U.S. Department of Transportation

National Highway Traffic Safety Administration

NHTSA

DOT HS 812 572 **August 2018**

Functional Safety Assessment Of a Generic Automated Lane Centering System and Related Foundational Vehicle Systems

Samsara EX1043
Samsara v. Motive Tech. Inc.
IPR2026-00034

Disclaimer

This document is disseminated under the sponsorship of the U.S. Department of Transportation, National Highway Traffic Safety Administration, 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 Department of Transportation or the National Highway Traffic Safety Administration. The U.S. Government assumes no liability for use of the information contained in this document.

This report does not constitute a standard, specification, or regulation.

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

Suggested APA Format Citation:

Brewer, J., Becker, C., Yount, L., & Pollard, J. (2018, August). *Functional safety assessment of a generic automated lane centering system and related foundational vehicle systems* (Report No. DOT HS 812 572). Washington, DC: National Highway Traffic Safety Administration.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No.0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	August 2018	September 2014 – January 2017

4. TITLE AND SUBTITLE Functional Safety Assessment of a Generic Automated Lane Centering System and Related Foundational Vehicle Systems	5. FUNDING NUMBERS Intra-Agency Agreement DTNH22-14-V-00136 51HS6CA100 and 51HS6CA200
6. AUTHORS John Brewer, Christopher Becker, Larry Yount, John Pollard	
7. PERFORMING ORGANIZATION NAME AND ADDRESS U.S. Department of Transportation Office of the Assistant Secretary for Research and Technology John A. Volpe National Transportation Systems Center Cambridge, MA 02142	8. PERFORMING ORGANIZATION REPORT NUMBER DOT-VNTSC-NHTSA-17-01
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) National Highway Traffic Safety Administration 1200 New Jersey Avenue SE Washington, DC 20590	10. SPONSORING/MONITORING AGENCY REPORT NUMBER DOT HS 812 572
11. SUPPLEMENTARY NOTES Paul Rau was the Contracting Officer's Representative.	
12a. DISTRIBUTION/AVAILABILITY STATEMENT This document is available to the public through the National Technical Information Service, www.ntis.gov.	12b. DISTRIBUTION CODE

13. ABSTRACT

This report describes research to assess the functional safety of a generic automated lane centering (ALC) system and three related foundational systems -- electric power steering (EPS), steer-by-wire (SbW), and conventional hydraulic braking (CHB). ALC systems are a key technology that supports vehicle automation by providing continuous lateral control to keep the vehicle within the travel lane. The studies of these systems follow the Concept Phase process in the ISO 26262 standard and applies Hazard and Operability study, functional failure mode effects analysis, and system-theoretic process analysis methods. The results of the individual analyses, including vehicle-level hazards, functional safety concepts, functional safety requirements (an output of the ISO 26262 process), and test scenarios, are contained in individual reports. This synthesis report examines the implications of analyzing foundational systems in the traditional non-automated case ("Automation Level 0") and how results might need to be modified for a foundational system that acts as an actuator for a highly-automated driving system. It also describes human factors implications of an operator being not engaged as a possible foreseeable misuse case, particularly in SAE Automation Level 2. Finally, it defines architectural options and notes that some hazards can have different ASIL levels depending on the malfunction and/or the automation level.

14. SUBJECT TERMS Automated lane centering, ALC, hazard and operability study, HAZOP, failure modes and effects analysis, FMEA, system-theoretic process analysis, STPA, ISO 26262, hazard analysis, risk assessment, HARA, and functional safety requirements, automated driving system, electric power steering, EPS, steer-by-wire, SbW, conventional hydraulic braking, CHB, Automotive Safety Integrity Level, ASIL	15. NUMBER OF PAGES 95 16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	

Foreword

NHTSA's Automotive Electronics Reliability Research Program

The mission of the National Highway Traffic Safety Administration is to save lives, prevent injuries, and reduce economic costs due to road traffic crashes. As part of this mission, NHTSA researches methods to ensure the safety and reliability of emerging safety-critical electronic control systems in motor vehicles. The electronics reliability research area focuses on the body of methodologies, processes, best practices, and industry standards that are applied to ensure the safe operation and resilience of vehicular systems. More specifically, this research area studies the mitigation and safe management of electronic control system failures and making operator response errors less likely.

NHTSA has established five research goals for the electronics reliability research program to ensure the safe operation of motor vehicles equipped with advanced electronic control systems. This program covers various safety-critical applications deployed on current generation vehicles, as well as those envisioned on future vehicles that may feature more advanced forms of automation and connectivity. These goals are:

1. Expand the knowledge base to establish comprehensive research plans for automotive electronics reliability and develop enabling tools for applied research in this area;
2. Strengthen and facilitate the implementation of safety-effective voluntary industry-based standards for automotive electronics reliability;
3. Foster the development of new system solutions for ensuring and improving automotive electronics reliability;
4. Research the feasibility of developing potential minimum vehicle safety requirements pertaining to the safe operation of automotive electronic control systems; and
5. Gather foundational research data and facts to inform potential future NHTSA policy and regulatory decision activities.

This Report

This publication is part of a series of reports that describe NHTSA's initial work in the automotive electronics reliability program. This research project specifically supports the first, second, fourth, and fifth goals of NHTSA's electronics reliability research program by gaining understanding of both the functional safety requirements (one output of the ISO 26262 process [14]) for automated lane centering (ALC) control systems and related foundational systems, and how the International Organization for Standardization's ISO 26262 industry standard may enhance safety. The analysis described in this report follows the Concept Phase of the ISO 26262 standard.

TABLE OF CONTENTS

EXECUTIVE SUMMARY ix
A. Introduction 1
A.1 Research Objectives 1
A.2 Levels of Automation 2
A.3 Full Functional Safety Analysis Reports 2
A.4 System Description 3
A.4.1 Automated Lane Centering 3
A.4.2 Foundational Systems 3
A.5 Human Factors Considerations for Automated Systems 5
A.6 Report Outline 5
B. Analysis Approach 7
B.1 Basis for the Analytical Process 7
B.2 Current Safety Issues 9
B.3 Hazard Analysis and Risk Assessment 10
B.3.1 Hazard and Safety Analysis Methods 10
B.3.2 ASIL Risk Assessment 14
B.4 Safety Goals 21
B.5 Functional Safety Concept 21
B.5.1 Safety Analysis 22
B.5.2 Safety Strategies 22
B.5.3 Example Safe States 24
B.5.4 Example Driver Warning Strategies 24
B.5.5 Application of the Functional Safety Concept 25
B.6 Example Test Scenarios 25
C. Fault Tolerant Architectures 27
C.1 Fail-Safe/Fail-Passive 27
C.2 Fail-Operational 28

C.3 Implications for Architecture of Relationship Between Actuating Foundational Systems and Control Systems 29
C.4 Practical Aspects of Architectural Strategies 30
D. Systems Analyses and Results 31
D.1 System Definition 31
D.2 Vehicle Level Hazard Analysis 36
D.3 Risk Assessment 38
D.4 Vehicle-Level Safety Goals 40
D.5 Functional Safety Concept 42
D.5.1 Safe States 42
D.5.2 Architectural Strategies for ALC Systems 47
D.6 Additional Human Factors Considerations 48
D.6.1 Possible Countermeasures to Reduce Operator Disengagement 48
D.6.2 DVI Considerations 49
D.6.3 Opportunities for Effective Mode Transition 53
E. Observations 55
E.1 Findings from Synthesis of ALC and Related Foundational System Studies 55
E.2 Considerations for the Interaction between Foundational and Automated Systems 55
E.3 Challenges in Applying ASIL Process Across Automation Levels 56
F. Summary and Conclusions 57
APPENDIX: Analysis of Current Safety Issues A-1
General Estimates System and Fatality Analysis Reporting System A-1
NHTSA Motor Vehicle Recall Campaigns A-5
NHTSA Vehicle Owners' Questionnaires A-9

LIST OF FIGURES

Figure 1. Safety Analysis and Requirements Development Process 8
Figure 2. HAZOP Study Process 10
Figure 3. STPA Process 12
Figure 4. Guidewords for UCAs 14
Figure 5. Depiction of Yerkes-Dodson Law From Diamond et al. 19
Figure 6. Functional Safety Concept Process 22
Figure 7. Example Fail-Safe Concepts Illustrated With Some ALC System Components 27
Figure 8. Example Fail-Operational Concepts Illustrated With Some ALC System Components 29
Figure 9. Block Diagram of a Generic ALC System 32
Figure 10. Block Diagram of a Generic EPS System With Active Steering and 4WS Features .. 33
Figure 11. Block Diagram of a Generic SbW System With Active Steering and 4WS Features . 34
Figure 12. Block Diagram of a Generic Conventional Hydraulic Braking System With ABS, TCS, and ESC Features 35
Figure 13: Unsafe Control Action Breakdown of EPS Recalls A-7
Figure 14: Unsafe Control Action Breakdown of Conventional Brake System Recalls A-8
Figure 15: Causal Factor Breakdown of EPS Recalls A-8
Figure 16: Causal Factor Breakdown of Conventional Brake System Recalls A-9
Figure 17: Unsafe Control Action Breakdown of EPS VOQs A-12
Figure 18: Unsafe Control Action Breakdown of SbW VOQs A-12
Figure 19: Unsafe Control Action Breakdown of Conventional Brake System VOQs A-13
Figure 20: Unsafe Control Action Breakdown of ALC/LKA VOQs A-14
Figure 21: Causal Factor Breakdown of EPS VOQs A-15
Figure 22: Causal Factor Breakdown of SbW VOQs A-16
Figure 23: Causal Factor Breakdown of Conventional Brake System VOQs A-17
Figure 24: Causal Factor Breakdown of ALC/LKA VOQs A-18

LIST OF TABLES

Table 1. Levels of Automation 2
Table 2. Key Human Factors Findings 5
Table 3. Exposure Assessment 15
Table 4. Severity Assessment 15
Table 5. Example Method for Assessing Severity 16
Table 6. Controllability Assessment 16
Table 7. ASIL Assessment 17
Table 8. Number of Operational Scenarios by System 18
Table 9. Automation Levels Considered for ASIL Assessment of the ALC System 21
Table 10. Synthesized List of Potential Vehicle-Level Hazards 36
Table 11. Potential Vehicle-Level Hazards by System 37

Table 12. Assigned ASIL for Potential Vehicle-Level Hazards for Foundational Systems..... 39
Table 13. Assigned ASIL for Potential Vehicle-Level Hazards for ALC System by Automation Level 40
Table 14. Safety Goals for the EPS System..... 40
Table 15. Safety Goals for the SbW System..... 41
Table 16. Safety Goals for the CHB System 41
Table 17. Safety Goals for the ALC System..... 42
Table 18. Possible EPS System Safe States..... 43
Table 19. Possible SbW System Safe States..... 44
Table 20. Possible CHB System Safe States 45
Table 21. Possible ALC System Safe States..... 47
Table 22. Example Allocation of Architectural Strategies to Levels of Automation..... 48
Table 23. Example Allocation of Architectural Strategies to Levels of Automation..... 58
Table 24: Percentage of Braking and Steering-Related Crashes A-2
Table 25: GES and FARS Crash Types for Braking and Steering System-Related Issues A-3
Table 26: Mapping Between GES/FARS Crash Types, Preliminary Hazards, and Potential Contributing Systems..... A-4
Table 27: List of OEMs Included in the VOQ Review A-11

LIST OF ACRONYMS

ABS	antilock braking system
ACC	adaptive cruise control
ACSF	automatically commanded steering function
AIS	Abbreviated Injury Scale
ALC	automated lane centering
ASIL	Automotive Safety Integrity Level
CAN	controller area network
CF	causal factor
CHB	conventional hydraulic braking
CMA	common mode analysis
DTC	Diagnostic Trouble Code
DVI	driver-vehicle interface
EPS	electric power steering
ESC	electronic stability control
FARS	Fatality Analysis Reporting System
FMEA	failure mode effects analysis[1]
FMVSS	Federal Motor Vehicle Safety Standard
FTTI	fault tolerant time interval
GES	General Estimates System
GPS	global positioning system
HARA	Hazard Analysis and Risk Assessment
HAZOP	Hazard and Operability Study
I/O	input/output
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
LDW	lane departure warning
LKA	lane keep assist
ms	millisecond
QM	quality management

[1] Editor's Note: The term "Failure Mode Effects Analysis," FMEA, was coined by the Department of Defense in 1949 in a military standard called MIL-P-1629, which later morphed into MIL-STD-1629 and its amended forms, cited in this report. Over the years, the term itself has changed, sometimes using "Modes," plural, instead of "Mode," and sometimes inserting the word "and," to Failure Mode *and* Effects Analysis. It is clear in the original that the term means the effects of a failure mode, not a failure mode or modes AND effects thereof. As such, the term must remain unitary as "failure mode effects," and the totality as an analysis of those effects. Thus, NHTSA prefers to use "failure mode effects analysis" as it preferred term in respect to father and son, MIL-P-1629 and MIL-STD-1629, without necessarily asserting that other forms of the term are "wrong." Variant terms are left as they are when quoting or citing a source, but are changed or "corrected" as well as lowercased (because it is a generic form of analysis) in text.

SAE	SAE International, formerly the Society of Automotive Engineers
SbW	steer-by-wire
SG	safety goal
STPA	system-theoretic process analysis
TBD	to be determined
TCS	traction control system
TJA	traffic jam assist
UCA	unsafe control action
UNECE	United Nations Economic Commission for Europe
Volpe	Volpe National Transportation Systems Center
VOQ	Vehicle Owner Questionnaire

EXECUTIVE SUMMARY

As advanced driver assistance systems and other automated technologies are introduced into the nation's fleet, the safety of these systems will depend in part on the functional safety of their underlying foundational vehicle systems. While emerging technologies may be designed in accordance with the ISO 26262 functional safety standard, many foundational systems currently deployed are legacy systems that predate ISO 26262 [14].

This report describes research by the Volpe National Transportation Systems Center, supported by National Highway Traffic Safety Administration, to conduct functional safety assessments of a generic automated lane centering system and three key foundational systems: electric power steering, steer-by-wire, and conventional hydraulic braking. ALC is a key technology that supports vehicle automation by providing continuous lateral control to keep the vehicle within the travel lane. Combining an ALC system with a longitudinal control system, such as adaptive cruise control, allows the driver to cede execution of steering, acceleration, and deceleration tasks to the vehicle. However, depending on the level of automation, the driver may still be responsible for other elements of the driving task, such as monitoring the roadway environment.

The primary purpose of this project is to analyze the potential hazards that could result from cases of electrical or electronic failures impacting the functions of vehicular control systems. The studies followed the ISO 26262 process to identify the integrity requirements of these functions at the concept level, independent of implementation variations. This project also considered potential causes that could lead to such functional failures and documents the technical requirements the ISO 26262 process suggests with respect to the identified Automotive Safety Integrity Level (ASIL) of the item under consideration. While this work does not go into implementation strategies to achieve these ASILs, the ISO 26262 process provides a flexible framework and explicit guidance for manufacturers to pursue different methods and approaches to do so. Manufacturers employ a variety of techniques, such as ASIL decompositions, driver warnings, fault detection mechanisms, plausibility checks, redundancies, etc., to achieve the necessary ASILs that effectively mitigate the underlying safety risks.

This project applied a method for developing a functional safety concept by following the Concept Phase (Part 3) of the ISO 26262 standard.[2] Individual functional safety assessments were conducted for each of the four systems considered. The results of those assessments are reported in detail in separate reports [1] [2] [3] [4]. Higher level findings are synthesized in this report.

[2] The Concept Phase of the ISO 26262 standard is the initial stage of the development process and can be implemented before the specifics of the system design are known.

The analysis approach used in these assessments included:

1. Defining the scope and functions of the generic ALC or foundational system.
2. Performing a vehicle-level hazard analysis using both the Hazard and Operability (HAZOP) study and the Systems-Theoretic Process Analysis methods.
3. Applying the ASIL assessment[3] approach in the ISO 26262 standard to evaluate the risks associated with each of the identified hazards.
4. Performing a safety analysis using both the functional failure mode effects analysis and the STPA methods.
5. Deriving functional safety requirements and additional safety requirements for each system by combining the results of the two safety analyses[4] (functional FMEA and STPA) and following the Concept Phase in the ISO 26262 standard.[5] At a system level, the functional safety requirements might be informed in part through the selection of a fault tolerant architecture.[6]
6. Identifying generic diagnostic trouble codes listed in the SAE International Recommended Practice J2012[7] that are relevant to each system.
7. Developing examples of potential test scenarios that could be used to validate the safety goals and functional safety requirements. The example test scenarios provided in these individual reports are a small fraction of the possible test scenarios that may be needed to validate the safety goals and functional safety requirements for the system.

In conducting the analysis approach outlined above, this report identified challenges in applying the ISO 26262 ASIL process across the different levels of automation. In particular, vehicle concepts proposed for higher levels of automation may have limited means for the driver to control the vehicle (e.g., the vehicle may not be equipped with steering wheels or pedals). This presents challenges to assessing the "controllability" dimension in the ASIL assessment. In this study, the analysts assumed that these vehicles may not be controllable in the event of a malfunction and assigned the most conservative controllability value (C3) to these cases.

This study also identified challenges assessing the controllability dimension of the ASIL assessment at lower levels of automation. Specifically, Level 2 automated systems assume that

[3] The ASIL is established by performing a risk analysis of a potential hazard that looks at the Severity, Exposure, and Controllability of the vehicle operational situation.

[4] The HAZOP study is not used directly in deriving the functional safety requirements. The HAZOP study is used to identify the relevant vehicle-level hazards, which are then assigned ASILs that cascade down to the functional safety requirements.

[5] All requirements presented in this report are intended to illustrate a set of requirements that could be drived from the safety analysis results. These safety requirements are not intended to represent NHTSA's official position or requirements on the ALC system.

[6] Fault tolerant architectures characterize a system's capacity to maintain full or partial control in the event of an electronic fault and whether that fault leads to the transition to a safe state. Possible options are fail-safe/fail-passive and fail-operational. For automated systems in which an operator is not expected to be available for immediate intervention, some degree of fail operability may be necessary.

[7] The SAE standard J2012 defines the standardized DTCs that on-board diagnostic systems in vehicles are required to report when malfunctions are detected.

the driver is able to immediately resume control of the vehicle when the automated system disengages. However, human factors research suggests that this assumption may not always be valid. Therefore, the ASIL assessment for Level 2 automated systems in this study considered both the case where the driver is engaged and can immediately resume control of the vehicle, and the "foreseeable misuse" case where the driver is not engaged and cannot safely and immediately resume control of the vehicle.

Finally this study outlined four potential fail-safe and fail-operable system architectures that could apply to the various levels of automation. In particular, this study highlights the importance of considering the flow down of architectural requirements for automated systems to the foundational systems. For example, if an automated system is required to be fail-operable, then this requirement may also influence the design of the foundational system or systems used to provide actuation for the automated systems. If a single electronic fault could potentially cause a foundational vehicle system to immediately revert to manual control, this may not support certain levels of vehicle automation that are required to continue operating safely while transitioning control back to the driver.

The results of these reports may be used to:

- Demonstrate how the Concept Phase of ISO 26262 may be implemented, including integration of multiple analysis methods.
- Demonstrate how the Concept Phase of ISO 26262 may be applied to across the different levels of automation, including an example of how to consider potential driver misuse of Level 2 automated systems.
- Establish a baseline functional safety concept for future development of ALC systems and related foundational systems.
- Provide research data for future NHTSA activities with respect to ALC systems and related foundational systems.
- Illustrate how the analysis results may be used to develop potential test scenarios to validate the safety goals and functional safety requirements.

A. INTRODUCTION

A.1 Research Objectives

In conjunction with the National Highway Traffic Safety Administration, the Volpe National Transportation Systems Center is conducting research to assess the functional safety of automated lane centering systems and associated foundational systems in light vehicles.[8] ALC is a key technology that supports vehicle automation by providing continuous lateral control to keep the vehicle within the travel lane. ALC systems may be operated in conjunction with longitudinal control systems, such as adaptive cruise control, to allow the driver to cede execution of steering, acceleration, and deceleration tasks to automated vehicle systems [5]. However, depending on the level of automation the driver may still be responsible for certain elements of the driving task, such as monitoring the roadway environment.

ALC systems currently on the market are largely implemented through the foundational steering system [6]. However, in the future, ALC systems may also use the foundational brake/stability control system or active differential system to expand the performance envelope or as back-up systems capable of implementing lateral control in the event of a failure in the foundational steering system [7] [8]. Therefore, the reliability of the ALC technology depends in part on the reliability of the foundational steering and brake/stability control systems. These foundational systems are shared resources that may also be used to implement commands from other longitudinal and lateral control systems such as ACC, forward collision avoidance, and emergency steer assist.

This project is part of NHTSA's electronics reliability research program for ensuring the safe operation of motor vehicles equipped with advanced electronic control systems. The objectives of this project are:

1. Identify and describe various ALC, foundational braking, and foundational steering system implementations, including system variations related to Automation Levels 1 through 5 [5].[9] In addition to assessing the functional safety of ALC systems, this research project will study the functional safety of two foundational steering system variants - electric power steering (EPS) and steer-by-wire (SbW) - and a conventional hydraulic brake (CHB) system with electronic stability control (ESC), traction control, and an antilock brake (ABS) features.
2. Determine the hazards and their severity levels pertaining to the functional safety of ALC controls and related foundational systems, and identify functional safety requirements and constraints.

[8] Light vehicles include passenger cars, vans, minivans, sport utility vehicles, and pickup trucks with a gross vehicle weight rating of 10,000 pounds or less.
[9] NHTSA adopts the five levels of vehicle automation defined in SAE Standard J3016, which are described in more detail in Section A.2 of this report.

3. Assess diagnostic and prognostic needs.
4. Identify performance parameters and recommend functional safety test scenarios.
5. Review human factors considerations, including driver-vehicle interface requirements and the need for driver awareness and training resources.

A.2 Levels of Automation

NHTSA adopted the five levels of automation defined by SAE International in SAE Standard J3016 -- Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. Table 1 describes the five SAE levels of automation, plus a sixth level ("Level 0") that describes traditional vehicles that do not have automated systems.

Table 1. Levels of Automation

Level and Name	Description
Level 0 (L0) No Driving Automation	The human driver does all the driving.
Level 1 (L1) Driver Assistance	The vehicle is controlled by the driver, but some driving assist features may be included in the vehicle that can assist the human driver with either steering or braking/accelerating, but not both simultaneously.
Level 2 (L2) Partial Driving Automation	The vehicle has combined automated functions, like speed control and steering simultaneously, but the driver must remain engaged with the driving task and monitor the environment at all times.
Level 3 (L3) Conditional Driving Automation	An automated driving system on the vehicle can itself perform all aspects of the driving task under some circumstances. The driver is still a necessity, but is not required to monitor the environment when the system is engaged. The driver is expected to be takeover-ready to take control of the vehicle at all times with notice.
Level 4 (L4) High Driving Automation	The vehicle can perform all driving functions under certain conditions. A user may have the option to control the vehicle.
Level 5 (L5) Full Driving Automation	The vehicle can perform all driving functions under all conditions. The human occupants never need to be involved in the driving task.

Although this report refers to "ALC systems," in Level 3 through Level 5 automation, lane centering may be one of several functions in a higher-level path planning algorithm that governs the lateral position of the vehicle.

A.3 Full Functional Safety Analysis Reports

Functional safety analyses were performed for the ALC system and the three foundational systems. The results of these functional safety analyses are described in individual research reports [1] [2] [3] [4]. Each of these reports details the assumptions, system descriptions and analytical details of the corresponding functional safety analysis. The present report extracts the important results from these reports to make observations and draw conclusions about the body of research as a whole. The step-by-step details and results of each analysis (e.g., function list,

functional safety requirements, test scenarios) are not included here for the purpose of providing a comprehensive but not unduly lengthy report.

A.4 System Description

A.4.1 Automated Lane Centering

This report discusses the analysis of a generic ALC system across all five SAE automation levels. The ALC system provides continuous lateral control to keep the vehicle on a reference trajectory[10] within the travel lane. Providing continuous lateral control differentiates the ALC system from two related technologies – lane keep assist[11] (LKA) and lane departure warning[12] (LDW).

ALC systems use lane detection sensors to collect data about the surrounding environment, such as the location of lane markings. ALC systems currently on the market rely primarily on vision sensors (e.g., visible or infrared cameras). Other sensor technologies, such as radar, lidar, or ultrasonic, may provide supplemental information to the ALC system, such as the locations of other vehicles and stationary objects, to further define and confirm viable pathways. In addition to on-board sensors, ALC systems may also rely on map and GPS data to supplement roadway information. The ALC control module uses this information to determine a reference trajectory and the vehicle's location relative to that reference trajectory. If the ALC control module determines that an adjustment is needed to return the vehicle to the reference trajectory it commands a steering or yaw rate adjustment from the foundational systems.

A.4.2 Foundational Systems

A.4.2.1 Electric Power Steering System

The EPS system is a power-assisted steering system that combines the steering input from the driver with torque from the power-assist motor. The combined steering forces are mechanically transmitted to the road wheels. Depending on the EPS system architecture, the power-assist motor may be located at the steering column or at the rack and pinion. This report is based on the column assist EPS system architecture, which connects the power-assist motor to the steering column through a gear set, such as a planetary gear.

In addition to providing power-assist to the driver's steering input, the generic EPS system analyzed in this study includes two additional features: active steering and four-wheel steering (4WS). These additional features may not be included in all EPS systems. The active steering

[10] The lane center may not always be the ideal trajectory for the vehicle. For example, when navigating a curve, an ALC system may mimic a driver's natural tendency to travel along a path closer to the inside lane boundary.
[11] LKA actively keeps the vehicle within the lane by intervening as the vehicle approaches the lane boundaries. However, there is a deadband near the center of the lane where the LKA system does not provide control.
[12] LDW does not actively intervene to change the vehicle's position within the lane. LDW only provides alerts to the driver as the vehicle approaches the lane boundary.

feature enables the EPS to adjust the steering ratio[13]as a function of vehicle speed and to provide steering independent of the driver's input (e.g., crosswind compensation). The 4WS feature operates the rear-wheel heading based on the driver's steering input and vehicle speed. These features are described in more detail in the EPS system report [1].

A.4.2.2 Steer-by-Wire System

The SbW system measures the torque and angle of the driver's steering input and electronically transmits the driver's steering input to the steering actuator assembly (e.g., a steering motor). The steering actuator assembly is responsible for providing all steering forces required to adjust the heading of the road wheels [9] [10] [11]. During normal operation of a SbW system, none of the driver's steering inputs are mechanically transmitted to the road wheels. Since there is no mechanical connection between the steering wheel and the road wheels, the SbW system also simulates all feedback to the driver via a separate feedback motor.
In particular, this study assesses two types of SbW systems:

- A *full SbW system* electrically transmits the driver's steering input to the wheels. Furthermore, full SbW systems do not include a steering column or other means of mechanically transmitting the driver's steering input to the wheels, including mechanical backup subsystems.
- An *intermediate SbW system* electronically transmits the driver's steering input to the wheels. However, intermediate SbW systems retain the steering column as a mechanical backup subsystem in the event of a failure of the electronic portion of the SbW system.

In addition to providing steering, the SbW systems considered in this study include active steering and 4WS features, as described in Section A.4.2.1.

A.4.2.3 Conventional Hydraulic Brake System

The CHB system uses hydraulic brake pressure to generate friction forces that are applied to the road wheels. The friction generated by CHB system converts the kinetic energy of the vehicle to thermal energy[14], which dissipates into the atmosphere [12]. As the rotation of the road wheel slows, braking forces are transferred to the road at the road-tire interface, ultimately stopping the vehicle.

In the CHB system, the driver's input is in the form of hydraulic brake pressure generated by brake pedal pressure and augmented with a brake booster. This results in a direct mechanical

[13] The steering ratio defines the relationship between how much the heading of the road wheels change in response to the driver's rotation of the steering wheel.
[14] Unlike CHB systems, regenerative braking systems recover a portion of the kinetic energy, which is stored as electrical energy in the rechargeable energy storage system. Regenerative braking is out of scope for this project.

application of braking forces.[15] In addition to the mechanical application of brake forces, the CHB system includes electronic braking functions, such as anti-lock brake system, traction control system, and ESC, which can further adjust the driver's braking input or generate braking forces independent of the driver. These features are described in more detail in the individual CHB system functional safety report [3].

A.5 Human Factors Considerations for Automated Systems

A separate report was generated that enumerated human factors considerations for automated systems such as ALC [13]. Examples of some of the human factors considerations include:

- Providing sufficient, but not excessive, information to the operator,
- Balancing warning algorithm sensitivity with the need to avoid excessive false alarms, and
- Reducing operator workload to reduce fatigue while maintaining appropriate levels of operator engagement.

In particular, the system must be designed to maintain sufficient automation during scenarios requiring unplanned transition from automated to manual control. Table 2 lists some of the important human factors issues that designers might consider.

Table 2. Key Human Factors Findings

Driver-Vehicle Interface Attributes	Opportunities for Effective Mode Transition
• Easy to Learn and Use • Clear Intuitive Indication of Current State of Operation • Instilled Trust of the System • Driver Training • Avoidance of complacency and loss of situational awareness • Prudent Design Tradeoffs	• Timely warnings of impending transitions • Shared Control • Minimize Opportunities for Mode Confusion

A.6 Report Outline

This report documents the approach and the findings of the analysis of the ALC system. In addition to this Introduction, the report contains the following sections:

[15] This is in contrast to brake-by-wire systems, which electrically transmit the driver's braking input to the system control module instead of a direct mechanical application of hydraulic pressure to generate brake forces. Brake-by-wire systems are out of scope for this project.

Section B: Analysis Approach: This section describes the analytical approaches for functional safety and discusses the specifics of how the methods are applied to ALC systems and their related foundational systems.

Section C: Fault Tolerant Architectures: The fault tolerance of electronic system designs depends on their capability to respond to detect and mitigate electronic faults. This section describes different fault tolerant architectures, specifically focusing on the ability to maintain full or partial functionality and the options for providing system and/or component redundancy.

Section D: System Analysis and Results: This section provides results of the analytical approach for the ALC, EPS, SbW and CHB systems, including analysis of hazards, risk assessment, and key elements from the functional safety concept.

Section E: Findings From Synthesis of ALC and Related Foundational System Studies: This section provides a comparison of hazards and functional safety concepts for ALC and its foundational systems, and discusses implications of automated control on foundational systems and challenges in applying ASIL process across automation levels.

Section F: Summary and Conclusions: This section reviews the results of the analyses of the systems and summarizes the implications for the functional safety of automated systems.

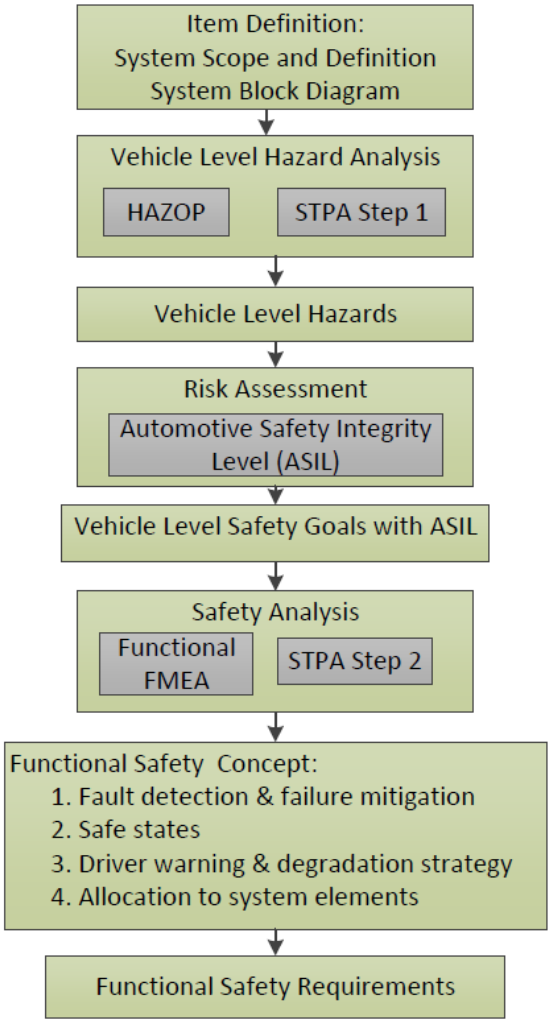
B. ANALYSIS APPROACH

B.1 Basis for the Analytical Process

The primary purpose of this work is to analyze the potential hazards that could result from cases of electrical or electronic failures and their impact on the functions of vehicular control systems. The study follows the ISO 26262 process to identify the integrity requirements of these functions at the concept level, independent of implementation variations. ISO 26262 is a functional safety process adapted from the International Electrotechnical Commission Standard 61508. It is intended for application to electrical and electronic systems in motor vehicles (Introduction in Part 1 of ISO 26262). Part 3 of ISO 26262 describes the steps for applying the industry standard during the concept phase of the system engineering process.

This study also considers potential causes of functional failures and documents the identified Automotive Safety Integrity Level of the item under consideration. This study does not suggest implementation strategies and design details appropriate for these ASILs. ISO 26262 provides a flexible framework and explicit guidance for manufacturers to pursue during the development and design process. Manufacturers might employ a variety of techniques, such as ASIL decompositions, driver warnings, fault detection mechanisms, plausibility checks, redundancies, etc., to achieve final designs that mitigate the underlying safety risks.

Figure 1 illustrates the safety analysis and safety requirements development process applied in this project, which is adopted from the Concept Phase (Part 3) of ISO 26262 .



HAZOP: Hazard and Operability study
STPA: Systems-Theoretic Process Analysis

- **STPA Step 1**: Identify Unsafe Control Actions
- **STPA Step 2**: Identify Causal Factors

FMEA: Failure Mode Effects Analysis

Note: ISO 26262 does not recommend or endorse a particular method for hazard and safety analyses. Other comparable and valid hazard and safety analysis methods may be used at the discretion of the analyst/engineer.

Figure 1. Safety Analysis and Requirements Development Process

As depicted in Figure 1, this project involves the following steps:

1. Define the system:
    a. Identify the system boundary. Clearly state what components and interactions are within the system boundary, and how the system interacts with other components and systems outside of the system boundary.
    b. Understand and document how the system functions.

   c. Develop system block diagrams to illustrate the above understandings and to assist the analysts in the rest of the process.
   d. Record any assumptions about the system operation or configuration made when defining the system.
2. Carry out the hazard analysis using both the Hazard and Operability process [15] and Step 1 of the Systems-Theoretic Process Analysis method. [16] The output of the hazard analysis step is a list of vehicle-level hazards. If the HAZOP and STPA methods do not generate a common list of hazards at the outset, an additional step may be necessary to synthesize the identified hazards into a consistent and comprehensive list.
3. Apply the ISO 26262 risk assessment approach to the identified vehicle-level hazards, and assign an ASIL to each hazard as defined in ISO 26262.
4. Generate vehicle-level safety goals, which are vehicle-level safety requirements based on the identified vehicle-level hazards. The ASIL associated with each hazard is also transferred to the corresponding vehicle-level safety goal. If a safety goal addresses more than one vehicle-level hazard, the ASIL of the hazard with the more critical ASIL is applied to the safety goal .
5. Perform safety analyses on the relevant system components and interactions as defined in the first step of this process. This project performs both a functional failure mode effects analysis [17] and STPA Step 2 to complete the safety analysis.
6. Follow the ISO 26262 process to develop the functional safety concept, including functional safety requirements at the system and component levels, based on results from the functional FMEA and STPA, ISO 26262 guidelines, and industry practice experiences.

Once the safety goals and functional safety requirements are determined, they are used along with the safety analysis results to develop potential test scenarios and performance parameters.

The individual system reports describe how the HAZOP, functional FMEA, and STPA methods were applied to a generic ALC system and the related foundational systems.[16] The results are detailed in the individual system reports and are summarized in Section D.

B.2 Current Safety Issues

This study reviewed current safety issues related to ALC and related foundational systems. In particular, this study included a review of crash data in the General Estimates System and Fatality Analysis Reporting System to understand the crash types at least partially attributable to failures related to these systems. NHTSA's recall and vehicle owner questionnaire (VOQ) databases were also reviewed to identify potential failure modes. The findings from the review of current safety issues are included in Appendix A.

[16] ISO 26262 does not recommend or endorse specific methods for hazard or safety analysis. Comparable and valid hazard and safety analysis methods may be used at the discretion of the analyst/engineer.

B.3 Hazard Analysis and Risk Assessment

B.3.1 Hazard and Safety Analysis Methods

This project uses multiple analysis methods to generate a list of hazard and safety analysis results.[17] These methods are described in this section.[18]

B.3.1.1 Hazard and Operability Study

This study uses the HAZOP study as one of the methods for identifying vehicle-level hazards. Figure 2 illustrates the analytical steps of the HAZOP study.

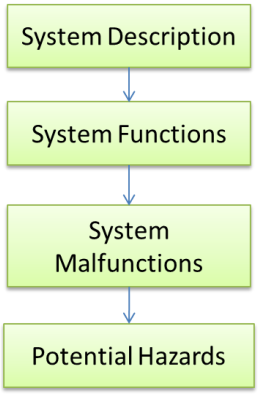


Figure 2. HAZOP Study Process

This study performs the HAZOP steps in Figure 2 as follows:

1. Define the system of study and the scope of the analysis. Draw a block diagram to illustrate the system components, system boundary, and interfaces. This step is accomplished in the first step of the overall project (Figure 1).
2. List all of the functions that the system components are designed to perform. This step is also accomplished in the first step of the overall project (Figure 1).

[17] ISO 26262 does not recommend or endorse specific methods for hazard or safety analysis. Comparable and valid hazard and safety analysis methods may be used at the discretion of the analyst/engineer.
[18] This report provides more details on the STPA than other methods because the application of the STPA method to automotive electronic control systems is relatively new. Unlike HAZOP and functional FMEA, a standard approach has not been defined and published for STPA. Therefore, this report provides more descriptions in order to better explain how the analysis is performed.

3. For each of the identified functions, apply a set of guidewords that describe the various ways in which the function may deviate from its design intent. IEC 61882[19] lists 11 suggested guidewords, but notes that the guidewords can be tailored to the particular system being analyzed [15]. The HAZOP study implemented in this project uses the following seven malfunction guidewords:
    - Loss of function
    - More than intended
    - Less than intended
    - Intermittent
    - Incorrect direction
    - Not requested
    - Locked function

    The combination of a system function and guideword may have more than one interpretation. In these situations, the analyst may identify more than one malfunction.
4. Assess the effect of these functional deviations at the vehicle level. If a deviation from an intended function could potentially result in a vehicle-level hazard, the hazard is then documented.

B.3.1.2 Functional Failure Mode Effects Analysis

The FMEA is a bottom-up reliability analysis method that relies on brainstorming to identify failure modes and determine their effects on higher levels of the system. There are several types of FMEAs, such as system or functional FMEAs, design FMEAs, and process FMEAs. This study uses a functional FMEA in the safety analysis to identify failure modes at the function level that could lead to the vehicle-level hazards. The failure modes identified by the functional FMEA are used to derive the safety requirements.

SAE Standard J1739 provides guidance on applying the functional FMEA method [17]. The analysis includes the following steps:

1. List each function of the item on an FMEA worksheet.
2. Identify potential failure modes for each item and item function.
3. Describe potential effects of each specific failure mode and assign a severity to each effect.
4. Identify potential failure causes or mechanisms.
5. Assign a likelihood of occurrence to each failure cause or mechanism.
6. Identify current design controls that detect or prevent the cause, mechanism, or mode of the failure.

[19] IEC 61882:2001, *Hazard and operability studies (HAZOP studies) - Application guide*, provides a guide for HAZOP studies of systems using a specific set of guide words defined in this standard. IEC 61882:2001 also gives guidance on application of the technique and on the HAZOP study procedure, including definition, preparation, examination sessions, and resulting documentation.

7. Assign a likelihood of failure detection to the design control.

This study applies the first four steps listed above for the functional FMEA. Since this study is implemented at the concept phase and is not based on a specific design, the FMEA does not assume controls or mitigation measures are present; there is no data to support Steps 5 through 7. The completed functional FMEA worksheet is intended to be a living document that would be continually updated throughout the development process.

B.3.1.3 Systems-Theoretic Process Analysis

The STPA is a top-down systems engineering approach to system safety [16]. In STPA, the system is modelled as a dynamic control problem, where proper controls and communications in the system ensure the desired outcome for emergent properties such as safety. In the STPA framework, a system will not enter a hazardous state unless an unsafe control action (UCA) is issued by a controller, or a control action needed to maintain safety is not issued. Figure 3 shows a process flow diagram for the STPA method.

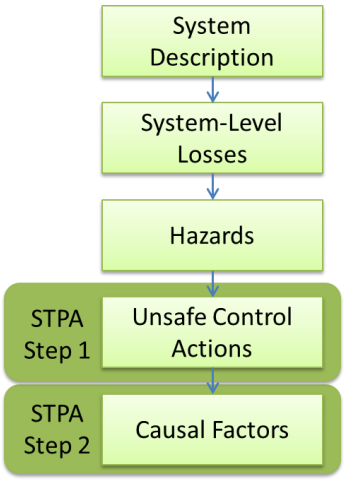


Figure 3. STPA Process

This project performs STPA following these steps:

1. Define the system of study and the scope of the analysis:
    a. Draw a hierarchical control structure of the system that captures the feedback control loops (controller, sensors, actuators, controlled process, and communications links). This control structure is a generic representation of the system, based on common implementation strategies.
    b. Identify the system boundary and interfaces with other vehicle systems and the external environment.

    This step is accomplished in the first step of the overall project (Figure 1).

2. Define the loss or losses at the system level that should be mitigated. STPA defines system-level losses as undesired and unplanned events that result in the loss of human life or injury, property damage, environmental pollution, etc. [16]. For this project, one loss was considered: occurrence of a vehicle crash.
3. Identify a preliminary list of vehicle-level hazards. STPA defines a hazard as a system state or set of conditions that, together with a particular set of adverse environmental conditions, will lead to a system-level loss [16]. In this project, a preliminary hazard list is generated based on engineering experience and a literature search. This list is refined during STPA Steps 1 and 2.
4. **STPA Step 1**: Identify potential UCAs issued by each of the system controllers that could lead to hazardous states for the system. Four sub-steps are involved:

    a. For each controller in the scope of the system, list all of the relevant control actions it can issue.

    b. For each control action, develop a set of context variables.[20] Context variables and their states describe the relevant external control inputs to the control system and the external environment that the control system operates in, which may have an impact on the safety of the control action of interest. The combinations of context variable states are enumerated to create an exhaustive list of possible states. This approach is based on a recent enhancement to the STPA method [18] that enumerates the process variable states during STPA Step 1. Process variables refer to variables that the control algorithm uses to model the physical system it controls. However, this study is not based on a specific design and a detailed process model algorithm is not available. Therefore, this study modifies this approach to focus on context variables instead of process variables.

    c. Apply the UCA guidewords to each control action. The original STPA literature includes four such guidewords [16]. This study uses a set of six guidewords for the identification of UCAs as illustrated in Figure 4.

[20] The context variables describe the context in which a controller issues a control action. For example, the control command "disengage ALC system" may operate in the context of the driver's request to disengage the ALC system, the driver's attentiveness, and disengage or suspend requests from other vehicle systems.

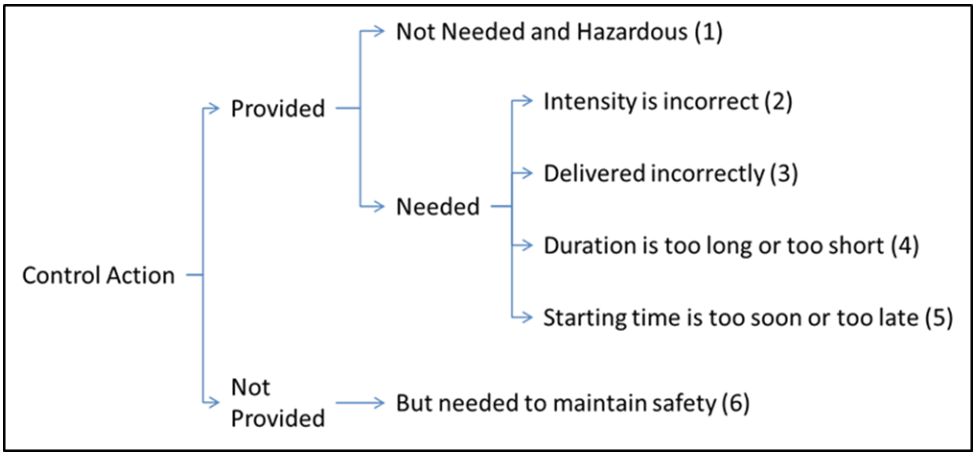


Figure 4. Guidewords for UCAs

For each control action, assess each of the six guidewords against each of the context variable combinations to determine if it could lead to any of the preliminary vehicle-level hazards. If this step identifies new hazards, add them to the vehicle-level hazard list initiated in the previous step.

d. Apply logical reduction to the resulting UCA matrix using the Quine-McCluskey minimization algorithm [19] in order to reduce the number of UCA statements.

STPA Step 1 produces a list of UCAs that can be used to derive safety requirements for software control logic and initiate the STPA Step 2 analysis.

5. **STPA Step 2:** Determine causal factors (CFs) for each UCA identified in STPA Step 1.

   Analyze each component and interaction in the control structure representation of the system to determine if the component or the interaction may contribute to one of the UCAs identified in STPA Step 1. STPA literature provides 17 guidewords to assist the analyst in identifying CFs [16]. This project uses an expanded list of 26 guidewords for identifying CFs. Appendix B provides the list of CF guidewords and detailed causes under each guideword that are used in this project.

As discussed above, there are two main analysis steps in STPA (Figure 3). This project applies STPA Step 1 in the hazard analysis stage of the study and STPA Step 2 as part of the safety analysis stage (Figure 1).

B.3.2 ASIL Risk Assessment

The analysis of each control system continues with a risk assessment of the identified vehicle-level hazards. Each vehicle-level hazard is assigned an ASIL.

B.3.2.1 General ASIL Assessment Process

ISO 26262 assesses the ASIL of identified hazards according to the severity, exposure, and controllability (Part 3 in ISO 26262). The ASIL assessment contains the following steps:

1. Identify vehicle operational scenarios
2. For each identified vehicle-level hazard, apply the ISO 26262 risk assessment framework:
    a. Assess the probability of exposure to the operational scenario.
    b. Identify the potential crash scenario.
    c. Assess the severity of the harm to the people involved if the crash occurred.
    d. Assess the controllability of the situation and the vehicle in the potential crash scenario.
    e. Look up the ASIL per ISO 26262 based on the exposure, severity, and controllability.
3. Assign the worst-case ASIL to the hazard.

Exposure is defined as the state of being in an operational situation that can be hazardous if coincident with the failure mode under analysis (Part 1 Clause 1.37 in ISO 26262). Table 3 is a reproduction of Table 2 in Part 3 of the ISO 26262 standard.

Table 3. Exposure Assessment

	Class				
	E0	**E1**	**E2**	**E3**	**E4**
Description	Incredible	Very low probability	Low probability	Medium probability	High probability

Severity is defined as the estimate of the extent of harm to one or more individuals that can occur in a potentially hazardous situation (Part 1 Clause 1.120 in ISO 26262). Table 4 is directly quoted from ISO 26262 Part 3 Table 1.

Table 4. Severity Assessment

	Class			
	S0	**S1**	**S2**	**S3**
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

Table 5 is one method for assessing severity that is provided in ISO 26262 (Part 3 Clause 7.4.3.2 and Annex B Table B.1).

Table 5. Example Method for Assessing Severity

	Class of Severity			
	S0	**S1**	**S2**	**S3**
Reference for single injuries (from AIS scale)	• AIS 0 and Less than 10% probability of AIS 1-6 • Damage that cannot be classified safety-related	More than 10% probability AIS 1- 6 (and not S2 or S3)	More than 10% probability of AIS 3-6 (and not S3)	More than 10% probability of AIS 5-6
AIS: Abbreviated Injury Scale				

ISO 26262 defines controllability as the "ability to avoid a specified harm or damage through the timely reactions of the persons[21] involved, possibly with support from external measures" (Part 1 Clause 1.19 in ISO 26262). Table 6 is ISO 26262's approach to assessing controllability (Table 3 in Part 3 in ISO 26262).

Table 6. Controllability Assessment

	Class			
	C0	**C1**	**C2**	**C3**
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

There is no clear guidance in ISO 26262 for assessing controllability for vehicles operating at Level 4 and Level 5 automation. Some Level 4 and Level 5 automated vehicle concepts include vehicle designs that do not include steering wheels or pedals [20]. In these cases, the driver would be unable to control the vehicle in the event of a failure. Furthermore, this study does not make assumptions on the availability of other vehicle systems capable of mitigating a failure of the ALC function in a Level 4 or Level 5 automated vehicle since no such system or systems are mandated. Therefore, this study adopts the most conservative controllability, "C3," for Level 4 and Level 5 automated systems [21].

Table 7 shows how ASIL is assessed based on exposure, severity, and controllability (Table 4 in Part 3 of ISO 26262).

[21] People involved can include the driver, passengers, or persons in the vicinity of the vehicle's exterior.

Table 7. ASIL Assessment

Severity Class	Probability Class (Exposure)	Controllability Class		
		C1	**C2**	**C3**
S1	**E1**	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	**E1**	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	**E1**	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D
QM: Quality Management; E: Exposure; S: Severity; C: Controllability				

B.3.2.2 Operational Scenarios

ASILs are determined for electronic failures based on the operational scenarios that the system will experience over the vehicle lifetime (Part 1 Clause 1.83 in ISO 26262). For example, high speed scenarios may have higher severity and lower controllability than moderate speed scenarios, though moderate speed scenarios might have higher exposure.

Analysts developed operational scenarios for each system, as described in ISO 26262 and the guidance document SAE J-2980. The operational scenarios include some universal variables (e.g., vehicle speed) and some variables that are specific to a particular system (e.g., braking force for the CHB system). Table 8 tallies the number of relevant operational scenarios evaluated for each system in the appropriate individual functional assessment report.

Table 8. Number of Operational Scenarios by System

System	Number of Scenarios
Automated Lane Centering	48
Electric Power Steering	26
Steer-by-Wire	14
Conventional Hydraulic Braking	201

B.3.2.3 Influence of Automation Level

In addition to the vehicle operational scenarios based on Table 8, the ASIL assessment for the ALC system also evaluated each hazard based on the level of vehicle automation. The automation levels were not considered as operational scenario variables, since the level of automation may be an intrinsic part of the vehicle design. However, the assumption of the driver's availability under the different automation levels may affect the controllability parameter in the ASIL assessment.

In contrast, the ASIL assessment of the foundational systems assumed that an engaged driver would constantly monitor and could expediently mitigate the effect of electronic malfunctions – essentially Automation Level 0 (no automation), Level 1 (driver assistance), or Level 2 – Driver Engaged scenarios. However, when these foundational systems act as actuators in a higher level automated system (e.g., ALC), that assumption may no longer be valid. This may have implications for the fault tolerance of the vehicle. Thus, if the analysis of an ALC system requires that a steering actuator component have certain architectural characteristics (e.g., a partial level of redundancy, see Section C), that requirement may cascade to the foundational system in the overall vehicle design. These architectural considerations may not apply to the foundational system when considered as a stand-alone component of a non-automated vehicle.

The consideration of operator engagement in an automated process is prudent in light of long-established human factors principles. The Yerkes-Dodson (Y-D) law (Figure 5), first proposed in 1908, states that for any task, there is an optimal level of arousal that maximizes performance of the task [22]. When a task becomes too demanding, performance suffers due to fatigue and stress. Automation should help reduce performance degradation in stressful driving situations. Unfortunately, the Y-D law also implies that automation can leave an operator with too little to do, resulting in loss of attention and interest.

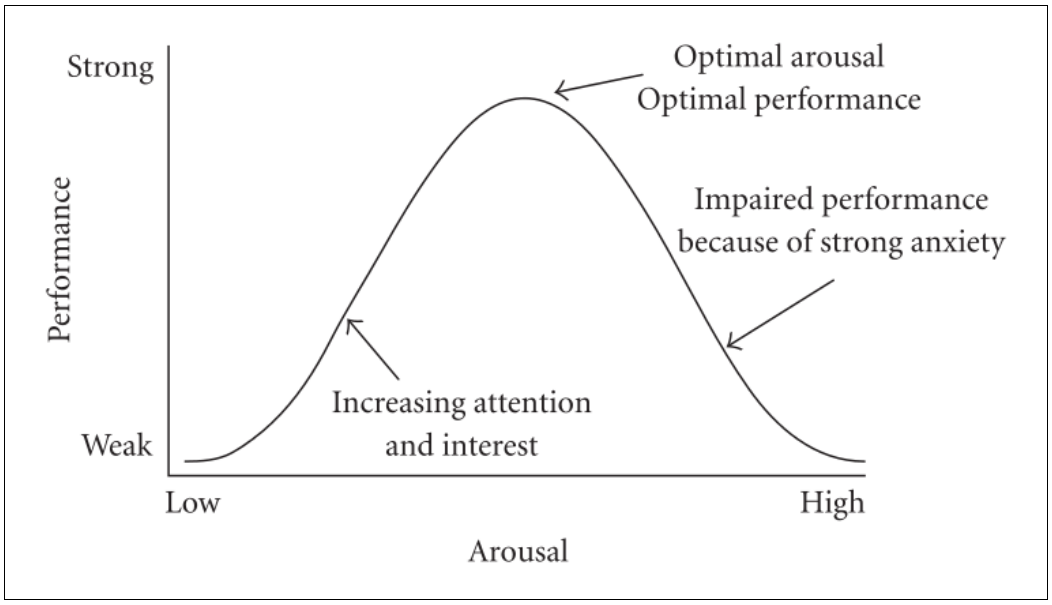


Figure 5. Depiction of Yerkes-Dodson Law from Diamond, et al.

By definition, Level 2 automated systems assume that the driver remains continuously aware of the driving situation and is always prepared to take over control immediately should the automated system, such as a combined ACC and ALC system, disengage. For example, if the ALC control module were to lose power causing the ALC system to disengage without advance warning, the expectation is that the driver would be able to resume lateral control of the vehicle without a transition period. However, there have been several reports of drivers misusing or potentially misusing Level 2 automated systems [23] [24] [25] [26]. Thus, a significant challenge facing Level 2 automated systems is ensuring that the driver can maintain situational awareness in a passive monitoring task.

The implications from the literature of psychology and neurophysiology [22] are that the task of abruptly taking over manual control of a vehicle at highway speed after an extended period of automated driving is inherently much more challenging than most other driving tasks. When an operator is required to resume control after several minutes of automated operation, several types of problems may arise:

i. The human may be unaware of changes in the driving environment for which the automated system has been compensating successfully. These unnoticed changes could include degradation in tire adhesion, malfunctions that would cause the vehicle to pull to one side, or the presence of aberrant drivers of nearby vehicles. Motor vehicles, trains, pedestrians, or bicyclists on an intersecting trajectory, but only intermittently visible, can also surprise an unengaged driver. An unengaged human may also miss road signs and variable-message displays warning of upcoming hazards.

ii. An unengaged operator may not comprehend which aspects of the automation are still functioning and which have disengaged. Surveying the instrument panel (IP) and trying to recall the meaning of numerous illuminated icons while steering a car in freeway traffic can be difficult. Identifying and comprehending the significance of icons that are *not* illuminated is even more challenging.

iii. Studies have found that after relatively brief exposure to automated driving (under one hour), drivers in simulator experiments show increased response times for braking compared with their baseline response time in manual driving. The reported increases in braking-response times range from 0.8 to 1.5 s [27] [28]. A study on the effectiveness of LDW notifications[22] indicated it may take approximately 700 milliseconds for a disengaged driver to provide a steering response after an auditory or haptic notification [29].[23] Other studies suggest a longer interval, on the order of 10 seconds, before the driver's attention is refocused on the roadway [30].

In a Level 2 automated vehicle in which the driver is not engaged, the controllability factor of the ASIL assessment required by ISO 26262 can be materially affected, resulting in higher overall ASILs. Distraction and lack of engagement in a low workload or monitoring environment could be interpreted as foreseeable misuse in which the ALC system is not being used in the manner for which it is designed.

Based on this information, the analysts agreed that assuming the driver is able to immediately resume control of a Level 2 automated vehicle may not always be correct. Therefore, the functional safety analysis of ALC considered two cases for Level 2 automated systems:

- Automation Level 2 – Driver Engaged: These systems are designed to *ensure* that the driver remains engaged with the driving task after ceding both lateral and longitudinal control to the vehicle.
- Automation Level 2 – Driver Not Engaged: This anticipates foreseeable driver misuse of Level 2 automated systems where the system design does not ensure that the driver remains engaged with the driving task. The ASIL assessment in this category considers that the driver may not be monitoring the roadway (e.g., distracted) or otherwise may not be able to immediately resume control of the vehicle.

Thus, the automation levels considered for the ASIL assessments of the ALC system are given in Table 9.

[22] In the event that a failure prevents the ALC system from actively controlling the vehicle's lateral position, the analysts agreed the notification to the driver could be comparable to a LDW notification.
[23] This same study documented a maximum lane exceedance on the order of one meter for LDW systems with auditory or haptic notifications [30].

Table 9. Automation Levels Considered for ASIL Assessment of the ALC System

Automation Level
Automation Level 1
Automation Level 2 – Driver Engaged
Automation Level 2 – Driver Not Engaged[1]
Automation Level 3
Automation Level 4
Automation Level 5
[1] Based on the assumption of foreseeable driver misuse that prevents the driver from immediately resuming control of the vehicle in the event of a failure.

B.4 Safety Goals

For each of the systems studied, the hazard analysis identified vehicle-level hazards as well as the underlying system issues that may lead to them. The determination of vehicle-level hazards enables the derivation of safety goals. Safety goals are top-level safety requirements derived from the hazard analysis and risk assessment (ISO 26262, Part 1, Clause 1.108).

While there is often a one-to-one mapping between a safety goal and the hazard from which it is derived, a single safety goal may also address multiple hazards or multiple safety goals may cover a single hazard. In instances where a single safety goal covers multiple hazards, the safety goal inherits the highest ASIL from the associated hazards. ISO 26262 states that safety goals should be expressed in terms of the functional objective, rather than as technological solutions (ISO 26262, Part 3, Clause 7.4.4.3).

The individual functional safety assessment reports on the individual systems each contain detailed derivations of the vehicle-level hazards and the associated safety goals. The safety goals are summarized in this report in Section D.4.

B.5 Functional Safety Concept

ISO 26262 defines functional safety as *the absence of unreasonable risk due to hazards caused by malfunctioning behavior of electric/electronic systems* (Part 1 Clause 1.51 in ISO 26262). Functional safety is one aspect of the overall system safety. The primary focus of functional safety is to address systemic protection from electronic faults. Thus, functional safety concepts may include adding functionality to the system to address specific safety issues. In particular, functional safety covers the safety behaviors or safety measures implemented by the system, such as fault detection, physical or systemic redundancy, or transitioning to a safe state, that reduce the overall risk due to faults in the electronic system [14] [31].

The objective of the functional safety concept is to develop a set of functional safety requirements from the safety goals and to allocate them either to the preliminary architectural

elements of the system or to external measures (Part 3 Clause 8.1 in ISO 26262). Figure 6 illustrates how the functional safety concept takes into consideration the results from the safety analysis; applies safety strategies, industry practices, and engineering experiences; and derives a set of safety requirements following the established process in ISO 26262.

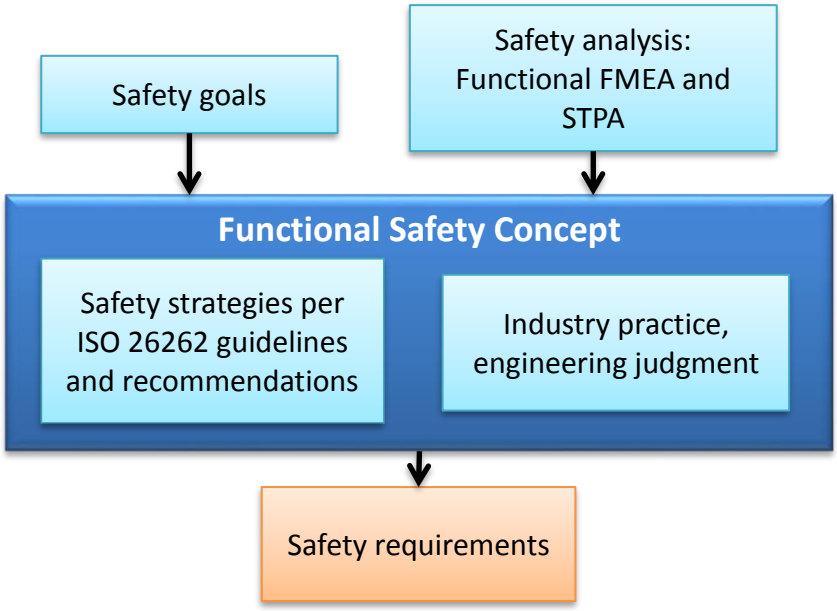


Figure 6. Functional Safety Concept Process

B.5.1 Safety Analysis

This study uses the functional FMEA and STPA to complete the safety analysis that supports the functional safety concept and the safety requirements. Overall, the functional FMEA examines subsystems and components as well as interfacing systems and subsystems. The functional FMEA identifies the failure modes of the components and the related potential faults. Note that some potential faults may lead to one or more failure modes. Each study also used STPA to conduct a parallel safety analysis. The goal of STPA Step 2 is to identify CFs that may lead to the UCAs, which then may result in one or more of the synthesized vehicle-level hazards.

B.5.2 Safety Strategies

As stated in ISO 26262 Part 3 Clause 8.2, "*the functional safety concept addresses:*

- *Fault detection and failure mitigation;*
- *Transitioning to a safe state;*
- *Fault tolerance mechanisms, where a fault does not lead directly to the violation of the safety goal(s) and which maintains the item in a safe state (with or without degradation)*
- *Fault detection and driver warning in order to reduce the risk exposure time to an acceptable interval (e.g., engine malfunction indicator lamp, anti-lock brake fault warning lamp);*

- *Arbitration logic to select the most appropriate control request from multiple requests generated simultaneously by different functions*."

Typical safety strategy elements may include the following:

1. Ensure that the system elements are functioning correctly.
2. Ensure that the critical sensors' inputs to the main controller are valid and correct (e.g., redundant measurements paths).
3. Validate[24] the health of the main controller (e.g., using an auxiliary processor or a redundant controller).
4. Ensure the validity and correctness[25] of critical parameters (e.g., mitigate latent faults through periodic checks).
5. Ensure the validity and correctness of the critical communication signals internal and external to the system (quality factors[26]).
6. Ensure that the correct steering torque or yaw (in terms of magnitude and direction) is requested from the foundational vehicle systems with the correct timing (for the ALC system).
7. Ensure that the correct braking torque (in terms of magnitude and direction) is delivered to the road wheels with the correct timing (for the CHB system).
8. Ensure that the correct steering torque in terms of magnitude and direction is delivered to the road wheels with the correct timing (for the EPS and SbW systems).
9. Ensure that low-voltage power is available until the safe state is reached under all hazardous conditions.
10. Mitigate the safety hazards when an unsafe condition is detected.
11. Ensure that the safe state is reached on time when a hazard is detected.
12. Ensure driver warnings are delivered when an unsafe condition is detected.
13. Ensure the correctness and timeliness of the arbitration strategy.

[24] "Validate" in this context means to ensure that the value of a parameter or the state of an element falls within a valid set of values or states.
[25] "Correctness" in this context means that the value of a parameter is the correct one from the valid set.
[26] Quality factors refer to techniques for error detection in data transfer and communication including checksums, parity bits, cyclic redundancy checks, error correcting codes, etc.

B.5.3 Example Safe States

A safe state of a system is an operating mode without an unreasonable risk. A safe state may be the intended operating mode, a degraded operating mode, or a switched off mode (Part 1 Clause 1.102 of ISO 26262). The developer of the functional safety concept attempts to maximize the availability of the vehicle while ensuring the safety of its operation. Therefore, careful consideration is given to selecting the safe states in relation to the potential failure modes.

The possible safe states for automated systems such as ALC may vary based on the automation level. The safe states for the foundational systems were developed under the assumption that the operator is able to maintain full control of the vehicle under nominal conditions, albeit not necessarily with all desirable or auxiliary functions – essentially this is equivalent to assuming Automation Level 0 (no automation), Level 1 (driver assistance), or Level 2 – Driver Engaged. In these analyses, however, when considering the interaction between the foundational vehicle systems and automated vehicle systems, such as ALC, this assumption may not always be appropriate. For instance, the operator may not be sufficiently engaged to immediately resume control of a foundational system in a system that operates in a Level 2 – Driver Not Engaged context or at higher levels of automation (e.g., Level 3 through 5). This concept is discussed further in Section D.6.

B.5.4 Example Driver Warning Strategies

In addition to defining safe states, driver notification is a key element for ensuring that the driver takes the proper course of action. The following is an example of driver warning strategies commonly seen in the automotive industry:

- Amber Light:
  - Potential violation of a safety goal is detected, but the probability of violating a safety goal is moderate.
- Red Light:
  - Potential violation of a safety goal is detected and the probability of violating a safety goal is high.
  - A violation of a safety goal is detected.
- Audio:
  - Chime: Audible notification of the driver is implemented whenever the conditions for the Red Light driver warning are identified. The chime may continue until the fault is removed.
  - Specific recorded (or simulated) verbal warning to the operator.
- Haptic: Haptic warnings, such as vibrating the steering wheel or driver's seat, may be an additional driver warning strategy. Dashboard lights and audible chimes are commonly used in conjunction with haptic warning. It may be beneficial to assess driver reactions to a haptic warning issued at the same time the system is attempting to reach safe state and degraded operation.

- Messages: Messages are displayed to the driver at least with the Red Light driver warning. The messages may inform the driver of the absence of system functions or, for a system like ALC, the remaining time before the system disengages.

B.5.5 Application of the Functional Safety Concept

The individual functional safety analysis reports identify vehicle-level safety requirements (Safety Goals) as well as safety requirements for the system and components.[27] The system and component functional safety requirements were developed by following the Concept Phase (Part 3) in the ISO 26262 standard, as carried out by the automotive industry.

The studies also included comprehensive hazard and safety analyses that identify potential failures that fall outside the functional safety scope of ISO 26262. In addition, these analyses also considered the additional risk reduction measures recommended by the system safety standard MIL-STD-882E [32] in order to ensure the generation of a comprehensive list of safety requirements:

- Eliminate hazards through design selection
- Reduce risk through design alteration

These additional safety requirements are out of the scope of the functional safety concept in ISO 26262 (Part 3 of the standard). However, the subsequent parts in ISO 26262—Systems Engineering (Part 4), Hardware Development (Part 5), and Software Development (Part 6)—cascade the functional safety concept requirements into additional development specific safety requirements, and may capture these additional safety requirements.

Example safety requirements are provided in each of the individual functional safety assessment reports [1] [2] [3] [4].

B.6 Example Test Scenarios

This study included development of potential test scenarios based on the functional safety concept for each system. Test scenarios such as these may be useful in verifying that the functional safety requirements are achieved. However, the test scenarios developed through this study do not represent a comprehensive set of test scenarios and additional test scenarios may be necessary to adequately verify the functional safety requirements are achieved.

[27] All requirements presented in this section are intended to illustrate a set of requirements that could be derived from the safety analysis results. These safety requirements are not intended to represent NHTSA's official position or requirements on the ALC system.

Each test scenario includes the following:

- **Test Goals**: Each of the safety goals identified in the analysis serves as the testing goal for a test scenario. The test objective is to ensure that the safety goal is not violated.
- **Driving Scenarios**: Each driving scenario is developed using a combination of the vehicle's operating scenario and key inputs to the system. Together, this represents the situation under which the system should avoid entering a hazardous state when a fault is injected.
- **Fault Injection**: The causal factors identified in STPA, and failure modes and faults identified in the functional FMEA may be used as the basis for determining faults to inject at the component and connection levels. Examples of potential faults that could be introduced to the system include inducing hardware failures in system components, transmitting erroneous measurements from sensors, or issuing incorrect controller commands (e.g., to simulate a flaw in the software algorithm).
- **Expected Safe Behavior**: The test scenarios can be evaluated by monitoring for expected safe behaviors. The following are examples of possible safe behaviors:
    - The system may transition into one of the identified safe states within the fault tolerant time interval.
    - The system's controller may still be capable of issuing the correct command when a fault is injected.

Although the role of the driver is considered in the hazard and safety analyses, the test scenarios developed in this study focus on the behavior of the electronic control system. Evaluation of driver behavior when certain faults are injected into the vehicle would require a separate human factors study.

The example test scenarios are provided in each of the individual functional safety assessment reports [1] [2] [3] [4].

C. FAULT TOLERANT ARCHITECTURES

In developing the functional safety concepts for the ALC system and its related foundational vehicle systems, this study considered two general fault tolerant architectural strategies: "Fail-Safe"/"Fail-Passive" and "Fail-Operational."

C.1 Fail-Safe/Fail-Passive

An electronic system is "fail-safe" if any single electronic fault is detected and results in the system transitioning to a safe state to ensure safety of the system. A system is "fail-passive" if it disengages after an electronic fault with no further action and does not interfere with operation of other systems [33]. In both fail-safe and fail-passive architectures, the system must not violate any of the safety goals when transitioning to a safe state or shutting down.

Fail-safe may include redundancy such that no single electronic fault is capable of resulting in a critical hazard. A fail-safe architecture may not require the same level of redundancy as a fail-operational architecture (see below), since a fail-safe system is designed to transition to a safe state immediately following detection of a fault. For example, a fail-safe architecture may only require two (redundant) controllers. If there is a disagreement due to an internal electronic fault in either of the controllers, the system transitions to a safe state. Figure 7 shows examples of key fail-safe concepts as applied to an ALC system.[28]

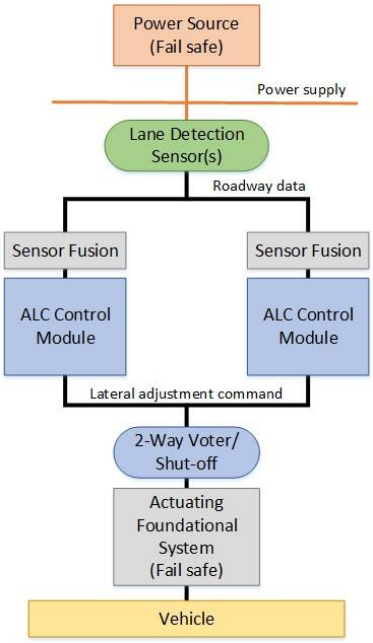


Figure 7. Example Fail-Safe Concepts Illustrated With Some ALC System Components

[28] Figure 7 is provided to illustrate some of the key concepts for a fail-safe architecture and is not intended to represent an actual system design.

C.2 Fail-Operational

An electronic system is "fail-operational" if any first electronic fault is detected and does not result in a loss of any primary electronic system functionality that is essential to the safety of the system [33]. In the example of an ALC system, this means (1) ensuring that the ALC system can continue to receive and process sensor data and (2) commanding the appropriate lateral adjustments necessary to keep the vehicle along the reference pathway without violation of any safety goals.

Following any first electronic fault, if the degraded system is no longer fail-operational to any subsequent fault, the system transitions to a status of fail-safe. Essentially, the system can safely sustain a minimum of two fully independent electronic faults prior to loss of primary system functionality and transition to an associated safe state. Independence of the effects of these faults can be validated using techniques such as common mode analysis.

Redundancy is commonly used to ensure a fail-operational architecture. Redundancy can be physical redundancy, such as multiple fully redundant computing elements that "vote" their outputs. Thus, when one element is "outvoted," a fault is presumed and that element is blocked from asserting control on the system. Alternatively, "analytical redundancy" may be used. By using independent data streams, encoding methods, and evaluation algorithms, fault effects associated with data corruption can be identified and mitigated.

Common fail-operational architectures include "triplex," which employs a three-way voting scheme, and "dual fail-safe," which employs two fail-safe or fail-silent elements. If either element detects a failure, that element is blocked from asserting control on the system. Figure 8 shows examples of key fail-operational concepts as applied to an ALC system.[29] It depicts a triplex architecture with a three-way voting scheme for the controllers and a dual fail-safe architecture for the power supply. As Figure 8 suggests, different fail-operational architectures may be employed for different subsystems, so long as the overall system has the property of being fail-operational.

[29] Figure 8 is provided to illustrate key concepts for a potentially fail-operational architecture and is not intended to represent, suggest, or recommend an actual system design.

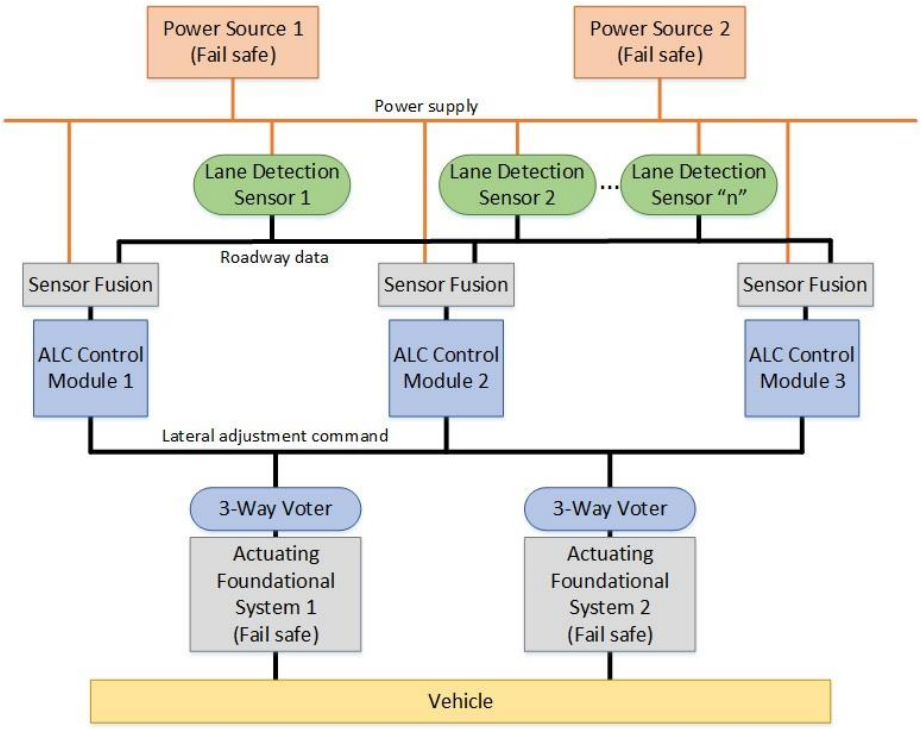


Figure 8. Example Fail-Operational Concepts Illustrated With Some ALC System Components

The cut-over to the redundant system (or removal of defective control path from contributing to the actual lateral control of the vehicle) happens with sufficient speed to avoid inducing errors. The driver is appropriately warned of the system fault and that service is required since the designed level of redundancy no longer exists.

C.3 Implications for Architecture of Relationship Between Actuating Foundational Systems and Control Systems

As illustrated in Figure 7 and Figure 8, the requirements of a fail-operational or fail-safe architecture also extends to the foundational systems that implement the ALC system commands. For example, if the ALC system's commands are implemented solely through the electronic actuation of the steering system, a single electronic fault that disables the electronic actuators of the steering system may effectively disable the ALC system. Therefore, for an ALC system to be fail-operational, the actuating foundational systems would also need to meet the fail-operational requirements.

Two possible architectures for the foundational systems that implement the ALC system commands include:

- A single fully fail-operational foundational system, such as a fail-operational SbW system.

- Multiple fail-safe or fail-passive foundational systems that provide redundant actuation of ALC system commands [34]. For example, differential braking via the CHB system may be able to execute ALC system commands in the event of a failure that disables electronic actuation of a fail-safe EPS system.

C.4 Practical Aspects of Architectural Strategies

ALC systems may be designed using different fail-operational or fail-safe strategies, depending on factors such as use cases, design details, and detailed safety calculations. In this study, for which system functionality is akin to providing full lateral control, the architectural strategies discussed in Sections C.1 and C.2 might be described by the following four classes:

- Class 1: Fail-Operational With Similar Redundancy – The configuration of controllers, sensors, power supplies, and actuators is sufficiently redundant to provide full lateral control capability following any single electronic failure. In this architecture, redundant components, such as lane detection sensors, would be of the same type (e.g., redundant cameras).
- Class 2: Fail-Operational With Dissimilar Redundancy – This architecture also includes redundant system components to provide full lateral control capability following any single electronic failure. However, unlike the fail-operational architecture with similar redundancy, this architecture may use different types of components to provide redundancy. For example, with dissimilar redundancy the three lane detection sensors shown in Figure 8 may include a combination of cameras and radar. This type of architecture may introduce additional complexity since the different perception data must be compared to detect faults in a lane detection sensor.
- Class 3: Fail-Safe With Redundant Actuation - This architecture combines a fail-safe or fail-passive ALC system with a fail-operational actuating foundational system architecture. This type of architecture may provide limited fail-operational capabilities. For example, the ALC system may able to predetermine the vehicle's trajectory for a time interval that provides the driver sufficient time to resume control of the vehicle following a failure in the ALC system
- Class 4: Fail-Safe or Fail-Passive – As described in Section C.1, this architecture does not exhibit the extent of redundancy described in the other example architectures. Furthermore, the actuating foundational systems also may not employ redundancy. In the event of a failure, the vehicle may immediately revert to manual control or transition to another safe state (e.g., stop the vehicle in the lane).

D. SYSTEMS ANALYSES AND RESULTS

D.1 System Definition

The systems as analyzed are defined in detail in the individual system functional safety assessment reports [1] [2] [3] [4]. In particular, the analysis scope and assumptions are carefully described. For reference, Figure 9 through Figure 12 show block diagram representations of the generic systems considered in this study. Interfacing vehicle systems are shown in gray and are treated as black boxes with respect to the analyzed system. This study assumes that these interfacing vehicle systems are functioning properly.

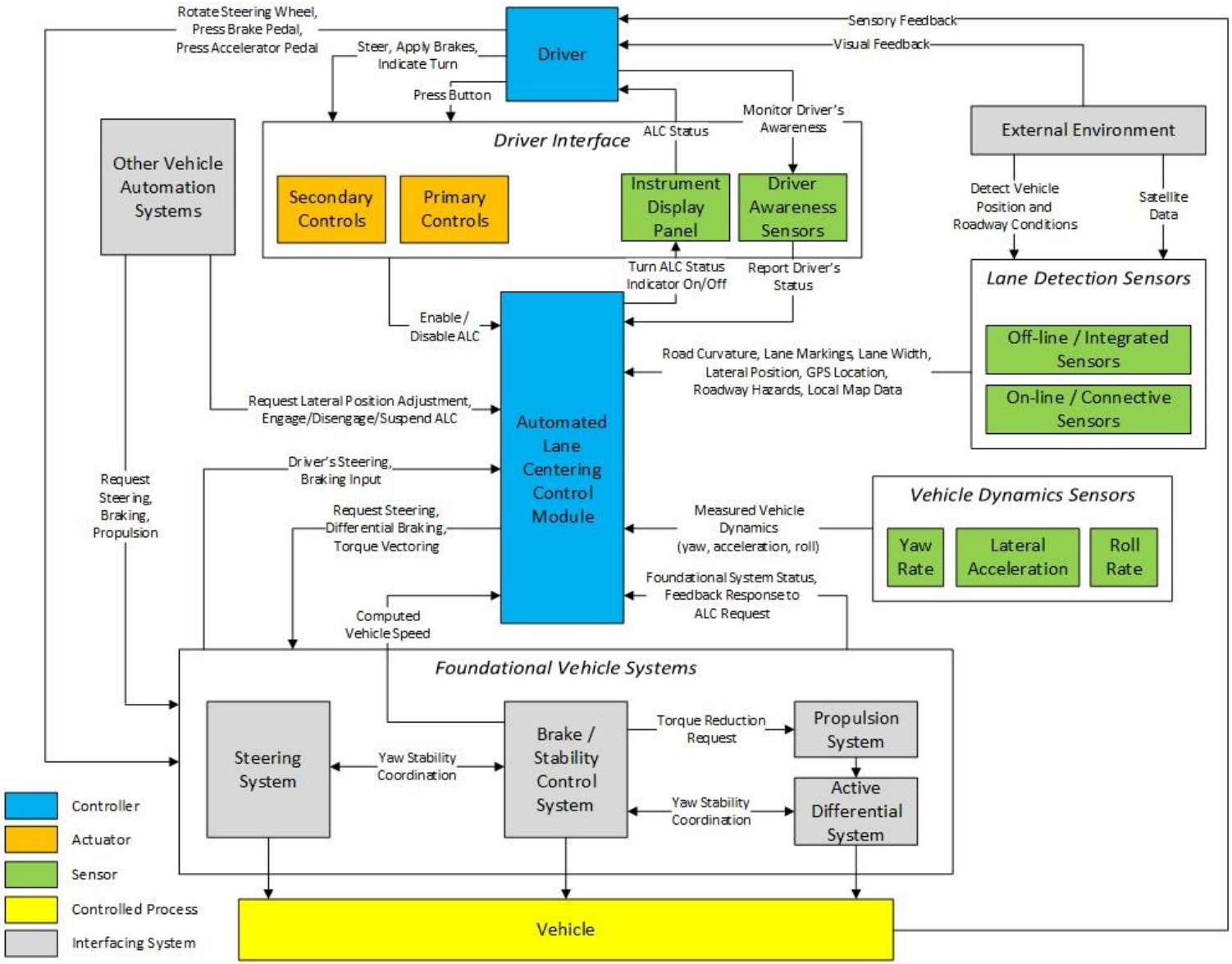


Figure 9. Block Diagram of a Generic ALC System

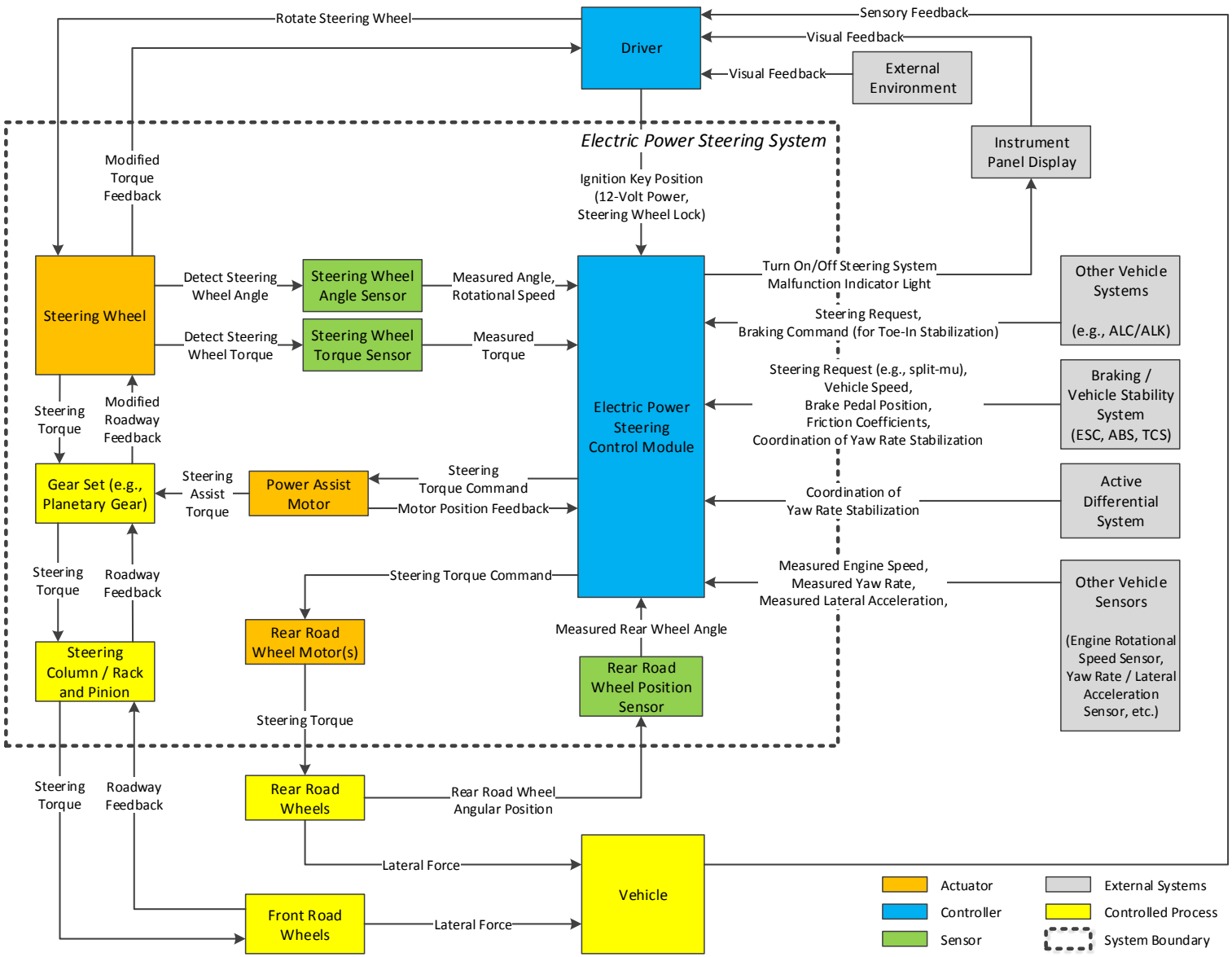


Figure 10. Block Diagram of a Generic EPS System With Active Steering and 4WS Features

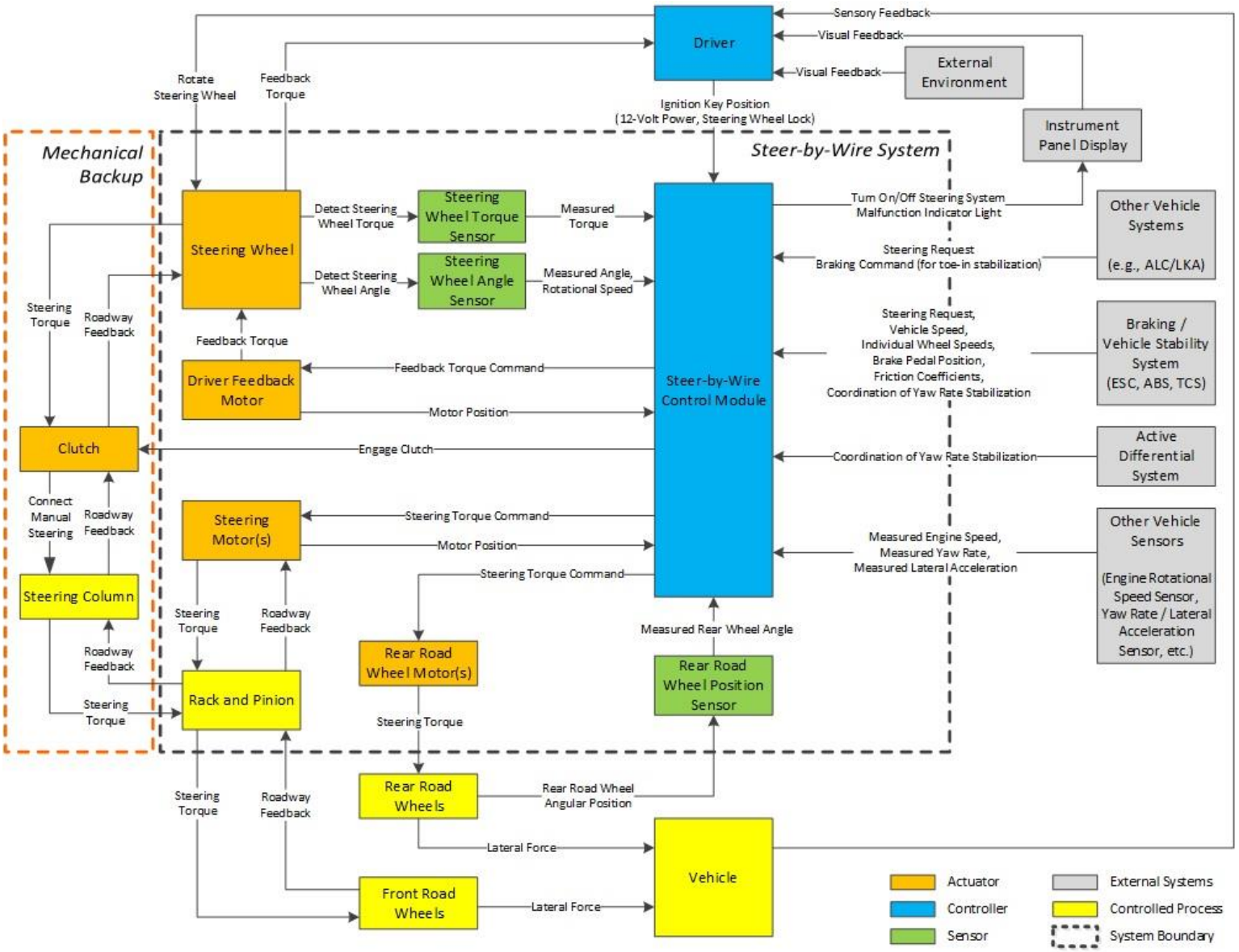


Figure 11. Block Diagram of a Generic SbW System With Active Steering and 4WS Features

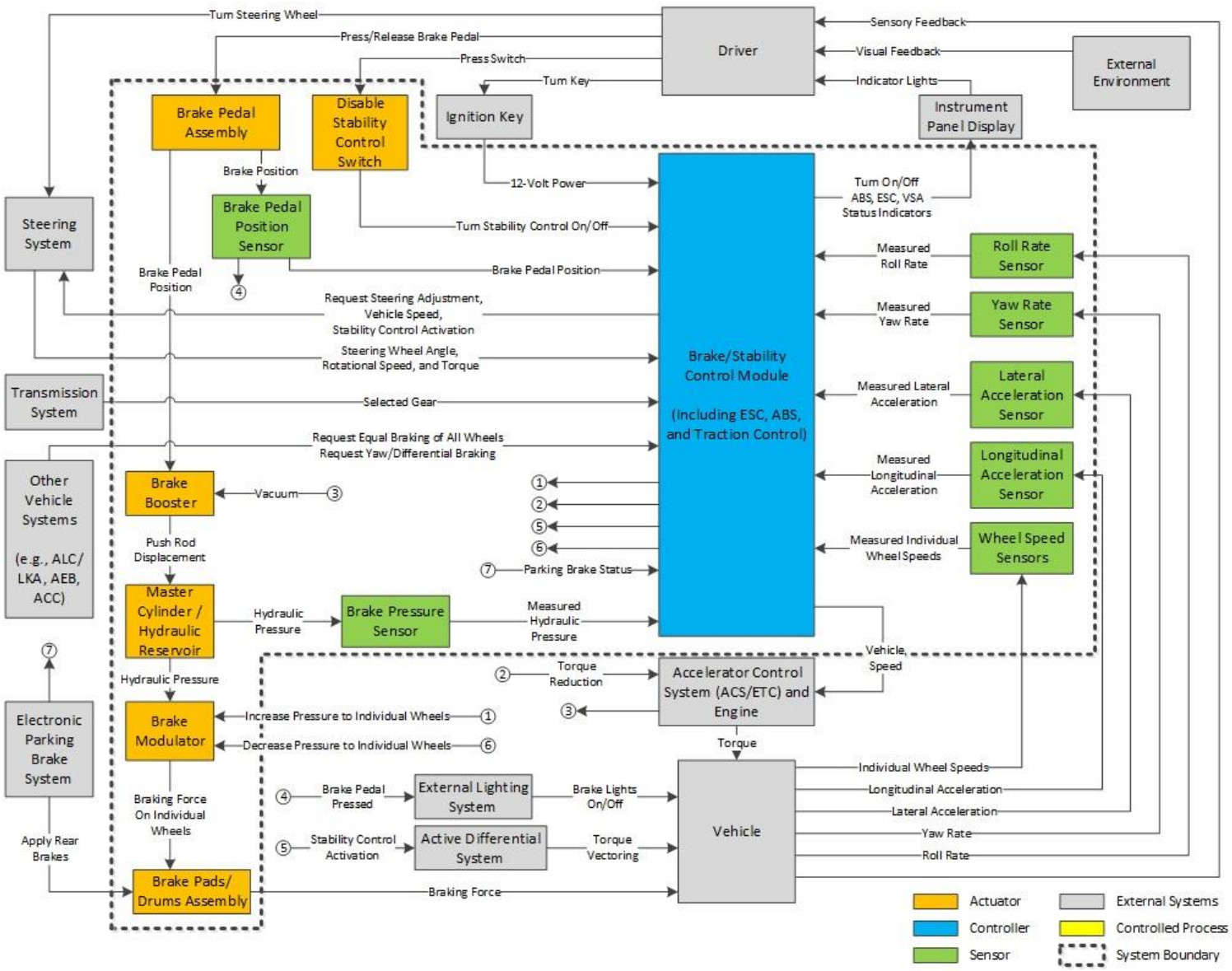


Figure 12. Block Diagram of a Generic Conventional Hydraulic Braking System With ABS, TCS, and ESC Features

D.2 Vehicle Level Hazard Analysis

The individual system functional safety assessment reports all performed two types of hazard analyses (HAZOP and STPA) on the systems as defined. The combined results of the synthesized hazard lists are presented in Table 10.

Table 11 indicates which hazards apply to each system included in this study.

Table 10. Synthesized List of Potential Vehicle-Level Hazards

Potential Hazard (Synthesized Term)	**Potential Hazard Description**
Unintended Vehicle Lateral Motion/Unintended Yaw	The vehicle moves laterally more than, at a faster rate than, or in the opposite direction of what is commanded by the driver or another vehicle system controller. (Only applicable to CHB under conditions where the wheels do not lock up.)
Insufficient Vehicle Lateral Motion/Insufficient Yaw	The vehicle moves laterally, but less than or at a slower rate than what is commanded by the driver or another vehicle system controller. (Only applicable to CHB under conditions where the wheels do not lock up.)
Unintended Loss of Steering-Assist[1]	The EPS system becomes unavailable in an uncontrolled manner (e.g., the loss of assist is sudden and the driver is not notified). However, mechanical steering is still available.
Reduced Responsiveness to the Driver's Commands Due to Increased Rear-Wheel Drag[2]	The rear-wheel position causes an increased drag effect, slowing the vehicle but not at a level that results in significant vehicle deceleration. This drag effect may also affect the vehicle response if the driver is trying to steer.
Loss of Vehicle Lateral Motion Control	The vehicle does not respond to steering inputs from the driver or other vehicle systems. (Only applicable to CHB under conditions where the front wheels lock up.)
Incorrect (e.g., delayed, missing, counterintuitive, etc.) Feedback Resulting in Incorrect Driver Reaction	The feedback provided at the steering wheel is incorrect and sufficiently misleading that it causes the driver to incorrectly steer the vehicle.
Intermittent Response to Driver's Steering Control Input	The SbW system does not provide a smooth or consistent response to steering inputs. Examples of this hazard may include a jerky response to steering inputs or a delayed steering response.
Unintended Vehicle Deceleration	The vehicle decelerates more than or at a faster rate than what is commanded by the driver or another vehicle system controller.
Insufficient Vehicle Deceleration	The vehicle decelerates, but less than or at a slower rate than what is commanded by the driver or another vehicle system controller.
Loss of Vehicle Longitudinal Motion Control	The vehicle does not respond to braking inputs from the driver or other vehicle systems (i.e., loss of braking).
Unintended Vehicle Propulsion	The vehicle accelerates more than or at a faster rate than what is commanded by the driver or another vehicle system controller.

Potential Hazard (Synthesized Term)	Potential Hazard Description
Insufficient Vehicle Propulsion	The vehicle does not accelerate to the level commanded by the driver. This includes cases where the vehicle's propulsion is reduced below the driver's set point.
Vehicle Movement in an Unintended Longitudinal Direction	The vehicle moves in a longitudinal direction that is not expected by the driver, including rolling forward/backward when the vehicle should be stopped.
Insufficient Lateral Adjustment Resulting in Lane/Roadway Departure while ALC is Engaged	The ALC system does not provide sufficient lateral control while the system engaged, allowing the vehicle to depart the lane/roadway. The rate at which the vehicle departs the lane/roadway depends heavily on the underlying roadway geometry.
Excessive Lateral Adjustment Resulting in Lane/Roadway Departure While ALC is Engaged	The ALC system actively causes the vehicle to depart the travel lane/roadway. This hazard does not assume that there are limits on the torque authority of the ALC system.
Unexpected Loss of ALC	The ALC system disengages unexpectedly (i.e., without prior warning to the operator). The ALC system is no longer able to provide lateral control.
Improper Transition of Control Between the Driver and ALC System[3]	The responsibility for lateral control is improperly coordinated between the driver and the ALC system. This hazard may cover: • Not providing a sufficient transition time to the driver (Level 2 or Level 3 automated systems) • Failure of the ALC system to suspend or disengage when requested Driver confusion related to control responsibilities
ALC System Impedes Actions of Other Vehicle Systems	The ALC system interferes with the operation of other vehicle systems by failing to disengage or suspend, or by failing to implement lateral positioning requests (e.g., from a higher-level controller).

[1] Unintended in this context is used to differentiate from intentional disabling of the EPS system as a potential safe state for the system. In particular, the unintended loss of steering-assist is not controlled and the driver is not notified that steering-assist is not available.
[2] Rear-wheel drag indicates a rear-wheel position (i.e., toe-in) that slows the vehicle when the brakes are not being applied. However, the amount of drag may not be sufficient for characterization as deceleration.
[3] This hazard may not apply to all Level 4 or Level 5 automated systems, which state that the driver is not expected to control the vehicle when the automated system is operating in its operational design domain.

Table 11. Potential Vehicle-Level Hazards by System

Potential Hazard (Synthesized Term)	EPS	SbW	CHB	ALC
Unintended Vehicle Lateral Motion/Unintended Yaw	●	●	●	
Insufficient Vehicle Lateral Motion/Insufficient Yaw	●	●	●	
Unintended Loss of Steering-Assist	●			

Potential Hazard (Synthesized Term)	EPS	SbW	CHB	ALC
Reduced Responsiveness to the Driver's Commands Due to Increased Rear-Wheel Drag	●	●		
Loss of Vehicle Lateral Motion Control		●	●	
Incorrect (e.g., delayed, missing, counterintuitive, etc.) Feedback Resulting in Incorrect Driver Reaction		●		
Intermittent Response to Driver's Steering Control Input		●		
Unintended Vehicle Deceleration			●	
Insufficient Vehicle Deceleration			●	
Loss of Vehicle Longitudinal Motion Control			●	
Unintended Vehicle Propulsion			●	
Insufficient Vehicle Propulsion			●	
Vehicle Movement in an Unintended Longitudinal Direction			●	
Insufficient Lateral Adjustment Resulting in Lane/Roadway Departure While ALC is Engaged				●
Excessive Lateral Adjustment Resulting in Lane/Roadway Departure While ALC is Engaged				●
Unexpected Loss of ALC				●
Improper Transition of Control Between the Driver and ALC System				●
ALC System Impedes Actions of Other Vehicle Systems				●

D.3 Risk Assessment

This study follows the risk assessment approach in ISO 26262. The assessment derives the ASIL for each of the identified vehicle-level hazards. The ASIL classification assigned to each hazard depends on the exposure, severity, and controllability (see Section B.3.2.1). The ISO 26262 process does not automatically assign a high ASIL to hazards with high severity. Following the ASIL assessment process, it is possible for a hazard with the highest severity (S3) to have a low ASIL, such as ASIL A or QM. This does not indicate that the hazard is any less severe. Rather, it reflects a situation that has lower exposure or is more controllable.

Although failures in different foundational systems may result in the same vehicle level hazard, the operational scenarios under which these hazards are assessed may have different exposure, severity, and controllability values. Thus, the same hazard may have different ASILs for

different systems or items.[30] As discussed in Section B.3.2.3, the ASIL assessment of the ALC system (particularly the controllability factor) can be substantially affected by the automation level and driver engagement. Thus, the ASIL assignments for ALC hazards are differentiated by Automation Level in Table 13.

Table 12. Assigned ASIL for Potential Vehicle-Level Hazards for Foundational Systems

Potential Hazard (Synthesized Term)	**EPS**	**SbW**	**CHB**
Unintended Vehicle Lateral Motion/Unintended Yaw	D	D	B[1]
Insufficient Vehicle Lateral Motion/Insufficient Yaw	C	D	B[1]
Unintended Loss of Steering-Assist	B		
Reduced Responsiveness to the Driver's Commands Due to Increased Rear-Wheel Drag	A	A	
Loss of Vehicle Lateral Motion Control		D	D
Incorrect (e.g., delayed, missing, counterintuitive, etc.) Feedback Resulting in Incorrect Driver Reaction		B	
Intermittent Response to Driver's Control Input		D	
Unintended Vehicle Deceleration			D
Insufficient Vehicle Deceleration[1]			D
Loss of Vehicle Longitudinal Motion Control[1]			D
Unintended Vehicle Propulsion			C[2]
Insufficient Vehicle Propulsion			C[2]
Vehicle Movement in an Unintended Longitudinal Direction			QM[3]

[1] This ASIL only considers malfunctions in the braking system which may lead to this hazard. Similar hazards in the steering system may have a higher ASIL rating.
[2] This ASIL only considers malfunctions in the braking system which may lead to this hazard. Similar hazards in the accelerator control system may have a higher ASIL rating.
[3] This ASIL is specific to the Hill Holder feature. Other situations related to insufficient braking while on an incline are covered under Insufficient Vehicle Deceleration and Loss of Vehicle Longitudinal Motion Control.

[30] For example, the potential hazard "unintended lateral motion/unintended yaw" may have a lower ASIL as a brake system hazard because of the assumption that a fully functional steering system is available to the driver for controlling the vehicle. When assessing the steering system, however, this same potential hazard may have a higher ASIL because the assumption in this case is that the steering system may not be available to the driver (although the brake system is assumed to be available to stop the vehicle).

Table 13. Assigned ASIL for Potential Vehicle-Level Hazards for ALC System by Automation Level

Potential Hazard	ASIL					
	Level 1	**Level 2 Driver Engaged**	**Level 2 Driver Not Engaged[1]**	**Level 3**	**Level 4**	**Level 5**
Insufficient Lateral Adjustment Resulting in Lane/Roadway Departure with ALC Engaged	B	B	D	D	D	D
Excessive Lateral Adjustment Resulting in Lane/Roadway Departure with ALC Engaged	D	D	D	D	D	D
Unexpected Loss of ALC	B	B	D	D	D	D
Improper Transition of Control between the Driver and ALC System	B	B	D	D	D[2]	D[2]
ALC System Impedes Actions by Other Vehicle Systems	B	B	D	D	D	D

[1] Based on the assumption of foreseeable driver misuse that prevents the driver from immediately resuming control of the vehicle in the event of a failure.
[2] This ASIL only applies if the human operator is able to resume control of the vehicle.

D.4 Vehicle-Level Safety Goals

Safety goals are top-level safety requirements derived from the hazard analysis and risk assessment (ISO 26262, Part 1, Clause 1.108). Based on the identified hazards and their corresponding ASILs, this study established the safety goals listed for each of the systems in Table 14, Table 15, Table 16, and Table 17, respectively.

Table 14. Safety Goals for the EPS System

ID	Safety Goals	ASIL
SG 1	Prevent unintended self-steering in any direction under all vehicle operating conditions.	D
SG 2	Provide the correct level of steering-assist under all vehicle operating conditions.	C
SG 3	Prevent the unintended[1] loss of steering-assist under all vehicle operating conditions.	B
SG 4	Prevent rear-wheel drag under all vehicle operating conditions.[2]	A

[1] Unintended in this context is used to differentiate from intentional disabling of the EPS system as a potential safe state for the system. Specifically, the unintended loss of steering-assist is not controlled and the driver is not notified that steering-assist is not available.
[2] Rear-wheel drag indicates a rear-wheel position (i.e., toe-in) that affects the vehicle dynamics or slows the vehicle when the brakes are not being applied. However, the drag effect may not reach the level of "deceleration".

Table 15. Safety Goals for the SbW System

ID	Safety Goals	ASIL
SG 1	Prevent unintended self-steering in any direction under all vehicle operating conditions.	D
SG 2	Provide the correct amount of steering within TBD[31] seconds under all vehicle operating conditions.	D
SG 3	Prevent the loss of vehicle lateral motion control (i.e., steering loss) under all vehicle operating conditions	D
SG 4	Prevent unintended rear wheel drag under all vehicle operating conditions.[1]	A
SG 5	Provide the correct amount of feedback to the driver under all vehicle operating conditions.	B

[1] Rear-wheel drag indicates a rear-wheel position (i.e., toe-in) that affects the vehicle dynamics or slows the vehicle when the brakes are not being applied. However, the drag effect may not reach the level of "deceleration".

Table 16. Safety Goals for the CHB System

ID	Safety Goals	ASIL
SG 1	Prevent unintended vehicle lateral motion and/or unintended yaw under all vehicle operating conditions.	B[1,2]
SG 2	Provide sufficient lateral motion under all vehicle operating conditions.	B[1,2]
SG 3	Prevent CHB system failures that lead to loss of lateral motion control under all vehicle operating conditions.	D
SG 4	Prevent unintended vehicle deceleration[3] under all vehicle operating conditions.	D
SG 5	Prevent insufficient braking and loss of braking under all vehicle operating conditions.	D
SG 6	Prevent CHB system failures that lead to unintended acceleration under all vehicle operating conditions.	C[2]
SG 7	Prevent CHB system failures that lead to insufficient propulsion or propulsion power reduction/loss under all vehicle operating conditions.	C[2]
SG 8	Prevent CHB system failures that lead to unintended vehicle motion (e.g., rolling backward) under all vehicle operating conditions.	QM[4]

[1] This ASIL is based on the assumption that the wheels do not lock for this hazard. Situations where wheel lock-up affects the vehicle's lateral motion are considered in SG 3.
[2] This ASIL is based on failures in the CHB system that may lead to this potential hazard. Hazards in other vehicle systems that may lead to this hazard may have different ASILs.
[3] Some manufacturers may specify threshold values for "unintended vehicle deceleration" (e.g., 0.2g).
[4] This ASIL is specific to the Hill Holder feature. Other situations related to insufficient braking while on an incline are covered in hazards H5 and H6.

[31] This study did not identify existing standards specifying the SbW response time to the driver's steering input.

Table 17. Safety Goals for the ALC System

ID	Safety Goals	ASIL					
		Level 1	**Level 2 Driver Engaged**	**Level 2 Driver Not Engaged[1]**	**Level 3**	**Level 4**	**Level 5**
SG 1	Prevent insufficient lateral adjustment resulting in lane/roadway departures while the ALC system is engaged in accordance with the identified ASIL.	B	B	D	D	D	D
SG 2	Prevent excessive lateral adjustment resulting in lane/roadway departures while the ALC system is engaged in accordance with the identified ASIL.	D	D	D	D	D	D
SG 3	Prevent unexpected loss of the ALC system in accordance with the identified ASIL.	B	B	D	D	D	D
SG 4	Ensure proper transition of control between the driver and the ALC system in accordance with the identified ASIL.	B	B	D	D	D[2]	D[2]
SG 5	Ensure coordination of lateral control actions with other vehicle systems or functions in accordance with the identified ASIL.	B	B	D	D	D	D

[1] Based on the assumption of foreseeable driver misuse that prevents the driver from immediately resuming control of the vehicle in the event of a failure.
[2] This ASIL only applies if the human operator is able to resume control of the vehicle.

D.5 Functional Safety Concept

The development of the functional safety concept is described in Section B.5.3. Key findings of the analyses are reported in this section.

D.5.1 Safe States

As discussed in Section B.5.3, a safe state is an operating mode of the item without an unreasonable risk. A safe state may be the intended operating mode, a degraded operating mode, or a switched off mode (Part 1 Clause 1.102 of ISO 26262). The developer of the functional safety concept attempts to maximize the availability of the vehicle while ensuring the safety of its operation. Therefore, careful consideration is given to selecting the safe states in relation to the potential failure modes.

A key finding in this study is that functional safety assessments of the foundational systems (below) often rely on a safe state in which immediately reverting to manual control is sufficient when the vehicle is operated by an engaged driver. When that same system supports a higher automation level, immediately reverting to manual control may not be an appropriate safe state.

D.5.1.1 Possible Safe States for EPS

The possible safe states for the EPS system may include full operation (full steering-assist availability), degraded operation (certain steering-assist modes are disabled), or switched off mode (no steering-assist available). Possible safe states for the EPS system may include, but are not limited to those listed in Table 18

Table 18. Possible EPS System Safe States

Safe State	SbW System Behavior	Example Triggering Event
EPS-1	Disable steering-assist at high speeds. • Steering assist is still available at low speeds	Failure in the steering wheel angle sensor
EPS-2	Disable rear-wheel steering. Return rear wheels to straight-ahead position	Failure in the rear-wheel steering mechanism
EPS-3	Disable all steering-assist	Failure in the EPS motor

Safe State 3 and the potential hazard "Unintended Loss of Steering-Assist" both describe a similar vehicle behavior — where the EPS system does not provide steering-assist to the driver. However, there are key differences between the safe state and potential hazard:

- When entering Safe State 3, the steering-assist is disabled in a controlled manner. For example, the steering-assist may be gradually reduced to prevent an abrupt change in the vehicle's response to the driver's steering input.
- When entering Safe State 3, the driver is informed that the vehicle is in a degraded operating state (e.g., through a driver warning light) and can take appropriate action. The driver may not be notified of the degraded operating state when the potential hazard "Unintended Loss of Steering-assist" manifests.

In the context of automated systems operating at Level 2 - Driver Not Engaged or at higher levels of automation (i.e., Level 3 through Level 5), Safe State 3 may not be a viable option for the EPS system, unless a second foundational system is capable of implementing lateral adjustment commands until the driver can safely resume control of the vehicle. If a second foundational vehicle system (e.g., differential braking via the CHB system) is capable of implementing the lateral adjustment commands from the ALC system, then Safe State 3 may continue to be a viable safe state for the EPS system.

D.5.1.2 Safe States for SbW

The safe states for the SbW system can be either full operation, degraded operation (e.g., loss of certain SbW functions), or switched off mode (e.g., the intermediate SbW system is not available). Possible safe states for the SbW system may include (but are not limited to) those listed in Table 21. The objective of the safe state is to reduce the overall risk at the vehicle level. Therefore, some of the safe states presented in Table 21 include degradation of other vehicle systems, such as the propulsion system [11], to maximize the driver's ability to control the vehicle and to reduce the potential severity in the event of a collision.

Table 19. Possible SbW System Safe States

Safe State	**SbW System Behavior**	**Example Triggering Event**
SbW-1A	Notify driver • SbW degrades from fail-operational to fail-safe, but retains full steering availability[1]	Failure of one element (e.g., minimum triple redundancy)
SbW-1B	Engage the mechanical backup subsystem[2]	Failure of one element (e.g., no redundancy)
SbW-2	Restrict propulsion (e.g., "limp-home" mode) • Limit vehicle operation to TBD[32] key cycles	Failure of two elements
SbW-3	Gradually reduce propulsion until vehicle stops • Brake/torque vectoring may be used for limited steering	Failure of all redundant elements
SbW-4	Disable feedback motor	Failure of driver feedback mechanism
SbW-5	Disable rear-wheel steering • Return rear wheels to straight-ahead position	Failure in the rear-wheel steering mechanism

[1] This safe state only applies for fail-operational architectures, as described in Section C.2
[2] This safe state applies to the intermediate SbW systems, as described in Section A.4.2.2.

As with the EPS system, Safe State 1B may not be a viable option for intermediate SbW systems supporting automated systems operating at Level 2 - Driver Not Engaged or higher levels of automation (i.e., Level 3 through 5), unless a second foundational system is capable of implementing lateral adjustment commands until the driver can safely resume control of the vehicle.

D.5.1.3 Safe States for CHB

The safe states for the CHB system can be either full operation, degraded operation (e.g., loss of certain CHB system functions), or switched off mode (e.g., the electronic portion of the CHB

[32] This value may vary between manufacturers based on the system design.

system is disabled). Possible safe states for the CHB system may include (but are not limited to) those listed in Table 21.

Table 20. Possible CHB System Safe States

Safe State	CHB System Behavior	Example Triggering Events
CHB-1	Disable TCS • Other unaffected CHB features may continue to operate	Fault in the TCS subsystem or in sensors critical to TCS operation
CHB-2	Disable ESC • Other unaffected CHB features may continue to operate	Fault in the ESC subsystem or in sensors critical to ESC operation
CHB-3	Disable ABS • Other unaffected CHB features may continue to operate	Fault in the ABS subsystem or in sensors critical to ABS operation
CHB-4	Limit the brake torque authority of electronic CHB features.	Fault in one of the brake pedal position sensors
CHB-5	Disable all electronic CHB features • Limit braking to the mechanical service brake	High severity hardware fault, CHB control module fault, low voltage power supply fault
CHB-6	Limit electronic portion of CHB system to implementing core braking functions (ABS, TCS, ESC). • Disable advanced features relying on the brake system (AEB, ACC, Hill Holder, LKA, etc.)	Communication system fault, arbitration logic fault

The objective of the safe states is to reduce the overall risk at the vehicle level. Some of the safe states listed in Table 21 include degraded operating modes of the CHB system, which may indirectly contribute to hazardous vehicle states. However, disabling these malfunctioning CHB functions may be preferable to allowing malfunctioning CHB functions from affecting the vehicle's dynamics. Furthermore, by transitioning to a safe state, degradation of the CHB system functionality is controlled and the driver is notified.

For example, disabling the ESC function as part of Safe State 2 may contribute to unintended or insufficient lateral motion/yaw since ESC may not be available to intervene in an oversteer or understeer condition. However, this may be preferable to allowing a malfunctioning ESC system from inadvertently inducing yaw in the vehicle. In addition, notifying the driver as part of the safety strategy may allow the driver to better control the vehicle (e.g., by taking more conservative driving maneuvers).

Although ALC systems currently on the market do not rely on the CHB system as the primary actuating system, if the CHB system is used as a redundant actuating system, a failure in the

CHB system that disables differential braking functions may effectively degrade an ALC system from a fail-operational status to fail-safe.

D.5.1.4 Safe States for ALC

The possible safe states for an ALC system may vary based on the automation level.

- For Automation Level 1 and Level 2 - Driver Engaged, the ALC system may be able to revert to manual control immediately. Therefore, potential safe states may include full operation, degraded operation, or a switched off mode.
- For Automation Level 2 - Driver Not Engaged and Automation Level 3, the ALC system may be able to revert to manual control after a suitable notification period. Therefore potential safe states may include full operation, degraded operation (with or without affecting other systems), or a switched off mode following adequate driver notification.
- For Automation Level 4 and Level 5, lane centering may be one of several functions in a higher level path planning algorithm. Additionally, reverting to manual control may not be possible in some Level 4 or Level 5 automated vehicles. Therefore potential safe states may include full operation, degraded operation (with or without affecting other functions), or a pulled-over or stopped mode.

Possible safe states for the ALC system may include (but are not limited to) those listed in Table 21. Table 21 also indicates which level of automation each safe state may support.

Table 21. Possible ALC System Safe States

Safe State	ALC System Behavior	Automation Level						Example Triggering Events
		1	2-E[1]	2-NE[2]	3	4	5	
ALC-1	Restrict ALC system operation (e.g., roadway type or allowable speed). • Reduce or restrict vehicle speed if appropriate.	●	●	●	●	●	●	Failure in a foundational steering system that limits steering authority
ALC-2	Disengage the ALC system and revert to an LKA or LDW system. • Depending on the level of automation, this may or may not require a transition period.	●	●	●	●	●[3]	●[3]	Failure in the algorithm that calculates the reference trajectory.
ALC-3	Disengage the ALC system following a predetermined period of time.	●	●	●	●	●[3]	●[3]	Failure of one element (e.g., minimum triple redundancy)
ALC-4	Disengage the ALC system immediately.	●	●					Failure of one element (e.g., no redundancy)
ALC-5	Reduce propulsion gradually. • The ALC system steers the vehicle to the side of the roadway.			●	●	●	●	Failure of two elements (e.g., minimum triple redundancy)
ALC-6	Reduce propulsion gradually. • Stop the vehicle in the lane. • Activate hazard lights or other indicators of a disabled vehicle to alert surrounding vehicles.			●	●	●	●	Failure of all redundant elements

[1] Driver Engaged - Assumes the system design ensures that the driver remains engaged in the driving task.
[2] Driver Not Engaged - Based on the assumption of foreseeable driver misuse that prevents the driver from immediately resuming control of the vehicle in the event of a failure.
[3] Safe state may not apply for vehicles that do not provide a mechanism for the driver to resume lateral control (e.g., no steering wheel).

The objective of the safe states is to reduce the overall risk at the vehicle level. Some of the safe states listed in Table 21 include degraded operating modes of the ALC system, which may otherwise be considered unsafe (e.g., stopping in the lane). However, entering these degraded operating modes may be preferable to allowing a malfunctioning ALC system to continue operating (e.g., loss of lane centering while travelling at full vehicle speed). Furthermore, by transitioning to a safe state, degradation of the ALC system is controlled and the driver is notified.

D.5.2 Architectural Strategies for ALC Systems

ALC systems allow the driver to cede lateral control of the vehicle to the automation system. Ensuring there is continuous control of the vehicle's lateral position – either by the driver or the

automation system – is a key component of the functional safety concept. ALC systems may be designed using different fail-operational or fail-safe strategies, depending on factors such as use cases, design details, and detailed safety calculations. Table 22 provides an example of how the different architectural strategies discussed in Section C.4 may be employed to support different levels of automation.

Table 22. Example Allocation of Architectural Strategies to Levels of Automation

Example System Architecture	**Level of Automation**					
	Level 1	**Level 2-E[1]**	**Level 2-NE[2]**	**Level 3**	**Level 4**	**Level 5**
Fail-Operational (Similar Redundancy)	●	●	●	●	●	●
Fail-Operational (Dissimilar Redundancy)	●	●	●	●	○	○
Fail-Safe/Fail-Passive with Redundant Actuation	●	●	●	●	○	○
Fail-Safe/Fail-Passive w/o Redundant Actuation	●	●	○	○	○	○

● – Generally supported
○ – Would require detailed analysis and validation of specific use cases and DVI strategies
[1] Driver Engaged - Assumes the system design ensures that the driver remains engaged in the driving task.
[2] Driver Not Engaged - Based on the assumption of foreseeable driver misuse that prevents the driver from immediately resuming control of the vehicle in the event of a failure.

D.6 Additional Human Factors Considerations

ALC systems, along with other automated vehicle systems, present additional human factor challenges that may not apply to the foundational vehicle systems. This section describes these challenges and presents potential countermeasures.

D.6.1 Possible Countermeasures to Reduce Operator Disengagement

Studies have demonstrated that operators often fail to remain engaged when they have little or nothing to do [35] [36] [27]. In applications in control rooms and commercial transportation, automation has allowed substantial reductions in crew size, but the remaining crew members usually have sufficient workloads to keep them engaged. There are no analogous countermeasures for unaccompanied drivers of personal vehicles. Simulator studies of automated driving show that if distractions (e.g., smartphones) are available, participants will use them [36]. Even in the absence of distractions, simply falling asleep becomes a significant risk.

The need to counteract the Y-D effect has been implicitly recognized throughout human history, but no universally satisfactory means to counteract the Y-D effect are available. Fear of punishment for dereliction of duty has been one approach. In the past, some industrial jobs exposed workers to hazards from nearby machinery if the worker did not pay close attention. Emphasizing the personal risk to drivers, occupants, and pedestrians that could result from driver disengagement may serve a similar role.

One widely used approach for maintaining engagement in automated cockpits and control rooms is for the operators to keep in frequent contact with each other and with remotely located controllers and supervisors [37]. These techniques may not be applicable to unaccompanied drivers in private automobiles. However, vehicle systems that verbally communicate with the driver (e.g., notification of upcoming navigation actions) may fill this role to some degree so long as they are not perceived as superfluous.

Loud alarms that alert operators to dangerous conditions are employed in commercial transportation and in industrial control rooms. Operators find this generally acceptable only when the technology has advanced to the point that false alarms are relatively rare. At the present state of the art, lane-departure and disengagement warnings occur so frequently that they would be unacceptably annoying if their sound pressure levels were as high as those used in other applications.

In aviation and other industries, sudden transitions from automated to manual operations sometimes occur. Organizations provide regular training and practice to prepare operators for such events, often in simulators. It is not apparent how equivalent training and practice could be provided to operators of personal motor vehicles. Fortunately, mapping locations where disengagements occur via crowdsourcing or other methods could eventually increase the typical warning interval and possibly reduce (but not eliminate) the likelihood of unanticipated disengagements.

Practical experience with self-steering vehicles is available from the railroad industry. The locomotive engineer's workload is highly variable, requiring frequent control movements in some situations while allowing extended periods with no control input in others (e.g., operating a heavy freight train up a long grade in a sparsely populated area). To prevent runaway trains when operators fell asleep or were medically incapacitated, railways began fitting "dead man's pedals" to street cars as early as the 1890s. More recently, the industry has employed "alerters," devices that automatically cut the throttle and apply the brakes if the operator does not respond to a prompt within a prescribed period time frame (typically 30 seconds). In the United States, alerters are reset by a simple movement (e.g., pushing a large mushroom-shaped button). They have greatly reduced, but not entirely eliminated, collisions and derailments resulting from engineers falling asleep. However, operators can develop habitual behaviors that reset the alerter and can be performed in a light sleep [38]. If ALC systems were to require similarly minimal actions, drivers could conceivably develop analogous responses in light sleep. This could call into question the ultimate effectiveness of approaches such as measuring the applied steering-wheel torque as a sole indicator of driver engagement in ALC-equipped automobiles.

D.6.2 DVI Considerations

To gain widespread acceptance and use, designers of driver-assistance and automated vehicle technologies such as ALC should consider employing the established human-factors principles

described in the following subsections. Unfortunately, full compliance can be difficult for several reasons:

- The required technology has not yet been developed.
- The most appropriate technology is too expensive for the intended market.
- The DVI display loses out in competition for space on the instrument panel with other features.
- Designers who know how their system works fail to appreciate how naïve or occasional users may be confused by its features.

D.6.2.1 Easy to Learn and Use

An ideal system would work for all driving conditions and road types and would always be active. Since current systems are typically intended for use only on highways with well-marked lanes, drivers must make judgments, usually based on prior experience, as to whether the system will work on a given stretch of highway under the prevailing environmental conditions. While it may be relatively easy to judge whether some situations are appropriate for ALC use, applicability in other scenarios may be questionable. These less certain situations may increase the likelihood of driver confusion if the ALC system does not engage when expected.

Employing ALC systems would likely be more common if the location and operation of the switches that enable or disable the ALC system were standardized. Controls should be convenient; placing controls to engage or disengage the system near the bottom of the instrument panel may make them more difficult to identify and use, especially for far-sighted drivers.

D.6.2.2 Clear Intuitive Indication of Current State of Operation

Current ALC systems typically display an icon in the central portion of the instrument panel or on the center stack. It generally shows the driver's vehicle and the lane boundaries when detected. The lane boundary indicators are usually gray or dashed or only outlines when not being detected and become solid when detected. Icons indicating that ACC and ALC are active are usually present in the same area. The lack of standardization in the position of these displays raises the possibility that drivers who are used to one system might be confused when driving unfamiliar vehicles.

One issue that remains to be determined through test driving is how useful these displays are in a stressful situation. In such scenarios, drivers are likely to focus their attention on the road and be oblivious to warnings in these displays, especially displays located in the center stack.

Mode confusion has been identified in the past as a cause of airliner crashes. It could contribute to future automotive crashes if drivers mistakenly believe the vehicle is steering itself when the ALC system is actually disengaged.

D.6.2.3 Instilled Trust of the System

An appropriately functioning lateral control system might demonstrate to the driver that it knows current positions of lane boundaries, the own-vehicle's location with respect to those boundaries, and positions of other nearby vehicles by displaying icons that accurately reflect what the driver is seeing. Most current systems perform this task well under intended-use conditions and working in combination with radar and other sensors in, for example, the ACC, automatic emergency braking, and blind-spot-warning systems.

The lateral control system could inspire further trust by steering the vehicle smoothly down the center of the lane. However, current systems (LKA systems in particular) are not always designed to do this. Some systems allow the vehicle to drift back and forth between lane markers if the driver is not actively steering continuously. Furthermore, many systems prompt the driver to resume active steering if they sense several seconds with hands off the wheel. If drivers make only minimal inputs, some systems generate pronounced wobbling within the lane that might be viewed as disconcerting.

A third aspect of trust-building is that the ALC system should avoid spontaneous disengagement, particularly when for no apparent reason. Some systems fare poorly in this regard. Systems in several luxury cars recently tested by *Car and Driver* magazine averaged at least one disengagement of the lane control system per mile travelled over a 50-mile test course [39].

Finally, systems could also instill trust by displaying that they are aware of other hazards besides lane boundaries and a few nearby vehicles (e.g., pedestrians, vehicles in the non-adjacent breakdown lane, emergency vehicles, construction workers, etc.).

Most especially, ALC systems should provide advance warning of situations that will cause automatic disengagement. The minimum lead time for such warnings has not been determined, but periods on the order of 20 seconds are used in aviation. However, this may be beyond the capability of current ALC systems.

D.6.2.4 Driver Training

ALC systems provide continuous steering control and thus produce a significantly different driving experience. Manufacturers might consider the degree to which naïve drivers might require training. Passages in an owner's manual may not be sufficient for all drivers. Consequently, one manufacturer provides a 15-minute video tutorial with the software download.

D.6.2.5 Avoidance of complacency and loss of situational awareness

There is no definitive evidence that ALC systems significantly increase crash risks caused by driver complacency or loss of situational awareness. Many of these systems spontaneously disengage with such high frequency that drivers apparently do not trust them to operate safely over any significant distance without driver intervention. Furthermore, current systems prompt the driver to regularly grip the steering wheel and make manual inputs.

A longer term issue is how industry might adjust driver-interaction protocols once ALC (along with ACC, full automatic braking, and blind-spot protection) perform with superior reliability (i.e., requiring only minimal and infrequent driver oversight). As discussed in Section A.5, evidence from other situations in which a human operator plays only a monitoring role suggests that complacency and loss of situational awareness can ensue.

Falling asleep, especially during night driving, may become a significant risk. In industrial control rooms, and in commercial transportation, employers usually deploy a range of measures to ensure that operators remain focused on their monitoring tasks. Typical measures include:

- Multiple operators on duty in the same work space,
- Supervisors who check-up from time to time,
- Frequent conversations with other operators and controllers via radio or intercom,
- Requirements to submit reports periodically during the work turn, and
- Alerting devices that require frequent responses.

In some industries, employers also subject operators to periodic medical screening for sleep disorders and drug use. None of these approaches are likely to be applicable to operators of private motor vehicles under current law. A few manufacturers offer video-based monitoring systems that can determine when a driver's eyes are open and directed toward the road. These systems can be configured to sound or display a message when the driver's eyes are no longer on the road, but their use is currently at the driver's discretion.

D.6.2.6 Design Tradeoffs

As with any engineered system, the design of lateral control systems will require design tradeoffs. In some currently deployed LKA systems, designers allow the drivers to adjust several operational attributes over a reasonable range. These adjustments are typically changes in parameter values in controller software and require no hardware changes. Some examples include:

- The width of the dead band in which the vehicle may drift about in a lane without triggering a system response
- Rise-time and decay-time for steering torques generated by the system. This can affect the driver's perception of "smoothness."
- The maximum corrective torque applied by the system. Too low a value could delay response to an imminent lane departure; too high a value could startle a driver trying to change lanes without first activating the turn signal.
- Timing and magnitude of audible and haptic warnings of imminent lane-boundary encroachment. Too late or too little can be ineffective; too soon or too much can be sufficiently annoying that drivers avoid engaging the system.
- The maximum time drivers may keep their hands off the steering wheel without triggering a warning message and/or automatic system disengagement.

The first three examples demonstrate the inherent tension between inducing discomfort as the vehicle approaches a lane boundary (e.g., by a relatively abrupt steering correction) and risking driver complacency by making all corrections early and smoothly. Designers might be expected to tweak the nominal values of these parameters in new hardware and software releases based on feedback from owners and dealers. Manufacturers that provide automatic software updates will likely consider whether a new functionality could require the resetting of any parameters and, if so, how to best inform the driver.

D.6.3 Opportunities for Effective Mode Transition

In the literature reviewed for this research, three promising approaches to mitigating the risks in the transitions between automated and manual driving in Level 2 and Level 3 ALC systems were identified. They are discussed in the subsections below.

D.6.3.1 Timely warnings of impending transitions

Recent developments in mapping technology suggest that it will be feasible to precisely geocode instances of disengagement due to loss of lane markings. This data could be made available to every equipped vehicle so that its automated systems can anticipate locations where disengagement is a risk and prompt the driver to assume full control with adequate warning time. Of course, this approach is not a panacea. Fluid situations (e.g., unforeseen roadway incidents) may require data augmentation with real-time crowdsourced data. Even that may be insufficient in remote regions.

D.6.3.2 Shared control

Shared control is a level of semi-automation in which the driver is never allowed to completely disengage from the driving task.[33] When sensors detect a potentially imminent crash, sufficient steering torque will be applied to prevent it if possible. When road markings are present, the system keeps the car in its lane. It may use other cues (e.g., guard rails or road edges) if lane markings are not present. However, these systems may allow the car to wander about within its lane so that drivers will be motivated to steer continuously. If a driver does not provide an input for an extended period of time, a haptic warning will be given. If that fails to elicit a driver response, the vehicle will slow to a stop. If the driver is actively steering, but inputs a torque that is insufficient or excessive, the system could exert a torque which serves both to prevent a crash and to train the driver regarding the proper steering torque for the particular conditions.

D.6.3.3 Minimize opportunities for mode confusion

Mode confusion has been blamed for airliner crashes despite the extensive simulator training pilots receive in coping with emergencies and malfunctions. As ALC systems become more

[33] Shared control is intended to address the problem of the driver's inability to resume control unexpectedly that is inherent in Level 2 systems. However, this type of system does not provide continuous control of the vehicle's lateral position. Since the driver is not ceding lateral control to the automated system, "shared control" may only meet the definition of Level 1 automation.

common, there is the potential for mode confusion (e.g., expecting its auto-braking function to be engaged despite being unwittingly disengaged). Original equipment manufacturers are investigating possible approaches to DVI design that minimizes whatever doubt may exist about who is in control of the vehicle.

E. OBSERVATIONS

E.1 Findings From Synthesis of ALC and Related Foundational System Studies

The hazards identified in this study for the foundational systems generally are stated in terms of the vehicle dynamics, since the primary mission of these systems is to implement lateral or longitudinal motion commands from either the driver or other vehicle systems. In this context, a hazard such as "unintended lateral motion/unintended yaw" may refer to any deviation from the control set-point established by the driver or another vehicle system. However, this same hazard is not as well-defined in the context of ALC systems. For example, an ALC system which meanders slightly but remains fully within the travel lane may exhibit "unintended lateral motion/unintended yaw" from the driver's perspective. However, since the system keeps the vehicle fully within the travel lane, this may not represent a hazard from the perspective of the ALC system. The hazard in the context of the ALC system may arise when this "unintended lateral motion/unintended yaw" results in the vehicle departing the travel lane. Essentially, the primary mission of the ALC system relies on context provided by the surrounding environment (e.g., roadway position). Therefore, the ALC system hazards identified in this study generally focus on the vehicle position in the lane. Other hazards identified for both the foundational vehicle systems and the ALC system describe vehicle states where a function intended to aid the operator is lost or compromised.

A key observation regarding the foundational systems is that the ASIL of a vehicle-level hazard can vary significantly depending on the system under consideration. For example, a malfunction of the braking system (e.g., errant ESC activation) can affect controllability, but a functioning steering system can provide at least some lateral control to the operator. In contrast, the ability of brake system features (e.g., differential braking) to provide more than minimal lateral control after the loss of the primary steering function is unlikely. This is demonstrated in Table 12.

As demonstrated in Table 13, the ASIL for ALC vehicle-level hazards is necessarily a function of the target automation level and driver engagement, specifically for its influence on the assessment of the controllability parameter. This presents a new challenge, particularly for Level 2 systems, which may have different assumptions regarding the ability of the driver to immediately resume control of the vehicle.

E.2 Considerations for the Interaction Between Foundational and Automated Systems

The functional safety assessments of the foundational systems employed the assumption that an engaged human operator is available to respond to any system malfunction. This is tantamount to an assumption of Automation Level 0 (no automation), Level 1 (driver assistance), or Level 2 – Driver Engaged. However, when considering an automated system such as ALC, the foundational vehicle systems may also be characterized as actuators for the automated system. If an automated system is designed to be fail-operational, then these design requirements would flow down to the actuating foundational systems. Either the actuating foundational system must

have sufficient capabilities to be fail-operational or the design may need to rely on multiple actuating foundational systems. Some of the design possibilities were referenced in Section C.3 and Section C.4.

Vehicle designers will make these architectural decisions, but it is critical that they consider the interface between the foundational systems and automated systems as part of the design process. In particular, they should be aware of whether a single electronic fault in the foundational system could violate the safety goals established for the automated system. It is important that assessment of these interactions not "fall through the cracks".

E.3 Challenges in Applying ASIL Process Across Automation Levels

The ASIL assessment is a key part of functional safety concept under ISO 26262. However, as automation is introduced into vehicles, a challenge in the ASIL assessment will be the assignment of the controllability factor under different levels of automation. This study assumed the worst-case controllability value, "C3," for automated systems operating at Level 2 – Driver Not Engaged and higher levels of automation (i.e., Level 3 through Level 5). This controllability assignment assumes that the driver may not able to immediately control the vehicle at these levels of automation. In particular, certain Level 4 and Level 5 concept vehicles may not include driver controls, such as a steering wheel [20]. Other vehicle systems may be capable of improving the controllability for automated systems, provided they are sufficiently independent as described in ISO 26262 Clause 7.4.1.2. However, this study does not assume the presence of such systems.

In the shorter term, one can contemplate the ISO 26262 concept of "foreseeable misuse" as applied to unengaged drivers as discussed in Section D.6. It is conceivable and expected that some operators will not remain engaged in the driving task when the bulk of the control is performed by a well-performing automation system. Regardless of warnings on the instrument panel or in the owner's manual, drivers could become significantly disengaged under these conditions. Therefore, a disengaged driver is quite likely within the realm of "foreseeable misuse" of the automation system unless a reliable system is in place to monitor and enforce driver engagement. Such a system would require a functional safety assessment as well.

F. SUMMARY AND CONCLUSIONS

This findings from this study may be used to:

- *Demonstrate how the Concept Phase of ISO 26262 may be implemented, including integration of multiple analysis methods.*

  The project described in this report produced functional safety assessments of three generic foundational systems (EPS, SbW, and CHB) and one generic automated control system [1] [2] [3] [4]. These assessments also considered human factors issues relevant to ALC systems. Two complementary hazard analysis approaches (HAZOP and STPA) were used to identify vehicle-level hazards and two complementary safety analysis approaches (FMEA and STPA) were used to identify potential underlying issues that might lead to these hazards. This comprehensive approach considered both control action failures and component malfunctions. ASILs were assigned to each vehicle-level hazard.

- *Establish a baseline functional safety concept for future development of ALC systems and related foundational systems, provide research data for future NHTSA activities with respect to ALC systems and related foundational systems, and illustrate how the analysis results may be used to develop potential test scenarios to validate the safety goals and functional safety requirements.*

  The results of these analyses were used to develop functional safety concepts for an EPS system, a SbW system, a CHB system, and an ALC system. The individual functional safety assessment reports provide more detail on the potential functional safety requirements and test scenarios for each system [1] [2] [3] [4].

  Designers of vehicles operating at high levels of automation should carefully consider the architectural options for the automation systems of their vehicles. Safety-critical functions will generally need some level of robustness that allows continued safe operation after a failure while transitioning to a safe state. The fail-safe and fail-operational architectures discussed can be used depending on the hazard, the operational scenario, the automation level, and the level of operator engagement. In addition, if a single electronic fault could potentially cause a foundational vehicle system to immediately revert to manual control, this may not support certain levels of vehicle automation that are required to continue operating safely while transitioning control back to the driver.

- *Demonstrate how the Concept Phase of ISO 26262 may be applied to across the different levels of automation, including an example of how to consider potential driver misuse of Level 2 automated systems.*

The human factors consideration led the analysts to recognize that "foreseeable misuse" as defined in ISO 26262 could result in an operator of an Automation Level 2 system becoming disengaged from the driving task if the system performance were sufficient to require only periodic monitoring. This led to the decision to evaluate Automation Level 2 in two categories, based on whether or not the operator was engaged. It may be prudent to presume the operator is not engaged unless a reliable mechanism is in place for verifying engagement.

The functional safety assessments of the foundational systems assumed their operation by an entirely engaged operator – essentially Automation Level 0 (No Automation), Level 1 (driver assistance), or Level 2 – Driver Engaged. When these foundational systems support automated systems operating at Level 2 – Driver Not Engaged or higher levels of automation (i.e., Level 3 through Level 5), the assumption that the driver is fully engaged and can immediately resume control of the vehicle may not be appropriate.

In addition, this report provides several example strategies to support different levels of automation, as shown in Table 23. These requirements may not be immediately apparent developing or analyzing the foundational systems in isolation.

Table 23. Example Allocation of Architectural Strategies to Levels of Automation

Example System Architecture	**Level of Automation**					
	Level 1	**Level 2-E[1]**	**Level 2-NE[2]**	**Level 3**	**Level 4**	**Level 5**
Fail-Operational (Similar Redundancy)	●	●	●	●	●	●
Fail-Operational (Dissimilar Redundancy)	●	●	●	●	○	○
Fail-Safe/Fail-Passive with Redundant Actuation	●	●	●	●	○	○
Fail-Safe/Fail-Passive w/o Redundant Actuation	●	●	○	○	○	○

● – Generally supported
○ – Would require detailed analysis and validation of specific use cases and DVI strategies
[1] Driver Engaged - Assumes the system design ensures that the driver remains engaged in the driving task.
[2] Driver Not Engaged - Based on the assumption of foreseeable driver misuse that prevents the driver from immediately resuming control of the vehicle in the event of a failure.

The results presented in this report and in the individual functional safety assessment reports are one team's analyses of some non-specific generic systems. Specific designs and technologies and their strengths and weaknesses with regard to robustness, resilience, and fault tolerance were not considered.

REFERENCES

[1] Becker, C., Nasser, A., Attioui, F., Arthur, D., Moy, A. & Brewer, J. (in press). *Functional safety assessment of a generic electric power steering system with active steering and four-wheel steering features* [Volpe Report Number DOT-VNTSC-NHTSA-16-02]. Washington, DC: National Highway Traffic Safety Administration.

[2] Becker, C., Brewer, J., Yount, L., Arthur, D. & Attioui, F. (in press). *Functional safety assessment of a generic steer-by-wire steering system with active steering and four-wheel steering features* [Volpe Report Number DOT-VNTSC-NHTSA-16-06]. Washington, DC: National Highway Traffic Safety Administration.

[3] Becker, C., Arthur, D. & Brewer, J. (in press). *Functional safety assessment of a generic conventional hydraulic braking system with antilock braking system, traction control system, and electronic stability control Features* [Volpe Report Number DOT-VNTSC-NHTSA-16-08]. Washington, DC: National Highway Traffic Safety Administration.

[4] Becker, C., Yount, L. (in press). Rozen-Levy, S., & Brewer, J., *Functional safety assessment of an automated lane centeringsystem* [Volpe Report Number DOT-VNTSC-NHTSA-17-01]. Washington, DC: National Highway Traffic Safety Administration.

[5] SAE International. (2014). *J3016: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems.* Warrendale, PA: SAE International.

[6] Stanyer, T., & Chutorash, R. (2014, October 27). *ESG Automotive Subject Matter Expert Interview on Automated Lane Centering.* [Interview].

[7] Lee, J.-W., Moshchuk, N. K., & Chen, S.-K. (2014, March 11). Lane Centering Fail-Safe Control Using Differential Braking. U.S. Patent No. 8,670,903.. Washington, DC: U.S. Patent Trademark Office.

[8] Kade, A., Bartz, D., Hudas, G., & D. G. Mikulski, D. G. (2014, October 28). *Tank Automotive Research, Development and Engineering Center Subject Matter Expert Interview on Automated Lane Centering.* [Interview].

[9] Pimentel, J. R. (2004). An architecture for a safety-critical steer-by-wire system (SAE Technical Paper 2004-01-0714), 2004, https://doi.org/10.4271/2004-01-0714. in *SAE 2004 World Congress & Exhibition*.

[10] Heitzer, H.-D. (2003). Development of a fault-tolerant steer-by-wire steering system, *Auto Technology, 4*, pp. 56-60.

[11] Cesiel, D., Gaunt, M. C., & Daugherty, B. (2006). Development of a Steer-by-Wire System for the GM Sequel Detroit: 2006 SAE World Congress, Detroit.

[12] Walker Jr., J. (2005). *Introduction to Brake Control Systems: An SAE Professional Development e-Seminar*. Warrendale, PA: SAE International.

[13] Pollard, J. (in press). Human factors issues related to automated lane centering (ALC) systems, DOT-VNTSC-NHTSA-17-02]. Washington, DC: National Highway Traffic Safety Administration.

[14] International Organization for Standardization. (2011). Road vehicles - functional safety(Final Draft). (ISO 26262). Geneva: Author.

[15] International Electrotechnical Commission. (2001). Hazard and operability studies (HAZOP Studies) - Application guide, Edition 1.0. (IEC 61882-2001). Geneva: Author.

[16] Leveson, N. (2012). Engineering a safer world. Cambridge: MIT Press.

[17] Society of Automotive Engineers. (1994). Potential failure mode and effects analysis in design and potential failure mode and effects analysis in manufacturing and assembly processes. (SAE J1739). Warrendale, PA: Author. [Editor's note: In 2006 the Society of Automotive Engineers changed its name to SAE International.]

[18] Thomas, J. (2013). Extending and Automating a Systems-Theoretic Hazard Analysis for Requirements Generation and Analysis (Ph.D. dissertation). Cambridge, MA: Massachusetts Institute of Technology.

[19] Coudert, O. (1994). Two-level logic minimization: An overview, *Integration, the VLSI Journal, 17*(2), pp. 97-140.

[20] Box, T. (2016, August 17). No Steering Wheel or Pedals in Ford's Plan for Fully Autonomous Car by 2021 Dallas: Dallas Morning News. Retrieved from www.dallasnews.com/business/autos-latest-news/20160817-no-steering- wheel-or-pedals-in-ford-s-plan-for-fully-autonomous-car-by-2021.ece

[21] Koopman, P., & Wagner, M. (2016). Challenges in Autonomous Vehicle Testing and Validation Detroit: SAE World Congress.

[22] Diamond, D., Campbell, A., Park, C., Halonen, J., & Zoladz, P. (2007, March 28). The

temporal dynamics of emotional memory processing: a synthesis on the nwurobiological basis of stress-induced amnesia, flashbulb and truamatic memories, and the Yerkes-Dodson law. *Neural Plasticity*. Retrieved from: www.ncbi.nlm.nih.gov/pmc/articles/PMC1906714/

[23] Mosher, A. (2016, July 1). Tesla drivers play Jenga, sleep, using Autopilot in nerve-wracking videos. McLean, VA: USA Today. Retrieved from www.usatoday.com/story/tech/news/2016/07/01/drivers-play-jenga-sleep- using-tesla-autopilot-nerve-wracking-videos/86613484/

[24] Krok, A. (2015, November 11). This is the stupidest misuse of Tesla's Autopilot yet, CNET: Road/Show.. Retrieved from www.cnet.com/roadshow/news/this- is-the-stupidest-misuse-of-teslas-autopilot-yet/

[25] Adams, E. Mercedes's New E-Class Kinda Drives Itself - and It's Kinda Confusing, Wired.com, 27 June 2016. [Online]. Available: www.wired.com/2016/06/ mercedess-new-e-class-kinda-drives-kinda-confusing/

[26] State Farm. (2016, August 31). Self-Driving Cars: What to Do With All That Spare Time, State Farm Mutual Automobile Insurance Company, 31 August 2016. Bloomington, IL: Author. Available at https://newsroom.statefarm.com/state-farm-releases-autonomous-vehicles-survey-results?cmpid=PArel083116autonomousvehicles&utm_source=Direct

[27] Rudin-Brown, C., & Parker, H. (2004). Behavioural adaptation to adaptive cruise control (ACC); implications for preventive strategies, *Transportation Research Part F-Traffic Psychology and Behaviour, 7*(2) pp. 59-76.

[28] Merat, N. & Jamson, A. H. (2009). How do drivers behave in a highly automated car? *Fifth International Driving Symposium on Human Factors in Driver Assessment, Training and Vehicle Design*, Big Sky, MT.

[29] Lemer, N., Jenness, J., Robinson, E., Brown, T., Baldwin, C., & Llaneras, R. (2011). Crash Warning Interface Metrics. (Report No. DOT HS 811 470a). Washington, D: National Highway Traffic Safety Administration Available at https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/811470a.pdf

[30] Merat, N., Jamson, A. H., Lai, F. C., Daly, M., & Carsten, O. M. Transition to Manual: Driver Behavior when Resuming Control from a Highly Automated Vehicle, *Elsevier: Transportation Research*, vol. Part F, no. 27, pp. 274-282, 2014.

[31] International Electrotechnical Commission. (2016). Functional Safety - IEC 61508 Explained (IEC 61508) Geneva: Author.Available at www.iec.ch/functionalsafety/explained/

[32] Department of Defense. (2012). Department of Defense Standard Practice: System Safety (MIT-STD-882E). Washington, DC: Author.

[33] Isermann, R., Schwarz, R., & Stölzl, S. (2002, October). Fault-Tolerant Drive-by-Wire Systems, IEEE Control Systems. Piscataway, NJ: Institute of Electrical and Electronics Engineers.

[34] Lee, J.-W., Moshchuk, N. K., & Chen, S.-K. U.S. Patent No. 20,120,283,907. Washington, DC: United States Patent and Trademark Office.

[35] Carsten, O., Lai, F., Jamson, A., & Merat, N. (2012). Control task substitution in semiautomated driving: does it matter what aspects are automated? *Human Factors, 54*(5).

[36] Llaneras, R., Salinger, J., & Green, C. (2013). Human factors issues associated with limited ability autonomous driving systems: Drivers' allocation of visual attention to the forward roadway *7th International Driving Symposium on Human Factors in Driver Assessment, Training and Vehicle Design*, Lake George, Bolton Landing, NY, June 17-20, 2013.

[37] Degani, A., Shafto M., & Kirlik, A. (1996). Modes in Automated Cockpits: Problems, Data Analysis, and a Modeling Framework. *Proceedings of the 36th Israel Annual Conference on Aerospace Sciences*, Haifa, Israel, 1996.

[38] Oman, C. Locomotive Alerter technology Assesment. (2013). *TRB Railroad Operational Safety Meeting*, Omaha, NB, 2013.

[39] Sherman, D. (2016, February). Home/Features/Semi-Autonomous Cars Compared! Tesla Model S vs. BMW 750i, Infiniti Q50S, and Mercedes-Benz S65 AMG – Feature. Ann Arbor, MI: Car and Driver.

[40] National Center for Statistics and Analysis. (2014, January.) National Automotive Sampling System (NASS) General Estimates System (GES) analytical user's manual 1988-2012 (Report No. DOT HS 811 853). Washington, DC: National Highway Traffic Safety Administration.

[41] National Center for Statistics and Analysis. (2013, November). 2012 Fatality Analysis Reporting System (FARS) and National Automotive Sampling System (NASS)

General Estimates System (GES) coding and validation manual (Report No. DOT HS 811 854). Washington, DC: National Highway Traffic Safety Administration.

[42] National Highway Traffic Safety Administration. (n.a.). NHTSA's Process for Issuing a Recall Web page). Washington, DC: Author. Available at www-odi.nhtsa.dot.gov/owners/RecallProcess

[43] 71 FR 75370, Dec. 14, 2006, as amended at 74 FR 29896, June 23, 2009, Part 573, —Defect and Noncompliance Responsibility and ReportsAvailable at www.gpo.gov/fdsys/pkg/CFR-2011-title49-vol7/pdf/CFR-2011-title49-vol7-part573.pdf

[44] National Highway Traffic Safety Administration (n.a.). Manufacturer's Noncompliance Recall Quarterly Guide and Forms (Web page). Washington, DC: Author. Available at www.nhtsa.gov/Vehicle+Safety/Recalls+&+Defects/Manufacturer's+Noncompliance+Recall+Quarterly+Guide+and+Forms

[45] Transportation Research Board. (2012). The Safety Promise and Challenge of Automotive Electronics: Insights from Unintended Acceleration (Special Report 308). Washington, DC: National Research Council.

[46] Wall Street Journal. (2015, February 3). Sales and Share of Total Market by Manufacturer (Web page). Retrieved from http://online.wsj.com/mdc/public/page/2_3022-autosales.html#autosalesE

[47] Wards Automotive. (2014). North America Light Vehicle Sales and Market Share. Detroit: Wards Automotive Yearbook.

APPENDIX: ANALYSIS OF CURRENT SAFETY ISSUES

Volpe reviewed the National Automotive Sampling System (NASS) General Estimates System (GES) and Fatality Analysis Reporting System (FARS), and NHTSA's Vehicle Recall Campaigns and Vehicle Owners' Questionnaires (VOQs) to better understand the safety issues related to ALC/LKA technologies and the foundational braking and steering systems. Analysis of these data sources will support the hazard analysis and safety analysis tasks in this project by:

1) Verifying the preliminary list of vehicle-level hazards;
2) Determining if the guide phrases used in both the Systems-Theoretic Process Analysis (STPA) and Hazard and Operability Study (HAZOP) hazard analysis methods are sufficient to capture the scope of observed problems;
3) Identifying known causal factors affecting the ALC/LKA, foundational braking, and foundational steering systems.

General Estimates System and Fatality Analysis Reporting System

The GES database contains crash statistics on police-reported crashes across the United States involving all types of vehicles. The information comes from samples of police reports for over five million crashes that occur annually. The database is weighted to characterize a nationally representative sample. Each crash must involve at least one motor vehicle travelling on a roadway that results in property damage, injury, or death, and it must be obtained from a police report [40].

The FARS database contains information on all crashes in the United States involving at least one fatality resulting from the crash. The fatality can be either an occupant of the vehicle or a non-motorist, such as a pedestrian, and it must have occurred within 30 days of the crash. The crash must have occurred on a public roadway [41].

Although they represent two distinct databases, as a result of an effort to standardize the FARS and GES databases in 2010, these two databases now include similar data. The data contained in FARS are actual counts and the data in GES are a nationally weighted sample of crashes.

Volpe analyzed the 2012 GES and FARS crash databases to identify crashes at least partially attributable to braking and steering issues. In 2012 there were an estimated 5.6 million police-reported crashes involving vehicles of all types in GES and 30,800 fatal crashes in FARS.

The data element "ACC_TYPE" was used to determine the crash category that best describes the type of crash that the vehicle was involved in based on the pre-crash circumstances. To determine if the vehicle had a pre-existing brake or steering issue that may have contributed to the crash, the data element "MFACTOR" was used. The brake system also includes the parking brakes. The steering system includes the tie rod ends, kingpins, power steering components and ball joints. More information on the coding can be found in the user's manuals of these

databases. The GES and FARS databases do not provide details on the specific failure modes that resulted in the braking or steering system issue.

Table 24 shows the percentage of crashes reportedly caused by a condition of or issue with the braking system, the steering system, or both. Of the three categories, issues with the braking system resulted in the greatest number of crashes.

Table 24: Percentage of Braking and Steering-Related Crashes

All 2012 Crash Types						
Database	Braking System	Steering System	Braking and Steering	All Braking or Steering Related	All Others Includes: No Issues, Other Issues, Not Reported, Unknown	**Total**
GES *	32,477 (0.58%)	9,497 (0.17%)	549 (0.01%)	42,523 (0.76%)	5,562,399 (99.24%)	**5,604,921 (100%)**
FARS	95 (0.31%)	20 (0.06%)	6 (0.02%)	121 (0.39%)	30,679 (99.61%)	**30,800 (100%)**
* This is the GES Weighted National Average						

The coded crash types in the GES and FARS databases provide information on the types of crashes that could result from braking or steering issues. Table 25 shows the number of crash types reported in the GES and FARS databases for braking and steering system related issues.

Table 25: GES and FARS Crash Types for Braking and Steering System-Related Issues

Crash Type	2012 GES Weighted National Average				2012 FARS			
	Braking System	Steering System	Braking and Steering	All Others	Braking System	Steering System	Braking and Steering	All Others
No Impact *	305	224	–	23,139	5	1	–	357
Category I: Single Driver								
Right Roadside Departure	3,533	4,440	88	526,691	21	11	–	6,923
Left Roadside Departure	2,608	2,064	266	357,117	15	4	3	5,347
Forward Impact	1,314	1,438	140	684,846	13	1	2	5,673
Category II: Same Trafficway, Same Direction								
Rear End	16,959	200	–	1,749,908	9	–	1	1,717
Forward Impact	–	–	–	1471	–	–	–	11
Sideswipe/Angle	1,271	467	–	427,315	2	–	–	595
Category III: Same Trafficway, Opposite Direction								
Head-On	162	109	–	33,513	1	2	–	2,578
Forward Impact	–	–	–	1,299	1	–	–	28
Sideswipe/Angle	236	117	–	73,151	2	–	–	1,243
Category IV: Change Trafficway, Vehicle Turning								
Turn Across Path	282	67	–	483,516	4	–	–	1,589
Turn Into Path	378	348	–	449,673	2	–	–	831
Category V: Intersecting Paths								
Straight Paths	2,937	–	–	374,394	9	–	–	1,916
Category VI: Miscellaneous								
Backing, Etc.	2,493	21	56	376,364	11	1	–	1,871

* No impact describes a range of non-collision events including vehicle fire, immersion, gas inhalation, jackknife, rollovers, injured in vehicle, etc. Vehicle rollover is the only no-impact crash type considered within scope for this project.

Volpe compared these crash types with the preliminary list of hazards to determine if all the identified crash types could reasonably result from one or more of the preliminary hazards. If a crash type could not be linked to one of the preliminary vehicle-level hazards, this would suggest an additional hazard may be necessary.

Since the GES and FARS databases do not provide detailed case-by-case information on the vehicle condition or state prior to the crash, the information contained in this table was carefully analyzed. For example, besides the possibility of a cause related to the steering system, the crash type “right roadside departure” could reasonably result from the hazard “insufficient vehicle deceleration” if a brake issue prevents the driver from sufficiently slowing the vehicle as it enters a curve to the left. Similarly, this crash type may be caused by brake issues that result in

incorrect application of a braking differential, resulting in "unintended lateral motion" and "unintended vehicle rotational motion (yaw)."

Table 26 lists the GES and FARS crash types and the preliminary hazards that may potentially lead to the listed crash types. Each preliminary hazard was assessed whether it could result from a braking issue, steering issue, or both.

Table 26: Mapping Between GES/FARS Crash Types, Preliminary Hazards, and Potential Contributing Systems

GES/FARS Crash Type	Preliminary Hazard(s)	Potentially Caused by Braking Issue	Potentially Caused by Steering Issue
No Impact *	Unintended Vehicle Rotational Motion (Roll)	X	X
Category I: Single Driver			
Right Roadside Departure	Unintended Vehicle Lateral Motion	X	X
	Unintended Vehicle Rotational Motion (Yaw)	X	X
	Insufficient Vehicle Deceleration	X	
Left Roadside Departure	Unintended Vehicle Lateral Motion	X	X
	Unintended Vehicle Rotational Motion (Yaw)	X	X
	Insufficient Vehicle Deceleration	X	
Forward Impact	Insufficient Vehicle Lateral Motion		X
	Insufficient Vehicle Rotational Motion (Yaw)		X
	Insufficient Vehicle Deceleration	X	
	Absence of Lateral Control Input		X
	Absence of Longitudinal Control Input	X	
Category II: Same Trafficway, Same Direction			
Rear End	Insufficient Vehicle Lateral Motion		X
	Unintended Vehicle Deceleration (*Lead vehicle*)	X	
	Insufficient Vehicle Deceleration (*Following vehicle*)	X	
Sideswipe/Angle	Unintended Vehicle Lateral Motion	X	X
Category III: Same Trafficway, Opposite Direction			
Head-On	Unintended Vehicle Lateral Motion	X	X
	Unintended Vehicle Rotational Motion (Yaw)	X	X
Forward Impact	Unintended Vehicle Lateral Motion	X	
	Unintended Vehicle Rotational Motion (Yaw)	X	
	Insufficient Vehicle Deceleration	X	
Sideswipe/Angle	Unintended Vehicle Lateral Motion	X	X
	Unintended Vehicle Rotational Motion (Yaw)	X	X
Category IV: Change Trafficway, Vehicle Turning			
Turn Across Path	Unintended Vehicle Lateral Motion	X	X
	Unintended Vehicle Rotational Motion (Yaw)	X	X
	Insufficient Vehicle Deceleration	X	
Turn Into Path	Unintended Vehicle Lateral Motion		X
	Insufficient Vehicle Lateral Motion		X
	Unintended Vehicle Rotational Motion (Yaw)		X

GES/FARS Crash Type	Preliminary Hazard(s)	Potentially Caused by Braking Issue	Potentially Caused by Steering Issue
	Insufficient Vehicle Deceleration	X	
Category V: Intersecting Paths			
Straight Paths	Insufficient Vehicle Deceleration	X	
Category VI: Miscellaneous			
Backing, etc.	Unintended Vehicle Lateral Motion		X
	Insufficient Vehicle Lateral Motion		X
	Unintended Vehicle Rotational Motion (Yaw)		X
	Insufficient Vehicle Deceleration	X	
* No impact describes a range of non-collision events including vehicle fire, immersion, gas inhalation, jackknife, rollovers, injured in vehicle, etc. Vehicle rollover is the only no-impact crash type considered within scope for this project.			

This comparison did not reveal any crash types in the GES or FARS database that could not reasonably result from one or more of the preliminary hazards.

NHTSA Motor Vehicle Recall Campaigns

Either NHTSA or the manufacturers may issue recalls due to vehicle or equipment defects once it is determined that a safety defect exists in a motor vehicle or items of motor vehicle equipment that poses a risk to safety [42]. CFR 49 Volume 7 Part 573.6 [43] requires the manufacturer to furnish a report to NHTSA for each defect once a recall is warranted. The information in these reports that are relevant to this project includes:

- A description of the defect or non-compliance.
- In the case of a defect, a chronology of all principal events.
- In the case of a non-compliance, the test results and other information that the manufacturer considered in determining the existence of the non-compliance.

Manufacturers submit this information in a compiled Part 573 document publicly available from NHTSA along with all other related recall information [43] [44].

Volpe reviewed 146 motor vehicle recall campaigns for model year 2002 through 2015 light vehicles related to the following electronic control systems:

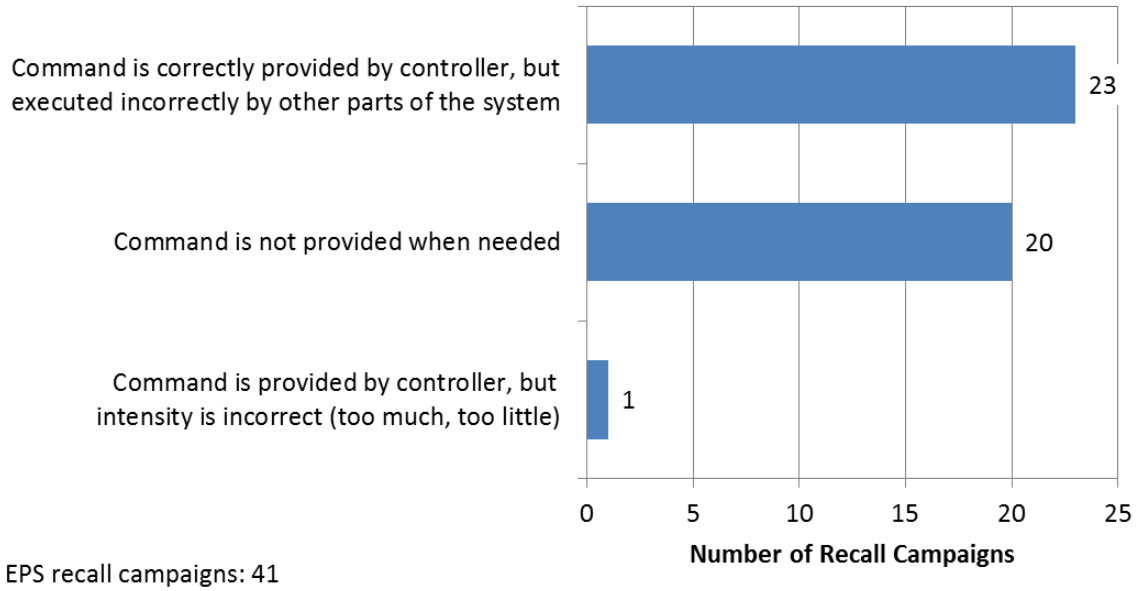
- ALC/LKA Systems,
- Conventional braking with antilock brakes and electronic stability control (ESC),
- Electronic power steering, and
- Steer-by-wire.

Volpe analyzed each recall to determine how the electronic control system may have become unsafe, contributing to the vehicle-level hazard. Volpe compared the unsafe control system behaviors to the six STPA unsafe control action guide phrases to determine if additional guide phrases are necessary to describe these recalls. The STPA unsafe control action guide phrases are:

1. Command is provided by controller when not needed.
2. Command is provided by controller, but the intensity is incorrect (too much or too little).
3. Command is provided by controller, but the duration is incorrect (too long or too short).
4. Command is provided by controller, but the starting time is incorrect (too soon or too late).
5. Command is correctly provided by controller, but is executed incorrectly by other parts of the system (e.g., actuators).
6. Command is not provided by controller when needed to maintain safety.

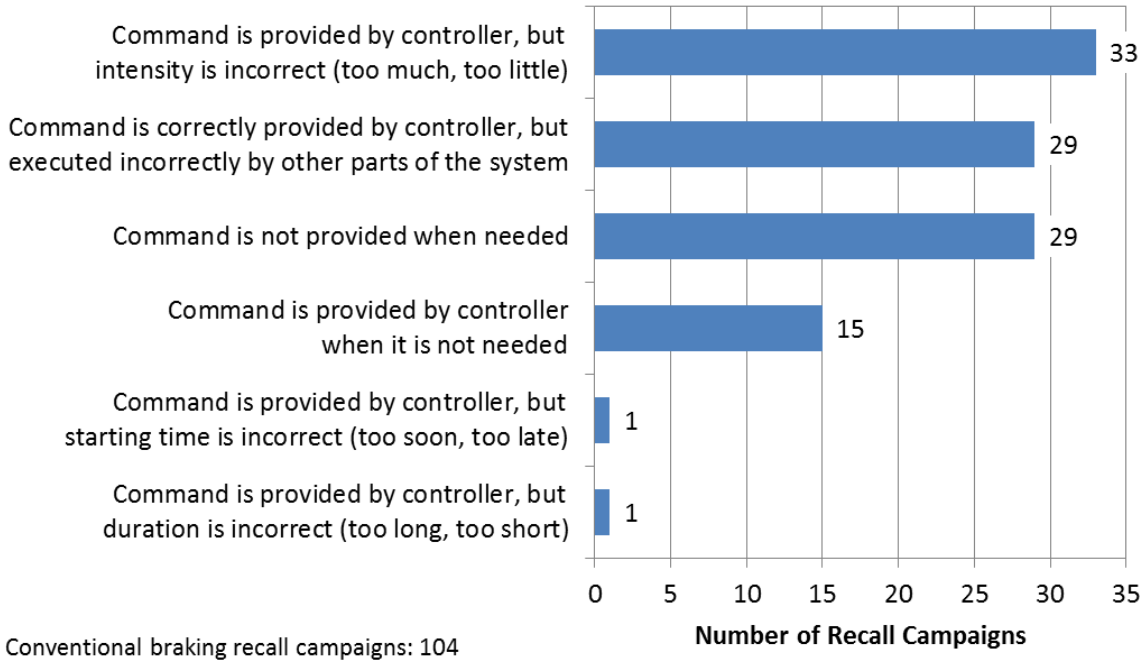
Each recall could be mapped to at least one of the STPA guide phrases, indicating that the set of guide phrases is sufficient to describe the types of recalls associated with these systems.

Figure 13 and Figure 14 show breakdowns of the recalls for the EPS and conventional brake system based on the unsafe control action guide phrases. Only one recall was related to the steer-by-wire system. This recall referenced a case in which the steer-by-wire system did not provide steering when needed and the activation of the mechanical backup system occurred too late. No recalls were related to ALC/LKA systems, although failures in the foundational steering and braking systems would affect ALC/LKA operation.



EPS recall campaigns: 41
44 recalls shown; 1 recall included multiple guide phrases

Figure 13: Unsafe Control Action Breakdown of EPS Recalls



Conventional braking recall campaigns: 104
108 recalls shown; 3 recalls included multiple guide phrases

Figure 14: Unsafe Control Action Breakdown of Conventional Brake System Recalls

Volpe also analyzed the recall data to develop an understanding of the types of causes for defects observed in these systems. Each recall was categorized using the 26 STPA causal factor guide phrases.

Figure 15 and Figure 16 show breakdowns of the recall campaigns based on the STPA causal factor guide phrases for the EPS and conventional brake system. The SbW system only had one recall campaign, which cited an external disturbance (e.g., a cold ambient temperature) as the cause. No recalls were related to the ALC/LKA system, although failures in the foundational steering and braking systems would affect ALC/LKA operation.

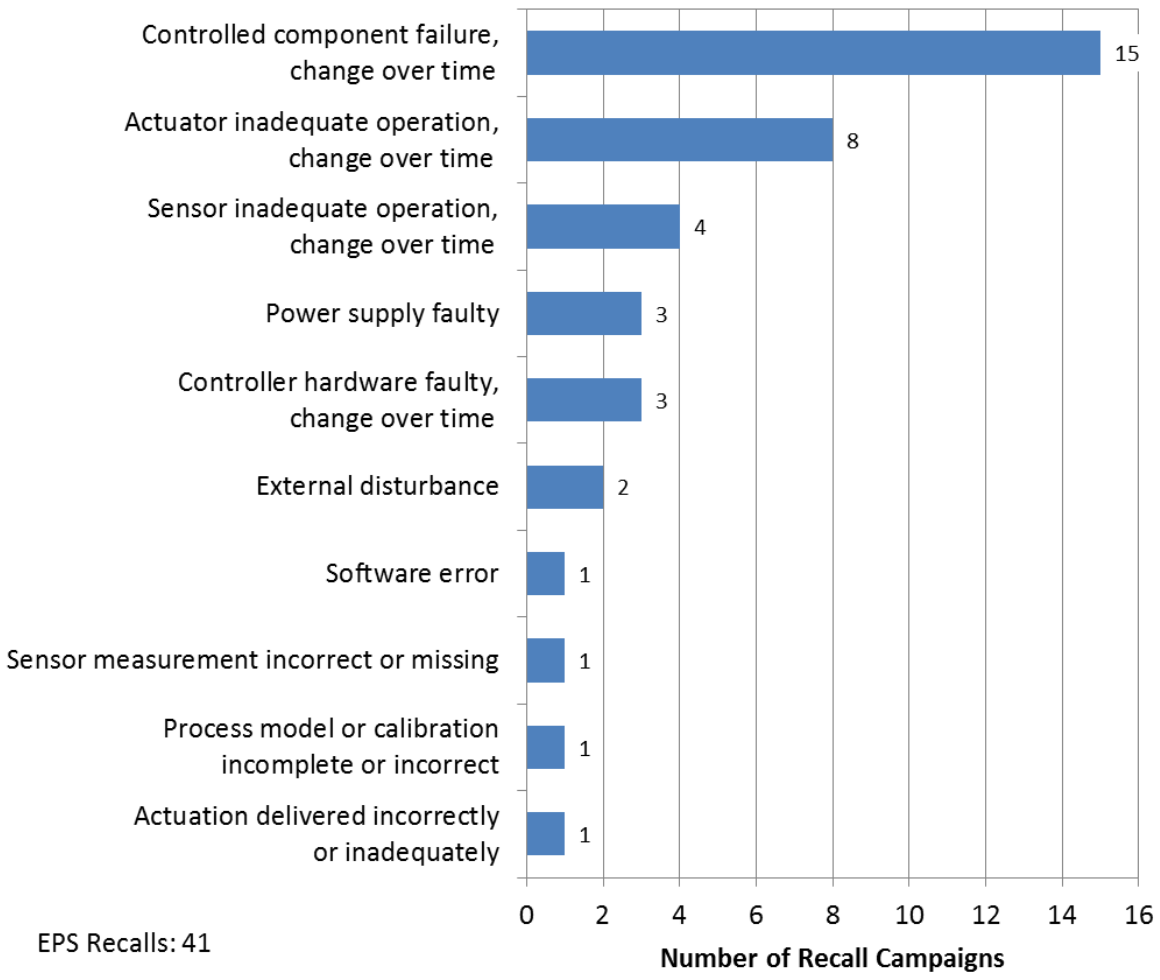


Figure 15: Causal Factor Breakdown of EPS Recalls

The largest percentage of recall campaigns related to the EPS cited failure of controlled components, such as tie rods, the steering column, and other mechanical parts associated with

adjusting the wheel position. The second highest percentage of recall campaigns cited failures with the actuator, such as the EPS motor.

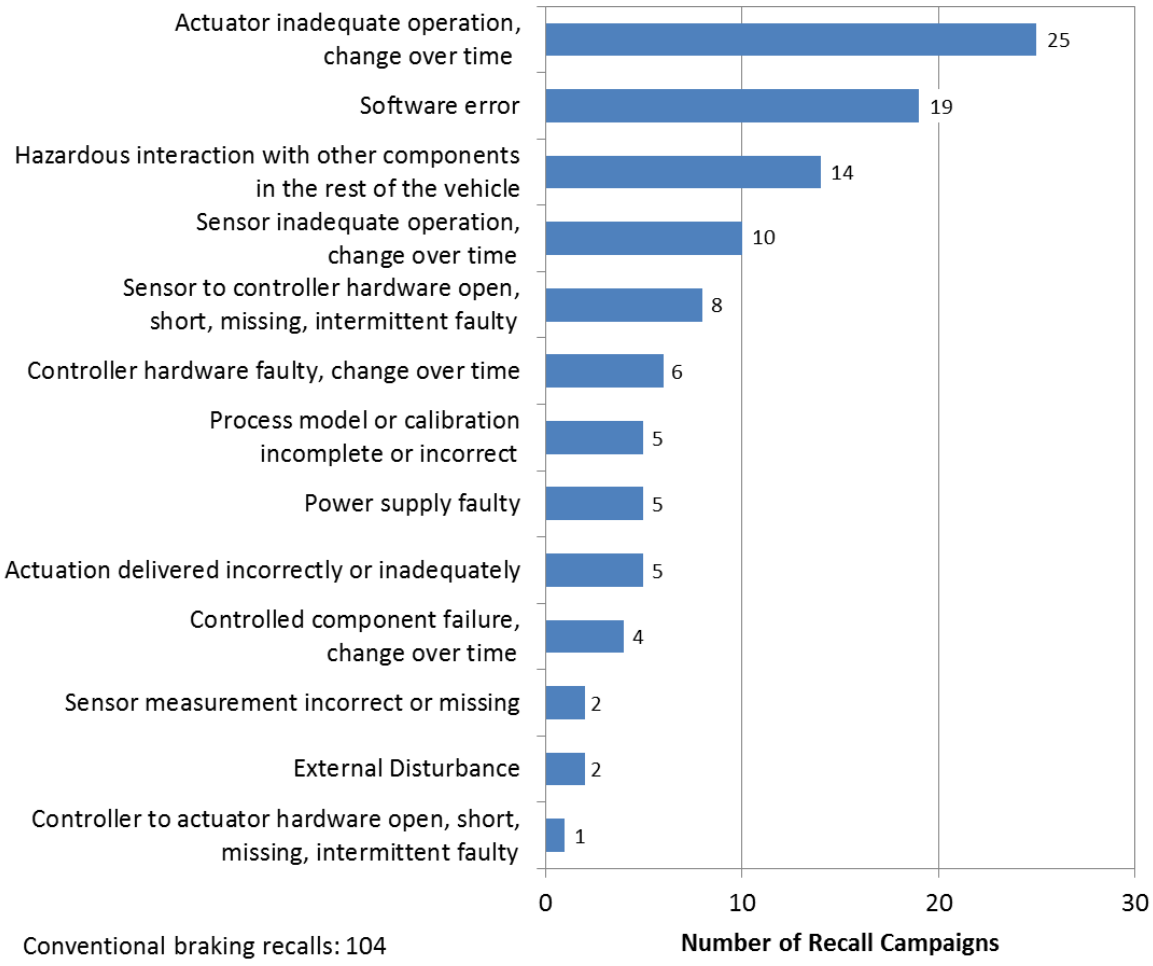


Figure 16: Causal Factor Breakdown of Conventional Brake System Recalls

The highest percentage of brake system related recalls cited failures of the actuator, such as the brake modulator. The second highest causal factor category was software errors in the vehicle stability assist module, which contains ESC, ABS, and traction control.

NHTSA Vehicle Owners' Questionnaires

Vehicle owners can express their safety concerns to NHTSA via the VOQ mechanism either by writing, phone call, or using the online form at www.safercar.gov/Vehicle+Owners. VOQs are monitored by NHTSA's ODI Defects Assessment Division. The complaints are stored in a

database available to the public. The Defects Assessment Division annually screens more than 30,000 VOQs to inform their decisions on issues requiring further investigation [45].

The VOQ database included over 57,000 VOQs related to the following systems for model year 2002 through 2015 light vehicles (as of February 10, 2015):

- ALC/LKA Systems,
- Conventional braking with ABS and ESC,
- EPS, and
- SbW.

Since the VOQ description is a free text entry field, the database must be searched using keywords. Volpe used the following key words or phrases to search for each of the above systems.

- ALC/LKA Systems
    - Lane Keep
    - Lane Keeping
    - Lane Center
    - Lane Centering
    - Traffic Jam Assist
    - Distronic Plus
    - Lane Departure Prevention
    - Lane Control
    - Lane Assist
- Conventional Braking with ABS and ESC
    - ABS brake
- EPS
    - Electric Power Steering
- SbW
    - Steering (search restricted to Infinity Q50 and Q50 hybrid models, the only known models currently implementing SbW technology)

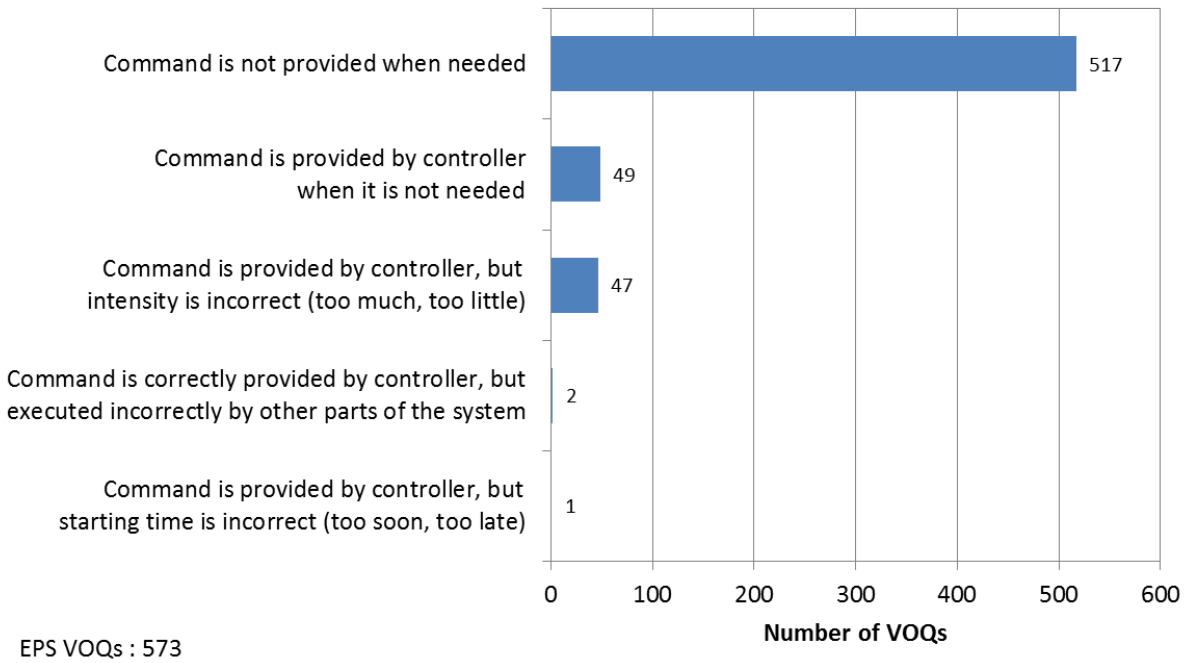
These key words or phrases were selected to constrain the total number of VOQs for this analysis, while including enough VOQs to understand the types of problems observed by vehicle owners. Additionally, Volpe focused the VOQ analysis on manufacturers with greater than one percent market share for light vehicles. Between restricting the key word search and focusing on major manufacturers, Volpe limited the total number of VOQs reviewed to 976. A list of these manufacturers is provided in Table 27.

Table 27: List of OEMs Included in the VOQ Review

Original Equipment Manufacturer (OEM)
GM
Ford
Chrysler
Toyota
Honda
Nissan
Hyundai
Mazda
Kia
Subaru
Mercedes-Benz
VW
Audi
BMW
Data obtained from the Wall Street Journal **[46]** Wards Automotive **[47]**.

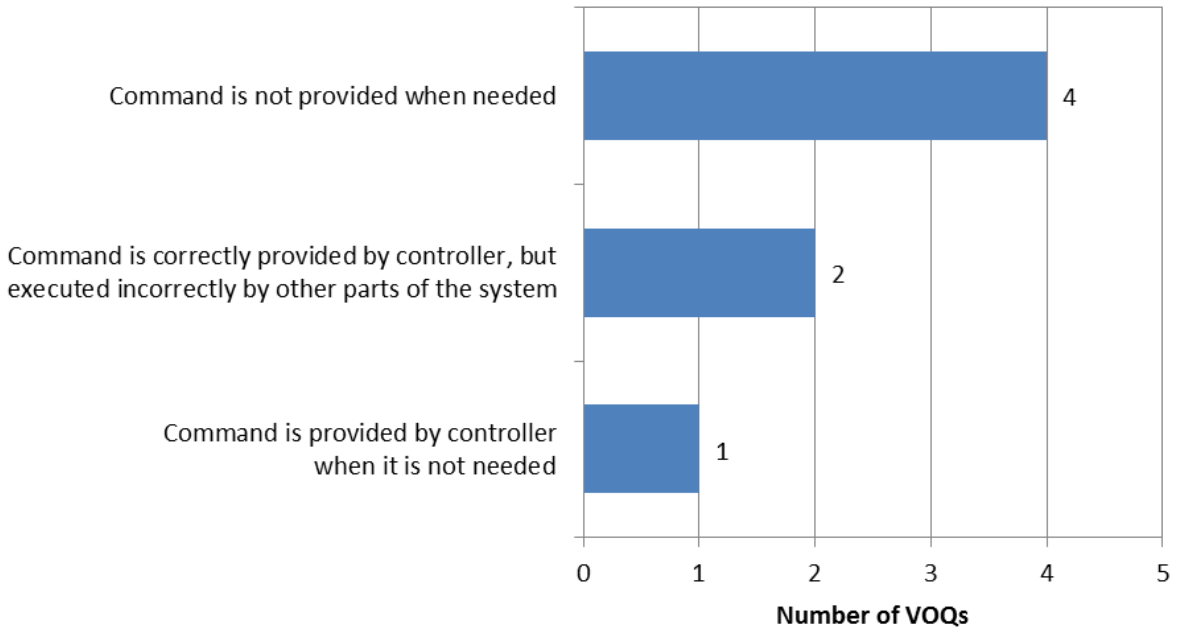
VOQs are submitted by vehicle owners and often describe observed symptoms of component malfunctions rather than causes of the malfunctions. The VOQ analysis was used to determine if the unsafe control action guide phrases are sufficient to identify the symptoms of the malfunctions observed by vehicle owners.

Volpe reviewed each VOQ entry and categorized the owner complaint using the STPA unsafe control action guide phrases. Figure 17 through Figure 20 show the breakdown of VOQs by unsafe control action guide phrase for the electric power steering, steer-by-wire, conventional braking, and ALC/LKA systems.



EPS VOQs : 573
616 VOQs shown; 43 VOQs included multiple guide phrases

Figure 17: Unsafe Control Action Breakdown of EPS VOQs



SbW VOQs : 7

Figure 18: Unsafe Control Action Breakdown of SbW VOQs

Review of the steering-system related VOQs indicates that most owner complaints refer to incidents where steering is not provided when needed.

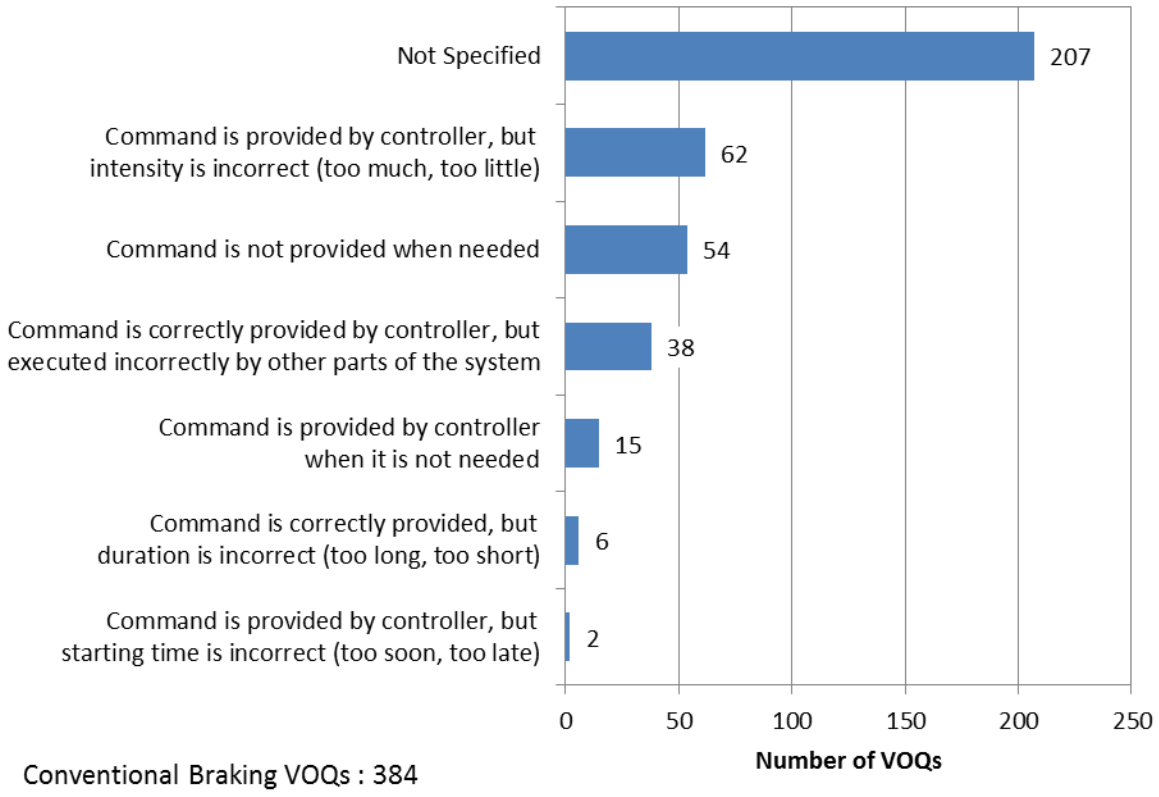


Figure 19: Unsafe Control Action Breakdown of Conventional Brake System VOQs

Most braking-related VOQs did not specify how the brake system malfunctioned. Of the VOQs that did provide a description of the brake system malfunction, most indicated that the brake system provided too little braking force.

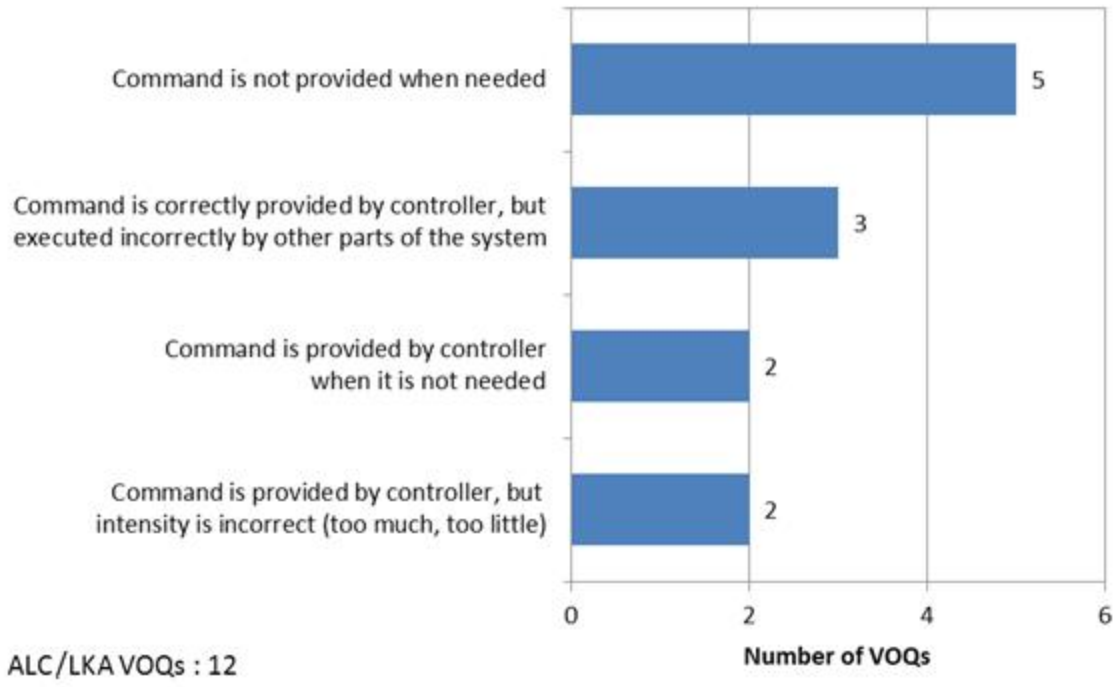
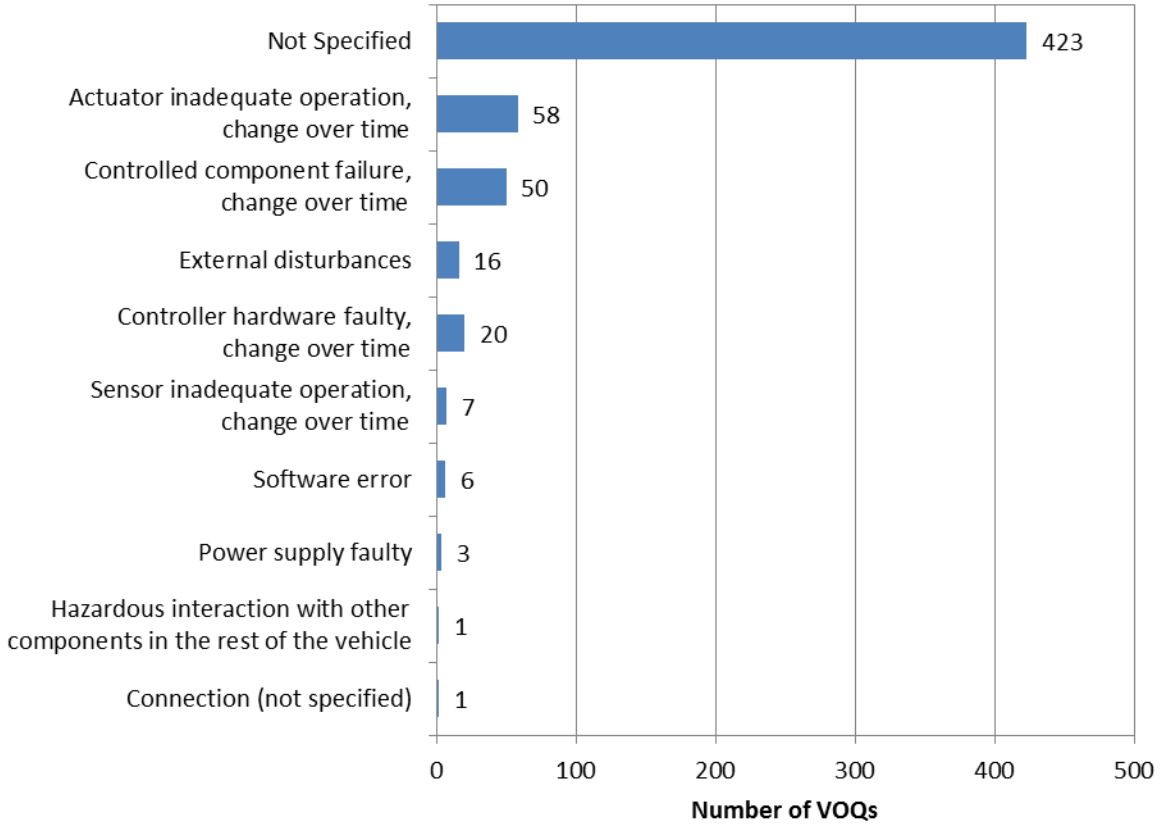


Figure 20: Unsafe Control Action Breakdown of ALC/LKA VOQs

Review of the ALC/LKA-related VOQs indicated that highest number of owner complaints referenced cases where the ALC/LKA system was not available or did not intervene when needed.

Additionally, Volpe used the VOQs to better understand the underlying causes of malfunctions in these systems. However, since the VOQs are not submitted by technical experts, some VOQs included hearsay or speculation about the cause of a malfunction. Volpe's analysis attempted to differentiate between causes identified by experts, such as mechanics and dealerships, and excluded more speculative causes; while these more speculative causes will inform the safety analysis, they are not reported in the following figures.

Volpe categorized the VOQs for the electric power steering, steer-by-wire, conventional braking, and ALC/LKA systems by the 26 STPA causal factor guide phrases. Figure 21 through Figure 24 show the result of this analysis.



EPS VOQs : 573
585 VOQs shown; 12 VOQs included multiple guide phrases

Figure 21: Causal Factor Breakdown of EPS VOQs

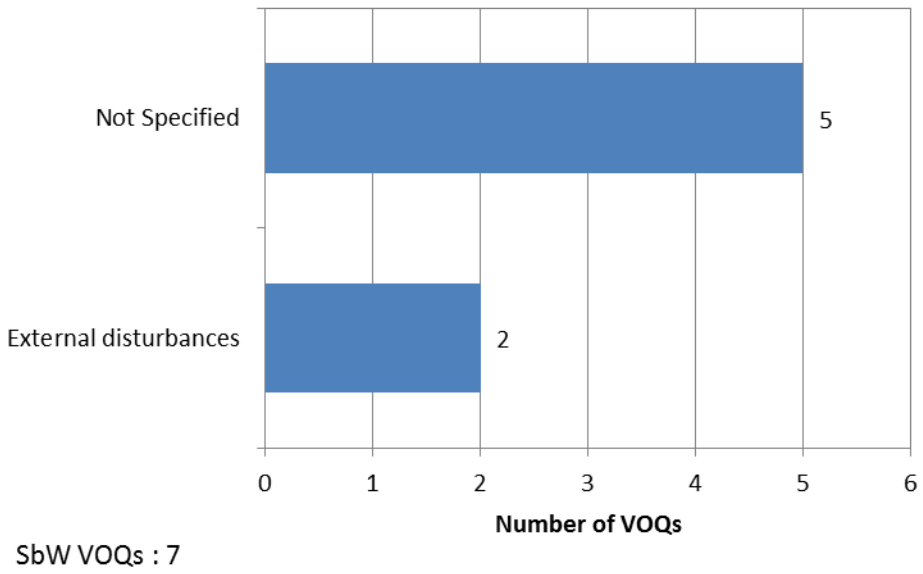
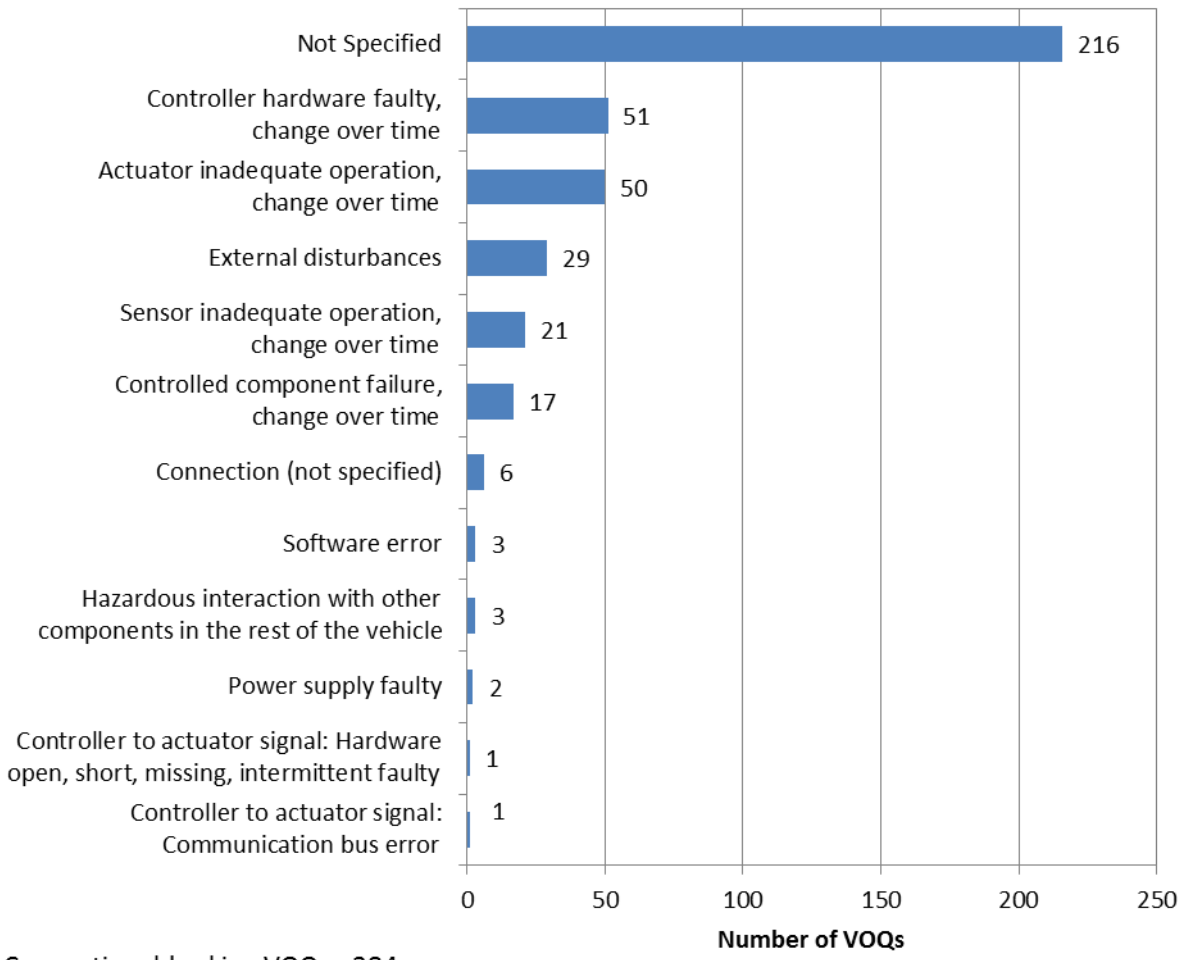


Figure 22: Causal Factor Breakdown of SbW VOQs

Most of the steering-related VOQs did not have a specified or even speculative cause of the failure. Of the VOQs that provided a cause, hardware failures in actuators in the system (e.g., power steering motor) were the most frequently reported cause of malfunctions of the EPS system. In the SbW system, external disturbances (e.g., ambient temperature) were the most reported cause of malfunctions of the system.



Conventional braking VOQs : 384
400 VOQs shown; 15 VOQs included multiple guide phrases

Figure 23: Causal Factor Breakdown of Conventional Brake System VOQs

As with the steering-related VOQs, most of the conventional braking VOQs did not specify a cause or include a speculative cause of the failure. Of the remaining conventional braking related VOQs, most owners indicated that hardware failures in the vehicle stability control module (which contains ESC, ABS, and traction control functions) led to the highest number of malfunctions.

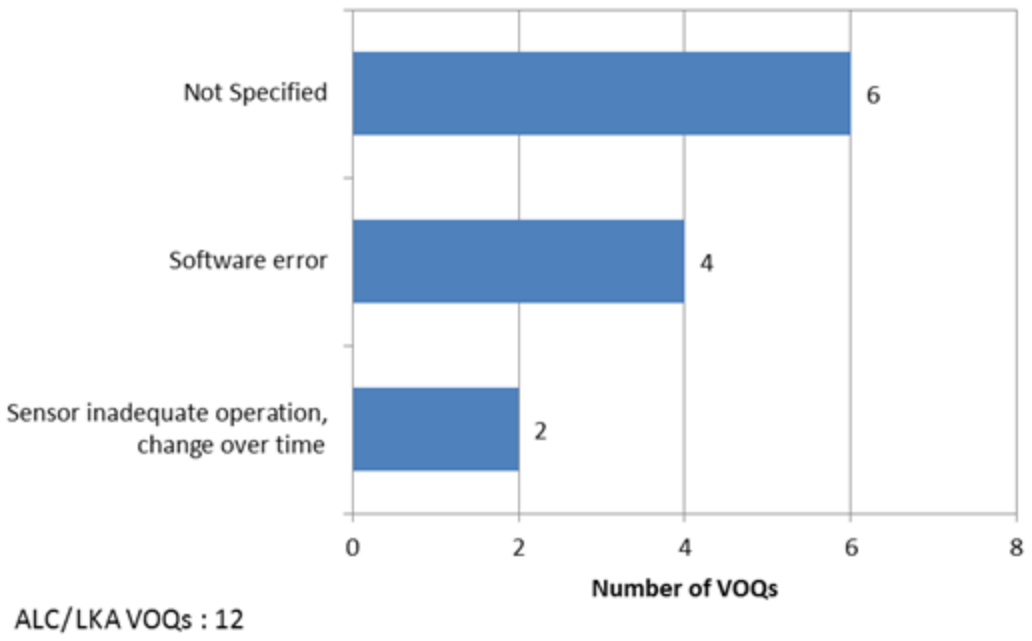


Figure 24: Causal Factor Breakdown of ALC/LKA VOQs

Of the ALC/LKA related VOQs with causal factors, most indicated that a software algorithm error in the ALC/LKA control module led to a malfunction of the ALC/LKA system.

DOT HS 812 572
August 2018

U.S. Department
of Transportation

**National Highway
Traffic Safety
Administration**

NHTSA

13496-080318-v2