operation Example: driver does not understand that his/her input is required at Level 2 Example: driver understands that input is required at Level 2 but does not realize the vehicle is in Level 2 (think it is in Level 3 or other)
Driver does not provide correct control, or provides control incorrectly, late or early, when control is needed to avoid a hazard, when automation is inactive	Driver shall correctly control the vehicle when control is needed to avoid a hazard and automation is inactive	For Level 2 automation, avoidance of hazards is dependent on the driver performing the OEDR subtask and completing the DDT.	Example: driver chooses not to brake when adaptive cruise control reaches maximum braking capability, yet more brake is required to avoid object ahead
Driver does not provide correct control, or provides control incorrectly, late or early, when control is needed to avoid a hazard, when automation is operational and human seeks means to take control	Driver shall correctly control the vehicle when control is needed to avoid a hazard when automation is operational	The vehicle shall be designed such that the driver is capable of performing the lateral and longitudinal control of the vehicle	Example: high-level automation (Level 4 or Level 5) with no steering wheel transitions to Level 2

Undesired Control Actions	Safety Constraints	Potential Safety Principles (SPs)	Notes on Causal Factors and
Driver does not provide correct control, or provides control incorrectly, late or early, when control is needed to avoid a hazard, when exiting automation due to human taking control and human OEDR is engaged	Driver shall correctly control the vehicle when control is needed to avoid a hazard and human OEDR is engaged	Avoidance of hazards is dependent on the driver performing the OEDR. Driving automation system shall enable driver to take full control of the vehicle at any time. Arbitration in total, combining command and final arbitration, must prioritize defined human input(s).	Mis-use: driver chooses not to brake when adaptive cruise control reaches maximum braking capability, yet more brake is required to avoid object ahead Causal factor may be inability of driver to overcome / counteract the incorrect actions of automation "Fighting the automation" situation if automation is too strong or will not yield
Driver provides incorrect control when control not needed, when human OEDR is engaged	Driver shall correctly control the vehicle *with zero inputs when control not needed*, when human OEDR is engaged	For Level 2 automation, avoidance of hazards is dependent on the driver performing the OEDR subtask and completing the DDT.	Driver does not understand (or forgets) that automation is enabled Driver does not understand the power of his/her input; careless input by driver
Driver does not provide correct control, or provides control incorrectly, late or early, when control is needed to avoid a hazard, when human OEDR is not engaged	Human OEDR shall be engaged	For Level 2 automation, avoidance of hazards is dependent on the driver performing the OEDR subtask and completing the DDT.	Driver does not pay attention and fails to brake when adaptive cruise control reaches maximum braking capability, yet more brake is required to avoid object ahead
Driver does not provide correct control, or provides control incorrectly, or late, when control is needed to avoid a hazard, when human OEDR engagement is slow	Human OEDR shall be engaged and timely	For Level 2 automation, avoidance of hazards is dependent on the driver performing the OEDR subtask and completing the DDT.	Driver determination of surroundings is slow and brakes too late when adaptive cruise control reaches maximum braking capability, yet more brake is required to avoid object ahead
Driver turns on automation incorrectly when control is not needed to avoid a hazard, and human OEDR is not engaged	Human OEDR shall be engaged	For Level 2 automation, avoidance of hazards is dependent on the driver performing the OEDR subtask and completing the DDT.	Driver turns on Level 2 automation when not paying attention

Undesired Control Actions	Safety Constraints	Potential Safety Principles (SPs)	Notes on Causal Factors and
Driver turns on automation incorrectly when control is not needed to avoid a hazard, and human OEDR engagement is slow	Human OEDR shall be engaged and timely	For Level 2 automation, avoidance of hazards is dependent on the driver performing the OEDR subtask and completing the DDT.	Driver turns on Level 2 automation when not paying attention
Driver turns on automation when control is needed to avoid a hazard and human OEDR is not available	Human OEDR shall be engaged	For Level 2 automation, avoidance of hazards is dependent on the driver performing the OEDR subtask and completing the DDT.	Mis-use: Driver on freeway has difficulty staying awake, so engages lane centering in order to take a nap
Driver turns on automation when control is needed to avoid a hazard and human OEDR engagement is slow	Human OEDR shall be engaged and timely	For Level 2 automation, avoidance of hazards is dependent on the driver performing the OEDR subtask and completing the DDT	Mis-use: Driver on freeway engages lane centering in order to eat a meal
Driver accidentally turns off automation incorrectly or too early, when control is needed to avoid a hazard and human OEDR is not engaged	Human OEDR shall be engaged Allow for driver takeover request to be specified for a given vehicle	For Level 2 automation, avoidance of hazards is dependent on the driver performing the OEDR subtask and completing the DDT. Allow for driver takeover request to be specified for a given vehicle.	Example: Driver turns off lane centering + adaptive cruise control without re-assuming control. Note: Human should be engaged in OEDR at all times in Level 2 operation
Driver turns off automation incorrectly or too early, when control is needed to avoid a hazard and human OEDR engagement is slow	Human OEDR shall be engaged and timely	For Level 2 automation, avoidance of hazards is dependent on the driver performing the OEDR subtask and completing the DDT. The driver's capability is controlled and enforced by existing structures such as driver licensing, traffic laws and norms, etc.	Example: Driver turns off lane centering + adaptive cruise control without properly re-engaging in OEDR. Note: Human should be engaged in OEDR at all times in Level 2 operation

A.2 UCA Matrix for Level 3 Driving Automation

Undesired Control Actions (UCAs)	Safety Constraint	Potential Safety Principle (SPs)	Notes on Causal Factors and Situations
Driving automation system does not provide (or stops providing too quickly, or provides too late) steering input, when steering input is required to avoid a hazard, and automated steering is in domain but **exiting due to domain limit,** and human OEDR is slow.	Driving automation system must provide steering input when exiting automation due to domain limit Before exiting domain due to environment change, automation control must transition steering control to driver	Before reaching the domain limit, the driving automation system shall transition control to driver to avoid operation outside of the intended domain limit. Transition time should be sufficient to allow driver to take over.	Example: Long curved section of road requiring steer input; but vehicle exceeds speed domain and so exits steering automation
Driving automation system does not provide (or stops providing too quickly, or provides too late) steering input, when steering input is required to avoid a hazard, and automated steering is in domain but **exiting due to driving automation system failure,** and human OEDR is slow	Before exiting domain due to driving automation system failure, automation control must transition steering control to driver	Before reaching the domain limit, the driving automation system shall transition control to driver to avoid operation outside of the intended domain limit. Transition time should be sufficient to allow driver to take over. Single-point failure and/or common mode failure must be avoided for any higher-level automation system (so that transition can be performed even in case of faults in the driving automation system.)	Example: Long curved section of road requiring steer input; but automation loses lane marking or roadway detection
Driving automation system does not provide (or stops providing too quickly, or provides too late) steering input, when steering input is required to avoid a hazard, and automated steering is in domain but **exiting due to vehicle failure,** and human OEDR is slow.	When exiting domain due to vehicle failure, automation control must allow driver to take over steering control.	"Driving automation system shall enable driver to take full control of the vehicle at any time." Driver must understand capabilities of automation: must understand the necessity of human to take over in case of vehicle failure.	Example: Long curved section of road requiring steer input; vehicle tire goes flat
Driving automation system does not provide (or provides insufficient amount, provides to early, stops providing too quickly, or provides too late) braking input, when braking input is required to avoid a hazard, and automated braking is in domain but **exiting due to change in environment**, and human OEDR is slow	When exiting domain due to environment change, automation control must transition braking control to driver	Before reaching the domain limit, the driving automation system shall transition control to driver to avoid operation outside of the intended domain limit.	Example: Level 3 ACC plus automated steering, rain causes slick roadway that is outside the domain of Level 3 automation

Undesired Control Actions (UCAs)	Safety Constraint	Potential Safety Principle (SPs)	Notes on Causal Factors
Driving automation system does not provide (or provides insufficient amount, provides to early, stops providing too quickly, or provides too late) braking input, when braking input is required to avoid a hazard, and automated braking is in domain but **exiting due to automation controller failure**, and human OEDR is slow	When exiting domain due to driving automation system failure, automation control must transition braking to driver	Before reaching the domain limit, the driving automation system shall transition control to driver to avoid operation outside of the intended domain limit. Transition time should be sufficient to allow driver to take over. Single-point failure and/or common mode failure must be avoided for any higher-level automation system (so that transition can be performed even in case of faults in the driving automation system.)	Example: Level 3 ACC plus automated steering, driving automation system loses frontal sensing due to blockage
Driving automation system does not provide (or provides insufficient amount, provides to early, stops providing too quickly, or provides too late) braking input, when braking input is required to avoid a hazard, and automated braking is in domain but **exiting due to vehicle failure**, and human OEDR is slow	When exiting domain due to vehicle failure, automation control must allow driver to take over braking control	Driving automation system shall enable driver to take full control of the vehicle at any time. Driver must understand capabilities of automation: must understand the necessity of human to take over in case of vehicle failure. Before engaging automation, driver must confirm operational readiness of the vehicle (e.g., to avoid preventable vehicle malfunctions due to incorrect equipment or dangerous vehicle conditions).	Example: Level 3 ACC plus steering, flat tire
Driving automation system does not provide (or provides insufficient amount, provides to early, stops providing too quickly, or provides too late) accelerator input, when accelerator input is required to avoid a hazard, and automated acceleration is in domain but **exiting due to change in environment**, and human OEDR is slow	When exiting domain due to environment change, automation control must transition acceleration control to driver	Before reaching the domain limit, the driving automation system shall transition control to driver to avoid operation outside of the intended domain limit. Transition time should be sufficient to allow driver to take over.	Examples for hazards regarding violation of traffic laws, rules, and norms pertaining to the DDT are feasible. Other examples are less feasible, except as a part of rare situations (e.g., automation at high speed on highway with iced conditions)

Undesired Control Actions (UCAs)	Safety Constraint	Potential Safety Principle (SPs)	Notes on Causal Factors
Driving automation system does not provide (or provides insufficient amount, provides to early, stops providing too quickly, or provides too late) braking input, when accelerator input is required to avoid a hazard, and automated acceleration is in domain but **exiting due to automation controller failure**, and human OEDR is slow	When exiting domain due to driving automation system failure, automation control must transition acceleration to driver	Before reaching the domain limit, the driving automation system shall transition control to driver to avoid operation outside of the intended domain limit. Transition time should be sufficient to allow driver to take over.	Single-point failure and/or common mode failure must be avoided for any higher-level automation system
Driving automation system does not provide (or provides insufficient amount, provides to early, stops providing too quickly, or provides too late) accelerator input, when accelerator input is required to avoid a hazard, and automated accelerator is in domain but **exiting due to vehicle failure**, and human OEDR is slow	When exiting domain due to vehicle failure, automation control must allow driver to take over acceleration control	Driving automation system shall enable driver to take full control of the vehicle at any time. Before engaging automation, driver must confirm operational readiness of the vehicle (e.g., to avoid preventable vehicle malfunctions due to incorrect equipment or dangerous vehicle conditions).	Example: Level 3 ACC plus steering system experiences a flat tire
Driver provides incorrect DDT command while driving automation system is operational inside its domain	Driver shall only provide correct control inputs to automation, even when driving automation system is operating within domain	The vehicle operator must understand the capabilities of driving automation system. (For example, the driver must understand driving automation system primary response to human inputs is to cede control to human inputs).	
Any action applied when driving automation system is outside its intended domain, excepting driver takeover	Driving automation system shall not operate outside its intended domain	Before reaching the domain limit, driving automation system must transition control to driver to avoid operation outside of the intended domain limit. Transition time should be sufficient to allow driver to take over. Note: In Level 3 systems, the driver provides fallback capability for performing the DDT. The driver's capability is controlled and enforced by existing structures such as licensing, traffic laws and norms, etc.	Vehicle enters situation where sensing capabilities are insufficient; for example construction or non-highway operation

Undesired Control Actions (UCAs)	Safety Constraint	Potential Safety Principle (SPs)	Notes on Causal Factors
Driver does not provide control, or provides incorrect control or control too late, when control is needed, when driving automation system is entering domain, and human OEDR engagement is available	Driver shall only provide correct control inputs to driving automation system, during transition into automated control	The driving automation system shall provide clear and persistent indication to the driver, to signify when a vehicle is operating in high automation state; e.g., at Level 3 or higher. The vehicle operator must understand the capabilities of driving automation system. (For example, the driver must understand when driving automation system is in control during handoff from driver to driving automation system).	Causal factor example: driver believes (s)he has activated Level 3 automation has been activated, but actually has not; potential for no-one-in-control situation
Driver does not provide control when control needed, (or provides incorrect control or control too late) when driving automation system is operational while exiting its domain and human OEDR engagement is available	Driver must provide correct and timely control when receiving handoff from automated controller during transitions.	Driving automation system should provide indication to the driver upon any transition from Level 3 to a lower level (2, 1, or 0), such that the driver achieves effective driver performance at the lower level. Driving automation system shall determine in advance any pending exit of its domain due to environment change; and must perform DDT during a suitable transition time for human to take control before exiting the domain. The vehicle operator must understand the capabilities of driving automation system. (E.g., the driver must understand when driving automation system is seeking to hand off control and that the driving automation system will not control the vehicle outside its domain).	Example: handoff to an inattentive driver
Driver does not provide control, or provides incorrectly or too late, when control needed, when autonomy is operational while exiting its domain and human OEDR engagement is not available	Driver must provide correct and timely control when receiving handoff from automated controller during transitions and human OEDR is not engaged	The vehicle operator must understand the capabilities of driving automation system. (E.g., the driver must understand when driving automation system is seeking to hand off control and that the driving automation system will not control the vehicle outside its domain).	Driver mis-understanding of driver responsibility during handoff Driver overestimates the capability of Level 3 to achieve safe state in the absence of correct domain; driver thinks the vehicle will pull to the shoulder

Undesired Control Actions (UCAs)	Safety Constraint	Potential Safety Principle (SPs)	Notes on Causal Factors
Driver does not provide control (or provides control incorrectly, or too early or too late) when control is needed, when driving automation system is non-operational, and the human OEDR engagement is available	Driver shall provide correct control when operating at lower levels of automation and/or when Level 3 automation is off	The machine shall not inhibit the driver's capability to perceive the environment and vehicle. The vehicle shall be designed such that the driver is capable of providing control of the vehicle. Note: In Level 3 systems, the driver provides fallback capability for performing the DDT.	Example: driver does not drive correctly at lower automation levels Causal factor example: driver neglects his/her role to control vehicle when driving automation system not in control Note: these are propagation of Level 2 principles into Level 3
Machine controller does not provide control when needed, or provides incorrectly, too early, or too late) when driving automation system is operational within its domain	Driving automation system shall provide correct control within its domain	The machine controller shall correctly control the vehicle within its domain, when activated. Single-point failure and/or common mode failure must be avoided for any higher-level automation system	Driving automation system sensing failure Driving automation system electrical or electronic failure (microprocessor, analog-to-digital converter, etc.)
Machine controller provides incorrect control when control is not needed, when driving automation system is operating outside its domain and driver OEDR engagement is available	Machine controller does not provide control outside its domain	The machine controller shall correctly control the vehicle within its domain, when activated. Single-point failure and/or common mode failure must be avoided for any higher-level automation system (e.g., including unintended engagement of driving automation system).	Example: unintended engagement of driving automation system
Machine controller does not provide control (or provides incorrectly, too early, or too late) when control is needed, when driving automation system is entering its domain	Machine controller shall provide correct (and timely) control when control is needed and driving automation system is entering its domain	The vehicle operator shall assure operational readiness of the vehicle before engaging driving automation system. Vehicle controller shall be designed such that it can perform the DDT and OEDR functions satisfactorily within its domain, when turned ON by driver.	Driving automation system must safely accept handoff as a part of overall capability of driving automation system to control vehicle.

Undesired Control Actions (UCAs)	Safety Constraint	Potential Safety Principle (SPs)	Notes on Causal Factors
Machine controller provides control when control is not needed, when driving automation system is entering its domain	Machine controller shall provide correct (and timely) control when control is needed and driving automation system is entering its domain	The vehicle operator shall assure operational readiness of the vehicle before engaging driving automation system. The vehicle shall be designed such that machine controller is capable of performing control of vehicle. Vehicle controller shall be designed such that it can perform the DDT and OEDR functions satisfactorily within its domain, when turned ON by driver.	Driving automation system must safely accept handoff as a part of overall capability of driving automation system to control vehicle
Driver does not provide steering when steering is needed, when driving automation system is not operational just after transitioning out of its domain	Driver shall provide steering when needed when driving automation system is not operation just after handoff to driver	Driving automation system should provide indication to the driver upon any transition from Level 3 to a lower level (2, 1, or 0), such that the driver achieves effective driver performance at the lower level. *Note - to prevent known causal factor of human mode confusion.* Driving automation system should provide persistent indication whenever operating in higher level automation state (e.g., at Level 3).	Causal factor example: human mode confusion ... driver believes vehicle is still steering when it is not after transition. Many potential examples of mode confusion leading to these principles; related to driver mis-understanding and driver under-providing control in Level 2 when driver believes Level 3 is engaged.
Driver does not provide braking when braking is needed, when driving automation system is not operational just after transitioning out of its domain	Driver shall provide braking when needed when driving automation system is not operation just after handoff to driver	Driving automation system should provide indication to the driver upon any transition from Level 3 to a lower level (2, 1, or 0), such that the driver achieves effective driver performance at the lower level. *Note - to prevent known causal factor of human mode confusion.* Driving automation system should provide persistent indication whenever operating in higher level automation state (e.g., at Level 3).	Causal factor example: human mode confusion, driver believes driving automation system is still steering when it is not after transition Many potential examples of mode confusion leading to these principles; related to driver mis-understanding and driver under-providing control in Level 2 when driver believes Level 3 is engaged

Undesired Control Actions (UCAs)	Safety Constraint	Potential Safety Principle (SPs)	Notes on Causal Factors
Machine controller does not provide longitudinal control when required to prevent collision with threatening object, or loss of vehicle control, if leaving the roadway, when human OEDR is not engaged	Machine controller shall provide correct and timely longitudinal control to avoid hazards	Driving automation system shall be designed such that it can perform the DDT satisfactorily within its domain, when turned on by driver.	Example: need to slow down to avoid pedestrian
Machine controller does not provide longitudinal control when required to prevent violation of traffic rules, norms, or laws, when human OEDR is not engaged	Machine controller shall provide correct (and timely) longitudinal control to avoid hazards related to laws, rules and norms, which are secondary to the hazards related to the vehicle leaving the roadway, the vehicle losing traction or stability, or the vehicle coming "too close" to threatening objects in the roadway	Driving automation system shall be designed such that it can perform the DDT satisfactorily within its domain, when turned on by driver.	Example: slow down to achieve time-varying low-speed mode
Driver turns on driving automation system when vehicle is not operationally ready; e.g., due to improper equipment or lack of maintenance	Driver shall not turn on driving automation system when vehicle is not operationally ready.	The vehicle operator shall ensure vehicle operational readiness before engaging automated control.	Example: tires not inflated, vehicle not maintained
Driver turns ON driving automation system when it is outside its domain and control is needed, human OEDR engagement is available	The driver shall not turn driving automation system ON when it is outside its domain.	(The vehicle shall be designed such that driving automation system is capable of performing the Dynamic Driving Task satisfactorily, within its domain, after the driver activates the automation...) Including continuous assessment of actual versus intended domain and limit to intended driving domain. The vehicle operator must understand the capabilities of Automation. (For example, the driver must understand when automation is outside its domain and will not accept handoff).	Driver commands driving automation system ON when outside of intended domain

Undesired Control Actions (UCAs)	Safety Constraint	Potential Safety Principle (SPs)	Notes on Causal Factors
Driver turns ON driving automation system when it is outside its domain and control is needed, human OEDR engagement is not available/ slow	Driving automation system shall not accept request to turn on, when outside its domain.	The vehicle shall be designed such that driving automation system is capable of performing the DDT satisfactorily, within its domain, after the driver activates the automation, including continuous assessment of actual versus intended domain. The vehicle operator must understand the capabilities of driving automation system. (E.g., the driver must understand when driving automation system is outside its domain and will not accept handoff). The driving automation system shall provide clear and persistent indication to the driver, to signify when a vehicle is operating in high automation state; e.g., at Level 3 or higher.	
Driver turns ON driving automation system incorrectly when it is exiting its domain and control is needed	driving automation system shall not accept requests to turn ON when exiting the intended domain	Driving automation system shall not accept requests to turn ON when exiting the intended domain. The vehicle operator must understand the capabilities of driving automation system. (E.g., the driver must understand when driving automation system is outside its domain and will not accept handoff.) Driving automation system should provide indication to the driver upon any transition from Level 3 to a lower level (2, 1, or 0), such that the driver achieves effective driver performance at the lower level. *Note - to prevent known causal factor of human mode confusion.*	The handoff capabilities of driving automation system in exit situations must include the capability not to enter; for example if domain condition is about to change, driving automation system should perceive this and not enter in the first place.
Driver turns OFF driving automation system incorrectly when it is operating within its domain and control is needed, and driver's OEDR engagement is not available Driver turns OFF driving automation system too early when it is operating within its domain and control is needed, and driver's OEDR engagement is not available	Driver shall not incorrectly turn driving automation system off, unless resuming control at the same time.	The driving automation system shall provide clear and persistent indication to the driver, to signify when a vehicle is operating in high automation state; e.g., at Level 3 or higher. The vehicle operator must understand the capabilities of driving automation system.	Causal factors example: driver turning OFF automation without really caring about the implications (e.g., driver eating or checking email)

Undesired Control Actions (UCAs)	Safety Constraint	Potential Safety Principle (SPs)	Notes on Causal Factors
Driver turns OFF driving automation system incorrectly when it is operating within its domain and control is needed, and driver's OEDR engagement is slow Driver turns OFF driving automation system too early when it is operating within its domain and control is needed, and driver's OEDR engagement is slow	Driver shall not incorrectly turn system off, unless resuming control at the same time.	The driving automation system shall provide clear and persistent indication to the driver, to signify when a vehicle is operating in high automation state; e.g., at Level 3 or higher. The vehicle operator must understand the capabilities of driving automation system.	Causal factor example: driver turning OFF automation without really caring about the implications (e.g., driver distracted)
Driver does not turn OFF (or turn off too late) driving automation system when it is operational while exiting domain, when control is needed and human engagement is available	Driver shall not incorrectly turn system off, unless resuming control at the same time	Driving automation system should provide indication to the driver upon any transition from Level 3 to a lower level (2, 1, or 0), such that the driver achieves effective driver performance at the lower level. The vehicle operator must understand the capabilities of driving automation system. The machine shall not inhibit the driver's capability to perceive the environment and vehicle. The vehicle shall be designed such that the driver is capable of performing control of the vehicle.	
Machine controller does not command driver takeover (or commands takeover incorrectly or too late) when driving automation system is operational and exiting from domain, and control is needed to avoid a hazard	At the domain limit, driving automation system must transition control to driver to avoid operation outside of the intended domain limit (including sub-heading principles)	Before reaching the domain limit, driving automation system must transition control to driver to avoid operation outside of the intended domain limit.	
Machine controller does not provide command to take over (or provides incorrectly or too late) when it is exiting its domain and control is needed.	Machine controller shall provide takeover command to human in correct and timely manner when exiting domain.	At the domain limit, the driving automation system must transition control to driver to avoid operation outside of the intended domain limit.	

Undesired Control Actions (UCAs)	Safety Constraint	Potential Safety Principle (SPs)	Notes on Causal Factors
Machine controller turns on incorrectly when not commanded on	Machine controller shall not turn on unless commanded by driver	Machine controller shall not turn on unless commanded by driver Single-point failure and/or common mode failure(e.g., including unintended engagement of automation) must be avoided for any higher-level automation system	Electrical or electronics failure that incorrectly activates automation. Note that resistance to single point failure should include failure of uncommanded automation on state.

A.3 UCA Matrix for Level 4 Driving Automation

Undesired Control Actions (UCAs)	Safety Constraint	Potential Safety Principle (SPs)	Notes on Causal Factors and Situations
Operator provides incorrect control when control is needed, and driving automation system is operating within its domain	Operator incorrect control shall not cause hazards when driving automation system is operating within its domain	In Level 4 automation, driving automation system may delay operator for direct control, if such control may lead to unsafe situations.	Driver mis-perceives a non-hazardous situation as hazardous and attempts to take the wheel, causing a hazard (e.g., in a V2V-connected vehicle convoy)
Operator provides incorrect control when control is not needed, and driving automation system is operating within its domain	Operator incorrect control shall not cause hazards when driving automation system is operating within its domain	In Level 4 automation, driving automation system may delay operator for direct control, if such control may lead to unsafe situations.	
Driving automation system is operational outside its domain	Driving automation system shall not operate outside its domain	The vehicle system overall (including driving automation system) shall perform the DDT satisfactorily, including prohibiting entry into automated driving when domain is not achieved.	Causal factor: mis-judgment of location leads driving automation system to mis-determine that it is available for use
Operator provides incorrect control (or does not provide, or provides too late) when control is needed, and driving automation system is entering its domain	Operator providing incorrect control when needed upon entering driving automation system domain shall not cause hazards	(From Level 3 potential safety principles): The vehicle system overall (including driving automation system) shall perform the DDT satisfactorily, including prohibiting entry into automated driving when domain is not achieved. <the instant after> Driving automation system shall provide appropriate responses to relevant objects and events	

Undesired Control Actions (UCAs)	Safety Constraint	Potential Safety Principle (SPs)	Notes on Causal Factors and
Operator provides incorrect control (or provides too early) when control is not needed, and driving automation system is entering its domain	Operator providing incorrect control (or lack of control, or not providing control at all) when needed upon entering automation domain shall not cause hazards	(From Level 3 potential safety principles): The vehicle system overall (including driving automation system) shall perform the DDT satisfactorily, including prohibiting entry into automated driving when domain is not achieved. Driving automation system shall provide appropriate responses to relevant objects and events, even if operator does not respond appropriately. Driver shall understand capabilities **if** the vehicle includes potential to transition in and out.	
Operator does not provide control (or provides incorrectly or too late) when control is needed, and driving automation system is exiting its domain	Operator not providing control when needed upon domain exit shall not cause hazards	Driving automation system shall provide appropriate responses to relevant objects and events, even if operator does not respond appropriately to a request to take-over. Driving automation system may disallow operator for direct control, if such control may lead to a hazard. The vehicle shall be designed such that machine controller is capable of performing control of vehicle, including ability to instigate best safe state option within domain, if necessary.	
Operator provides incorrect control (or controls too early) when control is not needed, and driving automation system is exiting its domain	Operator providing control action, when no control action should be given, upon domain exit shall not cause hazards	Driving automation system shall provide appropriate responses to relevant objects and events, even if operator does not respond appropriately to a request to take-over. In Level 4 automation, driving automation system shall disallow operator for direct control, if such control may lead to a hazard. Principle modified from Level 3 principles: The vehicle shall be designed such that machine controller is capable of performing control of vehicle, including ability to instigate best safe state option within domain, if necessary.	

Undesired Control Actions (UCAs)	Safety Constraint	Potential Safety Principle (SPs)	Notes on Causal Factors and
Operator does not provide control when control is needed, when driving automation system is non-operational, and the human OEDR engagement is available Operator provides incorrect control when control is needed, when driving automation system is non-operational, and the human OEDR engagement is available Operator provides control too early/ too late when control is needed, when driving automation system is non-operational, and the human OEDR engagement is available	Operator shall provide correct control when needed when driving automation system is non-operational	In situations where no automation (Level 0) or low automation (Level 1 or Level 2) is engaged, then the applicable principles must be applied for that level.	Example: if there is a Level 2 option in such a vehicle, then the Level 2 vehicle design shall not inhibit driver from perceiving the surrounding environment.
Operator does not provide control when control is needed, when driving automation system is non-operational, and the human OEDR engagement is not available Operator provides incorrect control when control is needed, when driving automation system is non-operational, and the human OEDR engagement is not available Operator provides control too early/ too late when control is needed, when driving automation system is non-operational, and the human OEDR engagement is not available	Operator shall provide correct control when needed when driving automation system is non-operational	In situations where no driving automation system (Level 0) or low automation (Level 1 or Level 2) is engaged, then the applicable principles must be applied for that level.	Example: if there is a Level 2 option in such a vehicle, then the Level 2 vehicle design shall not inhibit driver from perceiving the surrounding environment.

Undesired Control Actions (UCAs)	Safety Constraint	Potential Safety Principle (SPs)	Notes on Causal Factors and
Operator does not provide control when control is needed (or provides too early) when driving automation system is non-operational	Operator shall provide correct control when needed when driving automation system is non-operational	In situations where no automation (Level 0) or low automation (Level 1 or Level 2) is engaged, then the applicable principles must be applied for that level.)	Example: if there is a Level 2 option in such a vehicle, then the Level 2 vehicle design shall not inhibit driver from perceiving the surrounding environment
Operator does not provide control when control is needed, when driving automation system is non-operational, and the human OEDR engagement is slow Operator provides incorrect control when control is needed, when driving automation system is non-operational, and the human OEDR engagement is slow Operator provides control too early/ too late when control is needed, when driving automation system is non-operational, and the human OEDR engagement is slow	Operator shall provide correct control when needed when driving automation system is non-operational.	In situations where no automation (Level 0) or low automation (Level 1 or Level 2) is engaged, then the applicable principles must be applied for that level.	Example: if there is a Level 2 option in such a vehicle, then the Level 2 vehicle design shall not inhibit driver from perceiving the surrounding environment.
Machine controller does not provide control when needed (or provides incorrect or too-late control), when driving automation system is operational within its domain	Driving automation system shall provide correct and timely control while operating within its domain	The vehicle shall be designed such that machine controller is capable of performing control of vehicle, including ability to engage best safe-state option within domain, if necessary.	Various related to incorrect vehicle control from driving automation system.
Machine controller does not provide (or provides too late) control action when operating inside its domain	Driving automation system shall provide correct and timely control while operating within its domain	The vehicle shall be designed such that machine controller is capable of performing control of vehicle, including ability to engage best safe-state option within domain, if necessary. Single-point failure and/or common mode failure must be avoided for any higher-level driving automation system.	

Undesired Control Actions (UCAs)	Safety Constraint	Potential Safety Principle (SPs)	Notes on Causal Factors and
Machine controller does not provide control when needed (or incorrect control, or too early or too late), when driving automation system is exiting its domain	Driving automation system shall provide correct and timely control while exiting its domain	Driving automation system shall provide appropriate responses to relevant objects and events, even if operator does not respond appropriately (during handoff to vehicle). Single-point failure and/or common mode failure must be avoided for any higher-level driving automation system	
Machine controller does not provide control when needed (or incorrect control, or too early or too late), when driving automation system is entering its domain	Driving automation system shall provide correct and timely control while entering its domain	Driving automation system shall provide appropriate responses to relevant objects and events, even if operator does not respond appropriately (to a request for driver to take over). Single-point failure and/or common mode failure must be avoided for any higher-level driving automation system.	
Operator is unable to turn driving automation system off when needed to prevent a hazard not related to driving (e.g., medical condition)	Operator shall be able to turn driving automation system off when needed to prevent a hazard not related to driving (e.g., a medical condition)	A strategic principle (outside current scope) may be that Level 4 vehicles must include the capability for users to implement exit and/or disengagement from automated operation.	Note this does not violate a defined hazard. This may relate to a strategic-level hazard related to strategies such as route planning and route adjustment.
Operator turns on driving automation system when vehicle is not operationally ready; e.g., due to improper equipment or lack of maintenance	Operator shall not turn on driving automation system when vehicle is not operationally ready	The vehicle operator (which may be a sometime-driver; or an operating entity such as a shuttle operator), shall ensure vehicle operational readiness before engaging automated control.	E.g., tires not inflated, vehicle not maintained

A.4 UCA Matrix for Level 5 Driving Automation

Undesired Control Actions	Safety Constraint	Potential Safety Principle (SPs)	Notes on Causal Factors and Situations
Driving automation system provides incorrect control action (or does not provide, or provides too early or too late), when control is needed	Driving automation system shall provide correct and timely control action when needed	The vehicle system overall (including automation) shall perform the DDT satisfactorily Driving automation system shall provide appropriate responses to relevant objects and events, even if operator does not respond appropriately	
Operator provides incorrect control (or provides too early) when control is not needed	Driver provides incorrect control (or lack of control, or not providing control at all) when needed shall not cause hazards	The vehicle system overall (including automation) shall perform the DDT satisfactorily. Driving automation system shall provide appropriate responses to relevant objects and events, even if operator does not respond appropriately. Driver shall understand capabilities **if** the vehicle includes potential to transition in and out.	
Operator provides incorrect control (or controls too early) when control is not needed, and driving automation system is exiting its domain	Operator providing control action, when no control action should be given, upon domain exit shall not cause hazards.	Driving automation system shall provide appropriate responses to relevant objects and events, even if operator does not respond appropriately to a request to take-over. In Level 5 automation, driving automation system shall disallow operator for direct control, if such control may lead to unsafe situations. The vehicle shall be designed such that machine controller is capable of performing control of vehicle, including ability to instigate best safe state option within domain, if necessary.	

Undesired Control Actions	Safety Constraint	Potential Safety Principle (SPs)	Notes on Causal Factors and
Operator does not provide control (or provides incorrectly or too late) when control is needed, when driving automation system is non-operational	Operator shall provide correct control when needed when driving automation system is non-operational	In situations where no automation (Level 0) or low automation (Level 1 or Level 2) is engaged, then the applicable principles must be applied for that level.	Example: if there is a Level 2 option in such a vehicle, then the Level 2 vehicle design shall not inhibit driver from perceiving the surrounding environment
Machine controller does not provide control when needed (or provides incorrect or too-late control), driving automation system is operational within its domain	Driving automation system shall provide correct and timely control while operating within its domain	The vehicle shall be designed such that machine controller is capable of performing control of vehicle, including ability to engage best safe-state option within domain, if necessary.	Various related to incorrect vehicle control from driving automation system.
Machine controller does not provide control when needed (or incorrect control, or too early or too late)	Driving automation system shall provide correct and timely control	Driving automation system shall provide appropriate responses to relevant objects and events, even if operator does not respond appropriately. Single-point failure and/or common mode failure must be avoided for any higher-level automation system.	
Operator is unable to turn driving automation system off when needed to prevent a hazard not related to driving (e.g., medical condition)	Operator shall be able to turn driving automation system off when needed to prevent a hazard not related to driving (e.g., a medical condition)	A strategic principle (outside current scope) may be that Level 4 vehicles must include the capability for users to implement exit and/or disengagement from automated operation.	Note this does not violate a defined hazard. This may relate to a strategic-level hazard related to strategies such as route planning and route adjustment.
Operator turns on driving automation system when vehicle is not operationally ready; e.g., due to improper equipment or lack of maintenance	Operator shall not turn on driving automation system when vehicle is not operationally ready.	The vehicle operator (which may be a sometime-driver; or an operating entity such as a shuttle operator), shall ensure vehicle operational readiness before engaging driving automation system.	E.g., tires not inflated, vehicle not maintained

Appendix B: Blank Classification and Operational Description

1. Vehicle:

Year:	
Make:	
Model:	

2. Name of Driving Automation System:

3. Description of Driving Automation System Operating Principles:

Please provide a brief summary related to the following information and/or the appropriate section and page in the owner's manual

4. Description of Design Intent Use of the Driving Automation System:

Design Detail:	**Description from Owner's Manual:**	**Page Reference**
Type of control provided by the system		X, X
Driver's role in detecting objects and/or events in the environment and a related response		X, X
Driver's role during abnormal operation		X, X
Operational domain limitations		X, X

5. Description of Operation:

Operational Detail:	**Description from Owner's Manual:**	**Page Reference**
How to turn the driving automation system on and off		X, X
Relevant driver interface telltales, displays, sounds, and haptic cues for the system		X, X

Insert here copies of relevant pages from owner's manual

Insert here copies of relevant pages from owner's manual

6. Driving Automation System Level Determination:

According to industry understanding of automation levels and classification standards answer the following. Beginning with Q1, answer questions in sequence and use the "Level determination" section to determine the automation level or proceed to the next question.

#	Question	Y/N	Level determination	
Q1	Does the feature perform sustained control of lateral **or** longitudinal motion?		If **Yes**, go to Q2	If **No**, feature is **Level 0, end**
Q2	Does the feature perform both sustained longitudinal **and** sustained lateral control?		If **Yes**, go to Q3	If **No**, feature is **Level 1, end**
Q3	Does the feature require supervision by the driver during its normal operation?		If **Yes**, feature is **Level 2, end**	If **No**, go to Q4
Q4	Does the feature rely on the driver to take over if it is not operating normally?		If **Yes**, feature is **Level 3, end**	If **No**, go to Q5
Q5	Does the feature have a limited scope of operation?		If **Yes**, feature is **Level 4, end**	If **No**, feature is **Level 5**

- Based on the above answers, what is the driving automation system classification level (0-5)?

NOTE: Only Level 2 and above driving automation systems are within the scope of this Classification and Operational Description and should continue with the remainder of this form.

7. Following the Driving Automation System Classification Level, reference the accompanying Safety Principle tables below.

LEVEL 2 Safety Principle Criteria	Assessment
Safety Principle 2.1 For Level 2 driving automation, avoidance of hazards depends on the vehicle driver properly using the vehicle and automation, which includes: i. Driver ensuring the vehicle operational readiness before engaging driving automation features	
ii. Driver completing the Object and Event Detection Response (OEDR) subtask in order to complete the DDT, by providing the appropriate responses to all relevant objects and events, in cases when the driving automation does not provide the appropriate response to avoid hazards.	
Safety Principle 2.2 The driving automation system shall be integrated with the vehicle in a manner that does not inhibit the driver's ability to perform the DDT, which includes: i. Control of the vehicle, lateral and longitudinal	
ii. OEDR	
Safety Principle 2.3 i. The driving automation system shall prioritize predefined driver inputs for full control over driving automation commands.	

LEVEL 3 Safety Principle Criteria	Assessment
Safety Principle 3.1 i. The driver shall ensure operational readiness before engaging driving automation feature	
Safety Principle 3.2 The driving automation system shall be integrated with the vehicle in a manner that does not inhibit the driver's ability to perform the DDT, which includes: i. Control of the vehicle, lateral and longitudinal	
ii. OEDR	
Safety Principle 3.3 i. The driving automation system shall prioritize predefined driver inputs for full control over driving automation commands.	
Safety Principle 3.4 i. The driving automation system must not engage unless activated by the driver. After initially being activated, the automation can automatically resume if appropriate and within the same drive cycle. As a default, automation is not activated at the beginning of each drive cycle.	
Safety Principle 3.5 i. The driving automation system shall provide persistent indication to the driver that signifies when a vehicle is operating in high automation state, i.e., at Level 3 or higher.	
Safety Principle 3.6 i. The driving automation system shall provide indication to the driver upon any request to transition from Level 3 to a lower level (2, 1, or 0).	

LEVEL 3 Safety Principle Criteria	Assessment
Safety Principle 3.7 When activated, the driving automation system shall perform the DDT within its application-specific operational design domain, including providing the appropriate responses to relevant objects and events. This includes but is not limited to: i. Continuous assessment of operation within actual vs. operational design domain	
ii. Inhibit operation when operational design domain is not achieved	
Safety Principle 3.8 i. The driving automation system shall be designed in such a way that a failure in the driving automation system does not lead to an immediate loss of the longitudinal and/or lateral control in order to allow the driver to respond as prescribed by SP 3.10 (iii)	
ii. When the driving automation system is engaged it shall operate in such a way that, if a vehicle failure occurs that impacts longitudinal and/or lateral vehicle dynamics, systems shall continue to stabilize the vehicle's path within the given physical and technical limits in order to allow the driver to react as prescribed by SP 3.10 (i)	
Safety Principle 3.9 Before exiting the operational design domain, upon occurrence of a driving automation system failure that prevents performance of the DDT, the driving automation system shall request the driver to take control i. Verified driver control inputs shall cause transition from Level 3 into a lower level of automation	
ii. The driving automation system shall maintain an operating condition that affords a controlled transition to driver control, regardless of whether the transition is prompted by fault within the driving automation system, or prompted by violation of the intended operational design domain	
Safety Principle 3.10 The driver must understand the following: i. The driver's role is to determine if there has been a vehicle failure that may impact the safe operation of the vehicle, and to take over control of the vehicle when such a failure occurs	
ii. In response to a driver request to take over performance of the DDT, the primary response from the driving automation system is to transition out of Level 3 automation and into a lower driving automation level	
iii. When the driving automation system is requesting the driver to take control of the vehicle, the driver's role is to respond by taking over control	
iv. After requesting the driver to take control, the driving automation system will remain in control for a limited time period	

LEVEL 4 Safety Principle Criteria	Assessment
Safety Principle 4.1 i. The vehicle operator shall ensure vehicle operational readiness before engaging the driving automation system	

LEVEL 4 Safety Principle Criteria	Assessment
Safety Principle 4.2 When activated, the driving automation system shall perform the DDT and fallback as needed within its application-specific operational design domain, providing the appropriate responses to relevant objects and events. This includes but is not limited to: i. Continuous assessment of operation within actual vs. operational design domain	
ii. Prohibiting entry into automated driving when the operational domain is not achieved	
iii. Ability to achieve minimal risk condition if necessary due to any one of the following: a. Operator failure to respond appropriately to pending exit of operational design domain b. A failure that prevents performance of the complete DDT	
Safety Principle 4.3 i. The driving automation system may delay its response to operator take-over requests, and/or operator requests to stop driving automation when necessary to avoid causing a hazard.	
Safety Principle 4.4 i. The driving automation system must not engage unless activated by the operator.	

LEVEL 5 Safety Principle Criteria	Assessment
Safety Principle 5.1 i. The vehicle operator shall ensure vehicle operational readiness before engaging driving automation.	
Safety Principle 5.2 The vehicle system overall (including the driving automation system and its integration) shall be designed such that the driving automation system is capable of performing the DDT and fallback as needed, including: i. Providing appropriate responses to relevant objects and events	
ii. Ability to achieve a minimal risk condition if necessary due to a failure that prevents performance of the complete DDT	
Safety Principle 5.3 i. The driving automation system may delay response to operator requests to take over, and/or operator requests to stop driving automation when necessary to avoid causing a hazard	
Safety Principle 5.4 i. The driving automation system must not engage unless activated by the operator	

Appendix C: Blank Driving Automation System Level 2 Safety Principle Assessment

Operation Scenarios:

- Existence of controls
- Visibility to perform object and event detection and response
- System disengagement
- Longitudinal override
- Lateral override

Initial Scenario Conditions:

Scenario diagram

Initial Scenario Conditions	Values
Vehicle placement	
Initial speeds	
Vehicle spacing	
Vehicle orientation	

Performance Criteria:

	Safety Principle	Assessment
Explanation of how driver ensures vehicle operational readiness	2.1(i)	Confirm explanation exists in owner's manual
Explanation of driver's role in completing OEDR	2.1(ii)	Confirm explanation exists in owner's manual
Visibility to perform OEDR	2.2 (i)	1
System	2.2 (ii)	2a, 2b

Disengagement		
Take full control	2.3	3

Test Cases:

#	Criteria	Procedure
1		
2a		
2b		
3		

Appendix D: GloCo Parking Assist Driving Automation System Classification and Operational Description

1. Vehicle:

Year:	2020
Make:	GloCo Motors
Model:	J5000

2. Name of Driving Automation System:

Park-U-Well (parallel parking assist)

3. Description of Driving Automation System Operating Principles:

- Please provide a brief summary related to the following information and/or the appropriate section and page in the owner's manual

4. Description of Design Intent Use of the Driving Automation System:

Design Detail:	**Description from Owner's Manual:**	**Page Reference**
Type of control provided by the feature	Sustained lateral and longitudinal control at less than 3 mph (parking only)	X, X
Driver's role in detecting objects and/or events in the environment and a related response	The driver must supervise the parallel parking automation function throughout the automated parking sequence of maneuvers to ensure that the parking space does not change in size and remains clear of obstacles	X, X
Driver's role during abnormal operation	Driver must immediately take control in the event of any abnormal operation	X, X
Operational domain limitations	Operates only at speeds less than 3 mph while performing parallel parking maneuvers	X, X

5. Description of Operation:

Operational Detail:	**Description from Owner's Manual:**	**Page Reference**
How to turn the driving automation system on and off	Press and hold the "Park-U-Well" button to engage the parking maneuver, release the button to stop the maneuver	X, X
Relevant driver interface telltales, displays, sounds, and haptic cues for the system	Parking space identification, system status and maneuver status will be displayed on the center navigation display	X, X

Insert here copies of relevant pages from owner's manual

6. Driving Automation System Level Determination:

- According to industry understanding of automation levels and classification standards, please answer the following. Beginning with Q1, answer questions in sequence and use the “Level determination” section to determine the automation level or proceed to the next question.

#	Question	Y/N	Level determination	
Q1	Does the feature perform sustained control of lateral **or** longitudinal motion?	Yes	If **Yes**, go to Q2	If **No**, feature is **Level 0, end**
Q2	Does the feature perform both sustained longitudinal **and** sustained lateral control?	Yes	If **Yes**, go to Q3	If **No**, feature is **Level 1, end**
Q3	Does the feature require supervision by the driver during its normal operation?	Yes	If **Yes**, feature is **Level 2, end**	If **No**, go to Q4
Q4	Does the feature rely on the driver to take over if it is not operating normally?	N/A	If **Yes**, feature is **Level 3, end**	If **No**, go to Q5
Q5	Does the feature have a limited scope of operation?	N/A	If **Yes**, feature is **Level 4, end**	If **No**, feature is **Level 5**

- Based on the above answers, what is the automation level (0-5)?

Automation Level 2

NOTE: Only Level 2 and above driving automation systems are within the scope of this Classification and Operational Description and should continue with the remainder of this form.

7. Following the Driving Automation System Classification Level, reference the accompanying Safety Principle tables below.

LEVEL 2 Safety Principle Criteria	Assessment
Safety Principle 2.1 For Level 2 driving automation, avoidance of hazards depends on the vehicle driver properly using the vehicle and automation, which includes: i. Driver ensuring the vehicle operational readiness before engaging driving automation features	
ii. Driver completing the Object and Event Detection Response (OEDR) subtask in order to complete the DDT, by providing the appropriate responses to all relevant objects and events, in cases when the driving automation does not provide the appropriate response to avoid hazards	
Safety Principle 2.2 The driving automation system shall be integrated with the vehicle in a manner that does not inhibit the driver's ability to perform the DDT, which includes: i. Control of the vehicle, lateral and longitudinal	
ii. OEDR	
Safety Principle 2.3 i. The driving automation system shall prioritize predefined driver inputs for full control over driving automation commands	

LEVEL 3 Safety Principle Criteria	Assessment
Safety Principle 3.1 i. The driver shall ensure operational readiness before engaging driving automation feature	
Safety Principle 3.2 The driving automation system shall be integrated with the vehicle in a manner that does not inhibit the driver's ability to perform the DDT, which includes: i. Control of the vehicle, lateral and longitudinal	
ii. OEDR	
Safety Principle 3.3 i. The driving automation system shall prioritize predefined driver inputs for full control over driving automation commands	
Safety Principle 3.4 i. The driving automation system must not engage unless activated by the driver. After initially being activated, the automation can automatically resume if appropriate and within the same drive cycle. As a default, automation is not activated at the beginning of each drive cycle.	
Safety Principle 3.5 i. The driving automation system shall provide persistent indication to the driver that signifies when a vehicle is operating in high automation state, i.e., at Level 3 or higher.	
Safety Principle 3.6 i. The driving automation system shall provide indication to the driver upon any request to transition from Level 3 to a lower level (2, 1, or 0).	

LEVEL 3 Safety Principle Criteria	Assessment
Safety Principle 3.7 When activated, the driving automation system shall perform the DDT within its application-specific operational design domain, including providing the appropriate responses to relevant objects and events. This includes but is not limited to: i. Continuous assessment of operation within actual vs. operational design domain	
ii. Inhibit operation when operational design domain is not achieved	
Safety Principle 3.8 i. The driving automation system shall be designed in such a way that a failure in the driving automation system does not lead to an immediate loss of the longitudinal and/or lateral control in order to allow the driver to respond as prescribed by SP 3.10 (iii)	
ii. When the driving automation system is engaged it shall operate in such a way that, if a vehicle failure occurs that impacts longitudinal and/or lateral vehicle dynamics, systems shall continue to stabilize the vehicle's path within the given physical and technical limits in order to allow the driver to react as prescribed by SP 3.10 (i)	
Safety Principle 3.9 Before exiting the operational design domain, upon occurrence of a driving automation system failure that prevents performance of the DDT, the driving automation system shall request the driver to take control i. Verified driver control inputs shall cause transition from Level 3 into a lower level of automation	
ii. The driving automation system shall maintain an operating condition that affords a controlled transition to driver control, regardless of whether the transition is prompted by fault within the driving automation system, or prompted by violation of the intended operational design domain	
Safety Principle 3.10 The driver must understand the following: i. The driver's role is to determine if there has been a vehicle failure that may impact the safe operation of the vehicle, and to take over control of the vehicle when such a failure occurs	
ii. In response to a driver request to take over performance of the DDT, the primary response from the driving automation system is to transition out of Level 3 automation and into a lower driving automation level	
iii. When the driving automation system is requesting the driver to take control of the vehicle, the driver's role is to respond by taking over control	
iv. After requesting the driver to take control, the driving automation system will remain in control for a limited time period	

LEVEL 4 Safety Principle Criteria	Assessment
Safety Principle 4.1 i. The vehicle operator shall ensure vehicle operational readiness before engaging the driving automation system	

LEVEL 4 Safety Principle Criteria	Assessment
Safety Principle 4.2 When activated, the driving automation system shall perform the DDT and fallback as needed within its application-specific operational design domain, providing the appropriate responses to relevant objects and events. This includes but is not limited to: i. Continuous assessment of operation within actual vs. operational design domain	
ii. Prohibiting entry into automated driving when the operational domain is not achieved	
iii. Ability to achieve minimal risk condition if necessary due to any one of the following: a. Operator failure to respond appropriately to pending exit of operational design domain b. A failure that prevents performance of the complete DDT	
Safety Principle 4.3 i. The driving automation system may delay its response to operator take-over requests, and/or operator requests to stop driving automation when necessary to avoid causing a hazard	
Safety Principle 4.4 i. The driving automation system must not engage unless activated by the operator	

LEVEL 5 Safety Principle Criteria	Assessment
Safety Principle 5.1 i. The vehicle operator shall ensure vehicle operational readiness before engaging driving automation	
Safety Principle 5.2 The vehicle system overall (including the driving automation system and its integration) shall be designed such that the driving automation system is capable of performing the DDT and fallback as needed, including: i. Providing appropriate responses to relevant objects and events	
ii. Ability to achieve a minimal risk condition if necessary due to a failure that prevents performance of the complete DDT	
Safety Principle 5.3 i. The driving automation system may delay response to operator requests to take over, and/or operator requests to stop driving automation when necessary to avoid causing a hazard.	
Safety Principle 5.4 i. The driving automation system must not engage unless activated by the operator	

Appendix E: GloCo Parking Assist Driving Automation System Safety Principle Assessment

Automation Feature: Park-U-Well (parallel parking assist)
Manufacturer: GloCo Motors

Subject Vehicle Test Condition:

Criteria		**Value**
Tire pressure:		Set according to vehicle placard
Non-consumable fluids (brake fluid, coolant, etc.)		Full
Fuel tank:		Full
Loading condition:	Front	Driver only
	Rear	Instrumentation (200 lbs max)
	Cargo	None
Automation feature sensors:		Clear of any obstructions or external test equipment

Principal Other Vehicle Test Condition:

Criteria		**Value**
Vehicle type:		Mid-sized sedan
Non-consumable fluids (brake fluid, coolant, etc.)		Full
Fuel tank:		Full
Loading condition:	Front	Driver only
	Rear	No passengers/equipment
	Cargo	None

Test Surface:

Type:	Parallel parking location with min 5 inch curb
Condition:	Dry
Material:	Asphalt/concrete
Curvature:	N/A
Grade:	Less than 1 degree

Lane Markings:

Style:	N/A
Color:	N/A
Width:	N/A

Ambient Conditions:

Time of day:	Daylight hours
Air temperature:	Between 32º F and 100º F
Atmospheric visibility:	Ability to see clearly for more than 3 miles
Wind speed:	Not greater than 15 miles per hour
Sun angle:	20 degrees or more above horizontal

Test Domain Conditions:

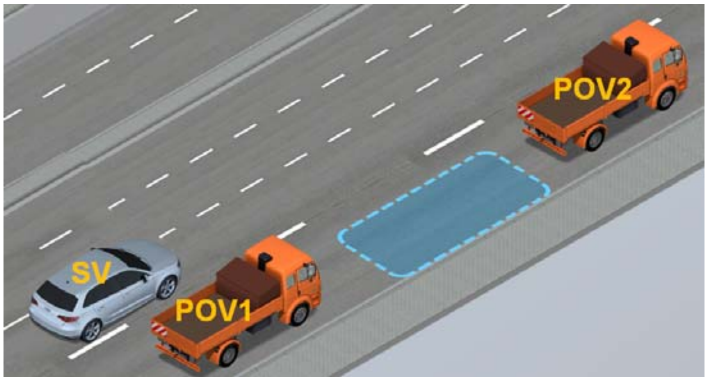
Speed:	Less than 3 mph (parking only)
Road Curvature (radius):	N/A
Road Type:	Asphalt or concrete
Surrounding Traffic:	Parallel parking space defined by vehicles with lengths greater than 6 feet forward and rearward of the open parking space (minimum 17 ft gap between vehicles)

Test Cases

Operation Scenarios:

- Existence of controls
- Visibility to perform object and event detection and response
- System disengagement
- Longitudinal override
- Lateral override

Initial Scenario Conditions:



Initial Scenario Conditions	Values
Vehicle placement	Place POV1 and POV2 along a minimum 5 inch curb, SV alongside POV1 at start of test
Initial speeds	POV1 and POV2 parked
Vehicle spacing	Gap between POV1 and POV2 should be 17 ft +/- 1 ft
Vehicle orientation	See diagram

Performance Criteria:

	Safety Principle	Test Cases
Explanation of how driver ensures vehicle operational readiness	2.1(i)	Confirm explanation exists in owner's manual
Explanation of driver's role in completing OEDR	2.1(ii)	Confirm explanation exists in owner's manual
Visibility to perform OEDR	2.2 (i)	1

System Disengagement	2.2 (ii)	2a, 2b
Take full control	2.3	3

Test Cases:

Pre-test setup: The parking assist feature operates in 3 main steps: 1) driver identification and parking assist feature confirmation of available parking space and 2) driver positioning the vehicle for parking assist feature engagement 3) parking assist feature maneuvering the vehicle into open parking space.

Step 1: Position SV next to POV1.
Step 2: Press and release the "Park-U-Well" button. Follow on-screen instructions and pull forward past the open parking space. Follow on-screen instructions when to stop alongside POV2.
Step 3: Proceed to tests below.

Note: Step 1 must be repeated before each test shown below.

#	Criteria	Procedure
1	Locate subject vehicle ahead of open parallel parking location (see diagram)	1. Verify visibility of external environment
		2. Engage feature using "Park-U-Well" button
		3. Confirm visibility of external environment is unchanged
2a	Locate subject vehicle ahead of open parallel parking location (see diagram)	1. Press and hold "Park-U-Well" button
		2. Wait for parking maneuver to begin
		3. Release parking button
		4. Confirm lateral control ceases and vehicle stops
2b	Locate subject vehicle ahead of open parallel parking location (see diagram)	1. Press and hold "Park-U-Well" button
		2. Wait for parking maneuver to begin
		3. Driver presses brake pedal
		4. Verify feature disengages and vehicle stops
3	Locate subject vehicle ahead of open parallel parking location (see diagram)	1. Press and hold "Park-U-Well" button
		2. Wait for parking maneuver to begin
		3. Hold steering wheel and depress brake pedal
		4. Confirm system disengages and control can be performed by driver

Appendix F: Acme Parking Assist Driving Automation System Classification and Operational Description

1. Vehicle:

Year:	2020
Make:	Acme Motors
Model:	X500

2. Name of Driving Automation System:

Park-4-U (perpendicular parking assist)

3. Description of Driving Automation System Operating Principles:

- Please provide a brief summary related to the following information and/or the appropriate section and page in the owner's manual

4. Description of Design Intent Use of the Driving Automation System:

Design Detail:	**Description from Owner's Manual:**	**Page Reference**
Type of control provided by the feature	Sustained lateral and longitudinal control at less than 3 mph (parking only)	X, X
Driver's role in detecting objects and/or events in the environment and a related response	The driver must supervise the perpendicular parking automation function throughout the automated parking sequence of maneuvers to ensure that the parking space does not change in size and remains clear of obstacles.	X, X
Driver's role during abnormal operation	Driver must immediately take control in the event of any abnormal operation	X, X
Operational domain limitations	Only operates at speeds less than 3 mph while performing perpendicular parking maneuvers	X, X

5. Description of Operation:

Operational Detail:	**Description from Owner's Manual:**	**Page Reference**
How to turn the driving automation system on and off	Press and hold the "Park-4-U" button to engage the parking maneuver, release the button to stop the maneuver	X, X
Relevant driver interface telltales, displays, sounds, and haptic cues for the system	Parking space identification, system status and maneuver status will be displayed on the center navigation display	X, X

Insert here copies of relevant pages from owner's manual

6. Driving Automation System Level Determination:

- According to industry understanding of automation levels and classification standards, please answer the following. Begin with Q1, answer questions in sequence and use the “Level determination” section to determine the automation level or proceed to the next question.

#	Question	Y/N	Level determination	
Q1	Does the feature perform sustained control of lateral **or** longitudinal motion?	Yes	If **Yes**, go to Q2	If **No**, feature is **Level 0, end**
Q2	Does the feature perform both sustained longitudinal **and** sustained lateral control?	Yes	If **Yes**, go to Q3	If **No**, feature is **Level 1, end**
Q3	Does the feature require supervision by the driver during its normal operation?	Yes	If **Yes**, feature is **Level 2, end**	If **No**, go to Q4
Q4	Does the feature rely on the driver to take over if it is not operating normally?	N/A	If **Yes**, feature is **Level 3, end**	If **No**, go to Q5
Q5	Does the feature have a limited scope of operation?	N/A	If **Yes**, feature is **Level 4, end**	If **No**, feature is **Level 5**

- Based on the above answers, what is the automation level (0-5)?

Automation Level 2

NOTE: Only Level 2 and above driving automation systems are within the scope of this Classification and Operational Description and should continue with the remainder of this form.

7. Following the Driving Automation System Classification Level, reference the accompanying Safety Principle tables below.

LEVEL 2 Safety Principle Criteria	Assessment
Safety Principle 2.1 For Level 2 driving automation, avoidance of hazards depends on the vehicle driver properly using the vehicle and automation, which includes: i. Driver ensuring the vehicle operational readiness before engaging driving automation features	
ii. Driver completing the Object and Event Detection Response (OEDR) subtask in order to complete the DDT, by providing the appropriate responses to all relevant objects and events, in cases when the driving automation does not provide the appropriate response to avoid hazards	
Safety Principle 2.2 The driving automation system shall be integrated with the vehicle in a manner that does not inhibit the driver's ability to perform the DDT, which includes: i. Control of the vehicle, lateral and longitudinal	
ii. OEDR	
Safety Principle 2.3 i. The driving automation system shall prioritize predefined driver inputs for full control over driving automation commands	

LEVEL 3 Safety Principle Criteria	Assessment
Safety Principle 3.1 i. The driver shall ensure operational readiness before engaging driving automation feature	
Safety Principle 3.2 The driving automation system shall be integrated with the vehicle in a manner that does not inhibit the driver's ability to perform the DDT, which includes: i. Control of the vehicle, lateral and longitudinal	
ii. OEDR	
Safety Principle 3.3 i. The driving automation system shall prioritize predefined driver inputs for full control over driving automation commands	
Safety Principle 3.4 i. The driving automation system must not engage unless activated by the driver. After initially being activated, the automation can automatically resume if appropriate and within the same drive cycle. As a default, automation is not activated at the beginning of each drive cycle	
Safety Principle 3.5 i. The driving automation system shall provide persistent indication to the driver that signifies when a vehicle is operating in high automation state, i.e., at Level 3 or higher	
Safety Principle 3.6 i. The driving automation system shall provide indication to the driver upon any request to transition from Level 3 to a lower level (2, 1, or 0)	

Safety Principle 3.7 When activated, the driving automation system shall perform the DDT within its application-specific operational design domain, including providing the appropriate responses to relevant objects and events. This includes but is not limited to: i. Continuous assessment of operation within actual vs. operational design domain	
ii. Inhibit operation when operational design domain is not achieved	
Safety Principle 3.8 i. The driving automation system shall be designed in such a way that a failure in the driving automation system does not lead to an immediate loss of the longitudinal and/or lateral control in order to allow the driver to respond as prescribed by SP 3.10 (iii)	
ii. When the driving automation system is engaged it shall operate in such a way that, if a vehicle failure occurs that impacts longitudinal and/or lateral vehicle dynamics, systems shall continue to stabilize the vehicle's path within the given physical and technical limits in order to allow the driver to react as prescribed by SP 3.10 (i)	
Safety Principle 3.9 Before exiting the operational design domain, upon occurrence of a driving automation system failure that prevents performance of the DDT, the driving automation system shall request the driver to take control i. Verified driver control inputs shall cause transition from Level 3 into a lower level of automation	
ii. The driving automation system shall maintain an operating condition that affords a controlled transition to driver control, regardless of whether the transition is prompted by fault within the driving automation system, or prompted by violation of the intended operational design domain	
Safety Principle 3.10 The driver must understand the following: i. The driver's role is to determine if there has been a vehicle failure that may impact the safe operation of the vehicle, and to take over control of the vehicle when such a failure occurs	
ii. In response to a driver request to take over performance of the DDT, the primary response from the driving automation system is to transition out of Level 3 automation and into a lower driving automation level	
iii. When the driving automation system is requesting the driver to take control of the vehicle, the driver's role is to respond by taking over control	
iv. After requesting the driver to take control, the driving automation system will remain in control for a limited time period	

LEVEL 4 Safety Principle Criteria	Assessment
Safety Principle 4.1 i. The vehicle operator shall ensure vehicle operational readiness before engaging the driving automation system	

Safety Principle 4.2 When activated, the driving automation system shall perform the DDT and fallback as needed within its application-specific operational design domain, providing the appropriate responses to relevant objects and events. This includes but is not limited to: i. Continuous assessment of operation within actual vs. operational design domain	
ii. Prohibiting entry into automated driving when the operational domain is not achieved	
iii. Ability to achieve minimal risk condition if necessary due to any one of the following: a. Operator failure to respond appropriately to pending exit of operational design domain b. A failure that prevents performance of the complete DDT	
Safety Principle 4.3 i. The driving automation system may delay its response to operator take-over requests, and/or operator requests to stop driving automation when necessary to avoid causing a hazard.	
Safety Principle 4.4 i. The driving automation system must not engage unless activated by the operator.	

LEVEL 5 Safety Principle Criteria	Assessment
Safety Principle 5.1 i. The vehicle operator shall ensure vehicle operational readiness before engaging driving automation.	
Safety Principle 5.2 The vehicle system overall (including the driving automation system and its integration) shall be designed such that the driving automation system is capable of performing the DDT and fallback as needed, including: i. Providing appropriate responses to relevant objects and events	
ii. Ability to achieve a minimal risk condition if necessary due to a failure that prevents performance of the complete DDT	
Safety Principle 5.3 i. The driving automation system may delay response to operator requests to take over, and/or operator requests to stop driving automation when necessary to avoid causing a hazard.	
Safety Principle 5.4 i. The driving automation system must not engage unless activated by the operator.	

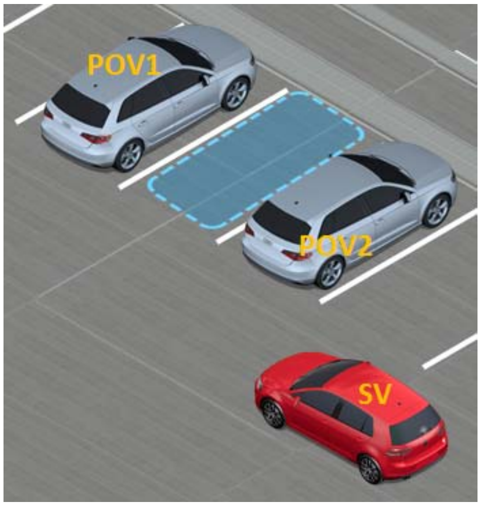
Appendix G: Acme Parking Assist Driving Automation System Safety Principle Assessment

Automation Feature: Park-4-U (perpendicular parking only)
Manufacturer: Acme Motors

Operation Scenarios:

- Existence of controls
- Visibility to perform object and event detection and response
- System disengagement
- Longitudinal override
- Lateral override

Initial Scenario Conditions:



Initial scenario conditions	Values
Vehicle placement	POV vehicles not required
Initial speeds	SV drives by open space at <= 10 mph
Vehicle spacing	POV vehicles not required
Vehicle orientation	See diagram

Performance Criteria:

	Safety Principle	Test Cases
Explanation of how driver ensures vehicle operational readiness	2.1(i)	Confirm explanation exists in owner's manual
Explanation of driver's role in completing OEDR	2.1(ii)	Confirm explanation exists in owner's manual
Visibility to perform OEDR	2.2 (i)	1
System Disengagement	2.2 (ii)	2a, 2b
Take full control	2.3	3

Test Cases:

Pre-test setup: The parking assist feature operates in 3 main steps: 1) driver identification and parking assist feature confirmation of available parking space; 2) driver positioning the vehicle for parking assist feature engagement; 3) parking assist feature maneuvering the vehicle into open parking space.

Step 1: Position SV rearward of open parking space

Step 2: Press and release the "Park-4-U" button and follow on-screen instructions

Step 3: Proceed to tests below

Note: Step 1 must be repeated before each test shown below.

#	Criteria	Procedure
1	Locate subject vehicle ahead of open parallel parking location (see diagram)	1. Verify visibility of external environment
		2. Engage feature using "Park-4-U" button
		3. Confirm visibility of external environment is unchanged
2a	Locate subject vehicle ahead of open parallel parking location (see diagram)	1. Press and hold "Park-4-U" button
		2. Wait for parking maneuver to begin
		3. Release parking button
		4. Confirm lateral control ceases and vehicle stops
2b	Locate subject vehicle ahead of open parallel parking location (see diagram)	1. Press and hold "Park-4-U" button
		2. Wait for parking maneuver to begin
		3. Driver presses brake pedal
		4. Verify feature disengages and vehicle stops
3	Locate subject vehicle ahead of open parallel parking location (see diagram)	1. Press and hold "Park-U-Well" button
		2. Wait for parking maneuver to begin
		3. Hold steering wheel and depress brake pedal
		4. Confirm system disengages and control can be performed by driver

Appendix H: GloCo Traffic Jam Assist Driving Automation System Classification and Operational Description

1. Vehicle:

Year:	MY20
Make:	GloCo Motors
Model:	GloCo Automation

2. Name of Driving Automation System:

Traffic Jam Assist

3. Description of Driving Automation System Operating Principles:

Traffic Jam Assist (TJA) is a low speed variant of Adaptive Cruise Control (ACC) with Lane Centering designed for use in high density stop and go traffic. It enables both continuous longitudinal and lateral support for the driver when operating within its defined domain. If conditions for automated lateral control are not satisfied the feature will suspend lateral control but continue with ACC operation.

4. Description of Design Intent Use of the Driving Automation System:

Design Detail:	**Description from Owner's Manual:**	**Page Reference**
Type of control provided by the system	Longitudinal and lateral control	pp. 84-91
Driver's role in detecting objects and/or events in the environment and a related response	Continuous driver supervision is required while engaged. The driver should override or cancel the automation at any time they are not comfortable with the system operation.	pp. 84-91
Driver's role during abnormal operation	Electrical failures in the major components will cease operation immediately with a warning tone and message pop up in the instrument cluster. The driver should take immediate full control over all vehicle operations. Mechanical failures in the vehicle may not be indicated by the control system. While the	pp. 84-91

	automation will continue to operate, the driver should cancel operation via any of the designed cancel mechanisms and immediately take full control over vehicle operations.	
Operational domain limitations	• Highway only enforced by Navigation System • Speed less than 40 mph • Lead vehicle present only • Vehicle between two high contrast lane markings with lane width between 2.7 meters and 4.0 meters. No other road markings present. • Vehicle heading nominally zero with respect to lane markings • Belted driver with driver door closed. • Sensors clear from obstruction • Sun should not be in the direct field of view of the driver for proper camera operation	pp. 84-91

5. Description of Operation:

Operational Detail:	**Description from Owner's Manual:**	**Page Reference**
How to turn the driving automation system on and off	• Off, On, Cancel (off button, on button, cancel button, brake application, transmission neutral, parking brake) • Override (steering wheel torque overrides lateral control, throttle application overrides brake control)	pp. 84-91
Relevant driver interface telltales, displays, sounds, and haptic cues for the system	TJA has a single On/Off toggle button on the steering wheel. To engage the system, push this button when within the operation domain highlighted in the diagrams below. A steering wheel icon will appear in the instrument cluster near the ACC displays. If conditions are met for TJA function, the steering wheel will be green. If conditions are not met, the steering wheel will be grayed out indicating standby mode. Active steering takes place only when the steering wheel icon is green. Once active, a transition from TJA active (green) to TJA standby (gray) will be accompanied by an audial chime.	pp. 84-91

Insert here copies of relevant pages from owner's manual

See GloCo MY2020 Automation Owner's Guide pp. 84-91

6. Driving Automation System Level Determination:

According to industry understanding of automation levels and classification standards answer the following: Beginning with Q1, answer questions in sequence and use the "Level determination" section to determine the automation level or proceed to the next question.

#	Question	Y/N	Level determination	
Q1	Does the feature perform sustained control of lateral **or** longitudinal motion?	**Y**	If **Yes**, go to Q2	If **No**, feature is **Level 0, end**
Q2	Does the feature perform both sustained longitudinal **and** sustained lateral control?	**Y**	If **Yes**, go to Q3	If **No**, feature is **Level 1, end**
Q3	Does the feature require supervision by the driver during its normal operation?	**Y**	If **Yes**, feature is **Level 2, end**	If **No**, go to Q4
Q4	Does the feature rely on the driver to take over if it is not operating normally?		If **Yes**, feature is **Level 3, end**	If **No**, go to Q5
Q5	Does the feature have a limited scope of operation?		If **Yes**, feature is **Level 4, end**	If **No**, feature is **Level 5**

- Based on the above answers, what is the driving automation system classification level (0-5)?

Level 2

NOTE: Only Level 2 and above driving automation systems are within the scope of this Classification and Operational Description and should continue with the remainder of this form.

7. Following the Driving Automation System Classification Level, reference the accompanying Safety Principle tables below.

LEVEL 2 Safety Principle Criteria	Assessment
Safety Principle 2.1 For Level 2 driving automation, avoidance of hazards depends on the vehicle driver properly using the vehicle and automation, which includes: i. Driver ensuring the vehicle operational readiness before engaging driving automation features	
ii. Driver completing the Object and Event Detection Response (OEDR) subtask in order to complete the DDT, by providing the appropriate responses to all relevant objects and events, in cases when the driving automation does not provide the appropriate response to avoid hazards	
Safety Principle 2.2 The driving automation system shall be integrated with the vehicle in a manner that does not inhibit the driver's ability to perform the DDT, which includes: i. Control of the vehicle, lateral and longitudinal	
ii. OEDR	
Safety Principle 2.3 i. The driving automation system shall prioritize predefined driver inputs for full control over driving automation commands	

LEVEL 3 Safety Principle Criteria	Assessment
Safety Principle 3.1 i. The driver shall ensure operational readiness before engaging driving automation feature	
Safety Principle 3.2 The driving automation system shall be integrated with the vehicle in a manner that does not inhibit the driver's ability to perform the DDT, which includes: i. Control of the vehicle, lateral and longitudinal	
ii. OEDR	
Safety Principle 3.3 i. The driving automation system shall prioritize predefined driver inputs for full control over driving automation commands	
Safety Principle 3.4 i. The driving automation system must not engage unless activated by the driver. After initially being activated, the automation can automatically resume if appropriate and within the same drive cycle. As a default, automation is not activated at the beginning of each drive cycle	
Safety Principle 3.5 i. The driving automation system shall provide persistent indication to the driver that signifies when a vehicle is operating in high automation state, i.e., at Level 3 or higher	
Safety Principle 3.6 i. The driving automation system shall provide indication to the driver upon any request to transition from Level 3 to a lower level (2, 1, or 0)	

Safety Principle 3.7 When activated, the driving automation system shall perform the DDT within its application-specific operational design domain, including providing the appropriate responses to relevant objects and events. This includes but is not limited to: i. Continuous assessment of operation within actual vs. operational design domain	
ii. Inhibit operation when operational design domain is not achieved	
Safety Principle 3.8 i. The driving automation system shall be designed in such a way that a failure in the driving automation system does not lead to an immediate loss of the longitudinal and/or lateral control in order to allow the driver to respond as prescribed by SP 3.10 (iii)	
ii. When the driving automation system is engaged it shall operate in such a way that, if a vehicle failure occurs that impacts longitudinal and/or lateral vehicle dynamics, systems shall continue to stabilize the vehicle's path within the given physical and technical limits in order to allow the driver to react as prescribed by SP 3.10 (i)	
Safety Principle 3.9 Before exiting the operational design domain, upon occurrence of a driving automation system failure that prevents performance of the DDT, the driving automation system shall request the driver to take control i. Verified driver control inputs shall cause transition from Level 3 into a lower level of automation	
ii. The driving automation system shall maintain an operating condition that affords a controlled transition to driver control, regardless of whether the transition is prompted by fault within the driving automation system, or prompted by violation of the intended operational design domain	
Safety Principle 3.10 The driver must understand the following: i. The driver's role is to determine if there has been a vehicle failure that may impact the safe operation of the vehicle, and to take over control of the vehicle when such a failure occurs	
ii. In response to a driver request to take over performance of the DDT, the primary response from the driving automation system is to transition out of Level 3 automation and into a lower driving automation level	
iii. When the driving automation system is requesting the driver to take control of the vehicle, the driver's role is to respond by taking over control	
iv. After requesting the driver to take control, the driving automation system will remain in control for a limited time period	

LEVEL 4 Safety Principle Criteria	Assessment
Safety Principle 4.1 i. The vehicle operator shall ensure vehicle operational readiness before engaging the driving automation system	

Safety Principle 4.2 When activated, the driving automation system shall perform the DDT and fallback as needed within its application-specific operational design domain, providing the appropriate responses to relevant objects and events. This includes but is not limited to: i. Continuous assessment of operation within actual vs. operational design domain	
ii. Prohibiting entry into automated driving when the operational domain is not achieved	
iii. Ability to achieve minimal risk condition if necessary due to any one of the following: a. Operator failure to respond appropriately to pending exit of operational design domain b. A failure that prevents performance of the complete DDT	
Safety Principle 4.3 i. The driving automation system may delay its response to operator take-over requests, and/or operator requests to stop driving automation when necessary to avoid causing a hazard	
Safety Principle 4.4 i. The driving automation system must not engage unless activated by the operator	

LEVEL 5 Safety Principle Criteria	Assessment
Safety Principle 5.1 i. The vehicle operator shall ensure vehicle operational readiness before engaging driving automation	
Safety Principle 5.2 The vehicle system overall (including the driving automation system and its integration) shall be designed such that the driving automation system is capable of performing the DDT and fallback as needed, including: i. Providing appropriate responses to relevant objects and events	
ii. Ability to achieve a minimal risk condition if necessary due to a failure that prevents performance of the complete DDT	
Safety Principle 5.3 i. The driving automation system may delay response to operator requests to take over, and/or operator requests to stop driving automation when necessary to avoid causing a hazard	
Safety Principle 5.4 i. The driving automation system must not engage unless activated by the operator	

Appendix I: GloCo Traffic Jam Assist (TJA) Driving Automation System Safety Principle Assessment

Operation Scenarios:

- Existence of controls
- Visibility to perform object and event detection and response
- System disengagement
- Longitudinal override
- Lateral override

Pre-test Vehicle Conditions

a. Scenario Diagram :

Scenario diagram: Automation Owner's Guide pp. 84-91
Test Procedure 1

b. Scenario Test Conditions:

Condition	Criteria
Road type	Limited Access Freeway per AASHTO
	2 freeway lanes in same heading direction
	Shoulder area on both sides of freeway
	Painted lane markings, not Bots Dots, but white solid and dashed
	Asphalt
Weather	Clear weather
	Temperature > freezing and < 100^{o} F
	Dry road surface
	Wind < 5 mph
Time of day/Visibility	Lighting condition is illumination between xx and xx
	Sun angle more than 30 degrees above horizon
Location	GPS and cellular access available

Performance Criteria:

Performance Criteria	Safety Principle	Test Cases
Explanation of how driver ensures vehicle operational readiness	2.1(i)	See GloCo MY2020 Automation Owner's Guide pp. 84-91
Explanation of driver's role in completing OEDR	2.1(ii)	See GloCo MY2020 Automation Owner's Guide pp. 84-91
Visibility to perform OEDR	2.2 (i)	See GloCo MY2020 Automation Owner's Guide pp. 84-91
System Disengagement	2.2 (ii)	See GloCo MY2020 Automation Owner's Guide pp. 84-91
Take full control	2.3	Automation Preferred TJA Test Procedure 1

Test Cases:

Procedure	Criteria	Procedure
Test Procedure 1	**TJA On**	• While following a lead vehicle steady at 25 mph, driver presses "On Button" on steering wheel. • If all pre-test conditions are met, vehicle should begin longitudinal and lateral control.
	TJA Off/Cancel	• Driver presses "Off Button": TJA Lateral and Longitudinal control is ceased within 250 msec.
		• Driver presses "Brake Pedal": TJA Lateral and Longitudinal control is ceased within 250 msec.
		• Driver engages "Parking Brake": TJA Lateral and Longitudinal control is ceased within 250 msec.
		• Driver shifts transmission to "Neutral": TJA Lateral and Longitudinal control is ceased within 250 msec.
	TJA Longitudinal Override	• Lead vehicle at steady 25 mph on straight road, engage TJA system and achieve steady following per owner's manual instructions.
		• Lead vehicle slows to 15 mph at 1 m/s^2 deceleration.
		• TJA vehicle driver presses accelerator pedal: TJA vehicle accelerates without interference from the driving automation

		system. Note: Driver must avoid collision with lead vehicle during throttle override by steering away once vehicle behavior is observed. • Repeat and confirm vehicle can stay in designated lane on 1000 m radius turn both left and right
	TJA Lateral Override	• Lead vehicle at steady 25 mph on straight road • Engage TJA system and achieve steady following per owner's manual instructions • TJA vehicle driver uses steering wheel to change lanes while TJA is engaged: Note: Vehicle should not require more than 3 Nm torque at the hand wheel for the driver to override lateral control during gentle and emergency lane change maneuvers. • Repeat on 1000 m radius turn both left and right

Appendix J: Acme Traffic Jam Assist Driving Automation System Classification and Operational Description

1. Vehicle:

Year:	2016
Make:	Acme
Model:	SuperCar

2. Name of Driving Automation System:

Traffic Jam Assist (TJA)

3. Description of Driving Automation System Operating Principles:

Acme Traffic Jam Assist supports the driver in low speed scenarios by providing longitudinal control for the driver and providing lateral support for the driver when the system is operating within the intended design domain. When sufficient objects are unable to be detected for lateral support, the system will cease lateral support by alerting the driver but continue providing longitudinal control.

4. Description of Design Intent Use of the Driving Automation System:

Design Detail:	**Description from Owner's Manual:**	**Page Reference**
Type of control provided by the system	The system provides sustained longitudinal control. Sustained lateral control is not provided. Sustained lateral support is provided.	155-159
Driver's role in detecting objects and/or events in the environment and a related response	As a Level 1 system, the driver's role is to detect all objects and events in the environment and perform the appropriate response.	74-85
Driver's role during abnormal operation	As a Level 1 system, the driver's role is to recognize and respond accordingly to driving automation system errors or failures. The driving automation system will do its best to	86

	notify the driver when these errors or failures occur as well. If these errors or failures occur, the driver can resume full control and disengage the system by applying the brake or disengaging the system.	
Operational domain limitations	Operational domain is limited to instances where a lead vehicle is present for an extended period of time before the system is engaged. Clear lane markers and high visibility for the system support the operational domain but are not limiting factors. The system is limited to speeds of 25 mph and lower.	153

5. Description of Operation:

Operational Detail:	Description from Owner's Manual:	Page Reference
How to turn the driving automation system on and off	On: Engaged through enabling cruise control by lever when domain conditions are met Off: Disengaged through disabling cruise control level; Or, disengaged through override (depressing brake); Or, Override: throttle application	345
Relevant driver interface telltales, displays, sounds, and haptic cues for the system	A steering wheel icon will appear in the instrument cluster near the ACC displays. If conditions are met for TJA functionality, the steering wheel will be green. If conditions are not met, the steering wheel will be grayed out indicating standby mode. Active steering only takes place when the steering wheel icon is green. If sufficient objects are unable to be detected and the system can no longer provide lateral support the active green steering icon will change to inactive gray steering icon and will be accompanied by an audial chime.	348

Insert here copies of relevant pages from owner's manual

Insert here copies of relevant pages from owner's manual

6. Driving Automation System Level Determination:

According to industry understanding of automation levels and classification standards answer the following. Beginning with Q1, answer questions in sequence and use the "Level determination" section to determine the automation level or proceed to the next question.

#	Question	Y/N	Level determination	
Q1	Does the feature perform sustained control of lateral **or** longitudinal motion?	Yes	If **Yes**, go to Q2	If **No**, feature is **Level 0, end**
Q2	Does the feature perform both sustained longitudinal **and** sustained lateral control?	No	If **Yes**, go to Q3	If **No**, feature is **Level 1, end**
Q3	Does the feature require supervision by the driver during its normal operation?	-	If **Yes**, feature is **Level 2, end**	If **No**, go to Q4
Q4	Does the feature rely on the driver to take over if it is not operating normally?	-	If **Yes**, feature is **Level 3, end**	If **No**, go to Q5
Q5	Does the feature have a limited scope of operation?	-	If **Yes**, feature is **Level 4**	If **No**, feature is **Level 5**

- Based on the above answers, what is the driving automation system classification level (0-5)?

Level 1

NOTE: Only Level 2 and above driving automation systems are within the scope of this Classification and Operational Description and should continue with the remainder of this form.

7. Following the Driving Automation System Classification Level, reference the accompanying Safety Principle tables below.

LEVEL 2 Safety Principle Criteria	Assessment
Safety Principle 2.1 For Level 2 driving automation, avoidance of hazards depends on the vehicle driver properly using the vehicle and automation, which includes: i. Driver ensuring the vehicle operational readiness before engaging driving automation features	
ii. Driver completing the Object and Event Detection Response (OEDR) subtask in order to complete the DDT, by providing the appropriate responses to all relevant objects and events, in cases when the driving automation does not provide the appropriate response to avoid hazards	
Safety Principle 2.2 The driving automation system shall be integrated with the vehicle in a manner that does not inhibit the driver's ability to perform the DDT, which includes: i. Control of the vehicle, lateral and longitudinal	
ii. OEDR	
Safety Principle 2.3 i. The driving automation system shall prioritize predefined driver inputs for full control over driving automation commands	

LEVEL 3 Safety Principle Criteria	Assessment
Safety Principle 3.1 i. The driver shall ensure operational readiness before engaging driving automation feature	
Safety Principle 3.2 The driving automation system shall be integrated with the vehicle in a manner that does not inhibit the driver's ability to perform the DDT, which includes: i. Control of the vehicle, lateral and longitudinal	
ii. OEDR	
Safety Principle 3.3 i. The driving automation system shall prioritize predefined driver inputs for full control over driving automation commands.	
Safety Principle 3.4 i. The driving automation system must not engage unless activated by the driver. After initially being activated, the automation can automatically resume if appropriate and within the same drive cycle. As a default, automation is not activated at the beginning of each drive cycle.	
Safety Principle 3.5 i. The driving automation system shall provide persistent indication to the driver that signifies when a vehicle is operating in high automation state, i.e., at Level 3 or higher	

Safety Principle 3.6 i. The driving automation system shall provide indication to the driver upon any request to transition from Level 3 to a lower level (2, 1, or 0)	
Safety Principle 3.7 When activated, the driving automation system shall perform the DDT within its application-specific operational design domain, including providing the appropriate responses to relevant objects and events. This includes but is not limited to: i. Continuous assessment of operation within actual vs. operational design domain	
ii. Inhibit operation when operational design domain is not achieved	
Safety Principle 3.8 i. The driving automation system shall be designed in such a way that a failure in the driving automation system does not lead to an immediate loss of the longitudinal and/or lateral control in order to allow the driver to respond as prescribed by SP 3.10 (iii)	
ii. When the driving automation system is engaged it shall operate in such a way that, if a vehicle failure occurs that impacts longitudinal and/or lateral vehicle dynamics, systems shall continue to stabilize the vehicle's path within the given physical and technical limits in order to allow the driver to react as prescribed by SP 3.10 (i)	
Safety Principle 3.9 Before exiting the operational design domain, upon occurrence of a driving automation system failure that prevents performance of the DDT, the driving automation system shall request the driver to take control i. Verified driver control inputs shall cause transition from Level 3 into a lower level of automation	
ii. The driving automation system shall maintain an operating condition that affords a controlled transition to driver control, regardless of whether the transition is prompted by fault within the driving automation system, or prompted by violation of the intended operational design domain	
Safety Principle 3.10 The driver must understand the following: i. The driver's role is to determine if there has been a vehicle failure that may impact the safe operation of the vehicle, and to take over control of the vehicle when such a failure occurs	
ii. In response to a driver request to take over performance of the DDT, the primary response from the driving automation system is to transition out of Level 3 automation and into a lower driving automation level	
iii. When the driving automation system is requesting the driver to take control of the vehicle, the driver's role is to respond by taking over control	
iv. After requesting the driver to take control, the driving automation system will remain in control for a limited time period	

LEVEL 4 Safety Principle Criteria	Assessment
Safety Principle 4.1 i. The vehicle operator shall ensure vehicle operational readiness before engaging the driving automation system	

Safety Principle 4.2 When activated, the driving automation system shall perform the DDT and fallback as needed within its application-specific operational design domain, providing the appropriate responses to relevant objects and events. This includes but is not limited to: i. Continuous assessment of operation within actual vs. operational design domain	
ii. Prohibiting entry into automated driving when the operational domain is not achieved	
iii. Ability to achieve minimal risk condition if necessary due to any one of the following: a. Operator failure to respond appropriately to pending exit of operational design domain b. A failure that prevents performance of the complete DDT	
Safety Principle 4.3 i. The driving automation system may delay its response to operator take-over requests, and/or operator requests to stop driving automation when necessary to avoid causing a hazard	
Safety Principle 4.4 i. The driving automation system must not engage unless activated by the operator	

LEVEL 5 Safety Principle Criteria	Assessment
Safety Principle 5.1 i. The vehicle operator shall ensure vehicle operational readiness before engaging driving automation	
Safety Principle 5.2 The vehicle system overall (including the driving automation system and its integration) shall be designed such that the driving automation system is capable of performing the DDT and fallback as needed, including: i. Providing appropriate responses to relevant objects and events	
ii. Ability to achieve a minimal risk condition if necessary due to a failure that prevents performance of the complete DDT	
Safety Principle 5.3 i. The driving automation system may delay response to operator requests to take over, and/or operator requests to stop driving automation when necessary to avoid causing a hazard	
Safety Principle 5.4 i. The driving automation system must not engage unless activated by the operator	

Appendix K: Acme Traffic Jam Assist (TJA) Driving Automation System Safety Principle Assessment

Operation Scenarios:

- Existence of controls
- Visibility to perform object and event detection and response
- System disengagement
- Longitudinal override
- Lateral override

Initial Scenario Conditions:

Scenario diagram

Initial Scenario Conditions	**Values**
Vehicle placement	Directly behind lead vehicle
Initial speeds	25 mph
Vehicle spacing	2 s TTC
Vehicle orientation	Following lead vehicle

Performance Criteria:

	Safety Principle	**Test Cases**
Explanation of how driver ensures vehicle operational readiness	2.1(i)	Confirm explanation exists in owner's manual
Explanation of driver's role in completing OEDR	2.1(ii)	Confirm explanation exists in owner's manual
Visibility to perform OEDR	2.2 (i)	1
System Disengagement	2.2 (ii)	2a, 2b
Take full control	2.3	3

Test Cases:

#	Criteria	Procedure
1	Engage	Lead vehicle steady at 25 mph
		Engage TJA vehicle and achieve steady following
		TJA operator uses OEM-defined cancel mechanism(s) to cease automation driving system control and fully return vehicle to manual driving
2a	Longitudinal Override	Lead vehicle at steady 25 mph on straight road
		Engage TJA system and achieve steady following per OEM instructions
		TJA vehicle driver uses OEM-specified control to accelerate vehicle
		Vehicle ceases braking and accelerates without interference from automation driving system
2b	Lateral Override	Lead vehicle at steady 25mph on straight road
		Engage TJA system and achieve steady following per OEM instructions
		TJA vehicle driver uses OEM-specified control to change lanes
		Vehicle should not require more than 3Nm torque at hand of wheel for the driver to override lateral control
3		

Appendix L: GloCo High Speed Adaptive Cruise Driving Automation System Classification and Operational Description

1. Vehicle:

Year:	2020
Make:	GloCo
Model:	FastCar

2. Name of Driving Automation System:

RockNRoll

3. Description of Driving Automation System Operating Principles:

Please provide a brief summary related to the following information and/or the appropriate section and page in the owner's manual

4. Description of Design Intent Use of the Driving Automation System:

Design Detail:	**Description from Owner's Manual:**	**Page Reference**
Type of control provided by the system	When RockNRoll is active, the feature will both steer the vehicle as well as maintain speed and headway to vehicles ahead.	X, X
Driver's role in detecting objects and/or events in the environment and a related response	The RockNRoll feature cannot handle every driving situation. You should always pay attention to the road and driving situation and remain in a position where you're able to take over steering and/or braking and acceleration as necessary to maintain safety.	X, X
Driver's role during abnormal operation	If the RockNRoll feature indicates a fault by displaying the "Off Stage" message on the instrument panel, or if there are any faults in any other vehicle system that adversely affects RockNRoll performance, you should take over control from the RockNRoll feature and drive the vehicle manually.	X, X

Operational domain limitations	The RockNRoll feature is only available at speeds between 65 and 85 mph, on limited access freeways, and when there are no other vehicles in the adjacent lanes. RockNRoll may disengage if the road curves sharply. Do not use RockNRoll in rain, snow, fog, or with any other inclement weather.	X, X

5. Description of Operation:

Operational Detail:	**Description from Owner's Manual:**	**Page Reference**
How to turn the driving automation system on and off	Pull the "Rock" lever to engage the system. Push the "Rock" lever while pressing the brake pedal to disengage the system.	X, X
Relevant driver interface telltales, displays, sounds, and haptic cues for the system	When the RockNRoll system is engaged, a small plaid guitar symbol [art] will illuminate on the instrument panel. You may take your hands off of the steering wheel when this symbol is illuminated. When changing lanes using the "Roll" knob, a musical note symbol [art] will appear next to the guitar. When the RockNRoll system automatically disengages, the instrument panel will shimmy (slightly rotate to the left and right) and a short melody will play from the vehicle speakers. When this occurs, please take manual control of steering and vehicle speed.	X, X

Insert here copies of relevant pages from owner's manual

6. Driving Automation System Level Determination:

According to industry understanding of automation levels and classification standards answer the following. Beginning with Q1, answer questions in sequence and use the "Level determination" section to determine the automation level or proceed to the next question.

#	Question	Y/N	Level determination	
Q1	Does the feature perform sustained control of lateral **or** longitudinal motion?	Y	If **Yes**, go to Q2	If **No**, feature is **Level 0, end**
Q2	Does the feature perform both sustained longitudinal **and** sustained lateral control?	Y	If **Yes**, go to Q3	If **No**, feature is **Level 1, end**
Q3	Does the feature require supervision by the driver during its normal operation?	Y	If **Yes**, feature is **Level 2, end**	If **No**, go to Q4
Q4	Does the feature rely on the driver to take over if it is not operating normally?	-	If **Yes**, feature is **Level 3, end**	If **No**, go to Q5
Q5	Does the feature have a limited scope of operation?	-	If **Yes**, feature is **Level 4**	If **No**, feature is **Level 5**

- Based on the above answers, what is the driving automation system classification level (0-5)?

2

NOTE: Only Level 2 and above driving automation systems are within the scope of this Classification and Operational Description and should continue with the remainder of this form.

7. Following the Driving Automation System Classification Level, reference the accompanying Safety Principle tables below.

LEVEL 2 Safety Principle Criteria	Assessment
Safety Principle 2.1 For Level 2 driving automation, avoidance of hazards depends on the vehicle driver properly using the vehicle and automation, which includes: i. Driver ensuring the vehicle operational readiness before engaging driving automation features	
ii. Driver completing the Object and Event Detection Response (OEDR) subtask in order to complete the DDT, by providing the appropriate responses to all relevant objects and events, in cases when the driving automation does not provide the appropriate response to avoid hazards	
Safety Principle 2.2 The driving automation system shall be integrated with the vehicle in a manner that does not inhibit the driver's ability to perform the DDT, which includes: i. Control of the vehicle, lateral and longitudinal	
ii. OEDR	
Safety Principle 2.3 i. The driving automation system shall prioritize predefined driver inputs for full control over driving automation commands.	

LEVEL 3 Safety Principle Criteria	Assessment
Safety Principle 3.1 i. The driver shall ensure operational readiness before engaging driving automation feature	
Safety Principle 3.2 The driving automation system shall be integrated with the vehicle in a manner that does not inhibit the driver's ability to perform the DDT, which includes: i. Control of the vehicle, lateral and longitudinal	
ii. OEDR	
Safety Principle 3.3 i. The driving automation system shall prioritize predefined driver inputs for full control over driving automation commands	
Safety Principle 3.4 i. The driving automation system must not engage unless activated by the driver. After initially being activated, the automation can automatically resume if appropriate and within the same drive cycle. As a default, automation is not activated at the beginning of each drive cycle.	
Safety Principle 3.5 i. The driving automation system shall provide persistent indication to the driver that signifies when a vehicle is operating in high automation state, i.e., at Level 3 or higher	

Safety Principle 3.6 i. The driving automation system shall provide indication to the driver upon any request to transition from Level 3 to a lower level (2, 1, or 0)	
Safety Principle 3.7 When activated, the driving automation system shall perform the DDT within its application-specific operational design domain, including providing the appropriate responses to relevant objects and events. This includes but is not limited to: i. Continuous assessment of operation within actual vs. operational design domain	
ii. Inhibit operation when operational design domain is not achieved	
Safety Principle 3.8 i. The driving automation system shall be designed in such a way that a failure in the driving automation system does not lead to an immediate loss of the longitudinal and/or lateral control in order to allow the driver to respond as prescribed by SP 3.10 (iii)	
ii. When the driving automation system is engaged it shall operate in such a way that, if a vehicle failure occurs that impacts longitudinal and/or lateral vehicle dynamics, systems shall continue to stabilize the vehicle's path within the given physical and technical limits in order to allow the driver to react as prescribed by SP 3.10 (i)	
Safety Principle 3.9 Before exiting the operational design domain, upon occurrence of a driving automation system failure that prevents performance of the DDT, the driving automation system shall request the driver to take control i. Verified driver control inputs shall cause transition from Level 3 into a lower level of automation	
ii. The driving automation system shall maintain an operating condition that affords a controlled transition to driver control, regardless of whether the transition is prompted by fault within the driving automation system, or prompted by violation of the intended operational design domain	
Safety Principle 3.10 The driver must understand the following: i. The driver's role is to determine if there has been a vehicle failure that may impact the safe operation of the vehicle, and to take over control of the vehicle when such a failure occurs	
ii. In response to a driver request to take over performance of the DDT, the primary response from the driving automation system is to transition out of Level 3 automation and into a lower driving automation level	
iii. When the driving automation system is requesting the driver to take control of the vehicle, the driver's role is to respond by taking over control	
iv. After requesting the driver to take control, the driving automation system will remain in control for a limited time period	

LEVEL 4 Safety Principle Criteria	Assessment
Safety Principle 4.1 i. The vehicle operator shall ensure vehicle operational readiness before engaging the driving automation system	

Safety Principle 4.2 When activated, the driving automation system shall perform the DDT and fallback as needed within its application-specific operational design domain, providing the appropriate responses to relevant objects and events. This includes but is not limited to: i. Continuous assessment of operation within actual vs. operational design domain	
ii. Prohibiting entry into automated driving when the operational domain is not achieved	
iii. Ability to achieve minimal risk condition if necessary due to any one of the following: a. Operator failure to respond appropriately to pending exit of operational design domain b. A failure that prevents performance of the complete DDT	
Safety Principle 4.3 i. The driving automation system may delay its response to operator take-over requests, and/or operator requests to stop driving automation when necessary to avoid causing a hazard	
Safety Principle 4.4 i. The driving automation system must not engage unless activated by the operator	

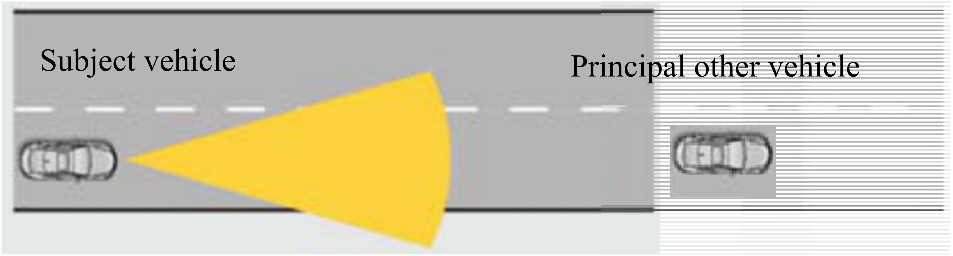
LEVEL 5 Safety Principle Criteria	Assessment
Safety Principle 5.1 i. The vehicle operator shall ensure vehicle operational readiness before engaging driving automation.	
Safety Principle 5.2 The vehicle system overall (including the driving automation system and its integration) shall be designed such that the driving automation system is capable of performing the DDT and fallback as needed, including: i. Providing appropriate responses to relevant objects and events	
ii. Ability to achieve a minimal risk condition if necessary due to a failure that prevents performance of the complete DDT	
Safety Principle 5.3 i. The driving automation system may delay response to operator requests to take over, and/or operator requests to stop driving automation when necessary to avoid causing a hazard	
Safety Principle 5.4 i. The driving automation system must not engage unless activated by the operator	

Appendix M: GloCo High Speed Adaptive Cruise Driving Automation System Safety Principle Assessment

Operation Scenarios:

- Existence of controls
- Visibility to perform object and event detection and response
- System disengagement
- Longitudinal override
- Lateral override

Initial Scenario Conditions:



Initial Scenario Conditions	Values
Vehicle placement	Test Case 3 – Subject vehicle 300 ft behind principal other vehicle, in same lane
Initial speeds	70 mph
Vehicle spacing	Test Case 3 – Subject vehicle 300 ft behind principal other vehicle, in same lane
Vehicle orientation	Forward

Performance Criteria:

	Safety Principle	**Test Cases**
Explanation of how driver ensures vehicle operational readiness	2.1(i)	Confirm explanation exists in owner's manual
Explanation of driver's role in completing OEDR	2.1(ii)	Confirm explanation exists in owner's manual
Visibility to perform OEDR	2.2 (i)	1
System Disengagement	2.2 (ii)	2a, 2b
Take full control	2.3	3

Test Cases:

#	Criteria	Procedure
1	External Environment Visible	Verify system disengaged
		Verify visibility of external environment
		Driver pulls "Rock" lever to engage system
		Verify visibility of external environment unchanged
2a	Verify System Disengaged	Driver pulls "Rock" lever to engage system
		Verify system engaged
		Driver pulls emergency brake lever while turning steering wheel at least 5 degrees with a rate of at least 5 degrees/sec
		Verify system disengaged
2b	Verify System Disengaged	Driver pulls "Rock" lever to engage system
		Verify system engaged
		Driver pushes "Rock" lever while braking to at least 20% pedal
		Verify system disengaged
3	Verify System Disengaged	Driver pulls "Rock" lever to engage system
		Verify system engaged
		Driver simultaneously uses throttle pedal to accelerate vehicle and twists "Roll" knob to move one lane to adjacent lane
		Verify system disengaged

Appendix N: Acme High Speed Adaptive Cruise Driving Automation System Classification and Operational Description

1. Vehicle:

Year:	2020
Make:	Acme
Model:	NuCar

2. Name of Driving Automation System:

Set-U-Strayt

3. Description of Driving Automation System Operating Principles:

Please provide a brief summary related to the following information and/or the appropriate section and page in the owner's manual

4. Description of Design Intent Use of the Driving Automation System:

Design Detail:	**Description from Owner's Manual:**	**Page Reference**
Type of control provided by the system	Under certain conditions, the Set-U-Strayt system can simultaneously maintain steering within a lane and speed/headway to a preceding vehicle	X, X
Driver's role in detecting objects and/or events in the environment and a related response	Because the Set-U-Strayt system cannot operate under every possible condition, the driver must always be prepared take full control of the vehicle and perform the appropriate response to minimize exposure to potentially hazardous situations	X, X
Driver's role during abnormal operation	If the "CHECK S-U-S" light appears in the instrument panel, there may be a problem with the Set-U-Strayt system. If the light appears, do not use the system and take the vehicle to a dealer to have the system checked	X, X

Operational domain limitations	The Set-U-Strayt system is designed to operate when all the following conditions exist simultaneously: - traveling on limited access freeways, and - speed is between 45 and 60 mph, and - no other vehicles are in front of you in the same lane	X, X

5. Description of Operation:

Operational Detail:	**Description from Owner's Manual:**	**Page Reference**
How to turn the driving automation system on and off	Turning system on: - push "S-U-S On/Off" button (light on button turns on), - then push "Set S-U-S" button Turning system off: - push "S-U-S On/Off" button (light on button turns off)	X, X
Relevant driver interface telltales, displays, sounds, and haptic cues for the system	While the Set-U-Strayt system is on, engaged and operating properly, the message "Set-U-Strayt ENGAGED" is projected in green briefly on the lower left area of the windshield. While engaged, when the Set-U-Strayt system encounters conditions under which it cannot operate properly, the message "Set-U-Strayt DISENGAGED" is projected in red on the lower left area of the windshield and a verbal message will be broadcast through the speakers. When this occurs, the driver must take full control of the vehicle.	X, X

Insert here copies of relevant pages from owner's manual

6. Driving Automation System Level Determination:

According to industry understanding of automation levels and classification standards answer the following. Beginning with Q1, answer questions in sequence and use the "Level determination" section to determine the automation level or proceed to the next question.

#	Question	Y/N	Level determination	
Q1	Does the feature perform sustained control of lateral **or** longitudinal motion?	Y	If **Yes**, go to Q2	If **No**, feature is **Level 0, end**
Q2	Does the feature perform both sustained longitudinal **and** sustained lateral control?	Y	If **Yes**, go to Q3	If **No**, feature is **Level 1, end**
Q3	Does the feature require supervision by the driver during its normal operation?	Y	If **Yes**, feature is **Level 2, end**	If **No**, go to Q4
Q4	Does the feature rely on the driver to take over if it is not operating normally?	-	If **Yes**, feature is **Level 3, end**	If **No**, go to Q5
Q5	Does the feature have a limited scope of operation?	-	If **Yes**, feature is **Level 4**	If **No**, feature is **Level 5**

- Based on the above answers, what is the driving automation system classification level (0-5)?

2

NOTE: Only Level 2 and above driving automation systems are within the scope of this Classification and Operational Description and should continue with the remainder of this form.

7. Following the Driving Automation System Classification Level, reference the accompanying Safety Principle tables below.

LEVEL 2 Safety Principle Criteria	Assessment
Safety Principle 2.1 For Level 2 driving automation, avoidance of hazards depends on the vehicle driver properly using the vehicle and automation, which includes: i. Driver ensuring the vehicle operational readiness before engaging driving automation features	
ii. Driver completing the Object and Event Detection Response (OEDR) subtask in order to complete the DDT, by providing the appropriate responses to all relevant objects and events, in cases when the driving automation does not provide the appropriate response to avoid hazards	
Safety Principle 2.2 The driving automation system shall be integrated with the vehicle in a manner that does not inhibit the driver's ability to perform the DDT, which includes: i. Control of the vehicle, lateral and longitudinal	
ii. OEDR	
Safety Principle 2.3 i. The driving automation system shall prioritize predefined driver inputs for full control over driving automation commands	

LEVEL 3 Safety Principle Criteria	Assessment
Safety Principle 3.1 i. The driver shall ensure operational readiness before engaging driving automation feature	
Safety Principle 3.2 The driving automation system shall be integrated with the vehicle in a manner that does not inhibit the driver's ability to perform the DDT, which includes: i. Control of the vehicle, lateral and longitudinal	
ii. OEDR	
Safety Principle 3.3 i. The driving automation system shall prioritize predefined driver inputs for full control over driving automation commands.	
Safety Principle 3.4 i. The driving automation system must not engage unless activated by the driver. After initially being activated, the automation can automatically resume if appropriate and within the same drive cycle. As a default, automation is not activated at the beginning of each drive cycle.	
Safety Principle 3.5 i. The driving automation system shall provide persistent indication to the driver that signifies when a vehicle is operating in high automation state, i.e., at Level 3 or higher.	

Safety Principle 3.6 i. The driving automation system shall provide indication to the driver upon any request to transition from Level 3 to a lower level (2, 1, or 0).	
Safety Principle 3.7 When activated, the driving automation system shall perform the DDT within its application-specific operational design domain, including providing the appropriate responses to relevant objects and events. This includes but is not limited to: i. Continuous assessment of operation within actual vs. operational design domain	
ii. Inhibit operation when operational design domain is not achieved	
Safety Principle 3.8 i. The driving automation system shall be designed in such a way that a failure in the driving automation system does not lead to an immediate loss of the longitudinal and/or lateral control in order to allow the driver to respond as prescribed by SP 3.10 (iii)	
ii. When the driving automation system is engaged it shall operate in such a way that, if a vehicle failure occurs that impacts longitudinal and/or lateral vehicle dynamics, systems shall continue to stabilize the vehicle's path within the given physical and technical limits in order to allow the driver to react as prescribed by SP 3.10 (i)	
Safety Principle 3.9 Before exiting the operational design domain, upon occurrence of a driving automation system failure that prevents performance of the DDT, the driving automation system shall request the driver to take control i. Verified driver control inputs shall cause transition from Level 3 into a lower level of automation	
ii. The driving automation system shall maintain an operating condition that affords a controlled transition to driver control, regardless of whether the transition is prompted by fault within the driving automation system, or prompted by violation of the intended operational design domain	
Safety Principle 3.10 The driver must understand the following: i. The driver's role is to determine if there has been a vehicle failure that may impact the safe operation of the vehicle, and to take over control of the vehicle when such a failure occurs	
ii. In response to a driver request to take over performance of the DDT, the primary response from the driving automation system is to transition out of Level 3 automation and into a lower driving automation level	
iii. When the driving automation system is requesting the driver to take control of the vehicle, the driver's role is to respond by taking over control	
iv. After requesting the driver to take control, the driving automation system will remain in control for a limited time period	

LEVEL 4 Safety Principle Criteria	Assessment
Safety Principle 4.1 i. The vehicle operator shall ensure vehicle operational readiness before engaging the driving automation system	
Safety Principle 4.2 When activated, the driving automation system shall perform the DDT and fallback as needed within its application-specific operational design domain, providing the appropriate responses to relevant objects and events. This includes but is not limited to: i. Continuous assessment of operation within actual vs. operational design domain	
ii. Prohibiting entry into automated driving when the operational domain is not achieved	
iii. Ability to achieve minimal risk condition if necessary due to any one of the following: a. Operator failure to respond appropriately to pending exit of operational design domain b. A failure that prevents performance of the complete DDT	
Safety Principle 4.3 i. The driving automation system may delay its response to operator take-over requests, and/or operator requests to stop driving automation when necessary to avoid causing a hazard.	
Safety Principle 4.4 i. The driving automation system must not engage unless activated by the operator	

LEVEL 5 Safety Principle Criteria	Assessment
Safety Principle 5.1 i. The vehicle operator shall ensure vehicle operational readiness before engaging driving automation	
Safety Principle 5.2 The vehicle system overall (including the driving automation system and its integration) shall be designed such that the driving automation system is capable of performing the DDT and fallback as needed, including: i. Providing appropriate responses to relevant objects and events	
ii. Ability to achieve a minimal risk condition if necessary due to a failure that prevents performance of the complete DDT	
Safety Principle 5.3 i. The driving automation system may delay response to operator requests to take over, and/or operator requests to stop driving automation when necessary to avoid causing a hazard	

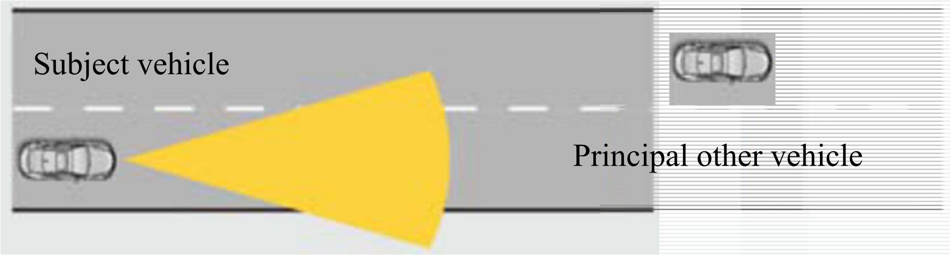
Safety Principle 5.4 i. The driving automation system must not engage unless activated by the operator	

Appendix O: Acme High Speed Adaptive Cruise Driving Automation System Safety Principle Assessment

Operation Scenarios:

- Existence of controls
- Visibility to perform object and event detection and response
- System disengagement
- Longitudinal override
- Lateral override

Initial Scenario Conditions:



Initial Scenario Conditions	Values
Vehicle placement	Test Case 3 – Subject vehicle 200 ft behind principal other vehicle, in adjacent lane
Initial speeds	55 mph
Vehicle spacing	Test Case 3 – Subject vehicle 200 ft behind principal other vehicle, in adjacent lane
Vehicle orientation	Forward

Performance Criteria:

	Safety Principle	Test Cases
Explanation of how driver ensures vehicle operational readiness	2.1(i)	Confirm explanation exists in owner's manual
Explanation of driver's	2.1(ii)	Confirm explanation exists in

role in completing OEDR		owner’s manual
Visibility to perform OEDR	2.2 (i)	1
System Disengagement	2.2 (ii)	2a, 2b
Take full control	2.3	3

Test Cases:

#	Criteria	Procedure
1	External Environment Visible	Verify Set-U-Strayt system is disengaged
		Verify visibility of external environment
		Driver pushes “S-U-S On/Off” button then pushes “Set S-U-S” button to engage system
		Verify visibility of external environment unchanged
2a	Verify System Disengaged	Driver pushes “S-U-S On/Off” button then pushes “Set S-U-S” button to engage system
		Verify system engaged
		Driver applies at least 3 pounds of force to brake pedal while turning steering wheel at least 5 degrees with a rate of at least 5 degrees/sec
		Verify system disengaged
2b	Verify System Disengaged	Driver pushes “S-U-S On/Off” button then pushes “Set S-U-S” button to engage system
		Verify system engaged
		Driver pushes “S-U-S On/Off” button
		Verify system disengaged
3	Verify System Disengaged	Driver pushes “S-U-S On/Off” button then pushes “Set S-U-S” button to engage system
		Verify system engaged
		Driver uses throttle pedal to accelerate and turns steering wheel to maneuver vehicle into adjacent lane, then turns steering wheel to return to original lane
		Verify system disengaged

Appendix P: Reccomendations for Follow On Proposal: Safety Principles on the Driver - Human Factors Research

The CAMP AVR consortium determined in the course of the first AVR project that, in Level 2 and Level 3 driving automation systems, there are a significant number and scope of safety principles that apply to the driver, not the automation or the vehicle. However, it is not clear that a naïve driver will have adequate awareness, desire, or capability to fulfill those principles in foreseeable situations when using these systems (though they may develop such capabilities with automated driving experience). Therefore, CAMP AVR consortium proposes to have Human Factors research conducted towards:

- Identifying the likelihood and the manner in which drivers may not comply with the Safety Principles in Level 2 and Level 3 Driving Automation System usages (i.e., analysis of 'things gone wrong')
- Identifying the likelihood and manner in which drivers will likely comply with the Safety Principles in Level 2 and Level 3 Driving Automation System usages (analysis of 'things gone right')
- Developing Human Machine Interface (HMI) design guidelines intended to support drivers in complying with the relevant Safety Principles for the system they are utilizing
- Providing measurements of the effectiveness of the HMI design guidelines developed

The consortium proposes to utilize Human Factors research institution(s) already selected by NHTSA for research in the area of Human Factors of Driving Automation, notably through their IDIQ for the same topic: Battelle, VTTI, and/or UMTRI. The consortium also proposes to re-open consortium membership to any interested OEMs in the United States.

The consortium expects that, given the extent and scope of the issues, the necessity in many cases for in-vehicle research, and the extended time element associated with certain potential behavioral issues, that this effort will be resource intensive, both in time as well as in expense. The consortium expects that the project would be multi-year (3-5 years) and require $5-$7 Million. These figures are comparable to past research efforts. For example, the HF4LAADS effort was 3 years and approximately $7 Million, and was scoped to only the first issue for Level 2 systems below (and only began the exploratory process for that issue).

Below, for reference, is material from the CAMP AVR project that makes a preliminary identification of Human Factors research issues associated with the Safety Principles that apply to the driver in Level 2 and Level 3 Driving Automation Systems. Note that some of these issues, and any HMI design guidelines that develop associated with the issues, may be related to training systems rather than in-vehicle systems.

Human Factors Research:

Several aspects of the Safety Principles (SP) and associated notes would benefit from Human Factors research. In particular:

For Level 2 Driving Automation Systems:

(SP2.1) ii. For Level 2 driving automation, avoidance of hazards depends on the driver properly using the vehicle and automation, which includes completing the Object and Event Detection and Response (OEDR) subtask in order to complete the Dynamic Driving Task (DDT), by providing the appropriate responses to relevant objects and events, in cases when the driving automation does not.

Thus the driver must understand these concepts in an L2 system:

- It is their role to detect and respond appropriately to all situationally relevant objects and events (OEDR) where the automation does not
- That the automation is designed such that driver attempts to take full control will be honored, and the vehicle will respond (see SP 2.3)

Research could be conducted (i.e. Task 8, transfer to other projects) to investigate:

- To what extent these concepts are already present as driver mental models (intuitive) in L2 executions (examples of “things gone right”)
- How such ‘smart’ intuition is developed (e.g., deliberate exploratory driver behaviors to test system boundaries or operation and that should not be construed as driver lack of understanding) and how this intuition is activated (e.g., cues that indicate a need or desire to resume manual control)
- HMI elements that could create affordances to support these driver mental models (and their effectiveness over time, especially as the automation demonstrates its ability)
- Educational approaches (e.g. training, owner’s manual text, advertising) to support the driver’s understanding of these concepts in L2 systems
- Methodologies to evaluate the driver’s understanding of these concepts in the context of a Level 2 automation equipped vehicle

For Level 3 Driving Automation Systems:

(SP 3.5) The driving automation system shall provide persistent indication to the driver that signifies when a vehicle is operating in high automation state; i.e., at Level 3 or higher.

- Research could be conducted to develop testing methodologies intended to assure that this indication is salient and understandable

- Research should be conducted to understand how drivers make use of such persistent indications over time and in light of growing experience that the automation is competent in a variety of driving conditions

(SP 3.6) The driving automation system shall provide indication to the driver upon any request to transition from Level 3 to a lower level (2, 1, or 0).

- Research could be conducted to develop testing methodologies and verify driver performance with the dynamic driving task following such an indication in a relevant context
- Research into defining the manner of transition (e.g., all-or-nothing handoff vs. graded handoff and what “graded handoff” might mean)

(SP 3.9) ii. The driving automation system shall maintain an operating condition that affords a reasonable transition to driver control, regardless of whether the transition is prompted by a driving automation system failure occurrence (which may require the soonest possible driver intervention), or prompted by violation of the intended design domain (which may provide a longer time horizon in which to alert the driver).

- Research could be conducted to determine the range and factors that affect “suitable transition times” wherein the driver is expected to be able to take control of the vehicle.
- Research into the salience of conditions in which automation might not be available by policy (e.g., road type, inclement weather, degraded roadways, toll plazas, work zones, etc.)

(SP 3.10) The driver must understand the following:

- i. The driver’s role is to determine if there has been a vehicle failure which impacts safe operation, and to take over control of the vehicle when such a vehicle failure occurs.
- ii. In response to a driver’s request to take over performance of the Dynamic Driving Task, the primary response from the driving automation system is to transition out of Level 3 automation and into a lower driving automation level.
- iii. When the driving automation system is requesting the driver to take control of the vehicle, the driver’s role is to respond by taking over control.
- iv. After requesting the driver to take control, the driving automation system will only remain in control for limited time period.

Research could be conducted to investigate:

- To what extent these concepts are already present as driver mental models (intuitive)
- The extent to which a particular vehicle failure can be detected by the driver, regardless of automation state, and the driver’s ability to control the vehicle in the face of that vehicle failure;
- HMI elements that could create affordances to support these driver mental models
- Educational approaches to support these concepts

- Methodologies to evaluate driver’s understanding of these concepts in the context of a Level 3 automation equipped vehicle

Note on Level 4: There may be human factors considerations in systems where both Level 3 and Level 4 capability coexist in the same vehicle. Level 3 requires the driver to understand that a driver direct control input will generally transition automation immediately into lower automation modes and driver control; whereas Level 4 automation may delay a response to operator input if hazards are present. These are very different responses to driver/operator inputs, and the dissonance between them may pose significant human factors considerations to vehicles containing both Level 3 and Level 4 automation capability.

- Research could be conducted to determine driver/operator performance with an indication to the driver/operator upon any transition from Level 3 versus 4 to a lower level (2,1, or 0), such that the driver/operator is enabled to achieve effective driver/operator performance with the DDT at the lower level; and where such transition may be temporarily prevented for the operator in a Level 4 system.

Glossary of Selected Terms

Driver	The person tasked with carrying out the performance of part or all of the DDT.
Driver Role	The portions of the DDT that the driver performs during operation of the vehicle.
Driving Automation System	A machine system or host of such systems that can carry out some or all portions of the DDT on a sustained basis.
Driving Environment	Conditions and surroundings intended for the legal operation of a motor vehicle on public and/or private roads.
Dynamic Driving Task (DDT)	The task of driving can be divided into three types of activities (Michon, 1985): • Operational behaviors such as longitudinal and lateral control as well as OEDR • Tactical behaviors such as speed selection, lane selection, object and event response selection, and maneuver planning • Strategic behaviors including destination planning and route planning Within the overall task of driving, the operational and tactical behaviors relate directly to the dynamic aspects of driving and are referred to as the dynamic driving task, or DDT (for further definition see SAE J3016:2014).
Higher Driving Automation (System)	A machine system or host of such systems that can carry out **all** portions of the DDT, whether on a part-time and/or limited basis, or on a full-time and unlimited basis. This term corresponds directly with the term “Automated Driving System” as defined by SAE J3016 (2014), and as such includes only Level 3, 4, and/or 5 in the driving automation taxonomy.
Lower Driving Automation (System)	A machine system or host of such systems that can carry out only **some** portions of the DDT on a part-time and/or limited basis. This term includes only Level 1 and/or 2 in the driving automation taxonomy.
Minimal Risk Condition	SAE J3016 definition: A low risk *motor vehicle* operating condition to which an *automated driving system* automatically resorts upon either a system failure or a failure of a *human driver* to respond appropriately to a request to take over the *dynamic driving task.*

No Driving Automation	A machine system or host of such systems that is not capable of performing any portion of the DDT on a sustained basis. This term refers to Level 0 in the driving automation taxonomy.
Object and Event Detection and Response (OEDR)	The subtask of the DDT allocated to either a driver/operator or to a driving automation system to both detect any circumstance situationally-relevant to the immediate DDT and to react with the appropriate action as required.
Operational Design Domain (ODD)	The specific operating conditions (e.g., geographic, weather, time of day, road type) under which a given driving automation system, or feature thereof, is designed to function.
Supervision	Anticipation, identification, and mitigation by a human driver of undesired actions by a Level 1 or Level 2 driving automation system
Sustained (Operation)	DDT performance (partial or complete) by a driving automation system that persists between and across external driving events, which necessitate appropriate responses, and thus entail system control to external objects and events.
System Role	The portions of the DDT that the system performs during operation of the vehicle.