U.S. Department
of Transportation
National Highway
Traffic Safety
Administration

NHTSA

DOT HS 813 065

May 2021

Hazard Analysis of Concept Heavy-Truck Platooning Systems

DISCLAIMER

This publication is distributed by 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 United States Government assumes no liability for its contents or use thereof. If trade or manufacturers' names are mentioned, it is only because they are considered essential to the object of the publication and should not be construed as an endorsement. The United States Government does not endorse products or manufacturers.

NOTE: This report is published in the interest of advancing motor vehicle safety research. While the report may provide results from research or tests using specifically identified motor vehicle models, it is not intended to make conclusions about the safety performance or safety compliance of those motor vehicles, and no such conclusions should be drawn.

Suggested APA Format Citation:

Polinori, T., Rice, T., & Monfalcone, M. (2021, May). *Hazard analysis of concept heavy-truck platooning systems* (Report No. DOT HS 813 065). National Highway Traffic Safety Administration.

Technical Report Documentation Page

1. Report No.
DOT HS 813 065

2. Government Accession No.

3. Recipient's Catalog No.

4. Title and Subtitle
Hazard Analysis of Concept Heavy-Truck Platooning Systems

5. Report Date
May 2021

6. Performing Organization Code

7. Authors
Tony Polinori, Tony Rice, and Marc Monfalcone

8. Performing Organization Report No.
100124970-6

9. Performing Organization Name and Address
Battelle Memorial Institute
505 King Avenue
Columbus, OH 43201

10. Work Unit No. (TRAIS)

11. Contract or Grant No.
DTNH2214D00327L
693JJ918F000211

12. Sponsoring Agency Name and Address
National Highway Traffic Safety Administration
1200 New Jersey Avenue SE
Washington, DC 20590

13. Type of Report and Period Covered
Final Report
September 2018 to March 2020

14. Sponsoring Agency Code

15. Supplementary Notes

Volvo Group, SAE International, and WABCO were subcontractors for this project. The NHTSA contract officer representative was Alrik L. Svenson.

16. Abstract

This study explores the potential safety implications of two heavy-truck platooning concepts. The findings summarized in this final report are intended to assist with identifying and assessing the potential safety hazards and risks associated with concept heavy-truck platooning systems. As part of background research, this study reviewed heavy-truck platooning systems and concepts under development. After the market assessment, two "reference" (or prototypical) systems representing alternative platooning concepts were identified and used as a basis for the hazards analysis. The study included creating a list of potential hazards and then categorizing them according to their risks as specified by the ISO 26262 Road Vehicles – Functional Safety standard. A safety of the intended function (SOTIF) analysis was also performed, guided by the ISO 21448 Road Vehicles – Safety of the Intended Functionality standard. Finally, a fault tree analysis was performed on selected hazards identified in the hazards analysis.

17. Key Words
heavy-truck platooning, safety analysis, ISO 26262, ISO 21448, safety of the intended function, SOTIF, fault tree analysis, FTA

18. Distribution Statement
The document is available to the public from the National Technical Information Service, www.ntis.gov.

19. Security Classif. (of this report)
Unclassified

20. Security Classif. (of this page)
Unclassified

21. No. of Pages
124

22. Price

Table of Contents

Executive Summary v

Chapter 1. Introduction 1

Background Information 1
Project Goals 1
Overall Approach 2
Document Organization 3

Chapter 2. Market Assessment of Heavy-Truck Platooning Systems 4

Objective 4
Approach 4
Findings 4
Diversity in Platooning Systems 4
Common System Architecture Components 5
Literature on Platooning Systems' Safety Analysis 6
Selection of Platooning Systems 6

Chapter 3. Hazard Analysis and Risk Assessment 7

Objective 7
Approach 7
2VL1 System 8
3VL2 System 9
2VL1 and 3VL2 System Operational Design Domain and Assumptions 10
ISO 26262 – Road Vehicles – Functional Safety Part 3 10
Stakeholder Engagement 20
Findings 21

Chapter 4. Safety Analysis 23

Objective 23
Approach 23
ISO 21448 – Road Vehicles – Safety of the Intended Functionality 23
Fault Tree Analysis 28
Findings 31
Safety of the Intended Functionality Analysis 31
Fault Tree Analysis 32

Chapter 5. Conclusion 33

APPENDIX A: Definitions of Acronyms and Terms and Supporting Graphics A-1

APPENDIX B: Hazard Analysis and Risk Assessment Summary B-1

APPENDIX C: Safety of the Intended Function Analysis C-1

APPENDIX D: Fault Tree Analysis D-1

Fault Tree 1 – An Unexpected Stoppage in Traffic Causes the FV of the Platoon to Crash into the LV. D-1
Fault Tree 2 – There Is a Loss of Steering in the FV. D-7

Fault Tree 3 – There Is a Collision Between the FV and a Motorcycle as a Result of the Motorcycle Performing a Cut-In Between the FV and the LV. D-12
Fault Tree 4 – The LV Crashes into Nearby Traffic or Infrastructure. D-16

APPENDIX E: Safety Mitigations E-1

APPENDIX F: References F-1

TABLES

Table 1. Heavy-Truck Platooning System Concepts...5
Table 2. Comparison of 2VL1 and 3VL2 Concept Heavy-Truck Platooning Systems 6
Table 3. ASIL Determination According to ISO 26262 10
Table 4. Class of Severity From ISO 26262 Standard 14
Table 5. Classes of Probability of Exposure Regarding Frequency in Operational Situations 15
Table 6. Examples of Possibly Controllable Hazardous Events by the Driver or People Potentially at Risk 17
Table 7. ASIL Determination From ISO 26262 Standard 19
Table 8. Platooning Hazards With the Highest Residual Risk Assessments.................................21
Table 9. SOTIF Analysis Activities Described in ISO 21448 Standard..26
Table 10. Hazards Analyzed in the FTA 30
Table 11. Fault Tree Symbol Definitions 30
Table 12. SAE J3016 Levels of Driving Automation A-3
Table 13. Truck Platooning Hazard Analysis and Risk Assessment..B-1
Table 14. Functional and System Specification of the ISO 21448 Standard C-1
Table 15. Hazardous Events Identified Caused by the Unintended Behavior of the Function and Their Triggering Events C-14
Table 16. Critical Sub-Functions and Safety Mitigations Applied to Mitigate or Avoid the SOTIF-Related Risks C-17
Table 17. Strategies for Performing System Verification...C-18
Table 18. Strategies for Performing System Validation C-19
Table 19. Verification Activities Described for Each of the System Components and Elements C-20
Table 20. Validation Activities Described for Each of the System's Sub-Functions...................C-23
Table 21. Event Descriptions for Fault Tree 1 ....D-1
Table 22. Event Descriptions for Fault Tree 2 ....D-7
Table 23. Event Descriptions for Fault Tree 3 ....D-12
Table 24. Event Descriptions for Fault Tree 4 ....D-16
Table 25. Safety Mitigations From Hazard Analysis and Risk Assessment E-1

FIGURES

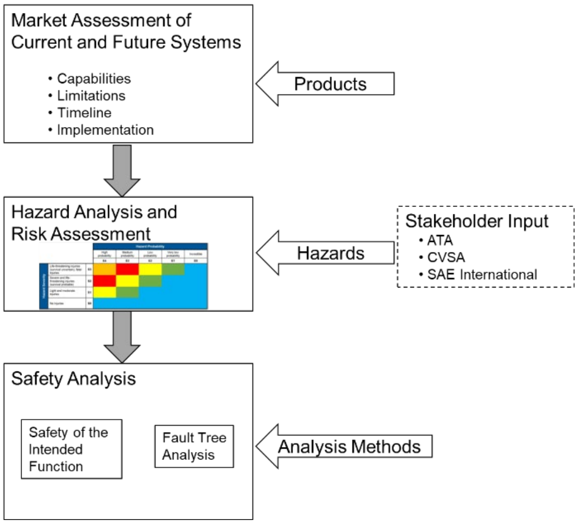
Figure 1. Project Workflow. v
Figure 2. Project Workflow. 2
Figure 3. Functional Block Diagram of the 2VL1 System. 8
Figure 4. Functional Block Diagram of the 3VL2 System. 9
Figure 5. Identification of Unknown Unsafe Scenarios in the SOTIF Analysis. 24
Figure 6. Activities and Processes Flowchart for Performing the SOTIF Analysis. 25
Figure 7. Methodology for Evaluating the Criteria for the SOTIF Release. 28
Figure 8. There Is an Unexpected Stoppage in Traffic (1). D-2
Figure 9. LV Inter-vehicle Communication System Failure (1.1). D-3
Figure 10. CMS Failure (1.2). D-4
Figure 11. FV Inter-vehicle Communication System Failure (1.3). D-5
Figure 12. FV Receives Speed Control Command Message, but Fails to Perform the Required Function (1.4). D-5
Figure 13. There Is a Loss of Steering Control in the FV (2). D-8
Figure 14. Vehicle System Failure (2.1). D-9
Figure 15. LV Platooning System Failure (2.2). D-10
Figure 16. FV Platooning System Failure (2.3). D-11
Figure 17. A Motorcycle Performs a Cut-In Between Two Platooning Vehicles (3) D-13
Figure 18. FV Driver Fails to Act in Response to a Cut-In (3.1). D-13
Figure 19. FV CMS Fails to Act in Response to a Cut-In (3.2). D-14
Figure 20. Platooning Operating Procedures Not Followed (3.3). D-15
Figure 21. FV Platoooning System Fails to Warn of a Cut-In (3.4). D-16
Figure 22. The Driver of the LV Performs an Evasive Maneuver (4). D-18
Figure 23. Vehicle System Failure (4.1). D-19
Figure 24. Platooning System Failure (4.2). D-20
Figure 25. Driver Monitoring and Performance (4.3). D-22

Executive Summary

Motor carriers continuously strive to increase their productivity through improving safety and operational efficiency and by reducing fuel consumption. One method of reducing aerodynamic drag is to reduce the following distance between vehicles. However, following closely enough to achieve high fuel efficiency raises questions of impacts on safety. For example, in platooning concepts that rely on the human drivers as the fallback, human drivers in the following platooning vehicles may not have adequate reaction time to avoid forward collisions if the lead vehicles (LVs) of the platoon brakes suddenly and the system transfers control over to the drivers due to some malfunction. Systems are being developed by industry stakeholders using electronic and pneumatic controls, camera, radar, vehicle-to-vehicle communications, and other sensors to, in concept, enable following vehicles to brake and/or steer in unison with lead vehicles, thus overcoming some limitations of human reaction time. This concept is termed "platooning." Following formal hazard and safety analysis methods can help identify potential risks associated with this concept as well as potential mitigation methods that could address such risks.

Truck platooning is (1) the "virtual" (or electronic) linking of two or more trucks using various communication and sensor technologies, and (2) closing the following distances between platooning units. The value proposition (or motivation) for platooning is that at highway speeds, aerodynamics of the trucks within the platoon are improved. In the concepts that are identified and covered in this study, the driver in the truck at the front of the platoon drives the LV and sets the traveling profile of the platoon and oversees its operation. The speed of the following vehicle (FV) is automatically controlled to maintain spacing between vehicles; however, the driver of the FV remains fully responsible for monitoring speed and headway gaps.

The purpose of this project was to provide an understanding of the heavy-truck platooning system concepts under development and their potential safety implications through use of established hazards and safety analysis techniques. The following tasks to explore the safety implications of heavy-truck platooning are illustrated in **Figure 1**.



Source: Battelle

Figure 1. Project Workflow.

First, a market assessment was conducted to summarize the current state of the technology and to identify heavy-truck platooning system concepts. The market assessment indicated there is little public information available on the designs and operations of heavy-truck platooning systems. High-level block diagrams and an abbreviated list of components are available for some systems; however, there was insufficient information available on how these systems initiate, form and dissolve the platoon. While the information likely exists, it is proprietary and potentially in development, and not necessarily ready for disclosure. Despite the lack of detail on the system operations, many of these systems shared a similar high-level architecture common across all systems. As anticipated, market assessment confirmed there is no publicly available hazards or safety analysis published on a heavy-truck platooning system.

After the market assessment, two "reference," or prototypical, platooning system concepts were then developed to represent a range of performance capabilities and operating concepts to be the focus of the hazard and safety analysis, respectively. These systems were termed 2-vehicle SAE Level 1 (2VL1) and 3-vehicle SAE Level 2 (3VL2). The 2VL1 system concept was defined as a two-truck platoon, each consisting of a single tractor-semitrailer combination with a driver in each vehicle. The FV automatically controlled its speed to maintain a close following distance to the LV. The driver in the FV was responsible for steering while platooning. The platoon had inter-vehicle communication, which facilitated coordinated operations allowing for a minimal gap between vehicles. This capability corresponds to SAE driving automation Level 1 (from SAE J3016[1]). The 3VL2 system concept is similar; however, there are three single tractor-semitrailers. Further, this system has speed and steering control, which corresponds to SAE driving automation Level 2. Both concepts[2] are considered types of advanced driver assistance systems (ADAS) and rely on a fully and continuously attentive driver in the platooning units.

After defining these concept-level platooning systems, a hazard analysis and risk assessment were performed. In this task, a list of potential hazardous events was identified, analyzed, and assessed. A comprehensive list of hazards applicable to the representative heavy-truck platooning concepts (2VL1 and 3VL2) was developed as part of the hazard analysis. This list was created based on the research team's platooning experience and expertise, with contributions from ATA, CVSA and SAE International standards committee members. Each hazard was assessed, guided by the ISO 26262 standard that provided a framework for assessing each hazard on its severity, probability of exposure and controllability. Potential design, operations, maintenance and safety mitigations were proposed to each hazard and their effects on the identified risks were assessed for the reference systems (2VL1 and 3VL2) considered by the research team (and as described in **Chapter 1**).

Finally, a fault tree and a safety of the intended function (SOTIF, Concept Draw. (n.d.) analyses were performed. The fault tree analysis (FTA) complements the hazard analysis by analyzing hazards with a top-down approach to identify lower-level hazards and faults that can lead-to the undesired system state. The FTA was conducted on the key hazards from the previous task that had the highest levels of estimated risk.

[1] "Platooning" can be implemented at higher driving automation levels as well, such as at SAE driving automation levels 3, 4, or 5. The analysis performed in this report should not be assumed to fully apply or cover the safety hazards and risks applicable to all levels and types of platooning concepts.

[2] The same as above.

Through the FTA (SAE International, 2019), two critical path safety-relevant events were identified: a failure of the Collision Mitigation System (CMS) implemented in platooning and operation of the platooning system by inadequately trained users. The failure of the CMS to maintain a safe following distance with vehicles engaged in a platoon (i.e., between the LV of the platoon and a non-platooning vehicle or between the LV of the platoon and an object ahead) is assessed as the most safety-critical design element of the platooning system. The CMS is integrated with the vehicle and interfaces directly with the engine management system (EMS) as well as the brake system. Inadequate integration or a failure of one of these components in the aforementioned systems represents a significant risk for a crash to occur. Fortunately, the CMS can be tested extensively through verification and validation (V&V) to demonstrate that the system is integrated properly for the designed use of the system.

Inadequate training and operation of the platooning system represents the other critical path event identified through the FTA. The criticality of the driver's performance on safety for the considered platooning concepts was magnified after identifying the relationships between system functions and driver responsibilities. The following events were identified as examples of potential hazardous situations that could result from inadequate driver training and/or a less-than-fully engaged driver in one or more of the platooning vehicles: failure to identify cut-ins or potential cut-ins, failure to disengage the platoon in qualifying conditions, distracted driving, driver inattentiveness, and other operating procedures not followed. It is acknowledged that distracted driving, driver inattentiveness, operating procedures not followed, and inadequate driver training are also applicable to non-platoon trucking.

Dissimilar to a failure of the CMS, testing for driver (human) error and implementing adequate safety mitigations is much more difficult. With the systems at SAE driving automation levels 1 and 2, human drivers are expected to be fully attentive at all times and be ready to resume control with or without warning that the system may no longer be functioning as intended. There is a near-infinite number of environmental factors and use case scenarios a driver must contend with compared to a discrete number of failure modes for an electronic-mechanical CMS. Systems with a human-in-the-loop require safety mitigations such as training and operating procedures that are fully dependent upon the human complying.

FTA is a quantitative analysis to account for differences in system designs and components used across different platooning system manufacturers. Using actual failure rates from the components in the system's design can be used to determine a failure rate for the entire system. Probability data such as how often a system will experience a certain scenario or operating condition are used to calculate a failure rate for the entire system as a whole.

The SOTIF analysis was performed on each platooning system function to identify critical functions for maintaining safety while platooning. This safety analysis methodology evaluates the absence of unreasonable risk due to a hazard caused by performance limitations of the intended behavior or reasonably foreseeable misuse by the user.

The SOTIF analysis was guided by the ISO 21448 Road Vehicles – Safety of the Intended Functionality standard. One challenge associated with performing the SOTIF analysis on a representative platooning system was not having an actual functional system specification. Since these were hypothetical concept systems, details about the system's functions and relationships between specific components had to be generated based off the team’s knowledge of platooning and publicly available information. The study team used engineering judgment to model what a real-world system may look like for the purposes of this study. It is assumed that a platooning system integrator or manufacturer would have this documentation prior to beginning the SOTIF activities. The approach outlined in this report can be a baseline for performing the SOTIF.

An attempt was made to identify known unsafe conditions as a baseline for establishing a list of example verification tasks. A system integrator would need to further develop validation use case scenarios to test the system in a real-world environment to identify unknown unsafe scenarios. The identification of these unexpected scenarios adds to the list of known unsafe conditions. This starts the SOTIF analysis process over again where the system integrator then identifies functional modifications to reduce SOTIF risks and to create new known unsafe conditions to test in verification. This feedback loop increases the safety and reliability of the platooning system.

Chapter 1. Introduction

Background Information

Motor carriers continuously strive to increase their productivity through improving safety and operational efficiency and reducing fuel consumption. One method of reducing aerodynamic drag is to reduce the following distance between vehicles. Following closely enough to achieve high fuel efficiency raises questions of safety. Human drivers may not have adequate reaction time to avoid a forward collision if the LV of the platoon brakes suddenly. Using electronic controls, radar, and communication between vehicles ("platooning") is being considered by the trucking industry as a means to achieve close following distances safely, while overcoming some limitations of human reaction time. Formal safety analysis of these systems can help determine risks associated with this strategy as well as potential mitigation methods to address such risks.

Truck platooning is (1) the virtual (or electronic) linking of two or more trucks using various communication and sensor technologies, and (2) closing the following distances between platooning units. The value proposition (or motivation) for platooning is that at highway speeds, aerodynamics of the trucks within the platoon are improved. In the concepts that are identified and covered in this study, the driver in the truck at the front of the platoon drives the lead vehicle (LV) and sets the traveling profile of the platoon and oversees its operation. The speed of the following vehicles (FVs) is automatically controlled to maintain spacing between vehicles; however, the drivers of the FVs remain fully responsible for monitoring speed and headway gaps.

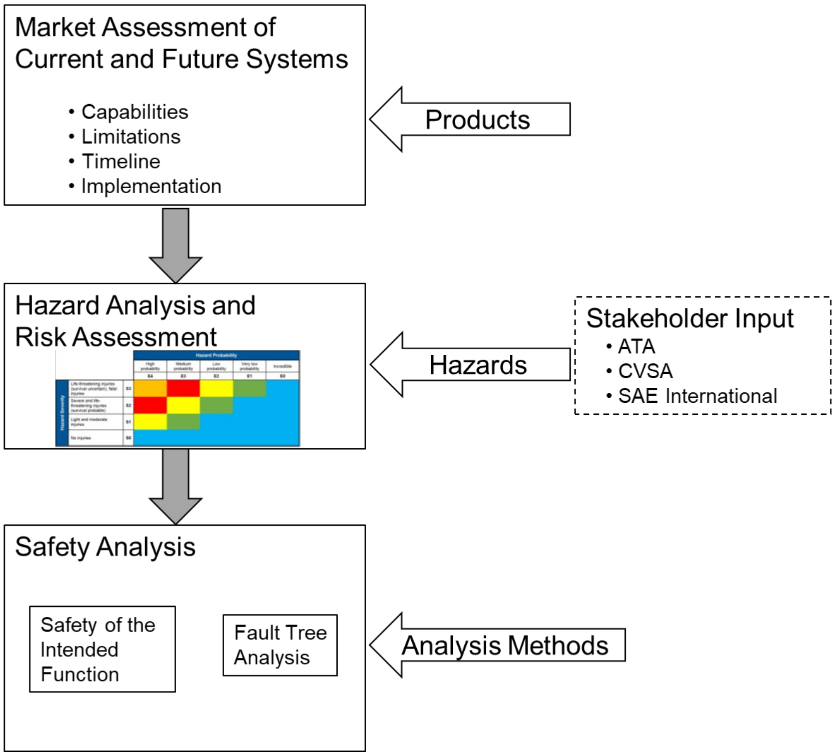
The safety of electronic platooning systems depends on the functional safety of the hardware and software. Safety also depends interaction with the environment, following distance between platooning vehicles, including surrounding traffic, human operators and other factors.

Project Goals

The purpose of this Safety Analysis of Heavy-Truck Platooning project is to provide an understanding of heavy-truck platooning system concepts and their potential safety implications. The project's goals are to identify existing and future heavy-truck platooning system concepts being developed, identify and analyze potential hazards associated with platooning, and to carry out established industry processes to perform safety risk analyses on typical heavy-truck platooning systems.

Overall Approach

The overall approach and workflow to this project is illustrated in **Figure 2**.



Source: Battelle

Figure 2. Project Workflow.

A high-level market assessment of heavy-truck platooning system concepts was performed to understand the current state of development and the operation of these systems. A list of existing systems and system concepts in development was developed. These systems were described according to their system architecture and design characteristics and operational features.

Based on the findings from the market assessment, two “reference,” or prototypical platooning system concepts were then developed to represent a range of performance capabilities and operating concepts to be the focus of the hazard and safety analysis, respectively. The hazard analysis and risk assessment were performed on these two platooning system concepts.

Once the draft hazard analysis and risk assessment were completed, three separate webinars were held with industry stakeholders to provide feedback into the analysis. An hour-long webinar was hosted for each of the following stakeholders: ATA, CVSA, and SAE International standards committee members. Each stakeholder group provided valuable feedback on hazards, safety mitigations and clarifying assumptions about each system. The feedback received was reflected into the final hazard analysis and risk assessment.

A SOTIF and fault tree analysis were selected as the safety analysis methodologies for further investigating the hazards associated with heavy-truck platooning system concepts. The SOTIF analysis was chosen because it evaluated the absence of unreasonable risk due to a hazard caused by performance limitations of the intended behavior or reasonably foreseeable misuse the by user. This analysis would be performed on each platooning system function to identify critical functions for maintaining safety, while platooning.

The FTA complemented the hazard analysis by analyzing hazards with a top-down approach as lower-level hazards are deduced to find all credible ways in which the undesired system state can occur. The FTA was conducted on the key hazards from the previous task that could not be reduced to an acceptable level of risk.

Document Organization

This final report is organized into five chapters, followed by the appendices. This introductory chapter discusses the goals and approach adopted in this final report, as well as the background of the project. The subsequent chapters summarize the market assessment of heavy-truck platooning systems, (Chapter 1), hazard risk analysis and risk assessment (Chapter 1) and safety analysis (Chapter 4) by providing the objective, approach and findings of each task deliverable. Chapter 5 presents the key conclusions from each of the previous task sections. Appendix A, for reference, includes terms and definitions used throughout this report. The supporting summary tables and resulting data from the hazard analysis and risk assessment, the SOTIF analysis, and the FTA are presented in **Appendix A – E.**

Chapter 2. Market Assessment of Heavy-Truck Platooning Systems

Objective

The objective of the market assessment was to describe several platooning systems being developed in the United States and around the world. From this task, two representative heavy-truck platooning systems were selected to be analyzed in the hazard analysis and risk assessment, and the safety analysis.

Approach

The research to support the market assessment of heavy-truck platooning systems included a literature search. The literature search was conducted using both publicly available online information sources, as well as subscription-based professional databases such as Scopus and IEEE Explore. The search focused on current and previous truck platooning projects and initiatives, and safety analysis of platooning systems, with a primary focus on heavy-truck platooning systems. Public information sources were searched using Boolean search logic and the following search terms: “truck platooning,” “automated truck platooning,” “cooperative adaptive cruise control” (CACC), and “driver assistive truck platooning.”

Search results using public information sources provided to be the most useful for finding project reports, presentations, and news releases on current platooning activities. The database searches provided valuable input about what types of analysis had been performed on platooning systems. A complementary search was also performed by reviewing references cited from project reports.

Following the literature search, the search results were sorted and reviewed to determine the most current and relevant resources published within the last five years.

Findings

Diversity in Platooning Systems

The market assessment research indicated that within the last decade, there have been approximately ten prototype heavy vehicle platooning systems developed or in development. These systems differ greatly in many aspects and are shown in **Table 1**. The SAE driving automation levels of these systems range from SAE driving automation Level 1 to Level 4. The number of vehicles within the platoon vary from two vehicles up to approximately twenty. Some platoons are single tractor trailers, while others are doubles or involve a combination of heavy and passenger vehicles. Most of the systems were designed for highway operation, while others were developed for battlefield or port operations. Some systems are approaching production quality, while others are research and development systems with no intention of ever being commercialized.

Table 1. Heavy-Truck Platooning System Concepts

Year	System or Project	SAE Level of Automation	Platoon Type
2011-Present	Peloton (Peloton Technology, 2018)	Level 1	Two tractor-semitrailer combinations
2017	Port of Singapore (Channel NewsAsia, 2017)	Level 4	Four tractor-semitrailer combinations
2018	Caltrans (PATH, Volvo) (Altan, 2017)	Level 1	Three tractor-semitrailer combinations
2018	Volvo (FedEx) Costlow, 2018)	Level 1	Three tractors, each with double 28-foot trailers
2017	Helm UK Cuerdan, 2018)	Level 2	Three tractor-semitrailer combinations
2017	TTI (Kuhn et al., 2017)	Level 2	Three tractor-semitrailer combinations
2012	Japan Energy ITS (Tsugawa, 2012)	Level 2	Heavy and light trucks
2012	SARTRE (Research Institutes of Sweden. 2012)	Level 2	Mixed heavy and passenger vehicles
2009	KONVOI (Kotte, 2016)	Level 2	Two to four tractor-semitrailer combinations

Common System Architecture Components

Despite differences in operational design domains (ODDs), the SAE driving automation level and the number of vehicles in a platoon, these platooning systems share similarities in system architectures. Shared technologies between systems include a unique configuration of the following:

- Sensors
- Computation device (processor)
- Actuators
- Inter-Vehicle Communication
- Intra-Vehicle Communication
- Software
- Driver Interfaces

Literature on Platooning Systems' Safety Analysis

In addition to scanning truck platooning project reports for information on the systems' ODD, the level of automation and the number of vehicles in the platoon, a complementary literature search was performed focusing on the types of safety analyses published on platooning systems. The results of this search confirmed there has not been a publicly accessible safety analysis published on truck platooning.

Selection of Platooning Systems

After conducting the market assessment of heavy-truck platooning systems, two concept-level platooning systems were established, which are not exact representations of any particular system. The two systems were selected from a functional design perspective among platooning products under development that might appear in the North American commercial market. One was a 2-vehicle SAE Level 1 (2VL1) system, and the second one was a 3-vehicle SAE Level 2 (3VL2) that had two complicating features. All vehicles were a single tractor-semitrailer combination, and all were to have a human driver present and alert in the in the driver's position. In both systems, the driver in the LV was fully responsible for driving the LV and for overseeing the platoon. The ODD was freeways at nominally steady cruising speed. Threats to safety from environmental conditions, such as weather or traffic, were included as appropriate.

The first of the two systems consisted of two tractor-trailer combination vehicles. The FV automatically controlled its speed to maintain a close following distance to the LV. The driver in the FV was responsible for steering when platooning. This capability is often referred to as Cooperative Adaptive Cruise Control (CACC), and it corresponds to SAE driving automation Level 1.

The second system had three tractor-trailer combination vehicles—a leader with two followers. In addition to automatically maintaining a close following distance, the FVs automatically steered to follow the path of the leader. With the vehicle under automatic speed and steering control while a human monitors it and is ready to take over, this roughly corresponds to SAE driving automation Level 2. A comparison of the two systems are shown in **Table 2**.

Table 2. Comparison of 2VL1 and 3VL2 Concept Heavy-Truck Platooning Systems

System	Truck Configuration	Number of Vehicles in Platoon	Driver Present in Each Vehicle	LV Driver Responsibilities	FV Driver Responsibilities
2VL1	Single tractor-semitrailer	2	Yes	Speed and steering control, and managing the platoon	Steering control only
3VL2	Single tractor-semitrailer	3	Yes	Speed and steering control, and managing the platoon	Neither steering nor speed control (FV driver is available to take over steering control if a failure or emergency event occurs)

Chapter 3. Hazard Analysis and Risk Assessment

Objective

The focus of this task was to perform a hazard analysis and risk assessment on the hypothetical heavy-truck platooning systems previously developed. These systems are described below as the 2VL1 system and 3VL2 system. The hazard analysis considered the following types of hazards and failures: inherent equipment failures, operational environment hazards, and human factors.

Approach

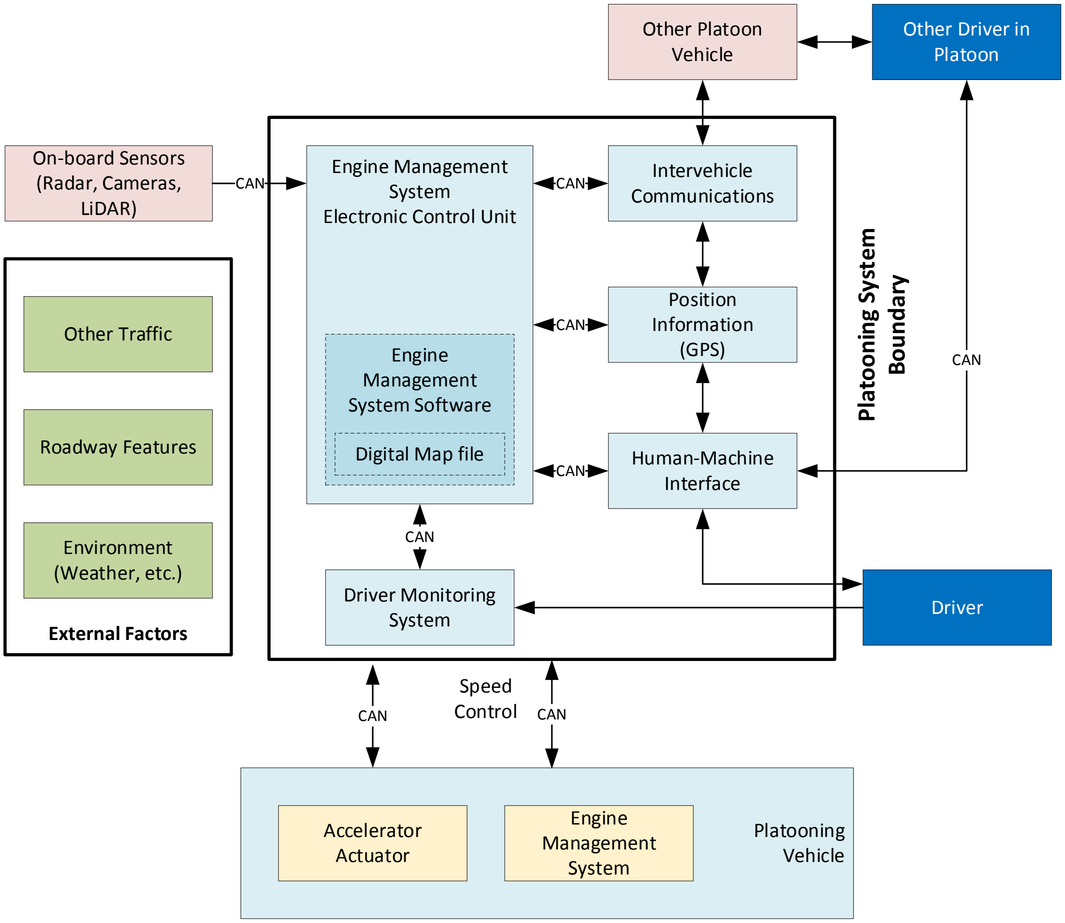
The hazard analysis and risk assessment were performed to characterize each hazard by following the approach of the ISO 26262 Road Vehicles – Functional Safety standard. The standard describes how to characterize each hazard by considering severity, probability, and controllability for the initial and residual risk. The subsequent safety analysis is driven by the results of this task, with greater focus given to the hazards posing the greatest risk to safety integrity.

The first step of the hazard analysis was to identify hazards tailored to the 2VL1 and 3VL2 systems. A comprehensive list of heavy-truck platooning hazards was developed to assess what can plausibly go wrong and reduce safety with input from the team's expertise and research conducted in the market assessment of heavy-truck platooning systems. A clear and concise description of each hazard was written and assigned a unique hazard identification number. Each hazard was then categorized by its type, which included: equipment failures, operational environmental hazards and human factors. Following the ISO 26262 standard, hazards are classified by three dimensions: severity, probability of exposure, and controllability. Together, these three dimensions formulate an Automotive Safety Integrity Level (ASIL), which is assigned to each hazard before and after a safety measure has been implemented. Although the ratings assigned to each of the three dimensions for the risk assessments follow the standard, the ratings are subjective to the party performing the safety analysis. The severity, probability of exposure, and controllability are dependent upon the system and its ODD. The potential causes or set of conditions that may lead to the hazards were also listed. The result or impacts of each hazard were also explained. The complete hazards analysis and risk assessment is presented in **Appendix B**.

As part of the risk assessment, safety mitigations were developed and assigned to each hazard. Various safety mitigation types were assigned to reduce or eliminate the hazard including design, operations, training, and maintenance. Safety mitigations were developed based on the team's experience with automated and safety-critical systems. Aligned with the approach for the project, which was decided in the market assessment of heavy-truck platooning systems task, some of the safety mitigations are futuristic in nature to represent the different "bookends" in automation. The safety mitigations in the analysis were recommendations for reducing the risk (for the complete list of safety mitigations developed in this study, refer to **Appendix E**). It is recognized that some safety mitigations required multiple sensors or technology that is not currently in production. A cost-benefit analysis was not performed to analyze the benefit received for implementing the safety mitigation versus its cost.

2VL1 System

The 2VL1 platooning system consisted of two trucks. Each truck consisted of a single tractor-semitrailer combination with a driver in each vehicle. This system is shown in **Figure 3**. The FV automatically controlled its speed to maintain a close following distance to the LV. The driver in the FV was responsible for steering while platooning. The platoon had inter-vehicle communication, which facilitates coordinated operations allowing for a minimal gap distance between vehicles. This capability is often referred to as CACC, and it corresponds to SAE driving automation Level 1. Both vehicles in the platoon have the same automation level capabilities.



Source: Battelle

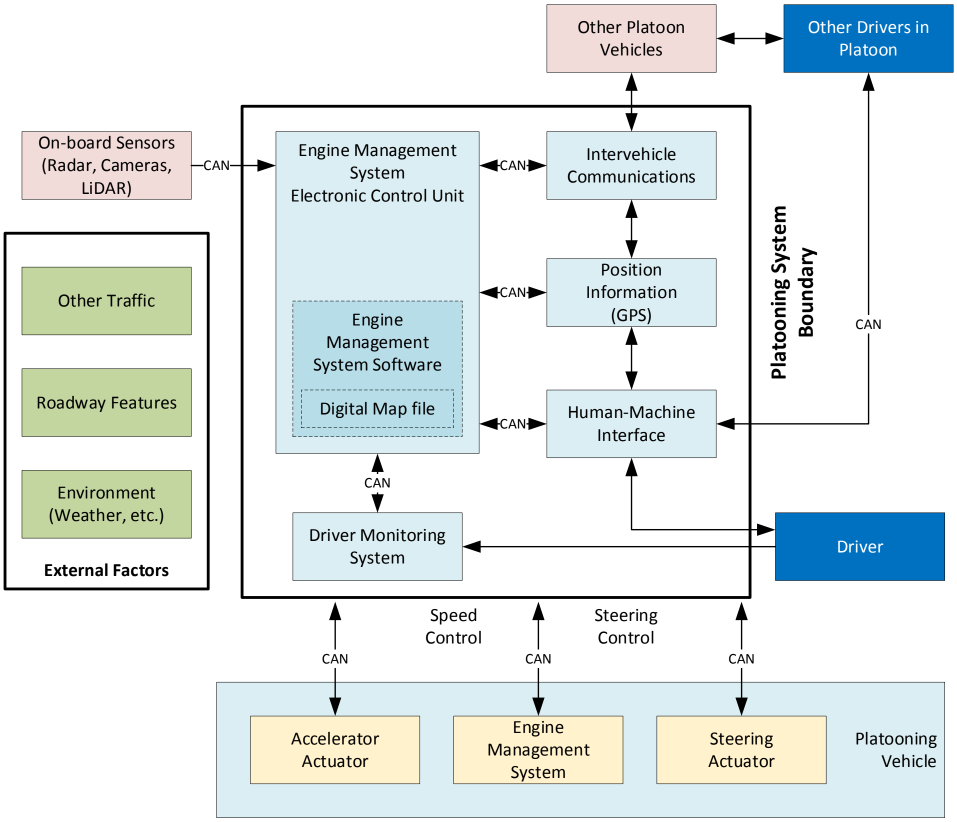
Figure 3. Functional Block Diagram of the 2VL1 System.

Figure 3 represents the platooning system components and elements that make up the 2VL1 vehicle platooning system. The yellow rectangles are representative of the vehicle's accelerator actuator and the engine management system within the platooning vehicle. The green rectangles represent external factors in a platooning environment that include other vehicle traffic, roadway features, and the overall environment. The pink rectangles are external support components of the platoon such as on-board sensors and the other platooning vehicle. The dark blue components represent the human operators of the system. The black arrows indicate the interface between components. This illustrates data being sent and received between components or elements of the system. The platooning system boundary is represented by the thick black lines drawn around the external factors and platooning system elements.

The engine management system electronic control unit is the core of the platooning system that processes system inputs and controls actuators in the vehicle's subsystems. The inter-vehicle communication enables the vehicles in the platoon to communicate with one another. The driver monitoring system monitors and helps to enforce the driver's attentiveness. The human machine interface (HMI) shown in **Figure 3** provides the driver of the FV with a live front-facing view from the LV.

3VL2 System

The 3VL2 system consisted of three single tractor-semitrailers – a leader with two followers. In addition to the system maintaining a close following distance between the lead and FVs, the FVs automatically steered to follow the path of the leader. With the vehicle under automatic speed and steering control, the driver of a FV monitored the system and was prepared to take over in the event of a failure or emergency. This roughly corresponds to SAE driving automation Level 2. All vehicles in the platoon have the same driving automation level capabilities.



Source: Battelle

Figure 4. Functional Block Diagram of the 3VL2 System.

Figure 4 also represents the platooning system components and elements that make up the 3VL2 platooning system. The items represented by colored rectangles, directional arrows, and thick black lines represent the same components and elements as explained in the 2VL1 platooning system description.

The only physical difference between the components of the systems is the addition of the steering subsystem and its interface to the platooning vehicle in the 3VL2 system. This enables the FVs to operate with steering control commands sent from the LV of the platoon.

2VL1 and 3VL2 System Operational Design Domain and Assumptions

Both the 2VL1 and 3VL2 systems were assumed to have the same ODDs. The ODD was restricted to freeways at nominal steady cruising speed. It was assumed that the platoons were already in formation, dangerous or hazardous materials were not being transported, and dedicated short-range communications (DSRC) was the communication medium. Threats to safety from environmental conditions, such as weather or traffic, were included as appropriate.

ISO 26262 – Road Vehicles – Functional Safety Part 3

The ISO 26262 provides a framework for conducting a hazard analysis and risk assessment. It describes how to assign an ASIL by characterizing each hazard with respect to severity, probability of exposure, and controllability. Based off the ASIL characterization, safety goals of the system can be determined and prioritized accordingly. In a production-level system, these safety goals would be translated to system requirements, where V&V activities would be performed in addition to safety analysis.

The ASIL is determined based on the classification of the hazard with respect to its severity, probability of exposure, and controllability in accordance with **Table 3**. There are four ASILs: A, B, C, and D. ASIL A is the lowest safety integrity level and ASIL D is the highest. There is also the quality management (QM) class that denotes the requirement to comply with ISO 26262.

Table 3. ASIL Determination According to ISO 26262

Severity Class	Probability Class	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

Severity Class	Probability Class	Controllability Class		
		C1	C2	C3
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

The hazard analysis considers the following types of hazards and failures: inherent equipment failures, operational environment hazards, and human factors.

Hazard Analysis

The first step of the hazard analysis was to identify the hazards. A comprehensive list of hazards was developed to assess what can plausibly go wrong and reduce safety. A clear and concise description of each hazard was written and assigned a unique hazard identification number in the hazard analysis and risk assessment in **Appendix B**. Each hazard was categorized by its type and the operational mode of the platoon when the hazard may occur. The potential causes or set of conditions that may lead to the hazards were also listed. The result or impacts of each hazard were explained in the Accident/Mishap column.

Hazard Identification Number

This is a unique identification number for each hazard analyzed in **Appendix B**. This reference will be associated with the hazard description, hazard type, potential cause, and accident/mishap.

Hazard Description

A detailed description of the potential hazard or hazardous scenario is explained.

Hazard Type

Each hazard is categorized into one of the following hazard types: inherent equipment failures, operational environment hazards, or human factors.

Inherent Equipment Failures: Of primary importance to the analysis are inherent equipment failure modes, of both the vehicle itself and the platooning system that has been installed. These failure modes, typically caused by hardware or software failures or system design flaws, are limited to the components installed on the vehicle. Analysis on these components were performed at the "black box" level. The functionality of these components was analyzed at component level.

Vehicular equipment failure modes:

Physical systems (electronic or mechanical)

Communication (Vehicle-to-Vehicle [V2V])

***Operational Environment Hazards*:** The platooning system must be designed to mitigate potential hazards from the operating environment—roadway geometry, traffic, weather conditions, and, due to the communications between platooning trucks, malicious actions including cyberattacks.

Roadway conditions:

Significant grade or sharp curvature

Line markings

Weather and lighting conditions:

Glare

Precipitation or ice

Traffic conditions:

Cut-ins

Truck behind the platoon (not controlled by platooning system) follows too closely

Malicious actions:

Cyber-based attacks

Vandalism

***Human Factors*:** The driver is required to steer, accelerate, brake, lane keep, and monitor roadway and traffic conditions. While platooning, the driver has these responsibilities along with the added responsibility of leading the platoon. The leader must monitor the performance of the platooning system and respond to any messages or alerts it generates. The leader must also be aware of surrounding traffic conditions and situations that could disrupt the platoon or threaten the safety of the following trucks. Additional workload requirements for the leader can also result if the platoon has trucks with different loading conditions, since the leader will have to know how the differences affect the overall performance of the platoon.

- Impacts of the increased workload for the lead driver, to perform the driving responsibilities associated with their truck while assuming additional responsibilities associated with leadership of the platoon.
- Driver engagement, both physical and cognitive, especially with control transitions between the driver and system.
- Importance of driver interface with information exchanges between the driver and vehicle system.
- Importance of information exchanges between the drivers of each truck within the platoon.
- The significance of stimulus-response compatibility to display and communicate information in the proper context to the drivers in the following trucks based on their position in the platoon.
- Environmental concerns with smaller gaps between trucks resulting in exhaust fumes entering the interior cabins of the following trucks in the platoon.

Potential Causes

The potential causes of a hazard are the sets of circumstances that could lead to the hazard defined. There may be one or more potential causes for each hazard.

Accident/Mishap

The effects of a hazard are the sets of consequences that would occur in response of the hazard being caused. This describes the accident or mishap that may occur.

Risk Assessment

Following the ISO 26262 standard, hazards are classified by three dimensions: severity, probability of exposure, and controllability. Together, these three dimensions formulate an ASIL, which is assigned to each hazard before and after a safety measure has been implemented. Although the ratings assigned to each of the three dimensions for the risk assessments follow the standard, the ratings are subjective to the party performing the safety analysis. The severity, probability of exposure, and controllability are dependent upon the system and its ODD. The following subsections are column headings of the hazard analysis and risk assessment hazard, which are explained below.

Initial Severity

Severity is defined as an estimate of the extent of harm to one or more people that can occur in a potentially hazardous situation. Initial severity is the severity of the hazard that exists prior to a safety measure being implemented. The initial severity assigned to each hazard will follow the severity definitions from the ISO 26262 standard. **Table 4** provides a description and examples for each class of severity from S0 to S3.

Table 4. Class of Severity From ISO 26262 Standard

	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
Reference for single injuries (from Abbreviated Injury Scale (AIS) scale)	• AIS 0 and less than 10% probability of AIS 1-6 • Damage that cannot be classified safety-related	• More than 10% probability of 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
Examples	• Bumps with roadside infrastructure • Pushing over roadside post, fence, etc. • Light collision • Light grazing damage • Damage entering/exiting parking space • Leaving the road without collision or rollover	• Side impact with a narrow stationary object, e.g. crashing into a tree (impact to passenger cell) with very low speed • Side collision with a passenger car (e.g. intrudes upon passenger compartment) with very low speed • Rear/front collision with another passenger car with very low speed • Collision with minimal vehicle overlap (10% to 20%) • Front collision (e.g. rear-ending another vehicle, semi-truck, etc.) without passenger compartment deformation	• Side impact with a narrow stationary object, e.g. crashing into a tree (impact to passenger cell) with low speed • Side collision with a passenger car (e.g. intrudes upon passenger compartment) with low speed • Rear/front collision with another passenger car with low speed • Pedestrian/bicycle accident while turning (city intersection and streets)	• Side impact with a narrow stationary object, e.g. crashing into a tree (impact to passenger cell) with medium speed • Side collision with a passenger car (e.g. intrudes upon passenger compartment) with medium speed • Rear/front collision with another passenger car with medium speed • Pedestrian/bicycle accident (e.g. 2-lane road)

Table 4 references to the AIS as it describes the severity of injuries as issued by the Association for the Advancement of Automotive Medicine. Each scale is described below:

AIS 0: no injuries;

AIS 1: light injuries such as skin-deep wounds, muscle pains, whiplash, etc.;

AIS 2: moderate injuries such as deep flesh wounds, concussion with up to 15 minutes of unconsciousness, uncomplicated long bone fractures, uncomplicated rib fractures;

AIS 3: severe but not life-threatening injuries such as skull fractures without brain injury, spinal dislocations below the fourth-cervical vertebra without damage to the spinal cord, more than one fractured rib without paradoxical breathing, etc.;

AIS 4: severe injuries (life-threatening, survival probable) such as concussion with or without skull fractures with up to 12 hours of unconsciousness, paradoxical breathing;

AIS 5: critical injuries (life-threatening, survival uncertain) such as spinal fractures below the fourth cervical vertebra with damage to the spinal cord, intestinal tears, cardiac tears, more than 12 hours of unconsciousness including intracranial bleeding;

AIS 6: extremely critical or fatal injuries such as fractures of the cervical vertebrae above the third cervical vertebra with damage to the spinal cord, extremely critical open wounds of body cavities (thoracic and abdominal cavities), etc.

Initial Probability of Exposure

Exposure is the state of being in an operational situation that can be hazardous if coincident with the failure mode under analysis. Each hazard is assigned a probability of exposure according to the defined in **Table 5**. The initial probability of exposure represents the exposure to the hazard without a safety measure implemented. **Table 5** provides a description and examples for the different classes of probability of exposure as defined in the ISO 26262 standard.

Table 5. Classes of Probability of Exposure Regarding Frequency in Operational Situations

	E1	**E2**	**E3**	**E4**
Description	Very low probability	Low probability	Medium probability	High probability
Frequency of situation	• Occurs less often than once a year for the great majority of drivers	• Occurs a few times a year for the great majority of drivers	• Occurs once a month or more often for an average driver	• Occurs during almost every drive on average
Road layout	-	• Mountain pass with unsecured steep	-	-
Road surface	-	• Snow and ice on road	• Wet road	-
Nearby elements	-	-	• In tunnel • In car wash • Traffic congestion	-

	E1	E2	E3	E4
Vehicle stationary state	• Stopped, requiring engine restart (at railway crossing) • Vehicle being towed • Vehicle during jump start	• Trailer attached • Roof rack attached	• Vehicle being refueled • Vehicle on a hill (hill hold)	-
Maneuver	-	• Evasive maneuver deviating from desired path	• Overtaking	• Starting from standstill • Shifting transmission gears • Accelerating • Braking • Executing a turn (steering) • Using indicators • Maneuvering vehicle into parking position • Driving in reverse

Initial Controllability

Controllability is the ability to avoid a specified harm or damage through the timely reactions of the people involved, possibly with support from external measures. Assigning the controllability class requires an estimation of the probability that the representative driver will be able to retain or regain control of a vehicle if a given hazard were to occur. Representative driving behaviors of the driver to consider may be related to the target market, person's age, hand-eye coordination, driving experience, cultural background, etc. The initial controllability does not include the hazard's safety measure (refer to **Table 6**).

Table 6. Examples of Possibly Controllable Hazardous Events by the Driver or People Potentially at Risk

		C0	C1	C2	C3
	Description	**Controllable in General**	**2VL1 Controllable**	**Normally Controllable**	**Difficult to Control or Uncomfortable**
Examples	**Driving factors and scenarios**	-	-	-	-
	Situations that are considered distracting	• Maintain intended driving path	-	-	-
	Unexpected radio volume increase	• Maintain intended driving path	-	-	-
	Warning message – gas low	• Maintain intended driving path	-	-	-
	Unavailability of a driver assisting system	• Maintain intended driving path	-	-	-
	Fault adjustment of seat position while driving	-	• Brake to slow/stop vehicle	-	-
	Blocked steering column when starting the vehicle	-	• Brake to slow/stop vehicle	-	-
	Failure of Anti-lock Braking System (ABS) during emergency braking	-	-	• Maintain intended driving path	-

		C0	C1	C2	C3
	Description	**Controllable in General**	**2VL1 Controllable**	**Normally Controllable**	**Difficult to Control or Uncomfortable**
	Headlights fail while night driving at medium/high speed on unlighted road	-	-	• Steer to side of road or brake to stop	-
	Motor failure of ABS when braking on low friction road surface while executing a turn	-	-	• Maintain intended driving path	-
	Failure of ABS when braking on low friction road surface while executing a turn	-	-	-	• Maintain intended driving path, stay in lane
	Failure of brakes	-	-	-	• Brake to slow/stop vehicle
	Incorrect steering angle with high angular speed at medium or high vehicle speed (steering angle change not aligned to driver intent)	-	-	-	• Maintain intended driving path, stay in lane
	Fault driver airbag release when traveling at high speed	-	-	-	• Maintain intended driving path, stay in lane • Brake to slow/stop vehicle

Initial ASIL Determination

The initial ASIL is determined based on the classification of the hazard with respect to its' severity, probability of exposure, and controllability in accordance with **Table 7** from the ISO 26262 standard. There are four ASILs: A, B, C, and D. ASIL A is the lowest safety integrity level and ASIL D is the highest. There is also the QM class that denotes the requirement to comply with ISO 26262.

Table 7. ASIL Determination From ISO 26262 Standard

Severity Class	Probability Class	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

Safety Measures

A safety measure is the activity of a technical solution to avoid or control systematic failures and to detect random hardware failures or control random hardware failures, or mitigate their harmful effects. Each hazard will have one or more safety measures, perhaps of different types that mitigate or eliminate the hazard. The safety measure types include design, operations, training and maintenance. The safety measures in the analysis are recommendations for reducing the risk to an acceptable level. A benefit-cost analysis was not performed to analyze the benefit received for implementing the safety measure versus its cost.

Measure Type

The measure type describes the category of safety measure implemented to mitigate the hazard. This may include the following types of safety measures: design, operations, training, and maintenance.

Final Severity

The final severity is the severity of the hazard that exists after the implementation of a safety measure. This will be assigned according to the classes of severity described in **Table 4**.

Accident/Mishap

This column of the table describes the result of the hazard. The majority of the hazards result in a crash.

Final Probability of Exposure

The final probability of exposure is the remaining risk of exposure that exists after the implementation of a safety measure. **Table 5** describes the classes of probability of exposure.

Final Controllability

Final controllability describes the class of controllability of a hazard after a safety measure has been implemented. **Table 6** describes these classes and provides examples.

Residual ASIL Determination

The residual ASIL is determined according to **Table 7** after safety measures have been implemented to reduce the severity, probability of exposure, or improve controllability.

Stakeholder Engagement

Once the draft hazard analysis and risk assessment were completed, three stakeholder engagement sessions were held with industry organizations. The hazard analysis and risk assessment were disseminated to members of the industry organizations to solicit feedback. During the webinar, an overview of the project and of the 2VL1 and 3VL2 systems was provided and then facilitated a working group discussion ranging between one and two hours. The team received contributions from the organization members including input on additional hazards and safety mitigations to consider, clarifications and assumptions of the 2VL1 and 3VL2 systems and overall discussion topics related to truck platooning. Findings were incorporated into the hazard analysis and risk assessment in the final report.

The first webinar was attended by an ATA representative. ATA is the largest national trade association for the trucking industry, which consists of a partnership with all 50 state trucking associations and industry-related councils.[3]

The second webinar was attended by over 15 CVSA members. CVSA is a non-profit association that is composed of law enforcement and CMV enforcement members, and industry representatives and safety officials from the federal, state, local, provincial, and territorial levels within Canada, Mexico, and the United States.[4]

Over 30 SAE International members from five different committees participated in the third webinar. The Total Vehicle Steering committee, Truck and Bus Body and Occupant

[3] American Trucking Associations. About. In ATA. Retrieved from https://www.trucking.org/About.aspx.

[4] Commercial Vehicle Safety Alliance. About the Alliance. In CVSA. Retrieved from https://cvsa.org/about-us-page/about-cvsa/overview-of-cvsa/about-the-alliance/.

Environment Steering committee, Electrical Electronic Steering committee, and Automated and Connected Vehicle and Active Safety Systems committee.

The complete hazard analysis and risk assessment are presented in **Table 13** of **Appendix** .

Findings

After reviewing the draft hazard analysis and risk assessment, two methodologies of safety analysis were selected. A SOTIF review and a fault tree analysis (FTA) were performed on the 2VL1 and 3VL2 systems described in **Chapter 1**. The SOTIF analysis was conducted in accordance with the ISO 21448 Road Vehicles – Safety of the Intended Functionality. The SOTIF was chosen as it evaluates risks due to hazards caused by as-designed performance limitations even with intended usage or behavior, as well as hazards associated with reasonably foreseeable misuse the by user. It is used to: identify areas of potential system performance and/or functional improvement; define system acceptance criteria; and develop possible verification and validation activities.

The FTA is a top-down approach to analyzing system hazards. After selecting several critical hazards of the system, lower-level hazards and faults that could contribute to the hazard are identified to find all credible ways in which the undesired system state can occur.

The majority of the hazards could be alleviated or reduced with appropriate safety mitigations as described in detail in **Appendix B**, Hazard Analysis and Risk Assessment Summary. However, there were a select number of hazards that remained with an undesirable ASIL. These hazards are summarized in **Table 8**. (Note that Hazard ID numbers in **Table 8** reference hazards identified in **Table 13**, **Appendix B**.)

Table 8. Platooning Hazards With the Highest Residual Risk Assessments

Hazard ID	Description of Safety Hazard	Residual Risk Assessment	System Applicability
17	There is an unexpected stoppage in traffic.	ASIL A	2VL1 and 3VL2
18	There is unexpected road debris.	ASIL B	2VL1 and 3VL2
28	There is a difference in tire wear (e.g., traction, tread depth, grip, etc.) between the LV and FVs.	ASIL A	2VL1 and 3VL2
33	There is a loss in steering control in the LV.	ASIL A	2VL1
34	There is a loss in steering control in the FV.	ASIL A	3VL2
41	There is a cyber-attack on the FV’s communication subsystem.[5]	ASIL A	2VL1 and 3VL2

[5] For more information, refer to: FMCSA (2020, May) Cybersecurity Best Practices for Integration/Retrofit of Telematics and Aftermarket Electronic Systems into Heavy Vehicles, [https://rosap.ntl.bts.gov/view/dot/49248].

Hazard ID	Description of Safety Hazard	Residual Risk Assessment	System Applicability
53	A motorcycle performs a cut-in between two platooning vehicles.	ASIL A	2VL1 and 3VL2
57	The driver of the LV performs an evasive steering maneuver.	ASIL B	3VL2

The safety mitigations developed to address the identified hazards were based on approaches and input received during the webinars focused on hazard analyses and risk assessment. The complete list of 71 safety mitigations is presented in **Table 25**, **Appendix E**. (Note that the numbers listed in the bulleted list below reference **Table 25**, **Appendix E**). It is important to note that several of the safety mitigations developed for the 2VL1 and 3VL2 platooning systems are also applicable to non-platooned trucks. These include:

- #6 – The HMI provides periodic driver engagement such as an alerter button (e.g., dead man switch).
- #7 – The platoon safety disengages and alerts the driver if there is failure to engage with the HMI.
- #11 – The front-facing camera and sensors detect moving objects approaching the front and sides of the vehicle and alert the driver.
- #37 – The system sensors detect precipitation and icy conditions and notify the driver of changing weather conditions.
- #40 – The driver does not operate in platooning mode during low visibility conditions.
- #41 – Drivers disengage platooning mode upon entering a work zone.
- #55 – The driver monitoring system monitors the driver’s attentiveness and fatigue.
- #63 – Each driver in the platoon is aware of the other driver’s hours of service.

Chapter 4. Safety Analysis

Objective

This task focuses on expanding on the hazard analysis and risk assessment by performing lower-level safety analyses. A SOTIF and an FTA were performed on the 2VL1 and 3VL2 systems described in **Chapter 1**. This chapter provides an overview of the methodology of conducting the SOTIF and FTA analyses. The result from the complete SOTIF analysis is presented in **Appendix C**. The result from the complete FTA analysis is presented in **Appendix D.**

Approach

ISO 21448 – Road Vehicles – Safety of the Intended Functionality

Technology advancements in vehicles, including the development of advanced driver assistance systems (ADAS), automate or assist drivers with aspects of the dynamic driving task (DDT). SAE J3016^{TM} defines the DDT as all of the real-time operational and tactical functions required to operate a vehicle in on-road traffic, excluding strategic functions such as trip scheduling and selection of destinations and waypoints.[6] The SOTIF analysis was guided by ISO 21448 Road Vehicles – Safety of the Intended Functionality standard.

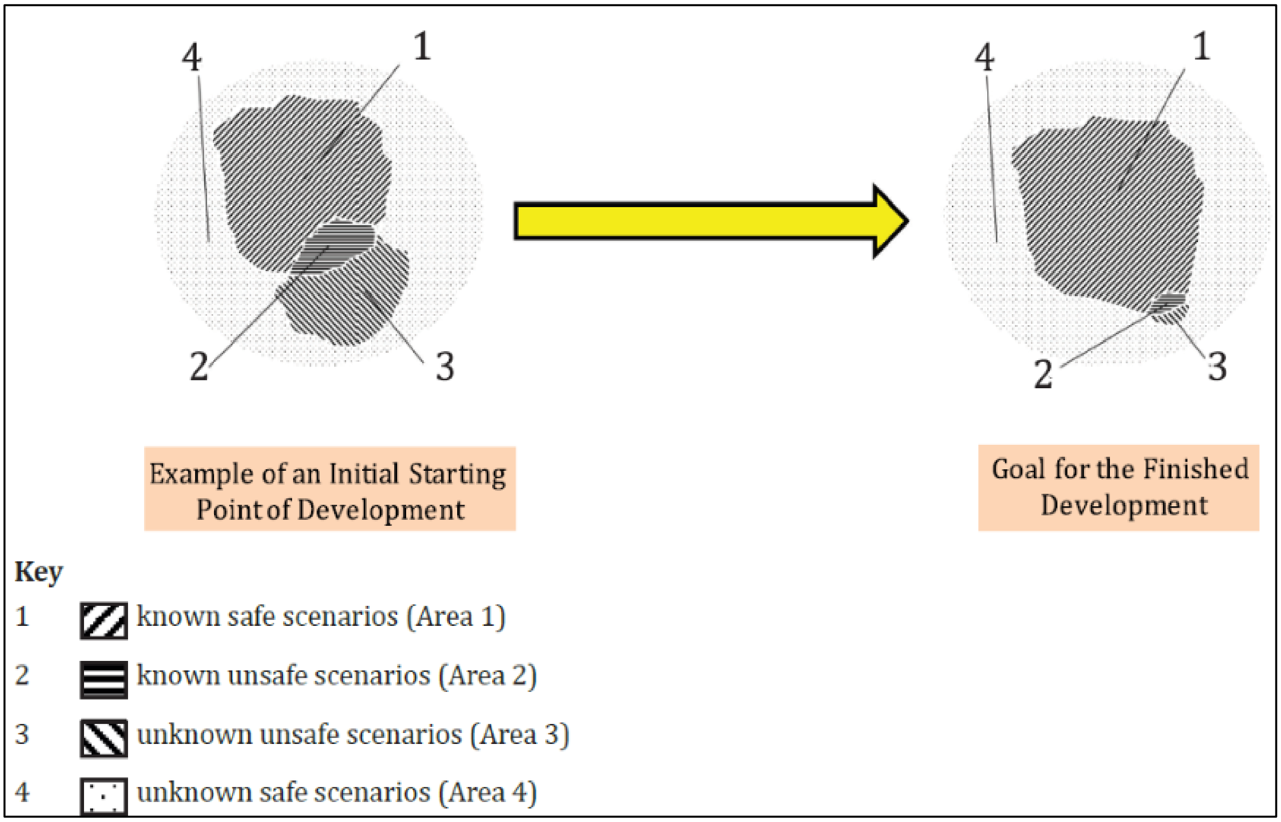
The ISO 21448 SOTIF standard provides a framework and process for analyzing intended functionality where proper situational awareness is critical to safety, and where that situational awareness is derived from 3VL2 sensors, and processing algorithms; especially emergency intervention systems (e.g., emergency braking systems) and ADAS with levels 1 and 2 on the SAE standard J3016^{TM} automation levels of driving automation. ADAS functionality is heavily dependent upon sensors and 3VL2 algorithms. SOTIF is defined as the absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or by reasonably foreseeable misuse by people.[7] This edition of the document can be considered for higher levels of automation; however additional mitigations might be necessary. The standard is not intended for functions of existing systems for which well-established and well-trusted design, V&V mitigations exist at the time of publication (e.g., dynamic stability control systems, air bags, etc.).

As illustrated in **Figure 5**, the purpose of the SOTIF is primarily twofold. First, the analysis explores each function associated with a system to determine potential hazards resulting from a failure of that particular function, such as risk of collision caused by failure of accelerator control. By this means, risks that were, prior to the analysis, unknown, can be identified. This is

[6] U.S. DOT. (2018, December 3). Preparing for the Future of Transportation: Automated Vehicles 3.0. In Transportation.gov. Retrieved from https://www.transportation.gov/av/3.

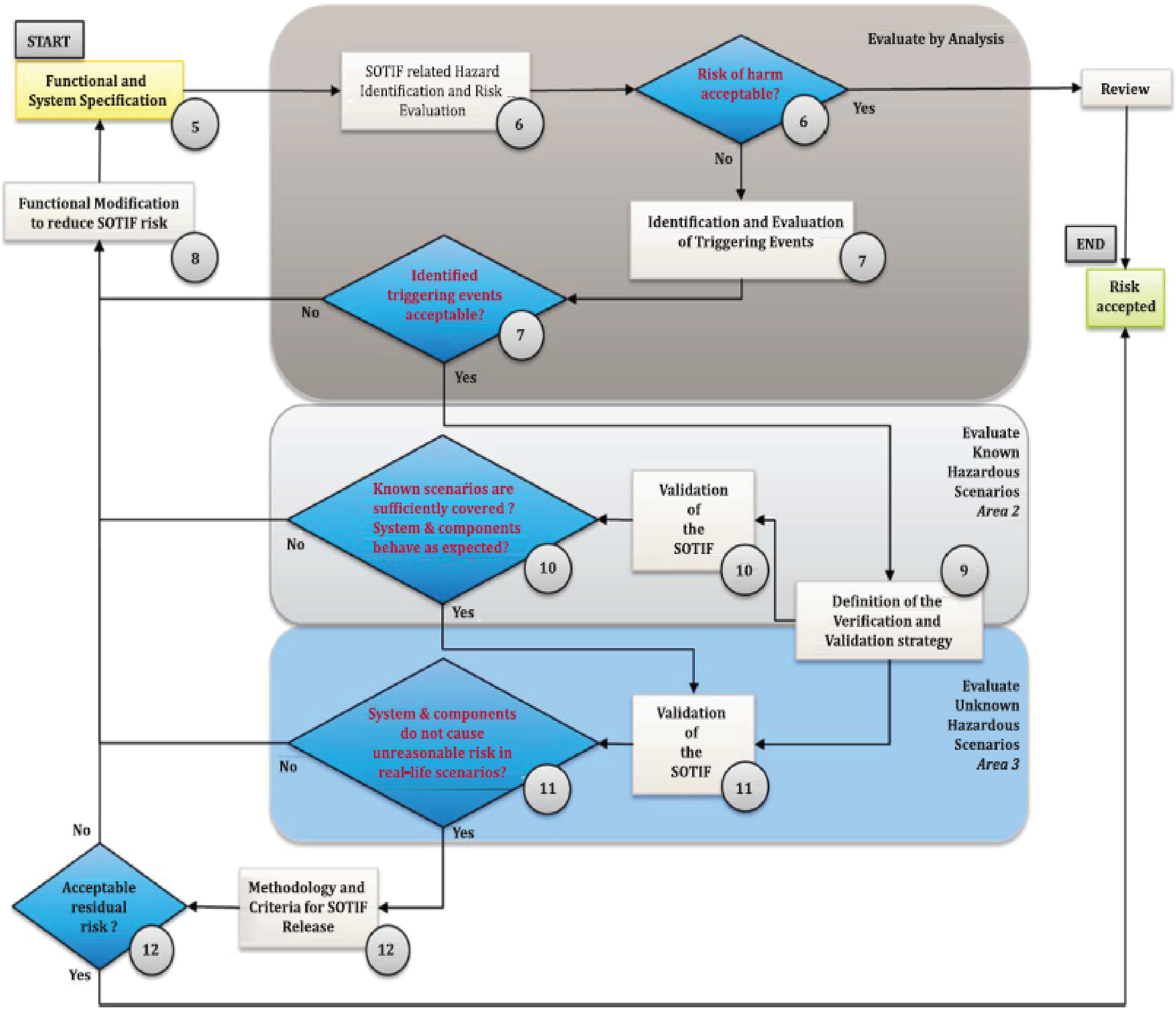
[7] International Standards Organization. (2019). Road vehicles — Safety of the intended functionality (2019-First ed., pp. 1-62). Switzerland: ISO.

represented in **Figure 5** by the reduction of Area 3 on the graphic, the unknown unsafe scenarios. As functional hazard scenarios are identified, Area 2, known unsafe scenarios, is increased. This leads to the second step of the SOTIF analysis, elimination or mitigation of functional hazards, and V&V of that mitigation.


4
1
2
3
4
1
2
3
Example of an Initial Starting Point of Development
Goal for the Finished Development
Key
1 ▨ known safe scenarios (Area 1)
2 ☰ known unsafe scenarios (Area 2)
3 ▧ unknown unsafe scenarios (Area 3)
4 ⬚ unknown safe scenarios (Area 4)

Source: ISO 21448 standard

Figure 5. Identification of Unknown Unsafe Scenarios in the SOTIF Analysis.


START
Functional and System Specification
5
SOTIF related Hazard Identification and Risk Evaluation
6
Risk of harm acceptable?
6
Yes
No
Evaluate by Analysis
Review
Identification and Evaluation of Triggering Events
7
Functional Modification to reduce SOTIF risk
8
Identified triggering events acceptable?
7
No
Yes
END
Risk accepted
Evaluate Known Hazardous Scenarios
Area 2
Known scenarios are sufficiently covered ? System & components behave as expected?
10
No
Yes
Validation of the SOTIF
10
9
Definition of the Verification and Validation strategy
Evaluate Unknown Hazardous Scenarios
Area 3
System & components do not cause unreasonable risk in real-life scenarios?
11
No
Yes
Validation of the SOTIF
11
No
Acceptable residual risk ?
12
Yes
Methodology and Criteria for SOTIF Release
12

Source: ISO 21448 standard

Figure 6. Activities and Processes Flowchart for Performing the SOTIF Analysis.

The numbers inside the circles shown in **Figure 6** refer to the section of the standard. For example, Functional and System Specification is described in section five of the standard. This represents the first SOTIF analysis activity. **Table 9** illustrates SOTIF analysis activities described in the ISO 21448 standard.

Table 9. SOTIF Analysis Activities Described in ISO 21448 Standard

Section of the Standard	Description of SOTIF Activity	Activity #	Table #
5	Functional and system specification (intended functionality content)	1	Table 14
6	Identification and evaluation of hazards caused by the intended functionality	2	Table 15
7	Identification and evaluation of triggering events	3	Table 15
8	Functional modifications to reduce SOTIF related risks	4	Table 16
9	Definition of the V&V strategy	5	Table 17 Table 18
10	Verification of the SOTIF (Area 2)	6	Table 19
11	Validation of the SOTIF (Area 3)	7	Table 20
12	Methodology and criteria release for SOTIF release	8	N/A

Refer to **Appendix** for the result of each SOTIF analysis activity. The methodology for the SOTIF release is described below.

As the final activity in the analysis, a SOTIF release is performed to evaluate the acceptability of the residual risk after the findings of the analysis. The following SOTIF activities are reviewed:

- functional and system specification;
- V&V targets;
- analysis of triggering events;
- functional improvements;
- V&V strategy, as defined;
- results of verification as defined; and
- results of the validation of the SOTIF.

ISO 21448 indicates the following questions should be asked to evaluate the SOTIF release. This process is illustrated in **Figure 7**. Some example questions that should be asked before passing along to successive phases (shown in **Figure 7**) are given below:

1. Did the validation strategy consider all the specified use cases within the scope of the intended functions?
    a. Did the testing comprehensively cover the identified triggering events?
    b. Did the validation cover boundary conditions, and ensure the system did not operate unsafely upon leaving the ODD?
    c. Did the validation ensure that invalid messages are rejected, or otherwise handled safely (i.e., does not cause unintended operation)?
2. Does the intended functionality achieve a minimum fallback risk condition, when necessary, providing a state without unreasonable risk to the occupants or other road users?

   a. Using only the specified driver intervention;
   b. Considering reasonably foreseeable misuse; and
   c. Warning to the vehicle occupants and/ or the other road users of the malfunctioning vehicle.

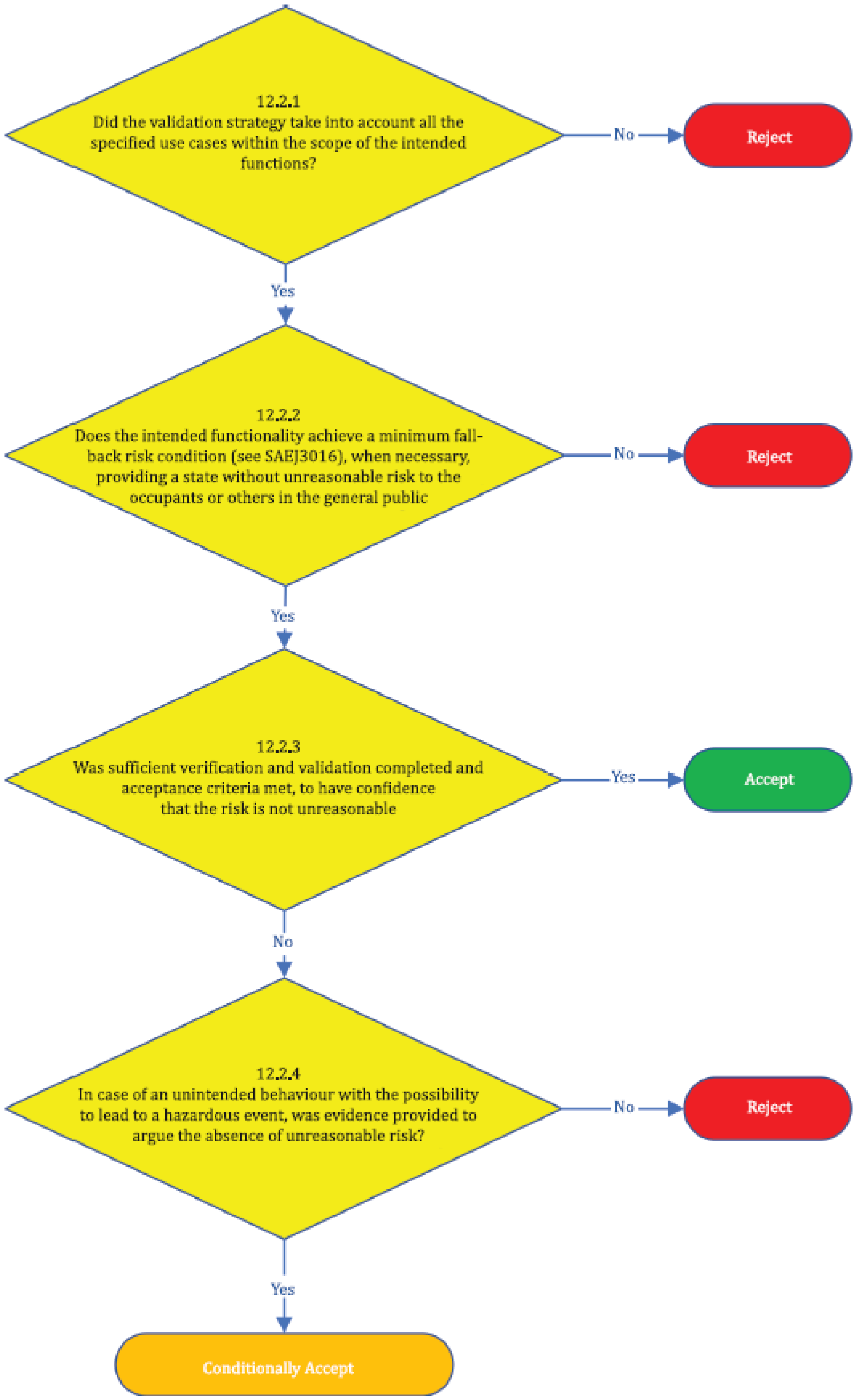
3. Was sufficient V&V completed and acceptance criteria met, to have confidence that the risk is not unreasonable?

   a. Has the intended function been exercised sufficiently to evaluate both nominal behavior and potential unwanted behavior?
   b. Have all safety-critical or safety-related requirements been verified in the implementation? Is the requirements traceability sufficient?
   c. Was no unintended behavior observed with the possibility to lead to a hazardous event?

4. In case of an unintended behavior with the possibility to lead to a hazardous event, was evidence provided to argue the absence of unreasonable risk?

   a. Does the validation strategy include scenarios where the system must respond safely upon leaving the ODD?
   b. Does the validation strategy include scenarios that include human error on the part of the operators?

For the complete result from the SOTIF analysis, refer to **Appendix C**.


12.2.1
Did the validation strategy take into account all the specified use cases within the scope of the intended functions?
No
Reject
Yes
12.2.2
Does the intended functionality achieve a minimum fall-back risk condition (see SAEJ3016), when necessary, providing a state without unreasonable risk to the occupants or others in the general public
No
Reject
Yes
12.2.3
Was sufficient verification and validation completed and acceptance criteria met, to have confidence that the risk is not unreasonable
Yes
Accept
No
12.2.4
In case of an unintended behaviour with the possibility to lead to a hazardous event, was evidence provided to argue the absence of unreasonable risk?
No
Reject
Yes
Conditionally Accept

Source: ISO 21448 standard

Figure 7. Methodology for Evaluating the Criteria for the SOTIF Release.

Fault Tree Analysis

The FTA was performed with a qualitative approach. A quantitative approach would have required failure rate and probability data about the system and its operational environment. These data were typically proprietary, which is specific to a certain manufacturer's component. The representative systems developed in this study were generic components that only identify function. There was also a lack of truck platooning system data publicly available to support the analysis as discovered in market assessment of heavy-truck platooning systems.

FTA is a deductive, top-down method aimed at analyzing the effects of initiating faults and events on a 3VL2 system. The analysis demonstrates how resistant a system is to single or multiple initiating events. The results of the FTA provide detailed insight into the design of the system by exploiting areas that may need additional safety mitigations. This process is described in five steps below:

1. ***Identify undesired events***: First the inputs, environmental conditions, users and any other influences on system behavior must be examined to identify which of these events have potential to result in undesired outcomes (system failures).
2. ***Understand the system***: Next, a thorough understanding and familiarity with the system is essential to developing a fault tree. Relationships between systems, interfaces, and inputs and outputs are necessary to correlate undesired initiating events and their propagation to top-level undesired outcomes.
3. ***Construct the fault tree***: After undesired events have been identified and relationships of subsystems are established, a top-level event is selected to construct the tree. For this analysis, four top-level events were selected. These are listed in **Table 10**. The FTA maps the relationship between faults, subsystems, and safety design elements by creating a logic diagram of the overall system, starting at the lowest level of Basic Events that feed into high-level “AND” and “OR” gates, eventually converging into the top-level fault.
4. ***Evaluate the fault tree***: Once the fault tree for the top-level fault of interest has been constructed, system engineers can evaluate the tree for unforeseen system interactions and potential critical paths between initiating and top-level events. Where available, reliability data can be entered for initiating faults and events so a probability of occurrence can be calculated for different cut sets of each fault. A qualitative approach was taken for this analysis as specific information on failure rates of specific system components and probabilities of events were unknown.
5. ***Control the hazard***: Finally, system and design changes can be considered to remove or mitigate the hazards identified in the fault tree. Critical paths can be identified, and control mitigations can be put in place such as design modifications. These modifications may include: redundancy, cross-strapping, or selecting high reliability components.

After the completion of the hazard analysis and risk assessment performed in the previous task, several hazards were selected to be analyzed in the FTA. Four hazards were selected for the analysis based on their Initial Risk Assessment according to the ISO 26262 standard, which considers a combination of the hazard’s severity, probability of exposure and controllability. As another criterion, hazards were selected to represent both the 2VL1 and 3VL2 systems. For example, some hazards developed in hazard analysis are only applicable to the 3VL2 system based on the steering actuation functionality of the FVs. These hazards are listed in **Table 10**. The Hazard IDs referenced in **Table 10** are consistent with the Hazard IDs assigned to the hazards identified in the previous hazard analysis and risk assessment (refer to **Table 13**, **Appendix B**).

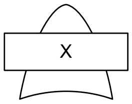
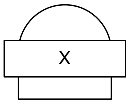
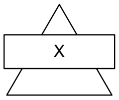
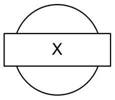
The first three hazards in **Table 10** are applicable to both the 2VL1 and 3VL2 systems; however, only the second and the fourth hazards are applicable to the 3VL2 system as the hazard would impact the steering actuator functionality of the FVs. The 2VL1 system does not contain this steering actuation in the FV.

Table 10. Hazards Analyzed in the FTA

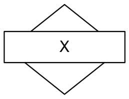
Hazard ID	Description of the Hazard	Hazard Type	Initial Risk Assessment	System Applicability
17	There is an unexpected stoppage in traffic.	Environmental Operation	ASIL B	2VL1 and 3VL2
34	There is a loss in steering control in the FV.	Inherent Equipment Failure	ASIL A	3VL2
53	A motorcycle performs a cut-in between two platooning vehicles.	Environmental Operation	ASIL B	2VL1 and 3VL2
57	The driver of the LV performs an evasive steering maneuver.	Human Factors	ASIL B	3VL2

Table 11 describes the standard set of symbols used to define the fault trees, and **Table 21** lists the basic Fault Tree elements and their use in fault trees.

Table 11. Fault Tree Symbol Definitions[8]

Symbol	Symbol Description	Symbol Definition
	Or Gate	Illustrates the output occurs if at least a single event occurs.
	And Gate	Illustrates the output occurs if and only if all inputs occur.
	Transfer Gate	Illustrates a transfer continuation from a different part within the fault tree that this was developed.
	Basic Event	Identifies a basic initiating System or Subsystem fault.

[8] Concept Draw. (n.d.). Design elements - Fault tree analysis diagrams. In www.ConceptDraw.com. Retrieved October 11, 2017, from https://conceptdraw.com/a183c3/preview.

Symbol	Symbol Description	Symbol Definition
	Undeveloped Event	Identifies an event that does not need to be further developed or resolved.

One event was considered for each fault tree. The hazard analysis and risk assessments were used to identify the top-level events for each tree. Each tree was constructed by identifying all possible hazards effecting the system in a direct or indirect way. The overall outcome of a fault tree analysis is to identify improvements or ways to manage the risk of the undesired event and to reduce its likelihood or its effect. This is often improved through system design.

As listed in Table 10, four hazards were selected for analysis through the FTA process. Of the four hazards selected, three may lead directly to a crash of one or more of the platooning vehicles. The fourth hazard analyzed, "*There is a loss of steering control in the FV,*" is also likely to result in a crash.

For the complete result of the FTA, refer to **APPENDIX D**:.

Findings

The SOTIF analysis and FTA were complementary. As the fault trees were developed and the SOTIF activities such as hazard identification were performed, themes emerged indicating which subsystems and functions are the most vulnerable. The findings of each analysis are summarized below.

Safety of the Intended Functionality Analysis

To perform a SOTIF on a heavy-truck platooning system, the system integrator would follow the steps outlined in **Figure 6** and also described in the subsequent paragraph. The analysis is quantitative in nature to account for differences in system designs and components used across different platooning system manufacturers. The result from the complete SOTIF analysis for the truck platooning systems is presented in **Appendix C**.

One challenge associated with performing the SOTIF analysis on a representative platooning system, was not having a functional system specification. Details about the system's functions and relationships between specific components had to be generated based off the team's knowledge of platooning and available resources. It is assumed that a platooning system integrator or manufacturer would have this documentation prior to beginning the SOTIF activities. This set of specifications would be the baseline for performing the SOTIF.

An attempt was made to identify known unsafe conditions in this analysis as a baseline for establishing a list of example verification tasks. A system integrator would need to further develop validation use case scenarios to test the system in a real-world environment to identify unknown unsafe scenarios. The identification of these unexpected scenarios adds to the list of known unsafe conditions. This starts the SOTIF analysis process over again where the system integrator then identifies functional modifications to reduce SOTIF risks and to create new known unsafe conditions to test in verification. This feedback loop increases the safety and reliability of the platooning system.

Fault Tree Analysis

The goal of conducting an FTA is to analyze the effects of initiating faults and events on a complex system. Critical failures or events that lead to hazards were identified through the creation of fault trees as documented in **APPENDIX D**: The fault trees illustrate the interfaces and relationships between hazards and system functions.

Two critical path events were identified as a result of the FTA: a failure of the CMS and inadequate training and operation of the platooning system. The failure of the CMS to maintain a safe following distance between vehicles in the platoon, between the LV of the platoon and a non-platooning vehicle and between the LV of the platoon and an object ahead, is the most integral part of the platooning system. The CMS is integrated with the vehicle and interfaces directly with the EMS as well as the brake system. Inadequate integration or a failure of one of these components represents a significant risk for a crash to occur. Fortunately, the CMS can be tested extensively through V&V to prove the system is integrated properly for the designed use of the system.

Inadequate training and operation of the platooning system represents a significant challenge for roadway safety. The following basic level events are examples illustrated in the fault tree that are pertinent to safe platooning operations.

- Failure to identify cut-ins or potential cut-ins
- Failure to disengage the platoon in qualifying conditions
- Distracted driving
- Driver inattentiveness
- Operating procedures not followed (e.g., platooning configuration, late attempt to merge, platooning outside the ODD)
- Inadequate driver training

These events are represented in Fault Trees 3.1, 3.3, and 4 listed in **Appendix D**.

Dissimilar to a failure of the CMS, testing for driver (human) error and implementing adequate safety mitigations is much more difficult. With the systems at SAE driving automation levels 1 and 2, human drivers are expected to be fully attentive at all times and be ready to resume control with or without warning that the system may no longer be functioning as intended. There is a near infinite number of environmental factors and use case scenarios a driver must contend with compared to a discrete number of failure modes for an electronic-mechanical CMS. Systems with a human-in-the-loop require safety mitigations such as training and operating procedures that are fully dependent upon the human complying.

Chapter 5. Conclusion

In this study, three tasks were performed to explore the safety implications of heavy-truck platooning. First, a market assessment was conducted to summarize the current state of the technology and to identify concept heavy-truck platooning systems. Next, a hazard analysis and risk assessment were performed on the representative 2VL1 and 3VL2 concept platooning systems to postulate a list of potential hazardous events to analyze. Finally, a SOTIF analysis was performed on each concept platooning system function to identify critical functions for maintaining safety, while platooning. The FTA was conducted on key hazards that were difficult to control or mitigate.

The market assessment indicated there was little public information available on the designs and operations of platooning system. High-level block diagrams and an abbreviated list of components were available for some systems; however, there was insufficient information available on how these systems initiate, form and dissolve the platoon. Despite the lack of detail on the system operations, many of these systems share a similar architecture common across all systems. A literature search confirmed there had not been a safety analysis published on a heavy-truck platooning system.

A list of hazards applicable to the representative heavy-truck platooning concepts (2VL1 and 3VL2) was developed as part of the hazard analysis. This list was created based on the research team's platooning experience and expertise with commendable contributions from ATA, CVSA and SAE International standards committee members. Each hazard was assessed, guided by the ISO 26262 standard that provided a framework for assessing each hazard on its severity, probability of exposure and controllability. Despite generating and applying design, operations, maintenance and safety mitigations to each hazard, several hazards could not be reduced to an acceptable level of risk for these systems described in Chapter 1. These hazards were:

- #17 There is an unexpected stoppage in traffic.
- #18 There is unexpected road debris.
- #28 There is a difference in tire wear (e.g., traction, tread depth, grip, etc.) between the LV and FVs.
- #33 There is a loss in steering control in the LV.
- #34 There is a loss in steering control in the FV.
- #41 There is a cyber-attack on the FV's communication subsystem.
- #53 A motorcycle performs a cut-in between two platooning vehicles.
- #57 The driver of the LV performs an evasive steering maneuver.

After the completion of the hazard analysis and risk assessment, a fault tree and SOTIF analysis were performed as the safety analysis methodologies. The FTA was conducted on the key hazards from the previous task that could not be reduced to an acceptable level of risk.

Through the FTA, two critical path events were identified.

- A failure of the CMS:
    - The failure of the CMS to maintain a safe following distance between vehicles in the platoon, between the LV of the platoon and a non-platooning vehicle and between the LV of the platoon and an object ahead, is the most critical part of the platooning system.
    - The CMS is integrated with the vehicle and interfaces directly with the EMS as well as the brake system. Inadequate integration or a failure of one of these components in the aforementioned systems represents a significant risk for a crash to occur.
    - The CMS can be tested extensively through verification and validation V&V to prove the system is integrated properly for the designed use of the system.
- Inadequate training and operation of the platooning system:
    - Failure to identify cut-ins or potential cut-ins.
    - Failure to disengage the platoon in qualifying conditions.
    - Distracted driving.
    - Driver inattentiveness.
    - Operating procedures not followed (e.g., platooning configuration, late attempt to merge, platooning outside the ODD).
    - Inadequate driver training.

The SOTIF analysis was guided by the ISO 21448 Road Vehicles – Safety of the Intended Functionality standard. One challenge associated with performing the SOTIF analysis on a representative concept platooning system, was not having a functional system specification. Details about the system's functions and relationships between specific components had to be generated based off the research team's knowledge of platooning and available resources. It is assumed that a platooning system integrator or manufacturer would have this documentation prior to beginning the SOTIF activities. This set of specifications would be the baseline for performing the SOTIF.

An attempt was made to identify known unsafe conditions in this analysis as a baseline for establishing a list of example verification tasks. A system integrator would need to further develop validation use case scenarios to test the system in a real-world environment to identify unknown unsafe scenarios. The identification of these unexpected scenarios adds to the list of known unsafe conditions. This starts the SOTIF analysis process over again where the system integrator then identifies functional modifications to reduce SOTIF risks and to create new known unsafe conditions to test in verification. This feedback loop increases the safety and reliability of the platooning system.

APPENDIX A: Definitions of Acronyms and Terms and Supporting Graphics

Terms	Definition
ACC	adaptive cruise control
ADAS	advanced driver assistance systems
ASIL	Automotive Safety Integrity Level - one of four levels to specify the items or elements necessary requirements of ISO 26262 and safety mitigations to apply for avoiding an unreasonable residual risk with D representing the most stringent and A the least stringent level
ATA	American Trucking Associations
CACC	cooperative adaptive cruise control
CMS	collision mitigation system
component	non-system level element that is logically and technically separable and is comprised of more than one hardware part or of one or more software units.
controllability	ability to avoid a specified harm or damage through the timely reactions of the peoplepeople involved, possibly with support from external mitigations
CVSA	Commercial Vehicle Safety Alliance
DDT	dynamic driving task
DSRC	dedicated short-range communications
ECU	electronic control unit
ELD	electronic logging device
element	system or part of a system including components, hardware, software, hardware parts, and software units.
EMS	engine management system
exposure	state of being in an operational situation that can be hazardous if coincident with the failure mode under analysis.
failure	termination of the ability of an element to perform a function as required
function	to work or operate in a proper or particular way
FTA	fault tree analysis
FV	following vehicle
hazard	potential source of harm caused by malfunctioning behavior of the item
hazard analysis and risk assessment	method to identify and categorize hazardous events of items and to specify safety goals and ASILs related to the prevention or mitigation of the associated hazards in order to avoid unreasonable risk
HIL	hardware-in-the-loop
HMI	human-machine interface
Initial ASIL	resulting from the hazard analysis or the ASIL resulting from a preceding ASIL decomposition

Terms	Definition
ISO	International Organization for Standardization
IEEE	Institute of Electrical and Electronics Engineers
LV	lead vehicle
MIL	model-in-the-loop
ODD	operational design domain
QM	quality management
Residual Risk	risk remaining after the deployment of safety mitigations
risk	combination of the probability of occurrence of harm and the severity of that harm
safety	absence of unreasonable risk
safety mitigation	activity of technical solution to avoid or control systematic failures and to detect or control random hardware failures, or mitigate their harmful effects
SOTIF	safety of the intended function
severity	estimate of the extent of harm to one or more people that can occur in a potentially hazardous situation
SIL	software-in-the-loop
system	set of elements that relates at least a sensor, a controller, and an actuator with one another
V&V	verification and validation

Table 12. SAE J3016 Levels of Driving Automation[9]

	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
What does the human in the driver's seat have to do?	You are driving whenever these driver support features are engaged – even if your feet are off the pedals and you are not steering.			You are not driving when these automated driving features are engaged – even if you are seated "in the driver's seat"		
	You must constantly supervise these support features; (steer, brake, or accelerate) as needed to maintain safety.			When the feature requests, you must drive.	These automated driving features will not require you to take over driving.	
	These are driver support features.			**These are automated driving features.**		
What do these features do?	These features are limited to providing warnings and momentary assistance.	These features provide steering OR brake/acceleration support to the driver.	These features provide steering AND brake/acceleration support to the driver.	These features can drive the vehicle under limited conditions and will not operate unless all required conditions are met.		This feature can drive the vehicle under all conditions.
Example features	• Automatic emergency braking • Blind spot warning • Lane departure warning	• Lane centering or adaptive cruise control	• Lane centering AND adaptive cruise control at the same time.	• Traffic jam chauffeur	• Local driverless taxi • Pedals/steering wheel may not be installed	• Same as level 4, but feature can drive everywhere in all conditions.

Source: Adapted from SAE International

[9] SAE International. (2019, January 7). SAE J3016 Levels of Driving Automation. In SAE International. Retrieved from https://www.sae.org/news/2019/01/sae-updates-j3016-automated-driving-graphic.

APPENDIX B: Hazard Analysis and Risk Assessment Summary

Table 13. Truck Platooning Hazard Analysis and Risk Assessment

Hazard ID	Hazard Description	Hazard Type	System	Potential Cause	Accident/Mishap	Initial Severity	Initial Probability of Exposure	Initial Controllability.	Initial Risk Assess.	Safety Mitigations	Mitigation Type	Final Severity.	Final Probability of Exposure	Final Controllability.	Final Risk Assess.
1	The platoon attempts a lane change without an adequate maneuvering space.	Operational Environment, Inherent Equipment Failure, Human Factors	3VL2	Stopped vehicle or debris in the roadway *On-board sensors or electronic control unit (ECU), human driver	Crash - the FVs changing lanes in a simultaneous fashion with the LV may crash into surrounding vehicle traffic.	S3	E2	C2	ASIL A	3: Forward and side-facing sensors will detect static road debris and alert the driver. 5: A visible strobe or signal indicates that the vehicles are platooning. 9: The platoon disengages if any truck receives a detection flag. 10: Drivers must be aware of passing space for FVs. 16: Train drivers on the proper use of the system. 19: Driver must be prepared to take over the system and brake. 50: Each following vehicle has an HMI that provides a live-video feed from the LV's front facing camera. 54: The driver of the LV must communicate with the driver of the FVs over a defined frequency. 64: System will take accepted reaction time limits into consideration for design of following distances. 65: Platooning system disengages during lane changes. 67: Platooning system notifies the drivers prior to the system disengaging. 69: Blind spot detection sensors notify the driver of a detected object. 71: When performing a lane change, the last FV initiates the change, allowing room for vehicles ahead of it to make the change in front of them.	3: Design 5: Design 9: Design 10: Operations 16: Training 19: Training 50: Design 54: Operations 64: Design 65: Design 67: Design 69: Design 71: Operations	S3	E2	C1	QM
2	A non-platooning vehicle performs a cut-in between two platooning vehicles.	Operational Environment, Human Factors	Both	Non-platooning vehicle does not recognize the trucks as a platoon Poor driver judgement *Other traffic	Crash - a cut-in may cause a crash between the FVs in the 3VL2 system or the FV and LV in the 2VL1 system. An unsafe emergency braking event from the vehicle being cut-off may also occur.	S3	E2	C2	ASIL A	3: Forward and side-facing sensors will detect static road debris and alert the driver. 5: A visible strobe or signal indicates that the vehicles are platooning. 11: The front-facing camera and sensors detect moving objects approaching the front and sides of the vehicle and alert the driver. 19: Driver must be prepared to take over the system and brake. 24: The Collision Mitigation System activates upon surpassing safe following distance, alerting the driver, braking and disengaging the platoon. 27: The driver of the FV can override the lateral control functionality (i.e., steering control).58: Driver training includes accident mitigation. 64: System will take accepted reaction time limits into consideration for design of following distances.	3: Design 5: Design 11: Design 19: Training 24: Design 27: Design 58: Training 64: Design	S3	E2	C1	QM

Hazard ID	Hazard Description	Hazard Type	System	Potential Cause	Accident/Mishap	Initial Severity	Initial Probability of Exposure	Initial Controllability.	Initial Risk Assess.	Safety Mitigations	Mitigation Type	Final Severity.	Final Probability of Exposure	Final Controllability.	Final Risk Assess.
3	The driver is operating the platoon outside of its ODD.	Operational Environment, Human Factors	Both	Lack of training Lack of ODD enforcement *human driver error	Unsafe operating conditions - the platoon may be forced to operate in scenarios or conditions that the platooning system was not designed or tested to handle.	S2	E2	C1	QM	16: Train drivers on the proper use of the system. 25: The driver of the FV can override the longitudinal control functionality (i.e., speed control). 51: The system automatically disengages platooning mode when any of the platooning vehicles are outside the geographic ODD. 52: The system alerts the driver when approaching an ODD roadway boundary, i.e., tunnel, border, bridge.	16: Training 25: Design 51: Design 52: Design	S2	E2	C1	QM
4	The FVs do not maintain position within the lane.	Operational Environment, Inherent Equipment Failure, Human Factors	3VL2	Camera failure Driver disengagement Weather (high wind gusts) *on-board sensors, ECU, inter-vehicle communications, failure of other platooning vehicle, weather	Crash - the FVs may crash into nearby traffic or barriers.	S3	E2	C2	ASIL A	6: The HMI provides periodic driver engagement such as an alerter button (i.e., dead man switch). 17: The driver will receive warnings from lane-keep assist system. 18: Drivers must be trained to maintain lateral control when platooning. 19: Driver must be prepared to take over the system and brake. 53: The driver of the FVs disengages platooning mode in high winds. 55: The driver monitoring system monitors the driver's attentiveness and fatigue. 56: The status of each platooning vehicle's driver must be indicated to other drivers in the platoon. 58: Driver training includes accident mitigation. 70: Platooning system disengages when lane position is not maintained.	6: Design 17: Design 18: Training 19: Training 53: Operations 55: Operations 56: Design 58: Training 70: Design	S3	E2	C1	QM
5	The LV does not maintain its position within the lane.	Human Factors	Both	Driver disengagement Poor driver judgement	Crash - the LV may crash into nearby traffic or barriers and force the FVs to also crash in a 3VL2 system.	S3	E2	C2	ASIL A	6: The HMI provides periodic driver engagement such as an alerter button (i.e., dead man switch). 17: The driver will receive warnings from lane-keep assist system. 18: Drivers must be trained to maintain lateral control when platooning. 19: Driver must be prepared to take over the system and brake. 53: The driver of the FVs disengages platooning mode in high winds. 55: The driver monitoring system monitors the driver's attentiveness and fatigue. 56: The status of each platooning vehicle's driver must be indicated to other drivers in the platoon. 65: Platooning system disengages during lane changes. 67: Platooning system notifies the drivers prior to the system disengaging. 70: Platooning system disengages when lane position is not maintained.	6: Design 17: Design 18: Training 19: Training 53: Operations 55: Operations 56: Design 65: Design 67: Design 70: Design	S3	E2	C1	QM
6	The FVs do not engage emergency braking when	Inherent Equipment	Both	Actuator failure Communication failure	Crash - the failure to emergency brake when commanded may result in crash.	S3	E1	C2	QM	19: Driver must be prepared to take over the system and brake.	19: Training 20: Design	S3	E1	C2	QM

Hazard ID	Hazard Description	Hazard Type	System	Potential Cause	Accident/Mishap	Initial Severity	Initial Probability of Exposure	Initial Controllability.	Initial Risk Assess.	Safety Mitigations	Mitigation Type	Final Severity.	Final Probability of Exposure	Final Controllability.	Final Risk Assess.
	commanded by the LV.	Failure		*failure of other platooning vehicle, vehicle communications						20: The Collision Mitigation System on FVs activates during a communication failure. 26: The communication system's redundant communication channels verify the integrity of the messages sent and received. 30: The system disengages from platooning mode upon a communication failure. 64: System will take accepted reaction time limits into consideration for design of following distances.	26: Design 30: Design 64: Design				
7	There is a data mismatch between the forward-looking sensors on the LV and the DSRC messages being sent from the LV.	Inherent Equipment Failure	Both	Inaccurate Global Positioning System (GPS) Software error *onboard sensors, ECU, inter-vehicle communications	Platooning system error - if data sources do not agree, there may be a platooning system error and may force the system to disengage on short notice to the driver.	S2	E1	C3	QM	19: Driver must be prepared to take over the system and brake. 21: Test all sensors and positioning system on all platoon-enabled vehicles prior to platooning. 22: The platoon disengages on data mismatch between information sources. 23: Test platooning vehicle's communication subsystem prior to platooning. 32: Operating procedures include a complete vehicle inspection and review of the platooning vehicle's maintenance logs prior to platooning. 64: System will take accepted reaction time limits into consideration for design of following distances.	19: Training 21: Operations 22: Design 23: Operations 32: Operations 64: Design	S2	E1	C2	QM
8	The FV does not maintain a safe following distance from the LV while platooning.	Operational Environment, Inherent Equipment Failure	Both	Hardware failure *onboard sensors, ECU, platooning vehicle, drivetrain performance Operational policy	Crash - a FV failing to stop or slow as quickly as the LV may result in the FV crashing into the rear of the LV.	S2	E1	C2	QM	3: Forward and side-facing sensors will detect static road debris and alert the driver. 9: The platoon disengages if any truck receives a detection flag. 11: The front-facing camera and sensors detect moving objects approaching the front and sides of the vehicle and alert the driver. 12: Driver must be aware of other trucks and platoons, and always ensure there is a safe following distance between other trucks. 16: Train drivers on the proper use of the system. 19: Driver must be prepared to take over the system and brake. 23: Test platooning vehicle's communication subsystem prior to platooning. 24: The Collision Mitigation System activates upon surpassing safe following distance, alerting the driver, braking and disengaging the platoon.	3: Design 9: Design 11: Design 12: Operations 16: Training 19: Training 23: Operations 24: Design	S2	E1	C1	QM

Hazard ID	Hazard Description	Hazard Type	System	Potential Cause	Accident/Mishap	Initial Severity	Initial Probability of Exposure	Initial Controllability.	Initial Risk Assess.	Safety Mitigations	Mitigation Type	Final Severity.	Final Probability of Exposure	Final Controllability.	Final Risk Assess.
9	The LV of the platoon does not maintain a safe following distance from non-platooning vehicles in front of the LV.	Operational Environment, Human Factors	Both	Lack of training Driver negligence *human driver, weather	Crash - the LV may crash into the rear of the non-platooning vehicle ahead of the LV.	S2	E1	C2	QM	3: Forward and side-facing sensors will detect static road debris and alert the driver. 9: The platoon disengages if any truck receives a detection flag. 12: Driver must be aware of other trucks and platoons, and always ensure there is a safe following distance between other trucks. 16: Train drivers on the proper use of the system. 19: Driver must be prepared to take over the system and brake. 24: The Collision Mitigation System activates upon surpassing safe following distance, alerting the driver, braking and disengaging the platoon. 60: The LV is equipped with adaptive cruise control (ACC). 64: System will take accepted reaction time limits into consideration for design of following distances.	3: Design 5: Design 9: Design 12: Operations 16: Training 19: Training 24: Design 60: Design 64: Design	S2	E1	C1	QM
10	Steering actuation of FV is inconsistent with commands sent from the LV to the FVs.	Inherent Equipment Failure	3VL2	Hardware failure Software failure *ECU, inter-vehicle communications, platooning vehicle	Crash - an actuator responding incorrectly to input data may result in the steering subsystem steering the vehicle in a direction other than intended, perhaps crashing into vehicle traffic surrounding the platoon.	S3	E1	C2	QM	19: Driver must be prepared to take over the system and brake. 26: The communication system's redundant communication channels verify the integrity of the messages sent and received. 27: The driver of the FV can override the lateral control functionality (i.e., steering control). 64: System will take accepted reaction time limits into consideration for design of following distances.	19: Training 26: Design 27: Design 64: Design	S3	E1	C1	QM
11	Acceleration actuation of the FV is inconsistent with commands sent from the LV to the FVs.	Inherent Equipment Failure	Both	Hardware failure Software failure *ECU, inter-vehicle communications, platooning vehicle	Crash - an actuator responding incorrectly to input data may result in the steering subsystem steering the vehicle in a direction other than intended, perhaps crashing into vehicle traffic surrounding the platoon.	S2	E1	C3	QM	19: Driver must be prepared to take over the system and brake. 24: The Collision Mitigation System activates upon surpassing safe following distance, alerting the driver, braking and disengaging the platoon. 25: The driver of the FV can override the longitudinal control functionality (i.e., speed control).. 26: The communication system's redundant communication channels verify the integrity of the messages sent and received. 28: The platoon disengages if the FV's acceleration is greater than the LV's acceleration (unless resuming safe distance). 64: System will take accepted reaction time limits into consideration for design of following distances.	19: Training 24: Design 25: Design 26: Design 28: Design 64: Design	S2	E1	C1	QM

Hazard ID	Hazard Description	Hazard Type	System	Potential Cause	Accident/Mishap	Initial Severity	Initial Probability of Exposure	Initial Controllability.	Initial Risk Assess.	Safety Mitigations	Mitigation Type	Final Severity.	Final Probability of Exposure	Final Controllability.	Final Risk Assess.
12	The acceleration actuation commands sent from the LV to the FVs are corrupted.	Inherent Equipment Failure	Both	Hardware failure Software failure *ECU, inter-vehicle communications, platooning vehicle	Platooning system error - if corrupted data is received the system may disengage on short notice.	S2	E2	C1	QM	19: Driver must be prepared to take over the system and brake. 25: The driver of the FV can override the longitudinal control functionality (i.e., speed control). 26: The communication system's redundant communication channels verify the integrity of the messages sent and received. 30: The system disengages from platooning mode upon a communication failure. 64: System will take accepted reaction time limits into consideration for design of following distances.	19: Training 25: Design 26: Design 30: Design 64: Design	S2	E1	C1	QM
13	The acceleration actuation commands sent from the LV to the FVs are conflicted with other data received via the FVs sensors.	Operational Environment	Both	Hardware failure Software failure *ECU, inter-vehicle communications, platooning vehicle	Platooning system error - if the LV is sending a message to the FVs to accelerate, but the sensors are indicating for the vehicle to brake, the system may disengage.	S2	E3	C2	ASIL A	2: Sensor data is received and evaluated for integrity prior to executing commands sent from the LV. 19: Driver must be prepared to take over the system and brake. 21: Test all sensors and positioning system on all platoon-enabled vehicles prior to platooning. 22: The platoon disengages on data mismatch between information sources. 32: Operating procedures include a complete vehicle inspection and review of the platooning vehicle's maintenance logs prior to platooning. System will take accepted reaction time limits into consideration for design of following distances.	2: Design 19: Training 21: Operations 22: Design 32: Operations 64: Design	S2	E3	C1	QM
14	Braking actuation of the FV is inconsistent with commands sent from the LV to the FV.	Inherent Equipment Failure	Both	Hardware failure Software failure *ECU, inter-vehicle communications, platooning vehicle	Crash - an actuator responding incorrectly to input data may result in the braking subsystem braking the vehicle excessively or without enough force required to stop the vehicle. If the vehicle does not stop in a timely fashion it may crash into the vehicle in front.	S2	E1	C2	QM	19: Driver must be prepared to take over the system and brake. 24: The Collision Mitigation System activates upon surpassing safe following distance, alerting the driver, braking and disengaging the platoon. 25: The driver of the FV can override the longitudinal control functionality (i.e., speed control).. 26: The communication system's redundant communication channels verify the integrity of the messages sent and received. 28: The platoon disengages if the FV's acceleration is greater than the LV's acceleration (unless resuming safe distance). 29: Platoon system must ensure FVs have shorter braking distance based on model, load, and performance. 64: System will take accepted reaction time limits into consideration for design of following distances.	19: Training 24: Design 25: Design 26: Design 28: Design 29: Design 64: Design	S2	E1	C1	QM

Hazard ID	Hazard Description	Hazard Type	System	Potential Cause	Accident/Mishap	Initial Severity	Initial Probability of Exposure	Initial Controllability.	Initial Risk Assess.	Safety Mitigations	Mitigation Type	Final Severity.	Final Probability of Exposure	Final Controllability.	Final Risk Assess.
15	The braking actuation commands sent from the LV to the FVs are corrupted.	Inherent Equipment Failure	Both	Hardware failure Software failure *ECU, inter-vehicle communications, platooning vehicle	Crash or platooning system error - the FVs may not stop in the required time or the system may disengage.	S2	E2	C1	QM	19: Driver must be prepared to take over the system and brake. 25: The driver of the FV can override the longitudinal control functionality (i.e., speed control). 26: The communication system's redundant communication channels verify the integrity of the messages sent and received. 30: The system disengages from platooning mode upon a communication failure. 64: System will take accepted reaction time limits into consideration for design of following distances.	19: Training 25: Design 26: Design 30: Design 64: Design	S2	E1	C1	QM
16	The braking actuation commands sent from the LV to the FVs are conflicted with other data received via the FVs sensors.	Operational Environment	Both	Hardware failure Software failure *ECU, inter-vehicle communications, platooning vehicle	Platooning system error - if the LV is sending a message to the FVs to brake, but the sensors are indicating for the vehicle not to brake, the system may disengage.	S2	E3	C2	ASIL A	2: Sensor data is received and evaluated for integrity prior to executing commands sent from the LV. 19: Driver must be prepared to take over the system and brake. 21: Test all sensors and positioning system on all platoon-enabled vehicles prior to platooning. 22: The platoon disengages on data mismatch between information sources. 32: Operating procedures include a complete vehicle inspection and review of the platooning vehicle's maintenance logs prior to platooning. 64: System will take accepted reaction time limits into consideration for design of following distances.	2: Design 19: Training 21: Operations 22: Design 32: Operations 64: Design	S2	E3	C1	QM
17	There is an unexpected stoppage in traffic.	Operational Environment	Both	Stopped vehicle *other traffic	Crash - a sudden braking event may cause the FVs to crash into the vehicle in front of it.	S3	E3	C2	ASIL B	3: Forward and side-facing sensors will detect static road debris and alert the driver. 11: The front-facing camera and sensors detect moving objects approaching the front and sides of the vehicle and alert the driver. 12: Driver must be aware of other trucks and platoons, and always ensure there is a safe following distance between other trucks. 14: The vehicle with the best braking capability takes the last following position of the platoon. 16: Train drivers on the proper use of the system. 19: Driver must be prepared to take over the system and brake. 24: The Collision Mitigation System activates upon surpassing safe following distance, alerting the driver, braking and disengaging the platoon. 27: The driver of the FV can override the lateral control functionality (i.e., steering control). 29: Platoon system must ensure FVs have shorter braking distance based on model, load, and performance.	3: Design 11: Design 12: Operations 14: Operations 16: Training 19: Training 24: Design 27: Design 29: Design 60: Design 64: Design	S3	E2	C2	ASIL A

Hazard ID	Hazard Description	Hazard Type	System	Potential Cause	Accident/Mishap	Initial Severity	Initial Probability of Exposure	Initial Controllability.	Initial Risk Assess.	Safety Mitigations	Mitigation Type	Final Severity.	Final Probability of Exposure	Final Controllability.	Final Risk Assess.
										60: The LV is equipped with ACC. 64: System will take accepted reaction time limits into consideration for design of following distances.					
18	There is unexpected road debris.	Operational Environment	Both	Debris in the roadway *environment	Operation in a dangerous condition - the vehicle may swerve or cause a sudden braking even causing a pile-up.	S3	E3	C3	ASIL C	3: Forward and side-facing sensors will detect static road debris and alert the driver. 16: Train drivers on the proper use of the system. 19: Driver must be prepared to take over the system and brake. 24: The Collision Mitigation System activates upon surpassing safe following distance, alerting the driver, braking and disengaging the platoon. 27: The driver of the FV can override the lateral control functionality (i.e., steering control). 33: Platoon system must ensure FVs have shorter braking distance based on load and performance. 64: System will take accepted reaction time limits into consideration for design of following distances. 70: Platooning system disengages when lane position is not maintained.	3: Design 16: Training 19: Training 24: Design 27: Design 33: Design 64: Design 70: Design	S2	E2	C2	ASIL B
19	The FV applies excessive acceleration.	Inherent Equipment Failure	Both	Hardware failure Software failure *onboard sensors, ECU, platooning vehicle	Operation in a dangerous condition - excessive acceleration may contribute to the probability of a crash occurring.	S2	E1	C1	QM	4: Platooning software limits the upper bound of the maximum acceleration rate. 16: Train drivers on the proper use of the system. 19: Driver must be prepared to take over the system and brake. The Collision Mitigation System activates upon surpassing safe following distance, alerting the driver, braking and disengaging the platoon. 25: The driver of the FV can override the longitudinal control functionality. 33: The driver of the LV or FV can disengage the platoon at any time. 64: System will take accepted reaction time limits into consideration for design of following distances.	4: Design 16: Training 19: Training 24: Design 25: Design 33: Design 64: Design	S2	E1	C1	QM
20	The driver of the LV becomes inattentive.	Human Factors	Both	Lack of training Driver disengagement *human driver	Crash - the LV may crash into a nearby vehicle or barrier.	S3	E1	C3	ASIL A	5: A visible strobe or signal indicates that the vehicles are platooning. 6: The HMI provides periodic driver engagement such as an alerter button (i.e., dead man switch). 7: The platoon safely disengages and alerts the driver if there is a failure to engage with the HMI. 16: Train drivers on the proper use of the system. 19: Driver must be prepared to take over the system and brake. 54: The driver of the LV must communicate with the driver of the FVs over a defined frequency.	5: Design 6: Design 7: Design 16: Training 19: Training 54: Operations 55: Design 56: Design 64: Design 66: Design	S3	E1	C2	QM

Hazard ID	Hazard Description	Hazard Type	System	Potential Cause	Accident/Mishap	Initial Severity	Initial Probability of Exposure	Initial Controllability.	Initial Risk Assess.	Safety Mitigations	Mitigation Type	Final Severity.	Final Probability of Exposure	Final Controllability.	Final Risk Assess.
										55: The driver monitoring system monitors the driver's attentiveness and fatigue. 56: The status of each platooning vehicle's driver must be indicated to other drivers in the platoon. 64: System will take accepted reaction time limits into consideration for design of following distances. 66: The communication system between drivers uses a hands-free design (i.e., brake pedal).					
21	The driver of the LV becomes incapacitated.	Human Factors	Both	Lack of training Driver disengagement *human driver	Crash - the LV may crash into a nearby vehicle or barrier.	S3	E1	C3	ASIL A	5: A visible strobe or signal indicates that the vehicles are platooning. 6: The HMI provides periodic driver engagement such as an alerter button (i.e., dead man switch). 7: The platoon safely disengages and alerts the driver if there is a failure to engage with the HMI. 16: Train drivers on the proper use of the system. 17: The driver will receive warnings from lane-keep assist system. 19: Driver must be prepared to take over the system and brake. 24: The Collision Mitigation System activates upon surpassing safe following distance, alerting the driver, braking and disengaging the platoon. 25: The driver of the FV can override the longitudinal control functionality (i.e., speed control). 27: The driver of the FV can override the lateral control functionality (i.e., steering control). 33: The driver of the LV or FV can disengage the platoon at any time. 54: The driver of the LV must communicate with the driver of the FVs over a defined frequency. 55: The driver monitoring system monitors the driver's attentiveness and fatigue. 56: The status of each platooning vehicle's driver must be indicated to other drivers in the platoon. 63: Each driver in the platoon is aware of the other driver's hours of service. 64: System will take accepted reaction time limits into consideration for design of following distances. 66: The communication system between drivers uses a hands-free design (i.e., brake pedal).	5: Design 6: Design 7: Design 16: Training 17: Design 19: Training 24: Design 25: Design 27: Design 33: Design 54: Operations 55: Design 56: Design 63: Operations 64: Design 66: Design	S3	E1	C2	QM

Hazard ID	Hazard Description	Hazard Type	System	Potential Cause	Accident/Mishap	Initial Severity	Initial Probability of Exposure	Initial Controllability.	Initial Risk Assess.	Safety Mitigations	Mitigation Type	Final Severity.	Final Probability of Exposure	Final Controllability.	Final Risk Assess.
22	The driver of the FV becomes inattentive.	Human Factors	Both	Lack of training Driver disengagement *human driver	Operation in a dangerous condition - this may contribute to a crash.	S3	E1	C3	ASIL A	5: A visible strobe or signal indicates that the vehicles are platooning. 6: The HMI provides periodic driver engagement such as an alerter button (i.e., dead man switch). 7: The platoon safely disengages and alerts the driver if there is a failure to engage with the HMI. 16: Train drivers on the proper use of the system. 19: Driver must be prepared to take over the system and brake. 54: The driver of the LV must communicate with the driver of the FVs over a defined frequency. 55: The driver monitoring system monitors the driver's attentiveness and fatigue. 56: The status of each platooning vehicle's driver must be indicated to other drivers in the platoon. 64: System will take accepted reaction time limits into consideration for design of following distances.	5: Design 6: Design 7: Design 16: Training 19: Training 54: Operations 55: Design 56: Design 64: Design	S3	E1	C2	QM
23	The driver of the FV becomes incapacitated.	Human Factors	Both	Medical conditions or impairments Hours of Service violation *human driver	Crash - in the instance that the platoon disengages, the FV driver would not be ready to take over steering responsibilities.	S3	E1	C3	ASIL A	5: A visible strobe or signal indicates that the vehicles are platooning. 6: The HMI provides periodic driver engagement such as an alerter button (i.e., dead man switch). 7: The platoon safely disengages and alerts the driver if there is a failure to engage with the HMI. 16: Train drivers on the proper use of the system. 19: Driver must be prepared to take over the system and brake. 54: The driver of the LV must communicate with the driver of the FVs over a defined frequency. 55: The driver monitoring system monitors the driver's attentiveness and fatigue. 56: The status of each platooning vehicle's driver must be indicated to other drivers in the platoon. 64: System will take accepted reaction time limits into consideration for design of following distances. 66: The communication system between drivers uses a hands-free design (i.e., brake pedal).	5: Design 6: Design 7: Design 16: Training 19: Training 54: Operations 55: Design 56: Design 64: Design 66: Design	S3	E1	C2	QM
24	There is a load difference between the LV (full) and FV (empty).	Operational Environment, Inherent Equipment Failure	2VL1	Hardware failure Software failure *platooning vehicle, ECU	Operation in a dangerous condition - the differences may lead to a crash caused by a braking event.	S2	E1	C1	QM	13: The vehicles are loaded according to operational policies and constraints. 14: The vehicle with the best braking capability takes the last following position of the platoon. 15: Each vehicle's load is independently verified (twice) prior to operating in platooning mode. 28: The platoon disengages if the FV's	13: Operations 14: Operations 15: Operations 28: Design 29: Design	S2	E1	C1	QM

Hazard ID	Hazard Description	Hazard Type	System	Potential Cause	Accident/Mishap	Initial Severity	Initial Probability of Exposure	Initial Controllability.	Initial Risk Assess.	Safety Mitigations	Mitigation Type	Final Severity.	Final Probability of Exposure	Final Controllability.	Final Risk Assess.
										acceleration is greater than the LV's acceleration (unless resuming safe distance). 29: Platooning system must ensure FVs have shorter braking distance based on model, load, and performance.					
25	There is a load difference between the LV (empty) and FV (full).	Operational Environment, Inherent Equipment Failure	2VL1	Hardware failure Software failure *platooning vehicle, ECU	Operation in a dangerous condition - the differences may lead to a crash caused by a braking event.	S2	E1	C1	QM	13: The vehicles are loaded according to operational policies and constraints. 14: The vehicle with the best braking capability takes the last following position of the platoon. 15: Each vehicle's load is independently verified (twice) prior to operating in platooning mode. 28: The platoon disengages if the FV's acceleration is greater than the LV's acceleration (unless resuming safe distance). 29: Platooning system must ensure FVs have shorter braking distance based on model, load, and performance.	13: Operations 14: Operations 15: Operations 28: Design 29: Design	S2	E1	C1	QM
26	There is a load difference between the LV (full), the FV #1 (empty), and the FV #2 (empty).	Operational Environment, Inherent Equipment Failure	3VL2	Hardware failure Software failure *platooning vehicle, ECU	Operation in a dangerous condition - the differences may lead to a crash caused by a braking event.	S2	E1	C1	QM	13: The vehicles are loaded according to operational policies and constraints. 14: The vehicle with the best braking capability takes the last following position of the platoon. 15: Each vehicle's load is independently verified (twice) prior to operating in platooning mode. 28: The platoon disengages if the FV's acceleration is greater than the LV's acceleration (unless resuming safe distance). 29: Platooning system must ensure FVs have shorter braking distance based on model, load, and performance.	13: Operations 14: Operations 15: Operations 28: Design 29: Design	S2	E1	C1	QM
27	There is a difference in brake performance between the LV and FVs due to the vehicles having different maintenance cycles.	Operational Environment	Both	Degraded hardware *platooning vehicle, human error (maintenance)	Crash - lack of brake performance monitoring and maintenance creates a risk for a crash.	S2	E1	C2	QM	19: Driver must be prepared to take over the system and brake. 31: Total Productive Maintenance ensures that platooning vehicles are for safe operation. 32: Operating procedures include a complete vehicle inspection and review of the platooning vehicle's maintenance logs prior to platooning. 64: System will take accepted reaction time limits into consideration for design of following distances.	19: Training 31: Maintenance 32: Operations 64: Design	S2	E1	C1	QM
28	There is a difference in tire wear (i.e., traction, tread depth, grip, etc.) between the LV and FVs.	Operational Environment	Both	Degraded hardware *platooning vehicle, human error (maintenance)	Operation in a dangerous condition - the differences may lead to a crash caused by a braking event.	S2	E3	C3	ASIL B	14: The vehicle with the best braking capability takes the last following position of the platoon. 19: Driver must be prepared to take over the system and brake. 31: Total Productive Maintenance ensures that platooning vehicles are for safe operation. 32: Operating procedures include a	14: Design 19: Training 31: Maintenance 32: Operations 64: Design	S2	E3	C2	ASIL A

Hazard ID	Hazard Description	Hazard Type	System	Potential Cause	Accident/Mishap	Initial Severity	Initial Probability of Exposure	Initial Controllability.	Initial Risk Assess.	Safety Mitigations	Mitigation Type	Final Severity.	Final Probability of Exposure	Final Controllability.	Final Risk Assess.
									🟧	complete vehicle inspection and review of the platooning vehicle's maintenance logs prior to platooning. 64: System will take accepted reaction time limits into consideration for design of following distances.					🟨
29	There is a loss of braking in the LV.	Inherent Equipment Failure	Both	Hardware failure Software failure *platooning vehicle (braking subsystem), human error (maintenance)	Crash - the vehicle may crash into nearby traffic or a barrier.	S3	E1	C2	QM	19: Driver must be prepared to take over the system and brake. 31: Total Productive Maintenance ensures that platooning vehicles are for safe operation. 32: Operating procedures include a complete vehicle inspection and review of the platooning vehicle's maintenance logs prior to platooning. 54: The driver of the LV must communicate with the driver of the FVs over a defined frequency. 58: Driver training includes accident mitigation. 64: System will take accepted reaction time limits into consideration for design of following distances. 66: The communication system between drivers uses a hands-free design (i.e., brake pedal).	19: Training 31: Maintenance 32: Operations 54: Operations 58: Training 64: Design 66: Design	S3	E1	C1	QM
30	There is a loss of braking in the FV.	Inherent Equipment Failure Operational	Both	Hardware failure Software failure *platooning vehicle (braking subsystem), human error (maintenance)	Crash - the vehicle may crash into nearby traffic or a barrier.	S3	E1	C2	QM	19: Driver must be prepared to take over the system and brake. 31: Total Productive Maintenance ensures that platooning vehicles are for safe operation. 32: Operating procedures include a complete vehicle inspection and review of the platooning vehicle's maintenance logs prior to platooning. 58: Driver training includes accident mitigation. 64: System will take accepted reaction time limits into consideration for design of following distances.	19: Training 31: Maintenance 32: Operations 58: Training 64: Design	S3	E1	C1	QM
31	There is a loss of steering in the LV (steering subsystem failure).	Inherent Equipment Failure Operational	Both	Hardware failure Software failure *platooning vehicle (steering subsystem), human error (maintenance)	Crash - the vehicle may crash into nearby traffic or a barrier.	S3	E1	C2	QM	19: Driver must be prepared to take over the system and brake. 31: Total Productive Maintenance ensures that platooning vehicles are for safe operation. 32: Operating procedures include a complete vehicle inspection and review of the platooning vehicle's maintenance logs prior to platooning. 54: The driver of the LV must communicate with the driver of the FVs over a defined frequency. 58: Driver training includes accident mitigation. 64: System will take accepted reaction time limits into consideration for	19: Training 31: Maintenance 32: Operations 54: Operations 58: Training 64: Design 66: Design 70: Design	S3	E1	C1	QM

Hazard ID	Hazard Description	Hazard Type	System	Potential Cause	Accident/Mishap	Initial Severity	Initial Probability of Exposure	Initial Controllability.	Initial Risk Assess.	Safety Mitigations	Mitigation Type	Final Severity.	Final Probability of Exposure	Final Controllability.	Final Risk Assess.
										design of following distances. 66: The communication system between drivers uses a hands-free design (i.e., brake pedal). 70: Platooning system disengages when lane position is not maintained.					
32	There is a loss of steering in the FV (steering subsystem failure).	Inherent Equipment Failure Operational	Both	Hardware failure Software failure *platooning vehicle (steering subsystem), human error (maintenance)	Crash - the vehicle may crash into nearby traffic or a barrier.	S3	E1	C2	QM	19: Driver must be prepared to take over the system and brake. 31: Total Productive Maintenance ensures that platooning vehicles are for safe operation. 32: Operating procedures include a complete vehicle inspection and review of the platooning vehicle's maintenance logs prior to platooning. 58: Driver training includes accident mitigation. 64: System will take accepted reaction time limits into consideration for design of following distances. 66: The communication system between drivers uses a hands-free design (i.e., brake pedal). 70: Platooning system disengages when lane position is not maintained.	19: Training 31: Maintenance 32: Operations 58: Training 64: Design 66: Design 70: Design	S3	E1	C1	QM
33	There is a loss in steering control in the LV.	Inherent Equipment Failure Operational	Both	Hardware failure Software failure Human error *platooning vehicle, human driver	Crash - the vehicle may crash into nearby traffic or a barrier.	S3	E1	C3	ASIL A	19: Driver must be prepared to take over the system and brake. 31: Total Productive Maintenance ensures that platooning vehicles are for safe operation. 32: Operating procedures include a complete vehicle inspection and review of the platooning vehicle's maintenance logs prior to platooning. 54: The driver of the LV must communicate with the driver of the FVs over a defined frequency. 56: The status of each platooning vehicle's driver must be indicated to other drivers in the platoon. 58: Driver training includes accident mitigation. 64: System will take accepted reaction time limits into consideration for design of following distances. 66: The communication system between drivers uses a hands-free design (i.e., brake pedal).	19: Training 31: Maintenance 32: Operations 54: Operations 56: Design 58: Training 64: Design 66: Design	S3	E1	C3	ASIL A
34	There is a loss in steering control in the FV.	Inherent Equipment Failure Operational	Both	Hardware failure Software failure Human error *platooning vehicle, human driver	Crash - the vehicle may crash into nearby traffic or a barrier.	S3	E1	C3	ASIL A	19: Driver must be prepared to take over the system and brake. 31: Total Productive Maintenance ensures that platooning vehicles are for safe operation. 32: Operating procedures include a complete vehicle inspection and review	19: Training 31: Maintenance 32: Operations 56: Design 58: Training 64: Design 66: Design	S3	E1	C3	ASIL A

Hazard ID	Hazard Description	Hazard Type	System	Potential Cause	Accident/Mishap	Initial Severity	Initial Probability of Exposure	Initial Controllability.	Initial Risk Assess.	Safety Mitigations	Mitigation Type	Final Severity.	Final Probability of Exposure	Final Controllability.	Final Risk Assess.
										of the platooning vehicle's maintenance logs prior to platooning. 56: The status of each platooning vehicle's driver must be indicated to other drivers in the platoon. 58: Driver training includes accident mitigation. 64: System will take accepted reaction time limits into consideration for design of following distances. 66: The communication system between drivers uses a hands-free design (i.e., brake pedal).					
35	There is a loss in inter-vehicle communication while platooning.	Inherent Equipment Failure	Both	Hardware failure Software failure *inter-vehicle communications, ECU	Platooning system error - the system may disengage.	S2	E2	C3	ASIL A	19: Driver must be prepared to take over the system and brake. 25: The driver of the FV can override the longitudinal control functionality. 30: The system disengages from platooning mode upon a communication failure 54: The driver of the LV must communicate with the driver of the FVs over a defined frequency. 58: Driver training includes accident mitigation. 64: System will take accepted reaction time limits into consideration for design of following distances. 66: The communication system between drivers uses a hands-free design (i.e., brake pedal).	19: Training 25: Design 30: Design 54: Operations 58: Training 64: Design 66: Design	S2	E2	C2	QM
36	A lower priority inter-vehicle communication message is acted upon before the higher priority message.	Inherent Equipment Failure	Both	Hardware failure Software failure *inter-vehicle communications, ECU	Platooning system error - depending on the nature of the messages, this error may result in a crash.	S2	E1	C1	QM	34: All inter-vehicle communication messages are assigned a priority for every combination of messages received. 35: The system software always acts upon the highest priority message received.	34: Design 35: Design	S2	E1	C1	QM
37	There is unexpected low road surface friction while platooning.	Operational Environment	Both	Weather (rain, ice, sleet, puddles) Environment (loose material on pavement) *human driver, platooning vehicle	Operation in a dangerous condition - insufficient friction may contribute to the likelihood of a crash.	S3	E2	C1	QM	19: Driver must be prepared to take over the system and brake. 36: The system software receives weather updates based on its geographical position. 37: The system sensors detect precipitation/icy conditions and notify the driver of changing weather conditions. 38: The driver disengages platooning mode when low road surface friction conditions are registered by the Electronic Stability Control (ESC) system. 57: The vehicle's Electronic Stability Control (ESC) system registers a slippery road condition and notifies the driver. 64: System will take accepted reaction time limits into consideration for design of following distances.	19: Training 36: Design 37: Design 38: Training 57: Design 64: Design	S3	E2	C1	QM

Hazard ID	Hazard Description	Hazard Type	System	Potential Cause	Accident/Mishap	Initial Severity	Initial Probability of Exposure	Initial Controllability.	Initial Risk Assess.	Safety Mitigations	Mitigation Type	Final Severity.	Final Probability of Exposure	Final Controllability.	Final Risk Assess.
38	There are unexpected low visibility conditions while platooning.	Operational Environment, Inherent Equipment Failure	Both	Weather (fog, rain, sleet) *onboard sensor failure, human driver	Operation in a dangerous condition - poor operating conditions may contribute to the likelihood of a crash.	S3	E2	C1	QM	19: Driver must be prepared to take over the system and brake. 32: Operating procedures include a complete vehicle inspection and review of the platooning vehicle's maintenance logs prior to platooning. 39: Driver training includes how to identify low visibility conditions. 40: The driver does not operate in platooning mode during low visibility conditions. 64: System will take accepted reaction time limits into consideration for design of following distances. 69: Blind spot detection sensors notify the driver of a detected object. 70: Platooning system disengages when lane position is not maintained.	19: Training 32: Operations 39: Training 40: Operations 64: Design 69: Design 70: Design	S3	E2	C1	QM
39	The vehicles are platooning in an unexpected work zone.	Operational Environment	Both	Unexpected roadway conditions *roadway features	Operation in a dangerous condition - drivers of the platooning vehicles may not be trained on how to operate in a work zone.	S3	E2	C2	ASIL A	16: Train drivers on the proper use of the system. 19: Driver must be prepared to take over the system and brake. 41: Drivers disengage platooning mode upon encountering a work zone. 50: Each FV has an HMI that provides a live-video feed from the LV's front facing camera. 54: The driver of the LV must communicate with the driver of the FVs over a defined frequency. 55: The driver monitoring system monitors the driver's attentiveness and fatigue. 64: System will take accepted reaction time limits into consideration for design of following distances. 66: The communication system between drivers uses a hands-free design (i.e., brake pedal). 70: Platooning system disengages when lane position is not maintained.	16: Training 19: Training 41: Training 50: Design 54: Operations 55: Design 64: Design 66: Design 70: Design	S3	E2	C1	QM
40	The FVs cannot identify lane markings, while platooning. Note: The lane markings are degraded.	Operational Environment	3VL2	Poor infrastructure *roadway features	Crash - the FVs may not be able to lane keep and could crash into nearby traffic or barriers.	S3	E3	C1	ASIL A	19: Driver must be prepared to take over the system and brake. 42: Driver disengages platooning mode if they cannot visually identify lane markings. 44: Drivers report areas of degraded lane markings to the system. 64: System will take accepted reaction time limits into consideration for design of following distances. 65: Platooning system disengages during lane changes. 70: Platooning system disengages when lane position is not maintained.	19: Training 42: Training 44: Operations 64: Design 65: Design 70: Design	S3	E3	C1	QM
41	There is a cyber-attack on the FV's communication subsystem.	Operational Environment	Both	Malicious attack *inter-vehicle communications, design failure	Crash - the system could be operated by the attacker and may purposely cause a crash.	S3	E2	C3	ASIL B	19: Driver must be prepared to take over the system and brake. 43: The system software is designed with high security credentials to prohibit	19: Training 43: Design 58: Training	S3	E2	C2	ASIL A

Hazard ID	Hazard Description	Hazard Type	System	Potential Cause	Accident/Mishap	Initial Severity	Initial Probability of Exposure	Initial Controllability.	Initial Risk Assess.	Safety Mitigations	Mitigation Type	Final Severity.	Final Probability of Exposure	Final Controllability.	Final Risk Assess.
									🟧	cyber-attacks. 58: Driver training includes accident mitigation.					🟨
42	A platooning vehicle (LV or FV) loses its positional awareness while platooning.	Operational Environment, Inherent Equipment Failure	Both	Hardware failure Software failure *ECU (positioning input)	Platooning system error - if the system does not have a positional input for operating the system (i.e., GPS, digital map, etc.) the system could operate outside of its ODD.	S1	E2	C2	QM	19: Driver must be prepared to take over the system and brake. 26: The communication system's redundant communication channels verify the integrity of the messages sent and received. 33: The driver of the LV or FV can disengage the platoon at any time. 45: The system safely disengages platooning mode and notifies the driver if the vehicle loses its positional awareness. 64: System will take accepted reaction time limits into consideration for design of following distances. 70: Platooning system disengages when lane position is not maintained.	19: Training 26: Design 33: Design 45: Design 64: Design 70: Design	S1	E2	C1	QM
43	The LV does not maintain a safe distance from the infrastructure. Note: i.e., median barriers, cones, guard rails, etc.	Operational Environment, Inherent Equipment Failure	Both	Hardware failure *onboard sensors, ECU, platooning vehicle Driver disengagement *human driver	Crash - the LV itself may crash into a barrier or other traffic or may cause the FVs of the 3VL2 system to crash into a barrier or other traffic as well.	S3	E3	C2	ASIL A	3: Forward and side-facing sensors will detect static road debris and alert the driver. 11: The front-facing camera and sensors detect moving objects approaching the front and sides of the vehicle and alert the driver. 16: Train drivers on the proper use of the system. 24: The Collision Mitigation System activates upon surpassing safe following distance, alerting the driver, braking and disengaging the platoon. 33: The driver of the LV or FV can disengage the platoon at any time. 46: The system maintains a safe following distance from the infrastructure. 55: The driver monitoring system monitors the driver's attentiveness and fatigue. 56: The status of each platooning vehicle's driver must be indicated to other drivers in the platoon. 60: The LV is equipped with ACC. 64: System will take accepted reaction time limits into consideration for design of following distances. 70: Platooning system disengages when lane position is not maintained.	3: Design 11: Design 16: Training 24: Design 33: Design 46: Design 55: Design 56: Design 60: Design 64: Design 70: Design	S3	E3	C1	QM
44	The LV experiences a tire blowout.	Operational Environment	Both	Hardware failure *platooning vehicle	Crash - unexpected sudden deceleration may cause the FV to crash into the rear of the LV.	S1	E1	C3	QM	1: The platooning vehicles are outfitted with run-flat tires. 31: Total Productive Maintenance ensures that platooning vehicles are for safe operation. 32: Operating procedures include a complete vehicle inspection and review of the platooning vehicle's maintenance	1: Design 31: Maintenance 32: Operations 58: Training 61: Design 62: Design 64: Design	S1	E1	C2	QM

Hazard ID	Hazard Description	Hazard Type	System	Potential Cause	Accident/Mishap	Initial Severity	Initial Probability of Exposure	Initial Controllability.	Initial Risk Assess.	Safety Mitigations	Mitigation Type	Final Severity.	Final Probability of Exposure	Final Controllability.	Final Risk Assess.
										logs prior to platooning. 58: Driver training includes accident mitigation. 61: The FV can monitor the condition of the tires in the LV. 62: The platooning system will disengage upon the detection of a tire blowout. 64: System will take accepted reaction time limits into consideration for design of following distances.					
45	FV number two experiences a flat tire while platooning.	Operational Environment	3VL2	Hardware failure *platooning vehicle	Crash - the vehicle may crash into the FV in front or vehicle traffic surrounding the platoon.	S1	E1	C3	QM	1: The platooning vehicles are outfitted with run-flat tires. 31: Total Productive Maintenance ensures that platooning vehicles are for safe operation. 32: Operating procedures include a complete vehicle inspection and review of the platooning vehicle's maintenance logs prior to platooning. 58: Driver training includes accident mitigation. 64: System will take accepted reaction time limits into consideration for design of following distances.	1: Design 31: Maintenance 32: Operations 58: Training 64: Design	S1	E1	C2	QM
46	An animal (e.g., deer) runs out in front of the LV of the platoon.	Operational Environment	Both	Environment *animal	Crash - the vehicle may crash into the animal causing unexpected deceleration, which may cause the FV to crash into the rear of the LV.	S1	E1	C3	QM	11: The front-facing camera and sensors detect moving objects approaching the front and sides of the vehicle and alert the driver. 14: The vehicle with the best braking capability takes the last following position of the platoon. 18: Drivers must be trained to maintain lateral control when platooning. 19: Driver must be prepared to take over the system and brake. 50: Each FV has an HMI that provides a live-video feed from the LV's front facing camera. 58: Driver training includes accident mitigation. 64: System will take accepted reaction time limits into consideration for design of following distances.	11: Design 14: Operations 18: Training 19: Training 50: Design 58: Training 64: Design	S1	E1	C1	QM
47	An unavoidable flying object from a non-platooning vehicle in front of the LV is projected at the LV.	Inherent Equipment Failure	Both	Environment *platooning vehicle	Crash - the object may crash into the LV causing unexpected deceleration, which may cause the FV to crash into the rear of the LV.	S1	E1	C2	QM	11: The front-facing camera and sensors detect moving objects approaching the front and sides of the vehicle and alert the driver. 18: Drivers must be trained to maintain lateral control when platooning. 19: Driver must be prepared to take over the system and brake. 50: Each FV has an HMI that provides a live-video feed from the LV's front facing camera. 58: Driver training includes accident mitigation. 64: System will take accepted reaction time limits into consideration for	11: Design 18: Training 19: Training 50: Design 58: Training 64: Design	S1	E1	C2	QM

Hazard ID	Hazard Description	Hazard Type	System	Potential Cause	Accident/Mishap	Initial Severity	Initial Probability of Exposure	Initial Controllability.	Initial Risk Assess.	Safety Mitigations	Mitigation Type	Final Severity.	Final Probability of Exposure	Final Controllability.	Final Risk Assess.
										design of following distances.					
48	An unavoidable flying object from the LV is projected at the FV.	Inherent Equipment Failure	3VL2	Environment *platooning vehicle	Crash - the object may crash into the LV causing unexpected deceleration, which may cause the second FV to crash into the rear of the first FV.	S1	E1	C2	QM	11: The front-facing camera and sensors detect moving objects approaching the front and sides of the vehicle and alert the driver. 18: Drivers must be trained to maintain lateral control when platooning. 19: Driver must be prepared to take over the system and brake. 50: Each FV has an HMI that provides a live-video feed from the LV's front facing camera. 58: Driver training includes accident mitigation. 64: System will take accepted reaction time limits into consideration for design of following distances.	11: Design 18: Training 19: Training 50: Design 58: Training 64: Design	S1	E1	C2	QM
49	The driver of the FVs is exposed to exhaust fumes from the platooning vehicle in front of the FV over a long duration of time.	Operational Environment	Both	Environment *platooning vehicle	Crash - the driver may become incapacitated.	S1	E3	C3	ASIL A	8: The FVs monitor exhaust fume inhalation. 16: Train drivers on the proper use of the system. 47: A safe following distance regarding driver inhalation of exhaust fumes is determined. 59: The system alerts the driver of the FV when the exhaust fume inhalation threshold has been met.	8: Design 16: Training 47: Design 59: Design	S1	E3	C2	QM
50	The platoon is operating on a freeway with high grade.	Operational Environment	Both	Environment *platooning vehicle	Crash - the platoon vehicles may be unable to travel up a hill and may crash into the vehicles behind it.	S1	E2	C1	QM	16: Train drivers on the proper use of the system. 33: The driver of the LV or FV can disengage the platoon at any time. 48: The system alerts the driver when platooning on grade that is not within the grade boundaries defined by the ODD.	16: Training 33: Design 48: Design	S1	E2	C1	QM
51	The platoon is operating on a freeway with a steep downgrade.	Operational Environment	Both	Environment *platooning vehicle	Crash - the platoon vehicles may be unable to stop and may crash into the vehicles in front.	S1	E2	C1	QM	16: Train drivers on the proper use of the system. 19: Driver must be prepared to take over the system and brake. 33: The driver of the LV or FV can disengage the platoon at any time. 48: The system alerts the driver when platooning on grade that is not within the grade boundaries defined by the ODD. 64: System will take accepted reaction time limits into consideration for design of following distances.	16: Training 19: Training 33: Design 48: Design 64: Design	S1	E2	C1	QM

Hazard ID	Hazard Description	Hazard Type	System	Potential Cause	Accident/Mishap	Initial Severity	Initial Probability of Exposure	Initial Controllability.	Initial Risk Assess.	Safety Mitigations	Mitigation Type	Final Severity.	Final Probability of Exposure	Final Controllability.	Final Risk Assess.
52	The platoon is operating on a freeway with sharp curves.	Operational Environment	Both	Environment *platooning vehicle	Crash - the platoon vehicles may roll over.	S1	E2	C1	QM	16: Train drivers on the proper use of the system. 19: Driver must be prepared to take over the system and brake. 33: The driver of the LV or FV can disengage the platoon at any time. 49: The system alerts the driver when platooning around a sharp curve that is not within the curvature boundaries defined by the ODD. 64: System will take accepted reaction time limits into consideration for design of following distances. 69: Blind spot detection sensors notify the driver of a detected object.	16: Training 19: Training 33: Design 49: Design 64: Design 69: Design	S1	E2	C1	QM
53	A motorcycle performs a cut-in between two platooning vehicles.	Operational Environment	Both	Non-platooning vehicle does not recognize the trucks as a platoon Poor driver judgement *Other traffic	Crash - a cut-in may cause a crash between the FVs in the 3VL2 system or the FV and LV in the 2VL1 system. An unsafe emergency braking event from the vehicle being cut-off may also occur.	S3	E2	C3	ASIL B	5: A visible strobe or signal indicates that the vehicles are platooning. 11: The front-facing camera and sensors detect moving objects approaching the front and sides of the vehicle and alert the driver. 14: The vehicle with the best braking capability takes the last following position of the platoon. 16: Train drivers on the proper use of the system. 19: Driver must be prepared to take over the system and brake. 24: The Collision Mitigation System activates upon surpassing safe following distance, alerting the driver, braking and disengaging the platoon. 33: The driver of the LV or FV can disengage the platoon at any time. 64: System will take accepted reaction time limits into consideration for design of following distances.	5: Design 11: Design 14: Operations 16: Training 19: Training 24: Design 33: Design 64: Design	S3	E2	C2	ASIL A
54	The driver of the FV has reduced situational awareness due to shortened or blocked forward field of view from the vehicle in front (LV or FV).	Human Factors	Both	Lack of training *human driver	Crash - the driver of the FV in the 2VL1 system may change lanes when the current conditions are unsafe. In the 3VL2 system, the driver of the FV may fully depend on the LV and its maneuvers for safe operation and may not be ready to take over in an emergency situation.	S2	E3	C2	ASIL B	14: The vehicle with the best braking capability takes the last following position of the platoon. 16: Train drivers on the proper use of the system. 19: Driver must be prepared to take over the system and brake. 33: The driver of the LV or FV can disengage the platoon at any time. 50: Each FV has an HMI that provides a live-video feed from the LV's front facing camera. 64: System will take accepted reaction time limits into consideration for design of following distances. 69: Blind spot detection sensors notify the driver of a detected object.	14: Operations 16: Training 19: Training 33: Design 50: Design 64: Design 69: Design	S2	E3	C1	QM
55	The driver of the FV engages in risky driving behavior in order to maintain the platoon.	Human Factors	Both	Lack of training *human driver Poor driver judgement *human driver	Crash - the driver may crash into nearby traffic performing unsafe maneuvers.	S3	E2	C3	ASIL B	16: Train drivers on the proper use of the system. 50: Each FV has an HMI that provides a live-video feed from the LV's front facing camera.	16: Training 50: Design 55: Design 56: Design 67: Design	S3	E2	C3	QM

Hazard ID	Hazard Description	Hazard Type	System	Potential Cause	Accident/Mishap	Initial Severity	Initial Probability of Exposure	Initial Controllability.	Initial Risk Assess.	Safety Mitigations	Mitigation Type	Final Severity.	Final Probability of Exposure	Final Controllability.	Final Risk Assess.
										55: The driver monitoring system monitors the driver's attentiveness and fatigue. 56: The status of each platooning vehicle's driver must be indicated to other drivers in the platoon. 67: Platooning system notifies the drivers prior to the system disengaging. 68: Platooning system will disengage upon an evasive steering maneuver (i.e., lateral acceleration limit). 70: Platooning system disengages when lane position is not maintained.	68: Design 70: Design				
56	Drivers are operating past the hours of service limitation.	Human Factors	Both	Lack of training *human driver	Crash - the driver may become drowsy or inattentive. The driver's performance may be negatively impacted.	S3	E1	C1	QM	6: The HMI provides periodic driver engagement such as an alerter button (i.e., dead man switch). 7: The platoon safely disengages and alerts the driver if there is a failure to engage with the HMI. 19: Driver must be prepared to take over the system and brake. 33: The driver of the LV or FV can disengage the platoon at any time. 54: The driver of the LV must communicate with the driver of the FVs over a defined frequency. 55: The driver monitoring system monitors the driver's attentiveness and fatigue. 56: The status of each platooning vehicle's driver must be indicated to other drivers in the platoon. 63: Each driver in the platoon is aware of the other driver's hours of service. 64: System will take accepted reaction time limits into consideration for design of following distances. 66: The communication system between drivers uses a hands-free design (i.e., brake pedal).	6: Design 7: Design 19: Training 33: Design 54: Operations 55: Design 56: Design 63: Operations 64: Design 66: Design	S3	E1	C1	QM
57	The driver of the LV performs an evasive maneuver.	Operational Environment	3VL2	Lack of training *human driver Poor driver judgement *human driver	Crash - the driver may crash into nearby traffic or infrastructure barriers, while performing unsafe maneuvers.	S3	E2	C3	ASIL B	9: The platoon disengages if any truck receives a detection flag. 12: Driver must be aware of other trucks and platoons, and always ensure there is a safe following distance between other trucks. 14: The vehicle with the best braking capability takes the last following position of the platoon. 16: Train drivers on the proper use of the system. 18: Drivers must be trained to maintain lateral control when platooning. 33: The driver of the LV or FV can disengage the platoon at any time. 46: The system maintains a safe distance from the infrastructure. 49: The system alerts the driver when platooning around a sharp curve that is	9: Design 12: Operations 14: Operations 16: Training 18: Training 33: Design 46: Design 49: Design 52: Design 60: Design 67: Design 68: Design 70: Design	S2	E1	C2	QM

Hazard ID	Hazard Description	Hazard Type	System	Potential Cause	Accident/Mishap	Initial Severity	Initial Probability of Exposure	Initial Controllability.	Initial Risk Assess.	Safety Mitigations	Mitigation Type	Final Severity.	Final Probability of Exposure	Final Controllability.	Final Risk Assess.
									🟧	not within the curvature boundaries defined by the ODD. 52: The system alerts the driver when approaching an ODD roadway boundary, i.e., tunnel, border, bridge. 60: The LV is equipped with ACC. 67: Platooning system notifies the drivers prior to the system disengaging. 68: Platooning system will disengage upon an evasive steering maneuver (i.e., lateral acceleration limit). 70: Platooning system disengages when lane position is not maintained.					🟩

APPENDIX C: Safety of the Intended Function Analysis

Table 14. Functional and System Specification of the ISO 21448 Standard

Sub function #	Goal of Intended Platooning Sub function	Use Cases of Intended Functionality	Description of Intended Functionality	Functional Dependencies and Interaction	Components Required and Their Function	Limitations	Assumptions About How the Intended Functionality Makes Use of Inputs From Other Elements	Assumptions About How Other Elements Make Use of Outputs From the Intended Functionality Makes Use of Outputs	System
1.1	Facilitate the sharing of information between vehicles to enable platooning through inter-vehicle communications (Vehicle-to-Vehicle (V2V)). V2V is restricted only to vehicles within the platoon.	**Activated:** Inter-vehicle communication is activated once the vehicles are powered on. **Deactivated:** Inter-vehicle communication is deactivated after the platoon has been powered off. **Active:** N/A, state is activated or deactivated.	CACC is achieved with two vehicles in frequent communication with one another. Vehicle telemetry such as information from the Controller Area Network (CAN) bus is communicated with other vehicles in the platoon. This telemetry is combined with onboard sensor inputs (radar, etc.) to maintain relative distance and speed to the next vehicle in the platoon.	**Dependencies:** -Adequate bandwidth of communication medium -Noise on communication channel, noise compensation on communication channel -High-speed processor in other platoon vehicles to decode and process safety-related messages in a timely manner -Reliable CAN bus to provide inputs required for inter-vehicle communication messages -Other platoon vehicles being within transmission and reception range of the inter-vehicle messages -Security of messages within platooning vehicles, authentication -Reliability of equipment (e.g. processor and inter-vehicle communication devices) of other platooning vehicles **Interactions:** -Other platoon vehicle's inter-vehicle communication devices	● Inter-vehicle communication devices - transmit and receive messages between platooning vehicles ● EMS ECU - processes inter-vehicle communication messages ● EMS ECU Software - generates and decodes the inter-vehicle communication messages ● HMI - present platooning status information, vehicle status and driver status.	● Inter-vehicle communication devices -hardware specifications (e.g., orientation, range, reliability) -geographical locations and environmental surroundings ● EMS ECU -hardware specifications (e.g., processing power) ● HMI - none	Inputs to EMS ECU and software: ● Inter-vehicle communication messages (e.g., vehicle telemetry)	Outputs from EMS ECU and software: ● All other functions require this function for any platooning activities to occur. Communication between vehicles is the minimum functionality required for CACC.	Both
1.2	Facilitate the sharing of information between drivers for platooning operations. This communication is restricted only to vehicles within the platoon.	**Activated:** Inter-vehicle communication is activated when the vehicles are powered on. **Deactivated:** Inter-vehicle communication is deactivated after the platoon has been	Driver-to-driver audio communication within the platoon enables drivers to discuss upcoming platoon maneuvers. Drivers may also communicate information such as an upcoming change in traffic or road hazards.	**Dependencies:** -Drivers using this system feature for communication -Adequate bandwidth of communication medium -Other platoon vehicles being within transmission and reception range of the inter-vehicle messages	● Inter-vehicle communication devices - transmit and receive messages between platooning vehicles ● Foot pedal (activates voice communication between drivers of platooning vehicles) ● EMS ECU - processes inter-vehicle communication	● Inter-vehicle communication devices -hardware specifications (e.g., orientation, range, reliability) -geographical locations and environmental surroundings	Inputs to EMS ECU and software: ● None	Outputs from EMS ECU and software: This function supports platooning operations and protocol, but does not impact the technical capability of the platoons to form, maintain or dissolve the platoon. Operators will have a	Both

Sub function #	Goal of Intended Platooning Sub function	Use Cases of Intended Functionality	Description of Intended Functionality	Functional Dependencies and Interaction	Components Required and Their Function	Limitations	Assumptions About How the Intended Functionality Makes Use of Inputs From Other Elements	Assumptions About How Other Elements Make Use of Outputs From the Intended Functionality Makes Use of Outputs	System
		powered off. **Active:** N/A, state is activated or deactivated.		-Reliability of equipment (e.g., processor and inter-vehicle communication devices) of other platooning vehicles **Interactions:** -Other platoon vehicle's inter-vehicle communication devices -Drivers operating the platooning vehicles	messages ● EMS ECU Software - generates and decodes the inter-vehicle communication messages ● HMI - present platooning status information and driver alerts	● EMS ECU -hardware specifications (e.g., processing power) ● EMS ECU Software - none ● HMI - none		required Commercial Driver's License endorsement. Lane changes are typically indicated from the FV to the LV via turn signal.	
1.3	Maintain a safe following distance from non-platooning vehicles	**CMS Activated:** This function is activated once the vehicle is powered on. **Deactivated:** This function is deactivated once the vehicle is powered off. **Active:** This function is always active once the vehicle is powered on. This feature does not require the driver to turn the CMS ON. This function can be active regardless of the mode of operation (e.g., platooning mode or manual mode).	The CMS uses the radar in the front of the vehicle to monitor the gap distance and speed of the vehicle ahead. When an unsafe following distance is detected, the system notifies the driver and reduces the vehicle's speed.	**Dependencies:** -Driver being attentive -Alerts being clear and easy to understand to the driver -Driver being responsive to alerts presented via the HMI -Adequate environmental conditions for radar -Non-platooning vehicles being within detection range of the radar **Interactions:** -Driver indirectly interacts with the vehicle driving ahead through the vehicle's radar detection and adapted operations	● Radar - detects vehicles ahead ● EMS ECU - serves as the interface between the radar and the HMI and processes the messages between them. ● EMS ECU Software - generates and decodes inter-vehicle communication messages. ● HMI - present platooning status information and driver alerts	● Radar - detection range and accuracy of detection ● EMS ECU - hardware specifications (e.g., processing power) ● Accelerator actuator - none ● EMS ECU Software - none ● HMI - none	Inputs to EMS ECU and software: ● The software used to generate HMI alerts uses the radar's input to detect the vehicle's distance from the non-platooning vehicle ahead.	Outputs from EMS ECU and software: ● HMI alerts will be presented to the driver based on the vehicle's radar detecting a vehicle ahead within a distance specified by the vehicle detection algorithm. The system modeled here assumes use of CMS. ACC may accomplish a similar function in other systems.	Both
1.4	Maintain positional awareness of the platoon	**Activated:** This function is activated when the vehicles are powered on. **Deactivated:** This function is deactivated when the vehicles are powered off. **Active:** This function is always active while all the vehicles are operating in platooning mode. This function is not	The platooning system must maintain its positional awareness so the ODD can be enforced and for notifications to be presented to the driver about upcoming environmental and infrastructure conditions. Positional awareness is maintained through various positional inputs such as GPS and digital mapping.	**Dependencies:** -Environmental conditions, such as impacting satellite reception (e.g., cloud cover) -Precise GPS information being made available via GPS satellite connections -Access to a highly detailed digital map -Digital map containing geographical conditions -V2V dependencies regarding vehicle status - Validation of ODD	● Position information (e.g., GPS, digital mapping) - GPS provides the location of the vehicle in coordination, while the digital map provides a reference location. ● EMS ECU - interfaces with the GPS antenna and receives the digital map file. ● EMS ECU Software - executes the positional awareness software to determine if position can be maintained for platooning operations. ● HMI - notifies the driver	● Position information (e.g., GPS, digital mapping) - GPS data is limited to the number of available satellites, existing weather conditions, geographical area where the platoon is operated. The digital map is limited in information based off when it was last updated. Temporary work zones and	Inputs to EMS ECU and software: ● The EMS ECU software will use the digital map file and GPS location as inputs for maintaining positional awareness.	Outputs from EMS ECU and software: ● The EMS ECU software will determine if positional awareness can be maintained. If positional awareness cannot be maintained, the driver will receive an informational alert explaining this information and platooning will not be permitted.	Both

Sub function #	Goal of Intended Platooning Sub function	Use Cases of Intended Functionality	Description of Intended Functionality	Functional Dependencies and Interaction	Components Required and Their Function	Limitations	Assumptions About How the Intended Functionality Makes Use of Inputs From Other Elements	Assumptions About How Other Elements Make Use of Outputs From the Intended Functionality Makes Use of Outputs	System
		active during manual mode as positional awareness is not required in manual mode.	The platoon also manages platoon status information for each vehicle, including position in the platoon (1 of 3, 2 of 3, etc.) and vehicle status, such as a warning that a vehicle may be entering or leaving the platoon.	boundaries **Interactions:** -Data from GPS/mapping software -Messages from other platooning vehicles (status, positioning)	when positional awareness cannot be maintained and displays status of platooning vehicles. ● Inter-vehicle communication devices - transmit and receive messages between platooning vehicles	construction of permanent structures may present operational challenges. ● EMS ECU - hardware specifications (e.g., processing power) ● EMS ECU Software - none ● HMI - none ● Inter-vehicle communication devices			
1.5	Maintain lane position	**Activated:** This function is activated when the vehicles begin platooning. **Deactivated:** This function is deactivated when the vehicles are no longer operating in platooning mode. **Active:** This function is only active while all vehicles in the platoon are operating in platooning mode. **NOTE: only applicable to the 3VL2 system**	This function detects when lane position is not maintained. Vehicle will adjust position as needed via inputs to the steering subsystem to maintain position. This function uses various inputs to detect a vehicle drifting in lane including: turn signal status, steering wheel angle and lane-keep assist cameras.	**Dependencies:** -Turn signal status indicated on the CAN bus -Steering wheel angle with respect to acceleration and lane width -Images of lane markings captured by lane-keep assist cameras **Interactions:** -Lane markings -V2V messages (announcement of intended lane change)	● Turn signal - creates a message on the CAN bus to indicate which direction the vehicle is seeking to merge to (left or right) ● Lane-keep assist cameras - detects lane markings ● EMS ECU - serves as the interface for the information received from the CAN bus (positional information) and the lane-keep assist cameras. ● EMS ECU Software - the lane detection algorithm ● HMI - notifies the driver that the vehicle is drifting via alerts and/or haptics.	● Turn signal - the rate of receiving the turn signal status is limited to the update rate of the CAN bus. ● Steering wheel angle - the rate of receiving the steering wheel angle is limited to the update rate of the CAN bus manufacturer ● Lane-keep assist cameras - detection of lane markings is limited to the resolution of the cameras and its performance in different weather and lighting conditions. ● EMS ECU - none ● HMI - none	Inputs to EMS ECU and software: ● The lane detection algorithm will use images from the lane-keep assist cameras, turn signal status from the CAN bus, steering wheel angle from the CAN bus, and position information as inputs to determine if lane position is being maintained.	Outputs from EMS ECU and software: ● If lane position is not being maintained, the driver will receive an alert through the HMI.	3VL2
1.6	Maintain a safe distance away from infrastructure	**Activated:** This function is activated when the vehicles begin platooning. **Deactivated:** This function is deactivated when the vehicles are no longer operating in platooning mode.	This function keeps the vehicle a safe distance away from the infrastructure. Infrastructure may include: road barriers, vehicles (such as work zones or first responder vehicles) parked on the side of the roadway, low	**Dependencies:** -Maintaining positional awareness of the platoon (function) -Reliability and detection accuracy of objects from the front-facing radar, sensors, and cameras -Weather and lighting conditions impacting the detection hardware as	● Radar - detects infrastructure components ahead of the vehicle ● Sensors - detects infrastructure components in-front of and around the vehicle (e.g., radar, LIDAR) ● Cameras - detects infrastructure signs and components in-front of and around the vehicle.	● Radar - detection range, performance in adverse weather conditions ● Sensors - detection range, performance in adverse weather or lighting conditions ● Cameras - resolution and	Inputs to Brake ECU and software: ● Detection inputs from the detection hardware combined with the digital map's location of infrastructure with respect to the vehicle's location will serve as a basis for determining where the vehicle is	Outputs from Brake ECU and software: ● If the vehicle exceeds the safe distance between it and the infrastructure, the driver will receive an HMI alerts and the platoon may be disengaged.	Both

Sub function #	Goal of Intended Platooning Sub function	Use Cases of Intended Functionality	Description of Intended Functionality	Functional Dependencies and Interaction	Components Required and Their Function	Limitations	Assumptions About How the Intended Functionality Makes Use of Inputs From Other Elements	Assumptions About How Other Elements Make Use of Outputs From the Intended Functionality Makes Use of Outputs	System
		Active: This function is only active while all vehicles in the platoon are operating in platooning mode.	clearance overpasses or low clearance bridges. This function uses a digital map and GPS information to know where infrastructure is located on the roadway. Infrastructure is also detected with a combination of radar, sensors and cameras.	well as receiving GPS location from the satellites. -System knowledge about the location of infrastructure components (e.g., digital map) -Frequent digital map updates to reflect changes in permanent infrastructure -Temporary infrastructure information available to the system (e.g., work zone and incident locations) **Interactions:** -Sensor readings of detection inputs (e.g., nearby vehicles) -Data from GPS/mapping software	● EMS ECU - serves as the interface between the radar, sensors and cameras and executes the software. ● EMS ECU Software - contains system knowledge about the locations and details of infrastructure components (e.g., digital map). The software also processes the detection inputs from the radar, sensors and cameras onboard the vehicle. ● HMI - alerts the driver when the vehicle is approaching at close proximity to an infrastructure component ● Inter-vehicle communication devices - transmit and receive messages between platooning vehicles	performance in adverse weather and lighting conditions ● EMS ECU - processing power required to receive and process large amounts of data from sensors and cameras and convert them to a system usable message in a safety-critical application ● EMS ECU Software - none ● HMI - none ● Inter-vehicle communication devices	located with respect to its surrounding infrastructure.		
1.7	Coordinate and maintain a safe following distance and speed control between vehicles in the platoon.	**Activated:** This function is activated when the vehicles begin platooning. **Deactivated:** This function is deactivated when the vehicles are no longer operating in platooning mode. **Active:** This function is only active while all vehicles in the platoon are operating in platooning mode.	This function coordinates inter-vehicle communication to achieve a close following distance between vehicles. Using vehicle telemetry data from the CAN bus, vehicles share dynamic data at low latency speeds to enable coordinated acceleration and braking between vehicles.	**Dependencies:** -Reliability of inter-vehicle communication devices -Weather and lighting conditions impacting inter-vehicle communication signals -Geographical features impacting inter-vehicle communication signals -Adequate processing capabilities of the Brake ECU to transmit and receive messages at a low latency -Infrastructure features (e.g., geofencing) impacting inter-vehicle communication signals -Timely execution of speed and brake actuators -Sensor inputs (radar, LiDAR) **Interactions:** -Sensor readings of detection inputs (e.g.,	● Inter-vehicle communication devices - transmits and receives steering control messages between vehicles in the platoon. ● Radar and LIDAR - detects between the front of the vehicle and vehicle ahead. ● EMS - adjust fuel delivery/supply or applies braking to control the vehicle's speed. ● EMS ECU - interfaces with the inter-vehicle communication devices to receive messages from other platooning vehicles, interfaces with the radar/sensors to compare position information sent from the CAN with a distance measurement of the radar. ● EMS ECU Software - executes the speed reduction algorithm with the values it received from the inter-	● Inter-vehicle communication devices - depending on the communication protocol and the devices used, communication may be intermittent or non-existent in certain geographical locations or may experience bandwidth issues ● Radar - detection range, performance in adverse weather conditions ● Sensors - detection range, performance in adverse weather or lighting conditions ● EMS ECU- processing power required to receive and process large	Inputs to EMS ECU and software: ● The speed reduction algorithm uses the vehicle telemetry data sent from the CAN bus in the form of an inter-vehicle communication message.	Outputs from EMS ECU and software: ● The logic of the speed control algorithm compares the distance between platooning vehicles using the radar and the position information sent from the CAN bus as a checking mechanism to ensure the safe following distance is being maintained.	Both

Sub function #	Goal of Intended Platooning Sub function	Use Cases of Intended Functionality	Description of Intended Functionality	Functional Dependencies and Interaction	Components Required and Their Function	Limitations	Assumptions About How the Intended Functionality Makes Use of Inputs From Other Elements	Assumptions About How Other Elements Make Use of Outputs From the Intended Functionality Makes Use of Outputs	System
				nearby vehicles) -Inter-vehicle messaging between vehicles	vehicle communication messages and the radar/sensors. The software determines if an alert should be presented to the drivers or when to apply a speed set point to the speed control system. ● HMI - notifies the driver that the vehicle is in platooning mode once speed control is maintained and coordinated with the other platooning vehicles. Allows setting or establishing of platooning gap distance and speed set point.	amounts of data from sensors and cameras and convert them to a system usable message in a safety-critical application ● EMS ECU Software - none ● HMI - lack of responsiveness, unable to present platooning information to the driver			
1.8	Maintain position of the vehicle within the lane	**Activated:** This function is activated when the vehicles begin platooning. **Deactivated:** This function is deactivated when the system is no longer in platooning mode. **Active:** This function is only active while all vehicles in the platoon are operating in platooning mode.	This function executes steering control between all three vehicles in a platoon. Steering maneuvers made by the driver of the LV are also carried out by the FVs.	**Dependencies:** -Reliability of inter-vehicle communication devices -Weather and lighting conditions impacting inter-vehicle communication signals -Geographical features impacting inter-vehicle communication signals -Adequate processing capabilities of the Speed control system and steering control system to transmit and receive messages at a low latency -Infrastructure features impacting inter-vehicle communication signals -Timely execution of steering actuators -Sensors detecting position in lane and relative position to other platooning vehicles. **Interactions:** -Sensor readings of detection inputs (e.g., nearby vehicles) -Data from GPS/mapping software	● Radar - detects infrastructure components ahead of the vehicle ● Sensors - detects infrastructure components in-front of and around the vehicle as well as lane markings (e.g., radar, LIDAR) ● Inter-vehicle communication devices - transmits and receives steering control messages between vehicles in the platoon. ● Steering actuator - activates the steering wheel to control the vehicle's motion. ● EMS system - directly interfaces with the inter-vehicle communication devices and processes the coordinating steering software algorithm. ● EMS software - it executes the following distance algorithm with the values received by the system to determine if an alert should be issued and if an alert should be presented to the drivers. ● HMI - notifies the driver that the vehicle's steering	● Sensors - interference, poor visibility due to environmental conditions. ● Infrastructure - tight roadway curvature, grade ● Inter-vehicle communication devices - depending on the communication protocol and the devices used, communication may be intermittent or non-existent in certain geographical locations or may experience bandwidth issues ● Steering actuator - none ● EMS - processing power required to receive and process large amounts of data from sensors and cameras and convert them to a system usable message in a safety-critical	Inputs to EMS ECU and software: ● The steering control algorithm uses the vehicle telemetry data sent from the can bus in the form of an inter-vehicle communication message.	Outputs from EMS ECU and software: ● The steering control function is a sub function of maintaining the 3VL2 system platoon. If this function cannot be maintained the vehicles cannot platoon.	3VL2

Sub function #	Goal of Intended Platooning Sub function	Use Cases of Intended Functionality	Description of Intended Functionality	Functional Dependencies and Interaction	Components Required and Their Function	Limitations	Assumptions About How the Intended Functionality Makes Use of Inputs From Other Elements	Assumptions About How Other Elements Make Use of Outputs From the Intended Functionality Makes Use of Outputs	System
					control is being coordinated with the vehicle ahead in the platoon.	application ● EMS ECU software - none ● HMI - none			
1.9	Detect and handle cut-ins within the platoon	**Activated:** This function is activated once the vehicles are platooning. **Deactivated:** This function is deactivated when platooning mode has been disabled. **Active:** This function is active for both the 2VL1 and 3VL2 systems when platooning mode is enabled.	Cut-ins are a safety risk for platooning operations. This function detects and handles cut-ins in as a safety feature of the platooning system. When a non-platooning vehicle merges in between two platooning vehicles, the system performs braking to the FV to prevent a delayed braking response by the driver. The system will tolerate short cut-ins, applying ACC to maintain distance and speed relative to vehicle in front of platooning vehicle. Extended cut-ins (non-platooning vehicle inserted between platooning vehicles longer than some time threshold) will cause cessation of platooning if range to LV exceeds some maximum threshold.	**Dependencies:** -Radar accurately detecting a vehicle ahead -Timely execution of speed reduction system -Inter-vehicle communication messages being transmitted from the FV to indicate to the other drivers that a cut-in is in process, or that the platoon has been dissolved. **Interactions:** -Platooning vehicle interfaces with the non-platooning vehicle cutting-in via sensors	● Radar - The CMS radar is used to detect vehicles merging in front of the FVs. ● Inter-vehicle communication devices - transmit and receive messages between platooning vehicles. ● EMS - interfaces with the CMS radar to receive the detection input for the EMS software. The EMS will process the HMI alert message through the inter-vehicle communication devices. ● EMS Software - the cut-in detection algorithm (part of following algorithm) determines when a cut-in is occurring. ● HMI - alerts the driver when a vehicle is attempting a cut-in and notifies the other drivers in the platoon that a cut-in is in process, or that the platoon has been dissolved.	● Radar - detection range, performance in adverse weather conditions ● Inter-vehicle communication devices - depending on the communication protocol and the devices used, communication may be intermittent or non-existent in certain geographical locations or may experience bandwidth issues ● EMS ECU - processing power required to receive and process large amounts of data from sensors and cameras and convert them to a system usable message in a safety-critical application ● EMS ECU software - none ● HMI - none	Inputs to EMS ECU and software: ● The cut-in detection algorithm uses the detection input from the radar in the front of the vehicle in addition to its detected speed to determine if the system should dissolve the platoon and engage the EMS.	Outputs from EMS ECU and software: ● If the cut-in detection algorithm indicates a cut-in is occurring, the FV EMS ECU will generate an inter-vehicle communication message sent to the other vehicles. This message will generate an HMI alert indicating the platoon has been dissolved.	Both

Sub function #	Goal of Intended Platooning Sub function	Use Cases of Intended Functionality	Description of Intended Functionality	Functional Dependencies and Interaction	Components Required and Their Function	Limitations	Assumptions About How the Intended Functionality Makes Use of Inputs From Other Elements	Assumptions About How Other Elements Make Use of Outputs From the Intended Functionality Makes Use of Outputs	System
1.10	Detect evasive steering maneuvers made by the LV.	**Activated:** This function is activated upon the formation of a platoon. **Deactivated:** This function is deactivated when platooning mode has been disabled. **Active:** This function is active for both the 2VL1 and 3VL2 systems when platooning mode is enabled.	This function detects evasive steering maneuvers by the driver of the LV or the first FV in the 3VL2 system. To maintain the safety of the platoon, the system will detect an evasive steering maneuver to disengage the platoon to prevent the FVs from following the same path as the LV.	**Dependencies:** -Road conditions (e.g., static or flying objects, damaged infrastructure) -Changes in surrounding traffic (e.g., sudden stoppage in traffic, accidents) -Driver attentiveness (e.g., fatigue or distraction) -Driver training -Position information -Lateral acceleration detection -Steering wheel turning radius -Adequate alert provided to the driver by the HMI -Timely adequate driver reaction time to respond to alert received via the HMI -The position of the platooning vehicles with respect to their lane (e.g., if the steering maneuver positions the vehicles outside the lane, the platoon is dissolved based on the lane-keeping algorithm.) **Interactions:**	● Position information (e.g., GPS, digital mapping) - serves as a redundant input for detecting lateral position with respect to the vehicle's speed. ● Accelerometer - serves as an input to determine lateral acceleration ● Steering wheel - serves as an input to measure evasive steering maneuvers ● EMS ECU - directly interfaces with the positional information, accelerometer data, and steering wheel turn radius data inputs, processes the software ● Steering actuator - activates the steering wheel to control the vehicle's motion. ● Inter-vehicle communication devices - relay information between platooning vehicles ● EMS ECU Software - executes the algorithm with the values received by the EMS ECU to determine if an alert should be issued and if an alert should be presented to the drivers ● HMI - provides an alert to the driver	● Position information (e.g., GPS, digital mapping) - accuracy may limited to the number of satellites that are accessible during a given route, weather conditions (e.g., cloud cover) ● Accelerometer - none ● Steering wheel - none ● EMS ECU - processing power required to receive and process large amounts of data from sensors and cameras and convert them to a system usable message in a safety-critical application ● Steering actuator - none ● Inter-vehicle communication devices - communication range is limited to the devices executing the communication protocol, geographical areas may not support certain protocols ● EMS ECU Software - none ● HMI - clearly indicate emergency situation, driver must take over immediately (assume no attempt to maintain partial platoon)	Inputs to EMS ECU and software: ● Position information – capturing sudden lane movements ● Accelerometer – capturing sudden lateral movements and rapid acceleration ● Steering wheel – capturing aggressive steering inputs from operator	Outputs from EMS ECU and software: ● Inter-vehicle communication – messages noting apparent aggressive control inputs from vehicle ● HMI alerts – indicating to drivers that evasive movement is occurring with a vehicle in the platoon	3VL2
1.11	Detect static road	**Activated:**	This function detects	**Dependencies:**	● Sensors - detect static	● Sensors, cameras	Inputs to EMS ECU and	Outputs from EMS ECU	Both

Sub function #	Goal of Intended Platooning Sub function	Use Cases of Intended Functionality	Description of Intended Functionality	Functional Dependencies and Interaction	Components Required and Their Function	Limitations	Assumptions About How the Intended Functionality Makes Use of Inputs From Other Elements	Assumptions About How Other Elements Make Use of Outputs From the Intended Functionality Makes Use of Outputs	System
	debris to ensure safe operation of the platoon	This function is activated once the vehicles are platooning. **Deactivated:** This function is deactivated when the vehicles are no longer operating in platooning mode. **Active:** This function is only active while all vehicles in the platoon are operating in platooning mode.	static objects located in the lane of travel (e.g., road debris). Once an object is detected, the driver of the vehicle is notified so platooning operations can be adjusted accordingly.	-Operational environment: roadway conditions, surrounding vehicle's may be carrying loads that are not appropriately being transported, infrastructure may be damaged -Sensors and cameras being positioned appropriately to cover a variety of angles -Sensors and cameras detecting a variety of objects -Timely processing of sensor, camera, and radar data by the EMS ECU -Adequate alert provided to the driver by the HMI -Timely driver reaction time to respond to alert received via the HMI **Interactions:** -Platooning vehicle hardware scans the roadway infrastructure for static debris ahead of the vehicle.	objects in the lane of travel of the platoon ● EMS ECU - serves as the interface between the sensors and cameras for detecting and processing static objects. The EMS ECU also interfaces with the inter-vehicle communication devices to send and receive messages. ● EMS ECU Software - it processes the vehicle inputs and executes the obstruction detection algorithm. ● HMI - alerts the driver of a static object detection.	and radar - only installed on the tractor, not the trailer due for operational purposes. ● EMS ECU - processing power required to receive and process large amounts of data from sensors and cameras and convert them to a system usable message in a safety-critical application ● HMI - none	software: ● The sensors and cameras serve as inputs to the EMS ECU where they are processed by the software for detecting objects.	and software: ● The static object detection algorithm generates alerts and presents them to the driver via the HMI. The drivers in the other platooning vehicles will receive an alert that the platoon has been dissolved.	

Sub function #	Goal of Intended Platooning Sub function	Use Cases of Intended Functionality	Description of Intended Functionality	Functional Dependencies and Interaction	Components Required and Their Function	Limitations	Assumptions About How the Intended Functionality Makes Use of Inputs From Other Elements	Assumptions About How Other Elements Make Use of Outputs From the Intended Functionality Makes Use of Outputs	System
1.12	Detect flying objects approaching a platooning vehicle to ensure safe operation of the platoon	**Activated:** This function is activated once the vehicles are platooning. **Deactivated:** This function is deactivated when the vehicles are no longer operating in platooning mode. **Active:** This function is only active while all vehicles in the platoon are operating in platooning mode.	This function detects unavoidable flying objects approaching the platooning vehicles. While the objects may be unavoidable, this function notifies the driver via the HMI to prepare the driver for the event.	**Dependencies:** -Operational environment: certain weather conditions may increase the likelihood of flying objects, surrounding vehicle's may be carrying loads that are not appropriately being transported, infrastructure -Sensors and cameras being positioned appropriately to cover a variety of angles -Sensors and cameras detecting a variety of objects -Radar identifying velocity, direction and proximity to flying objects -Timely processing of sensor, camera, and radar data by the EMS -Adequate alert provided to the driver by the HMI -Timely adequate driver reaction time to respond to alert received via the HMI **Interactions:** -Platooning vehicle hardware scans the roadway infrastructure for static debris ahead of the vehicle.	● Sensors, cameras and LIDAR - detect flying objects approaching the platoon ● EMS ECU - serves as the interface between the sensors and cameras for detecting and processing flying objects. The EMS ECU also interfaces with the inter-vehicle communication devices to send and receive messages. ● EMS ECU Software - it processes the vehicle inputs and executes the obstruction detection algorithm. ● HMI - alerts the driver of a flying object detection.	● Sensors, cameras and radar - only installed on the tractor, not the trailer due for operational purposes. ● EMS ECU - processing power required to receive and process large amounts of data from sensors and cameras and convert them to a system usable message in a safety-critical application ● HMI - none	Inputs to EMS ECU and software: ● The sensors, cameras and radar serve as inputs to the EMS ECU where they are processed by the software.	Outputs from EMS ECU and software: ● The HMI alerting algorithm generates alerts and presents them to the driver via the HMI.	Both
1.13	Detect vehicles approaching the platoon's blind spots to maintain the safety of the platoon	**Activated:** This function is activated once the vehicles are platooning. **Deactivated:** This function is deactivated when the vehicles are no longer operating in platooning mode. **Active:** This function is only active while all vehicles in the platoon are	This function detects non-platooning vehicles in the platooning vehicle's blind spots (e.g., left and right sides of the tractor). The driver will receive a blind spot detection alert only when the vehicle's turn signal is activated, and a vehicle is in the blind spot. The driver will not receive an alert when the platooning	**Dependencies:** -Radars being positioned appropriately to cover a variety of angles -Radar accurately detecting a vehicle in the blind spot of the platooning vehicle (e.g., other tractor-trailers or other heavy vehicles may be constructed of reflective materials that negatively impact the accuracy of detection.) -Adequate alert provided	● Radar - The radar on the side of the tractor is used to detect vehicles traveling alongside the vehicle. ● EMS ECU - interfaces with the radar to receive the detection input for the EMS ECU software. The EMS ECU will process this input and generate an alert based on the EMS ECU software. ● EMS ECU Software - the blind spot detection algorithm determines when an alert should be presented.	● Radar - detection range, performance in adverse weather conditions ● EMS ECU - processing power required to receive and process large amounts of data from sensors and cameras and convert them to a system usable message in a safety-critical	Inputs to EMS ECU and software: ● The blind spot detection algorithm uses the detection input from the radar in the sides of the tractor in addition to its turn signal status from the CAN bus to determine if the system should generate an HMI alert.	Outputs from EMS ECU and software: ● If the blind spot detection algorithm indicates a detection, an alert will be generated to the driver of that vehicle only.	Both

Sub function #	Goal of Intended Platooning Sub function	Use Cases of Intended Functionality	Description of Intended Functionality	Functional Dependencies and Interaction	Components Required and Their Function	Limitations	Assumptions About How the Intended Functionality Makes Use of Inputs From Other Elements	Assumptions About How Other Elements Make Use of Outputs From the Intended Functionality Makes Use of Outputs	System
		operating in platooning mode.	vehicle is not attempting to change lanes.	to the driver by the HMI -Timely processing of radar detection by the EMS ECU so it can be translated into an alert presented by the HMI. **Interactions:** -Platooning vehicle interfaces with the non-platooning vehicles traveling alongside the platooning vehicles.	● HMI - alerts the driver when a vehicle is approaching from the platooning vehicle's blind spot while it has intent to change lanes.	application ● EMS ECU Software - none ● HMI - none			
2.1	Enforce geographical location limitations of the ODD	**Activated:** This function is activated once the vehicles begin platooning. **Deactivated**: This function is deactivated once the vehicles are no longer operating in platooning mode. **Active:** This function is only active while all vehicles in the platoon are operating in platooning mode.	The platooning system must be able to detect its geographical location to ensure operation is occurring within its ODD. The platoon operation must obey rules and protocols specific to different geographic regions (e.g., state borders). Geographical location will be maintained similar to how the vehicle maintains its positional awareness.	**Dependencies:** -Environmental conditions impacting satellite reception (e.g., cloud cover) -Precise GPS information being made available via GPS satellite connections -Access to a highly detailed digital map -Digital map containing geographical conditions -Frequent digital map updates to reflect changes in permanent infrastructure -Federal, state and local regulations **Interactions:** -Data from GPS/mapping software -Messages from other platooning vehicles (status, positioning)	● Position information (e.g., GPS, digital mapping) - GPS provides the location of the vehicle in coordination, while the digital map provides a reference location. ● EMS ECU - interfaces with the GPS antenna and received and the digital map file. ● EMS ECU Software - executes the positional awareness software to determine if position can be maintained for platooning operations. ● HMI - notifies the driver when positional awareness cannot be maintained or when the system has continued operating past an ODD boundary.	● Position information (e.g., GPS, digital mapping) - GPS data is limited to the number of available satellites, existing weather conditions, geographical area where the platoon is operated. The digital map is limited in information based off when it was last updated. Temporary work zones and construction of permanent structures may present operational challenges. ● EMS ECU - processing power required to receive and process large amounts of data from sensors and cameras and convert them to a system usable message in a safety-critical application ● EMS ECU Software - none ● HMI - none	Inputs to EMS ECU and software: ● The EMS ECU software will use the digital map file and GPS location as inputs for maintaining geographical location.	Outputs from EMS ECU and software: ● The EMS ECU software will determine if positional awareness can be maintained. If positional awareness cannot be maintained the driver will receive an informational alert explaining this information and platooning will not be permitted.	Both
2.2	Enforce roadway grade limitations of the ODD	**Activated:** This function is activated once the	The platooning system must know the grade of the roadway it is	**Dependencies:** -Environmental conditions impacting	● Positional information (e.g., GPS, digital mapping) - GPS provides the location of the	● Position information (e.g., GPS, digital	Inputs to EMS ECU and software: ● The EMS ECU	Outputs from EMS ECU and software: ● The EMS ECU software	Both

Sub function #	Goal of Intended Platooning Sub function	Use Cases of Intended Functionality	Description of Intended Functionality	Functional Dependencies and Interaction	Components Required and Their Function	Limitations	Assumptions About How the Intended Functionality Makes Use of Inputs From Other Elements	Assumptions About How Other Elements Make Use of Outputs From the Intended Functionality Makes Use of Outputs	System
		vehicles begin platooning. **Deactivated**: This function is deactivated once the vehicles are no longer operating in platooning mode. **Active:** This function is only active while all vehicles in the platoon are operating in platooning mode.	traversing to ensure the platoon is operating within its ODD. Steep upgrades may prevent the platoon from maintaining the time-gap between vehicles, while steep downgrades present introduce excessive acceleration from the vehicles. The grades permitted for travel should consider the vehicle's load, brake performance and powertrain performance.	satellite reception (e.g., cloud cover) -Precise GPS information being made available via GPS satellite connections -Access to a highly detailed digital map containing specific grade information -Frequent digital map updates to reflect changes in permanent infrastructure **Interactions:** -Data from GPS/mapping software	vehicle in coordination, while the digital map provides a reference location. ● EMS ECU - interfaces with the GPS antenna and received and the digital map file. ● EMS ECU Software - executes the digital map file with the GPS input to determine the roadway grade where the platoon is located. ● HMI - notifies the driver when positional awareness cannot be maintained.	mapping) - GPS data is limited to the number of available satellites, existing weather conditions, geographical area where the platoon is operated. The digital map is limited in information based off when it was last updated. ● EMS ECU - processing power required to receive and process large amounts of data from sensors and cameras and convert them to a system usable message in a safety-critical application ● EMS ECU Software - none ● HMI - none	software will use the digital map file and GPS location as inputs for maintaining determining the grade of the roadway where the platoon is located.	will determine if the grade of the roadway is known. If the grade is unknown, the driver will receive an alert from the HMI notifying the driver of this failure and the platoon will be disengaged. If the roadway grade is outside the ODD's tolerance, the driver will also receive an alert from the HMI notifying the driver and the platoon will be disengaged.	

Sub function #	Goal of Intended Platooning Sub function	Use Cases of Intended Functionality	Description of Intended Functionality	Functional Dependencies and Interaction	Components Required and Their Function	Limitations	Assumptions About How the Intended Functionality Makes Use of Inputs From Other Elements	Assumptions About How Other Elements Make Use of Outputs From the Intended Functionality Makes Use of Outputs	System
2.3	Enforce roadway curvature limitations of the ODD	**Activated:** This function is activated once the vehicles begin platooning. **Deactivated**: This function is deactivated once the vehicles are no longer operating in platooning mode. **Active:** This function is only active while all vehicles in the platoon are operating in platooning mode.	Detecting roadway curvature is required for operating within the platooning system's ODD. Roadways with high curvature create stability challenges for tractor trailers given the high clearance of these vehicles.	**Dependencies:** -Electronic Stability Control (ESC) -Roadway curvature -Roadway friction conditions -Environmental conditions impacting satellite reception (e.g., cloud cover) -Precise GPS information being made available via GPS satellite connections -Access to a highly detailed digital map containing specific grade information **Interactions:** -Data from GPS/mapping software	● Positional information (e.g., GPS, digital mapping) - GPS provides the location of the vehicle in coordination, while the digital map provides a reference location. ● EMS ECU - interfaces with the GPS antenna and received and the digital map file. ● EMS ECU Software - executes the digital map file with the GPS input to determine the roadway grade where the platoon is located. The ESC algorithm (not part of the platooning system) is also executed on the Brake ECU. ● HMI - notifies the driver when positional awareness cannot be maintained.	● Position information (e.g., GPS, digital mapping) - GPS data is limited to the number of available satellites, existing weather conditions, geographical area where the platoon is operated. The digital map is limited in information based off when it was last updated. ● EMS ECU - processing power required to receive and process large amounts of data from sensors and cameras and convert them to a system usable message in a safety-critical application ● EMS ECU Software - none ● HMI - none	Inputs to EMS ECU and software: ● The EMS ECU software will use the digital map file and GPS location as inputs for maintaining determining the position of the platoon with respect to the roadway curvature at that location. Each vehicle's speed, truck load, steering wheel angle (CAN bus), stability control capabilities and roadway friction conditions will serve as inputs to determine the curvature angles that the vehicles may operate within.	Outputs from EMS ECU and software: ● The EMS ECU software will determine if the curvature of the roadway is known. If the curvature of the roadway is unknown, the driver will receive an alert from the HMI notifying the driver of this failure and the platoon will be disengaged. If the curvature of the roadway is outside the ODD's tolerance, the driver will also receive an alert from the HMI notifying the driver and the platoon will be disengaged.	Both
2.4	Enforce roadway or infrastructure features limitations of the ODD	**Activated:** This function is activated once the vehicles begin platooning. **Deactivated**: This function is deactivated once the vehicles are no longer operating in platooning mode. **Active:** This function is only active while all vehicles in the platoon are operating in platooning mode.	The platooning system must know the roadway or infrastructure features ahead. The ODD prohibits traveling through tunnels and work zones and on bridges. Platooning mode must be disabled prior to approaching these features.	**Dependencies:** -LV guiding the platoon (FVs have a limited field of view) -LV driver attentiveness -Environmental conditions impacting satellite reception (e.g., cloud cover) -Precise GPS information being made available via GPS satellite connections -Access to a highly-detailed digital map containing specific grade information -Frequent digital map updates to reflect changes in permanent infrastructure -Temporary infrastructure	● Positional information (e.g., GPS, digital mapping) - GPS provides the location of the vehicle in coordination, while the digital map provides a reference location. ● EMS ECU - interfaces with the GPS antenna and received and the digital map file. ● EMS ECU Software - executes the digital map file with the GPS input to determine the roadway grade where the platoon is located. ● HMI - The HMI notifies the driver when there is an upcoming roadway or infrastructure feature is ahead and when the platoon is dissolved until the feature	● Positional information (e.g., GPS, digital mapping) - GPS data is limited to the number of available satellites, existing weather conditions, geographical area where the platoon is operated. The digital map is limited in information based off when it was last updated. ● EMS ECU - processing power required to receive and process large amounts of data from sensors and	Inputs to EMS ECU and software: ● The EMS ECU software will use the digital map file and GPS location as inputs for maintaining determining the location of the platoon. Information on temporary infrastructure will also serve as an input to the system to indicate where work zones and other temporary infrastructure is located.	Outputs from EMS ECU and software: ● The EMS ECU software will determine when the LV driver will receive an alert that the platoon is being dissolved because there is a roadway or infrastructure ahead that is prohibited by the ODD. The FV drivers will receive the same alert.	Both

Sub function #	Goal of Intended Platooning Sub function	Use Cases of Intended Functionality	Description of Intended Functionality	Functional Dependencies and Interaction	Components Required and Their Function	Limitations	Assumptions About How the Intended Functionality Makes Use of Inputs From Other Elements	Assumptions About How Other Elements Make Use of Outputs From the Intended Functionality Makes Use of Outputs	System
				information being made available to the system (e.g., work zone and accident locations). **Interactions:** -Data from GPS/mapping software	is no longer in the path of travel.	cameras and convert them to a system usable message in a safety-critical application ● EMS ECU Software - none ● HMI - none			
2.5	Enforce pavement conditions limitations of the ODD	**Activated:** This function is activated once the vehicles begin platooning. **Deactivated**: This function is deactivated once the vehicles are no longer operating in platooning mode. **Active:** This function is only active while all vehicles in the platoon are operating in platooning mode.	The platooning system must be able to detect the pavement conditions of the roadway. The ODD prohibits platooning in wet pavement conditions.	**Dependencies:** -LV guiding the platoon (FVs have a limited field of view) -LV driver attentiveness -Time-gap distance of system determines the distance between the vehicles -Braking performance -ESC detecting wet pavement conditions -Braking performance differences in platooning vehicles represent a challenge when ESC is activated. **Interactions:** -Data from GPS/mapping software	● EMS ECU - interfaces with the GPS antenna and received and the digital map file. ● EMS ECU Software - executes to detect wet pavement conditions. ● HMI - notifies the driver when the driver is not being attentive or is fatigued. The HMI also notifies the driver when there are wet pavement conditions and when the platoon is dissolved.	● EMS ECU - processing power required to receive and process large amounts of data from sensors and cameras and convert them to a system usable message in a safety-critical application ● EMS ECU Software - none ● HMI - none	Inputs to EMS ECU and software: ● The EMS ECU software will use the detection from the ESC to determine if an alert should be issued.	Outputs from EMS ECU and software: ● The EMS ECU software will alert the driver via the HMI when a wet pavement condition is detected and when the platoon is dissolved based on its detection.	Both
2.6	Enforce weather conditions limitations of the ODD	**Activated:** This function is activated once the vehicles begin platooning. **Deactivated**: This function is deactivated once the vehicles are no longer operating in platooning mode. **Active:** This function is only active while all vehicles in the platoon are operating in platooning mode.	The platooning system must be able to detect the weather conditions where the platoon is operating. This function is required for enforcing the ODD. The ODD prohibits platooning in adverse weather conditions such as rain, sleet, and snow.	**Dependencies:** -Weather conditions (e.g., precipitation and visibility) -Geographical location of the platoon (over-the-air weather updates may not be accessible everywhere) -Driver's response to the HMI notifications -Ability of the sensors to accurately detect precipitation and low visibility conditions **Interactions:** -The ECU uses weather data and sensor detection inputs to determine permittable platooning conditions.	● Sensors - detects precipitation in-front of and around the vehicle ● EMS ECU - interfaces with the GPS antenna and received and the digital map file. ● EMS ECU Software - executes the weather detection algorithm to determine when HMI notifications should be issued. ● HMI - notifies the driver of current and upcoming weather conditions that are restricted by the ODD.	● Sensors - detection range, performance in adverse weather or visibility conditions ● EMS ECU - processing power required to receive and process large amounts of data from sensors and cameras and convert them to a system usable message in a safety-critical application ● EMS ECU Software - none ● HMI - none	Inputs to EMS ECU and software: ● The EMS ECU software will use the data detected by the sensors as well as the over-the-air weather updates as inputs to determine whether an HMI notification should be issued. The system will also read the status of the windshield wipers as an input. The HMI notification would instruct the driver to disengage platooning mode.	Outputs from EMS ECU and software: ● The driver of the LV or FV can dissolve the platoon at any time due to adverse weather conditions or visibility conditions. The driver does not need to receive a notification to disengage platooning mode; however, the driver is expected to disengage platooning mode within a specified time of receiving the notification.	Both

Table 15. Hazardous Events Identified Caused by the Unintended Behavior of the Function and Their Triggering Events

Sub function #	Goal of Intended Platooning Function	Hazardous Event Caused by Unintended Behavior of the Function	Triggering Events	Severity	Probability of Exposure	Controllability
1.1	Facilitate the sharing of information between vehicles to enable platooning through inter-vehicle communications.	• Crash situation (FV rear-ends LV) • Unintended acceleration • Unintended braking • Unintended close following distance • Reduced situational awareness of FV driver	• Incorrect telemetry information, untimely information, stale information, lack of information • Interference from other vehicles (physical- cut-in, electronic-manipulation of signals) • Loss of forward-facing camera	S3	E2	C1
1.2	Facilitate the sharing of information between drivers for platooning operations.	• Lane change without coordination	• Loss of inter-vehicle communications • Improper usage of communications	S1	E2	C1
1.3	Maintain a safe following distance from non-platooning vehicles.	• Crash (rear end) • Unintended acceleration • Unintended braking • Unintended close following distance over a long duration of time	• Incorrect telemetry information, untimely information, stale information, lack of information • Interference from other vehicles (physical- cut-in, electronic-manipulation of signals) • Unexpected sharp/blind curve	S3	E1	C1
1.4	Maintain positional awareness of the platoon	• Inadvertent exiting ODD • Loss of "look ahead" for upcoming environmental/infrastructure issues • Loss of platooning functionality (unavailability)	• Loss or delay in GPS signals • Incorrect/corrupted/outdated map • • Loss or delay of telemetry messages	S1	E1	C1
1.5	Maintain lane position	• Crash (rear end or sideswipe) • Unintended braking • Overcorrection of steering • Unintended acceleration	• Driver error/inattentiveness • Loss of lane-keeping sensors • Loss of critical ECU/messages (steering, turn signal status) • Degraded/absent lane markings • Obscured visibility due to environmental conditions	S3	E2	C1
1.6	Maintain a safe distance away from infrastructure	• Crash with infrastructure (with possible cascading events)	• Loss of sensor functions • Obscured visibility due to environmental conditions • Incorrect/outdated/corrupted maps • Driver error	S3	E2	C1
1.7	Coordinate and maintain speed control	• Crash (rear end) • Unintended acceleration • Unintended braking	• Loss of inter-vehicle communications • Loss of sensor readings • Obscured visibility due to environmental conditions (fog/rain, etc.) • Incorrect speed/gap distance set points • Failure of speed control system/lack of responsiveness • Uncompensated road conditions (grade, moisture, etc.)	S3	E1	C1

Sub function #	Goal of Intended Platooning Function	Hazardous Event Caused by Unintended Behavior of the Function	Triggering Events	Severity	Probability of Exposure	Controllability
1.8	Coordinate steering control	• Overcorrection • Swerve into other lane	• Loss inter-vehicle communications • Loss sensor readings • Speed control system/software failure • Inadequate lane marking recognition (particularly for work zones/temporary markings) • Lack of feedback to driver during platooning may cause driver not to notice steering issues/failures	S2	E1	C1
1.9	Detect and handle cut-ins	• Collision with cut-in vehicle	• Failure of sensors to detect vehicle • Loss of inter-vehicle communications • Failure of the EMS	S3	E2	C2
1.10	Detect evasive steering maneuvers	• Overcorrection • Swerve into another lane	• Run off road • Road obstruction/undetected cut-in • Erratic behavior by other vehicles • Steering/speed control failure • Medical emergency of other drivers	S2	E1	C2
1.11	Detect static road debris	• Late reaction to debris, causing evasive steering • Collision with road debris	• Sensor failures • Insufficient sensor data processing speed • Driver inattentiveness	S3	E2	C2
1.12	Detect flying objects approaching a platooning vehicle.	• Late reaction to flying object, causing evasive steering • Collision with flying object	• Sensor failures • Insufficient sensor data processing speed • Driver inattentiveness	S2	E2	C3
1.13	Blind spot detection	• Late reaction to vehicle in blind spot, causing evasive steering • Collision with vehicle in blind spot	• Failure of sensors • Driver inattentiveness • EMS failure • Failure to use turn signals	S3	E1	C3
2.1	Enforce geographical location of the ODD	• Route/map information incorrect/inaccurate	• Failure of configuration management • Corruption of route/map data	S1	E1	C2
2.2	Enforce roadway grade of the ODD	• Platoon not prepared to ascend/descend slope	• Failure to correctly determine position • Incorrect/corrupt map or route data.	S1	E1	C2
2.3	Enforce roadway curvature of the ODD	• Platoon traveling at too high of speed to be able to make turn	• Failure to correctly determine position • Incorrect/corrupt map or route data.	S1	E1	C2
2.4	Enforce roadway or infrastructure features of the ODD	• Crash with infrastructure	• Unusual traffic density/traffic speeds • Toll road operation • Unusual overpass heights (low) • Legal permission to platoon	S3	E1	C2
2.5	Enforce pavement conditions of the ODD	• Platoon traveling at too high of speed or too close in formation for given road conditions	• Failure to correctly determine position • Failure to correct determine speed. • Incorrect/corrupt map or route data	S2	E1	C2
2.6	Enforce weather conditions of the ODD	• Platoon traveling at too high of speed or too close in formation for given road conditions	• Sensor failure • Driver inattentiveness	S2	E1	C2
3.1	Monitor and enforce driver's hours-of-service	• Driver driving under sub-optimal conditions (lower reaction times, drowsy)	• Failure to correctly plan routes for hours of service	S1	E1	C2

Sub function #	Goal of Intended Platooning Function	Hazardous Event Caused by Unintended Behavior of the Function	Triggering Events	Severity	Probability of Exposure	Controllability
3.2	Ensure the drivers are operating the platoon with full attentiveness	• Driver susceptible to drowsy conditions leading to degraded abilities, leading to crash	• Failure to correctly plan routes for hours of service • Failure to confirm driver attentiveness	S1	E2	C2
4.1	Ensures the vehicle's tire pressure is acceptable for platooning conditions.	• Unable to brake if vehicle ahead has blow-out or sudden loss of tire pressure	• Failure to tire pressure monitoring • Failure to perform routine vehicle maintenance	S3	E1	C2
4.2	Ensures the driver is not being exposed to excessive amounts of exhaust fumes	• Driver drowsy, incapacitated, sick	• Exhaust sensor failure • Insufficient following distance	S2	E2	C3
5.1	To allow manual override by any of the drivers in the platoon at any time while platooning	• Platooning system and driver in conflict with control over truck, leading to unsafe speed, steering and crash	• HMI fails to communicate driver command to disengage platoon • Driver inattentiveness (does not disengage platoon)	S1	E1	C1

Table 16. Critical Sub-Functions and Safety Mitigations Applied to Mitigate or Avoid the SOTIF-Related Risks

Sub function #	Goal of Intended Platooning Function	Triggering Events	Safety Mitigations Applied	Safety Mitigation Type
1.9	Detect and handle cut-ins	1.9.1.1 Failure of sensors to detect vehicle 1.9.2.1 Loss of inter-vehicle communications 1.9.3.1 Failure of the EMS	11: The front-facing camera and sensors detect moving objects approaching the front and sides of the vehicle and alert the driver. 19: Driver must be prepared to take over the system and brake. 20: The CMS on FVs activates during a communication failure. 21: Test all sensors and positioning system on all platoon-enabled vehicles prior to platooning. 24: The CMS activates upon surpassing safe following distance, alerting the driver, braking and disengaging the platoon.	11: Design 19: Training 20: Design 21: Operations 24: Design
1.11	Detect static road debris	1.11.1.1 Sensor failures 1.11.2.1 Insufficient sensor data processing speed 1.11.3.1 Driver inattentiveness	3: Forward and side-facing sensors will detect static road debris and alert the driver. 6: The HMI provides periodic driver engagement such as an alerter button (e.g., dead man switch). 11: The front-facing camera and sensors detect moving objects approaching the front and sides of the vehicle and alert the driver. 21: Test all sensors and positioning system on all platoon-enabled vehicles prior to platooning.	3: Design 6: Design 11: Design 21: Operations
1.12	Detect flying objects approaching a platooning vehicle.	1.12.1.1 Sensor failures 1.12.2.1 Insufficient sensor data processing speed 1.12.3.1 Driver inattentiveness	6: The HMI provides periodic driver engagement such as an alerter button (e.g., dead man switch). 11: The front-facing camera and sensors detect moving objects approaching the front and sides of the vehicle and alert the driver. 21: Test all sensors and positioning system on all platoon-enabled vehicles prior to platooning.	6: Design 11: Design 21: Operations
1.13	Blind spot detection	1.13.1.1 Failure of sensors 1.13.2.1 Driver inattentiveness 1.13.3.1 EMS failure 1.13.4.1 Failure to use turn signals	6: The HMI provides periodic driver engagement such as an alerter button (e.g., dead man switch). 19: Driver must be prepared to take over the system and brake. 21: Test all sensors and positioning system on all platoon-enabled vehicles prior to platooning. 69: Blind spot detection sensors notify the driver of a detected object.	6: Design 11: Design 21: Operations 69: Design
3.2	Ensure the drivers are operating the platoon with full attentiveness	3.2.1.1 Failure to correctly plan routes for hours of service 3.2.1.2 Failure to confirm driver attentiveness	6: The HMI provides periodic driver engagement such as an alerter button (e.g., dead man switch). 7: The platoon safely disengages and alerts the driver if there is a failure to engage with the HMI. 55: The driver monitoring system monitors the driver's attentiveness and fatigue. 63: Each driver in the platoon is aware of the other driver's hours of service.	6: Design 7: Design 55: Design 63: Operations
4.2	Ensures the driver is not being exposed to excessive amounts of exhaust fumes	4.2.1.1 Exhaust sensor failure 4.2.1.2 Insufficient following distance	8: The FVs monitor exhaust fume inhalation. 12: Driver must be aware of other trucks and platoons, and always ensure there is a safe following distance between other trucks. 21: Test all sensors and positioning system on all platoon-enabled vehicles prior to platooning. 47: A safe following distance regarding driver inhalation of exhaust fumes is determined. 59: The system alerts the driver of the FV when the exhaust fume inhalation threshold has been met.	8: Design 12: Operations 21: Operations 47: Design 59: Design

Table 17. Strategies for Performing System Verification

Activity	Description	Type of Activity
Requirements Traceability	• Verify safety-related requirements are implemented in the final system. • Revise the requirements as necessary with newly discovered system limitations or needs.	Analysis
Unit Testing	• Verify all compatibility between all platooning system and vehicle interfaces. • Confirm the impacts of aging equipment of each component of the platooning system.	Software Testing
On-board Sensor Verification	• Conduct an analysis to identify problematic environmental conditions and use cases for the on-board sensors. • Use the results to refine the boundary values accepted by the EMS software.	Hardware Testing
EMS	• Confirm the software is receiving data from all ECU inputs. • Test EMS software through MIL and SIL to confirm functionality and use of component inputs.	Hardware Testing
HMI	• Confirm the HMI presents timely alerts and warnings generated by the EMS software. • Verify the HMI was installed in a location effective for the driver of the platooning vehicle.	Hardware and Software Testing
Accelerator Actuator	• Confirm operations of accelerator actuators in FVs in response to system commands.	System Testing
Steering Actuator	• Confirm operations of steering actuators in FVs in response to system commands (3VL2 system only).	System Testing
Inter-vehicle Communications	• Confirm correct messages are passed between platooning vehicles, using the specified interface. • Confirm voice communications between drivers are sufficiently noise-free.	System Testing
Position Information	• Confirm the system can receive sufficient position information within the ODD.	Hardware Testing
Integration Testing	• Verify system software functions according to requirements. • Verify the interfaces shown in Figure 3 and Figure 4.	Hardware and Software Testing

Table 18. Strategies for Performing System Validation

Activity	Description	Type of Activity
Inter-vehicle Communications	Confirm messages that do not comply with interface specification are rejected and do not adversely affect operation.	System Testing
On-board Sensor Verification	Confirm sensor still functions at ODD limits. Confirm system response appropriately during loss of input from sensor (outside of ODD, sensor failure).	System Testing
EMS	Confirm system balances braking effort between air brakes and engine braking. Confirm system responds appropriately to control inputs and responds safely to inputs out of range.	System Testing
Accelerator Actuator	Confirm system handles actuator inputs that are at actuator physical limits or out of valid range. Invalid inputs should be rejected.	System Testing
Steering Actuator	Confirm system handles actuator inputs that are at actuator physical limits or out of valid range. Invalid inputs should be rejected.	System Testing
ODD	Measure system response to environmental conditions outside design range, such as slippery road conditions, low visibility.	System Testing
Residual Risk Assessment	Based on initial risk assessment and safety mitigations assigned to protect safety-critical functions, estimate final system risk.	Analysis
HMI	The display has sufficient resolution and the alerts presented are timely.	System Testing

Table 19. Verification Activities Described for Each of the System Components and Elements

Platooning System Components and Elements and Their Function	Verification Activities
Inter-vehicle communication devices - transmit and receive messages between platooning vehicles.	-Verify the communication devices performance (e.g., range, latencies) -Verify reliability of communication devices (e.g., signal-to-noise ratio) -Verify the functionality of the communication devices with the system requirements -Perform testing under different operating conditions (e.g., weather, temperature, traffic) -Perform accelerated life testing on the communication devices -Perform testing on a degraded communication device
EMS ECU - processes inter-vehicle communication messages.	-Verify the ECU's performance (e.g., processing capabilities) -Verify the functionality of the radars in accordance with the system requirements -Verify all physical interface connections with the ECU -Perform testing under different operating conditions (e.g., humidity, temperature, vibration) -Perform accelerated life testing on the ECU -Perform testing on a degraded ECU
EMS ECU Software - generates and decodes the inter-vehicle communication messages and provides the vehicle with a digital map	-Verify reliability of algorithms (e.g., white noise, audio frequencies, signal-to-noise ratio -Verify the functionality of the algorithms are in accordance with the system requirements -Verify the architectural properties of the software -Perform in-the-loop testing on applicable scenarios and use cases (e.g., HIL, SIL, MIL) -Perform vehicle level testing in a closed course operating environment -Inject the radars with problematic detection inputs that could trigger hazardous behavior -Verify all data interfaces
HMI - present platooning status information, vehicle status and driver status, driver-to-driver communication.	-Verify the HMI's performance with presenting information to the driver -Verify the functionality of the HMI in accordance with the system requirements -Perform testing under different environmental conditions (e.g., lighting, temperature) -Perform accelerated life testing on the HMI -Perform testing on a degraded HMI -Verify HMI alignment and configuration
Foot pedal - activates voice communication between drivers of platooning vehicles)	-Test the interface connection to the EMS ECU -Verify voice communication is activated via the HMI when the foot pedal is pressed
Radar - detects vehicles ahead as well as vehicles approaching to merge	-Verify the radar's performance (e.g., range, precision, resolution, bandwidth) -Verify the functionality of the radars in accordance with the system requirements -Inject the radars with problematic detection inputs that could trigger hazardous behavior -Perform in-the-loop testing on applicable scenarios and use cases (e.g., HIL, SIL, MIL) -Perform radar testing under different operating conditions (e.g., weather, lighting, traffic) -Perform accelerated life testing on the radars -Perform testing on a degraded radar -Verify radar alignment and configuration on the vehicle
Position information (e.g., GPS) - GPS provides the location of the vehicle in coordination, while the digital map provides a reference location.	-Verify the GPS performance (e.g., precision) -Verify the functionality of the GPS antennas in accordance with the system requirements -Inject the GPS antennas with problematic detection inputs that could trigger hazardous behavior -Perform in-the-loop testing on applicable scenarios and use cases (e.g., HIL, SIL, MIL) -Perform GPS testing under different operating conditions (e.g., weather, visibility, geographical locations) -Perform accelerated life testing on the GPS antenna -Perform testing on a degraded GPS antenna -Verify GPS configuration on the vehicle
Turn signal - creates a message on the CAN bus to indicate which direction the vehicle is seeking to merge to (left or right).	-Verify the turn signal indicates illuminates the vehicle's lights accordingly. -Test the interface connection to the CAN bus
Lane-keep assist cameras - detects lane markings	-Verify the camera's performance (e.g., range, precision, resolution, bandwidth) -Verify the functionality of the cameras in accordance with the system requirements -Inject the cameras with problematic detection inputs that could trigger hazardous behavior -Perform in-the-loop testing on applicable scenarios and use cases (e.g., HIL, SIL, MIL) -Perform sensor testing under different operating conditions (e.g., weather, lighting, traffic) -Perform accelerated life testing on the cameras -Perform testing on a degraded camera -Verify camera alignment and configuration on the vehicle

Platooning System Components and Elements and Their Function	Verification Activities
Sensors - detects infrastructure components in-front of and around the vehicle (e.g., LIDAR) as well as static objects as the platoon is approaching.	-Verify the sensor's performance (e.g., range, precision, resolution, bandwidth) -Verify the functionality of the sensors in accordance with the system requirements -Inject the sensor with problematic detection inputs that could trigger hazardous behavior -Perform in-the-loop testing on applicable scenarios and use cases (e.g., HIL, SIL, MIL) -Perform sensor testing under different operating conditions (e.g., weather, lighting, traffic). -Perform accelerated life testing on the sensors -Perform testing on a degraded sensor -Verify sensor alignment and configuration on the vehicle
Cameras - detect flying objects approaching the platoon	-Verify the camera's performance (e.g., range, precision, resolution, bandwidth) -Verify the functionality of the cameras in accordance with the system requirements -Inject the cameras with problematic detection inputs that could trigger hazardous behavior -Perform in-the-loop testing on applicable scenarios and use cases (e.g., HIL, SIL, MIL) -Perform sensor testing under different operating conditions (e.g., weather, lighting, traffic) -Perform accelerated life testing on the cameras -Perform testing on a degraded camera -Verify camera alignment and configuration on the vehicle
Steering wheel sensors (e.g., grip strength detection) - detects the driver's grip on the steering wheel	-Verify the sensor's performance (e.g., precision) -Verify the functionality of the sensors in accordance with the system requirements -Inject the sensor with problematic detection inputs that could trigger hazardous behavior -Perform in-the-loop testing (e.g., HIL, SIL, MIL) -Perform sensor testing under different grip strengths -Perform accelerated life testing on the sensors -Perform testing on a degraded sensor -Verify sensor calibration on the vehicle
Tire pressure monitoring sensors - detect tire pressure in vehicles.	-Verify the sensor's performance (e.g., range, precision, resolution, bandwidth) -Verify the functionality of the sensors in accordance with the system requirements -Inject the sensor with problematic detection inputs that could trigger hazardous behavior -Perform in-the-loop testing on applicable scenarios and use cases (e.g., HIL, SIL, MIL) -Perform sensor testing under different operating conditions (e.g., weather, lighting, traffic). -Perform accelerated life testing on the sensors -Perform testing on a degraded sensor -Verify sensor alignment and configuration on the vehicle
Driver monitoring system - monitors the driver's attentiveness and fatigue.	-Verify the camera's performance (e.g., range, precision, resolution, bandwidth) -Verify the functionality of the camera in accordance with the system requirements -Inject the camera with problematic detection inputs that could trigger hazardous behavior -Perform in-the-loop testing on applicable scenarios and use cases (e.g., HIL, SIL, MIL) -Perform sensor testing under different operating conditions (e.g., lighting, driver clothing (hats)) -Perform accelerated life testing on the cameras -Perform testing on a degraded camera -Verify camera alignment and configuration on the vehicle
Exhaust fume monitoring equipment - monitor exhaust fumes being exposed to the drivers of the FVs in the platoon.	- Verify the functionality of the monitoring equipment in accordance with the system requirements (e.g., fume particulates, precision of detection, range of detection) -Test different detection capabilities under different weather and traffic conditions -Verify the monitoring functions as expected when fully integrated within the platooning vehicle -Test the interface connection to the EMS ECU for data collection -Verify the monitoring equipment sends a message to the ECU when the fume detection limit has been exceeded -Perform testing on closed course with another platooning vehicle
Steering actuator - activates the steering wheel to control the vehicle's motion. (3VL2 system only)	- Verify the functionality of the sensors in accordance with the system requirements (e.g., precision, resolution, timing constraints, bandwidth) -Verify the actuator functions as expected when fully integrated within the platooning vehicle -Test the actuator under different environmental conditions (e.g., hot/cold temperatures, high/low levels of precipitation, high/low levels of humidity) -Test different amounts of loading conditions (e.g., change from minimum to maximum load) -Perform accelerated life testing to determine the aging effects -Perform in-the-loop testing on applicable scenarios and use cases (e.g., HIL, SIL) -Perform vehicle level testing on a closed course.

Platooning System Components and Elements and Their Function	Verification Activities
Accelerator actuator - activates the accelerator when commanded by the EMS ECU	- Verify the functionality of the sensors in accordance with the system requirements (e.g., precision, resolution, timing constraints, bandwidth) -Verify the actuator functions as expected when fully integrated within the platooning vehicle -Test the actuator under different environmental conditions (e.g., hot/cold temperatures, high/low levels of precipitation, high/low levels of humidity) -Test different amounts of loading conditions (e.g., change from minimum to maximum load) -Perform accelerated life testing to determine the aging effects -Perform in-the-loop testing on applicable scenarios and use cases (e.g., HIL, SIL) -Perform vehicle level testing on a closed course.
Electronic Logging Device (ELD) - monitors the driver's hours-of-service	-Verify the functionality of the ELD in accordance with the system requirements (e.g., size, form, function, performance, interoperability) -Test the interface connection to the EMS ECU for data collection.

Table 20. Validation Activities Described for Each of the System's Sub-Functions

Sub function #	Goal of Intended Platooning Function	Platooning System Components and Elements and Their Function	Validation Activities
1.1	Facilitate the sharing of information between vehicles to enable platooning through inter-vehicle communications.	● Inter-vehicle communication devices - transmit and receive messages between platooning vehicles ● EMS ECU - processes inter-vehicle communication messages ● EMS ECU Software - generates and decodes the inter-vehicle communication messages ● HMI - present platooning status information, vehicle status and driver status.	-Test to confirm system rejects inter-vehicle messages that fail to comply with the defined interface, are corrupted, or are deleted, erroneously transmitted (inserted), out of order, or outdated. -Test to confirm that HMI displays are accurate. -Confirm that HMI meets user expectations and is readable and understandable.
1.2	Facilitate the sharing of information between drivers for platooning operations.	● Inter-vehicle communication devices - transmit and receive messages between platooning vehicles ● Foot pedal (activates voice communication between drivers of platooning vehicles) ● EMS ECU - processes inter-vehicle communication messages ● EMS ECU Software - generates and decodes the inter-vehicle communication messages ● HMI - present platooning status information and driver alerts	-Test to confirm foot pedal output is in expected range for the boundaries of the physical limits of the pedal. -Test to confirm that foot pedal output does not exceed established boundaries. -Test to confirm system reacts correctly to foot pedal output out of established bounds. -Test to confirm system rejects inter-vehicle messages that fail to comply with the defined interface, are corrupted, or are deleted, erroneously transmitted (inserted), out of order, or outdated. -Test to confirm that HMI displays are accurate. -Confirm that HMI meets user expectations and is readable and understandable.
1.3	Maintain a safe following distance from non-platooning vehicles.	● Radar - detects vehicles ahead ● EMS ECU - serves as the interface between the radar and the HMI and processes the messages between them. ● EMS ECU Software - generates and decodes inter-vehicle communication messages. ● HMI - present platooning status information and driver alerts	-Test to confirm Radar detects both large and small vehicles, in defined operational envelope (particularly in worst case conditions). -Test to confirm system reacts correctly to Radar failures. -Test to confirm system rejects inter-vehicle messages that fail to comply with the defined interface, are corrupted, or are deleted, erroneously transmitted (inserted), out of order, or outdated. -Test to confirm that HMI displays are accurate. -Confirm that HMI meets user expectations and is readable and understandable.
1.4	Maintain positional awareness of the platoon	● Position information (e.g., GPS, digital mapping) - GPS provides the location of the vehicle in coordination, while the digital map provides a reference location. ● EMS ECU (expand to engine management system architecture) - interfaces with the GPS antenna and receives the digital map file. ● EMS ECU Software - executes the positional awareness software to determine if position can be maintained for platooning operations. ● HMI - notifies the driver when positional awareness cannot be maintained and displays status of platooning vehicles. ● Inter-vehicle communication devices - transmit and receive messages between platooning vehicles	-Test to confirm that system rejects GPS output indicating impossible changes in location. -Test to confirm that system reacts correctly to GPS failures. -Test to confirm system rejects inter-vehicle messages that fail to comply with the defined interface, are corrupted, or are deleted, erroneously transmitted (inserted), out of order, or outdated. -Test to confirm that HMI displays are accurate. -Confirm that HMI meets user expectations and is readable and understandable.
1.5	Maintain lane position	● Turn signal - creates a message on the CAN bus to indicate which direction the vehicle is seeking to merge to (left or right) ● Lane-keep assist cameras - detects lane markings ● EMS ECU - serves as the interface for the information received from the CAN bus (positional information) and the lane-keep assist cameras. ● EMS ECU Software - the lane detection algorithm ● HMI - notifies the driver that the vehicle is drifting via alerts and/or haptics.	-Test to confirm system reacts correctly to user control inputs (turning) that conflict with turn signal indication (i.e., system alerts user or otherwise reacts if the user has a right turn signal on and moves leftward). -Test to confirm lane-keep cameras detect partial obscured markings and still function at the boundaries of the operational envelope. -Test to confirm the system reacts correctly to loss of turn-signal or lane-keep assist cameras function. -Test to confirm system rejects inter-vehicle messages that fail to comply with the defined interface, are corrupted, or are deleted, erroneously transmitted (inserted), out of order, or outdated.

Sub function #	Goal of Intended Platooning Function	Platooning System Components and Elements and Their Function	Validation Activities
			-Test to confirm that HMI displays are accurate. -Confirm that HMI meets user expectations and is readable and understandable.
1.6	Maintain a safe distance away from infrastructure	● Radar - detects infrastructure components ahead of the vehicle ● Sensors - detects infrastructure components in-front of and around the vehicle (e.g., LIDAR) ● Cameras - detects infrastructure signs and components in-front of and around the vehicle. ● EMS ECU - serves as the interface between the radar, sensors and cameras and executes the software. ● EMS ECU Software - contains system knowledge about the locations and details of infrastructure components (e.g., digital map). The software also processes the detection inputs from the radar, sensors and cameras onboard the vehicle. ● HMI - alerts the driver when the vehicle is approaching at close proximity to an infrastructure component ● Inter-vehicle communication devices - transmit and receive messages between platooning vehicles	-Test to confirm radar detects both large and small vehicles, in defined operational envelope (particularly in worst case conditions). -Test to confirm system reacts correctly to radar failures. -Test to confirm system reacts correctly to sensor or camera failures. -Test to confirm system rejects inter-vehicle messages that fail to comply with the defined interface, are corrupted, or are deleted, erroneously transmitted (inserted), out of order, or outdated. -Test to confirm that HMI displays are accurate. -Confirm that HMI meets user expectations and is readable and understandable.
1.7	Coordinate and maintain speed control	● Inter-vehicle communication devices - transmits and receives steering control messages between vehicles in the platoon. ● Radar or other sensors - detects between the front of the vehicle and vehicle ahead. ● EMS - adjust fuel delivery/supply or applies braking to control the vehicle's speed. ● EMS ECU - interfaces with the inter-vehicle communication devices to receive messages from other platooning vehicles, interfaces with the radar/sensors to compare position information sent from the CAN with a distance measurement of the radar. ● EMS ECU Software - executes the speed control algorithm with the values it received from the inter-vehicle communication messages and the radar/sensors to determine if an alert should be issued and if an alert should be presented to the drivers or when to apply a speed set point to the speed control system. ● HMI - notifies the driver that the vehicle is in platooning mode once speed control is maintained and coordinated with the other platooning vehicles. Allows setting or establishing of platooning gap distance and speed set point.	-Test to confirm Radar detects both large and small vehicles, in defined operational envelope (particularly in worst case conditions). -Test to confirm system reacts correctly to Radar failures. -Test to confirm system reacts correctly to sensor or camera failures. -Test to confirm system rejects inter-vehicle messages that fail to comply with the defined interface, are corrupted, or are deleted, erroneously transmitted (inserted), out of order, or outdated. -Test to confirm that HMI displays are accurate. -Confirm that HMI meets user expectations and is readable and understandable.
1.8	Coordinate steering control	● Inter-vehicle communication devices - transmits and receives steering control messages between vehicles in the platoon. ● Steering actuator - activates the steering wheel to control the vehicle's motion. ● EMS system - directly interfaces with the inter-vehicle communication devices and processes the coordinating steering software algorithm. ● EMS software - it executes the following distance algorithm with the values received by the system to determine if an alert should be issued and if an alert should be presented to the drivers. ● HMI - notifies the driver that the vehicle's steering control is being coordinated with the vehicle ahead in the platoon. ● Lane marking sensors, vehicle detection sensors	-Test to confirm steering wheel output is in expected range for the boundaries of the physical limits of the wheel. -Test to confirm that steering wheel output does not exceed established boundaries. -Test to confirm system reacts correctly to steering wheel output out of established bounds. -Test to confirm system rejects inter-vehicle messages that fail to comply with the defined interface, are corrupted, or are deleted, erroneously transmitted (inserted), out of order, or outdated. -Test to confirm that HMI displays are accurate. -Confirm that HMI meets user expectations and is readable and understandable.
1.9	Detect and handle cut-ins	● Radar - The CMS radar is used to detect vehicles merging in front of the FVs.	-Test to confirm radar detects both large and small vehicles, in defined operational envelope (particularly in

Sub function #	Goal of Intended Platooning Function	Platooning System Components and Elements and Their Function	Validation Activities
		● Inter-vehicle communication devices - transmit and receive messages between platooning vehicles. ● EMS - interfaces with the CMS radar to receive the detection input for the Speed Control System software. The Speed Control System will process the HMI alert message through the inter-vehicle communication devices. ● EMS Software - the cut-in detection algorithm determines when a cut-in is occurring. ● HMI - alerts the driver when a vehicle is attempting a cut-in and notifies the other drivers in the platoon that a cut-in is in process, or that the platoon has been dissolved.	worst case conditions). -Test to confirm system reacts correctly to Radar failures. -Test to confirm system reacts correctly to sensor or camera failures. -Test to confirm system rejects inter-vehicle messages that fail to comply with the defined interface, are corrupted, or are deleted, erroneously transmitted (inserted), out of order, or outdated. -Test to confirm that HMI displays are accurate. -Confirm that HMI meets user expectations and is readable and understandable.
1.10	Detect evasive steering maneuvers	● Position information (e.g., GPS, digital mapping) - serves as a redundant input for detecting lateral position with respect to the vehicle's speed. ● Accelerometer - serves as an input to determine lateral acceleration ● Steering wheel - serves as an input to measure evasive steering maneuvers ● Steering actuator - activates the steering wheel to control the vehicle's motion. ● EMS ECU - directly interfaces with the positional information, accelerometer data, and steering wheel turn radius data inputs, processes the software ● Inter-vehicle communication devices - relay information between platooning vehicles ● EMS ECU Software - executes the algorithm with the values received by the EMS ECU to determine if an alert should be issued and if an alert should be presented to the drivers ● HMI - provides an alert to the driver	-Test to confirm that system rejects GPS output indicating impossible changes in location. -Test to confirm that system reacts correctly to GPS failures. -Test to confirm that accelerometer output does not exceed established boundaries. -Test to confirm system reacts correctly to accelerometer output out of established bounds. -Test to confirm steering wheel output is in expected range for the boundaries of the physical limits of the wheel. -Test to confirm that steering wheel output does not exceed established boundaries. -Test to confirm system reacts correctly to steering wheel output out of established bounds. -Test to confirm system rejects inter-vehicle messages that fail to comply with the defined interface, are corrupted, or are deleted, erroneously transmitted (inserted), out of order, or outdated. -Test to confirm that HMI displays are accurate. -Confirm that HMI meets user expectations and is readable and understandable.
1.11	Detect static road debris	● Sensors - detect static objects approaching the platoon ● Cameras - detect flying objects approaching the platoon ● Inter-vehicle communication devices - transmits and receives braking control messages between vehicles in the platoon. ● EMS ECU - serves as the interface between the sensors and cameras for detecting and processing static objects. The EMS ECU also interfaces with the inter-vehicle communication devices to send and receive messages. ● EMS ECU Software - it processes the vehicle inputs and executes the static object detection algorithm. ● HMI - alerts the driver of a static object detection.	-Test to confirm system reacts correctly to sensor or camera failures. -Test to confirm system rejects inter-vehicle messages that fail to comply with the defined interface, are corrupted, or are deleted, erroneously transmitted (inserted), out of order, or outdated. -Test to confirm that HMI displays are accurate. -Confirm that HMI meets user expectations and is readable and understandable.
1.12	Detect flying objects approaching a platooning vehicle.	● Sensors - detect static objects approaching the platoon ● Cameras - detect flying objects approaching the platoon ● Inter-vehicle communication devices - transmits and receives braking control messages between vehicles in the platoon. ● EMS ECU - serves as the interface between the sensors and cameras for detecting and processing static objects. The EMS ECU also interfaces with the inter-vehicle communication devices to send and receive messages. ● EMS ECU Software - it processes the vehicle inputs and executes the static object detection algorithm.	-Test to confirm system reacts correctly to sensor or camera failures. -Test to confirm system rejects inter-vehicle messages that fail to comply with the defined interface, are corrupted, or are deleted, erroneously transmitted (inserted), out of order, or outdated. -Test to confirm that HMI displays are accurate. -Confirm that HMI meets user expectations and is readable and understandable.

Sub function #	Goal of Intended Platooning Function	Platooning System Components and Elements and Their Function	Validation Activities
		● HMI - alerts the driver of a static object detection.	
1.13	Blind spot detection	● Radar - The radar on the side of the tractor is used to detect vehicles traveling alongside the vehicle. ● EMS ECU - interfaces with the radar to receive the detection input for the EMS ECU software. The EMS ECU will process this input and generate an alert based on the EMS ECU software. ● EMS ECU Software - the blind spot detection algorithm determines when an alert should be presented. ● HMI - alerts the driver when a vehicle is approaching from the platooning vehicle's blind spot while it has intent to change lanes.	-Test to confirm Radar detects both large and small vehicles, in defined operational envelope (particularly in worst case conditions). -Test to confirm system reacts correctly to Radar failures. -Test to confirm system rejects inter-vehicle messages that fail to comply with the defined interface, are corrupted, or are deleted, erroneously transmitted (inserted), out of order, or outdated. -Test to confirm that HMI displays are accurate. -Confirm that HMI meets user expectations and is readable and understandable.
2.1	Enforce geographical location of the ODD	● Position information (e.g., GPS, digital mapping) - GPS provides the location of the vehicle in coordination, while the digital map provides a reference location. ● EMS ECU - interfaces with the GPS antenna and received and the digital map file. ● EMS ECU Software - executes the positional awareness software to determine if position can be maintained for platooning operations. ● HMI - notifies the driver when positional awareness cannot be maintained.	-Test to confirm that system rejects GPS output indicating impossible changes in location. -Test to confirm that system reacts correctly to GPS failures. -Test to confirm system rejects inter-vehicle messages that fail to comply with the defined interface, are corrupted, or are deleted, erroneously transmitted (inserted), out of order, or outdated. -Test to confirm that HMI displays are accurate. -Confirm that HMI meets user expectations and is readable and understandable.
2.2	Enforce roadway grade of the ODD	● Positional information (e.g., GPS, digital mapping) - GPS provides the location of the vehicle in coordination, while the digital map provides a reference location. ● EMS ECU - interfaces with the GPS antenna and received and the digital map file. ● EMS ECU Software - executes the digital map file with the GPS input to determine the roadway grade where the platoon is located. ● HMI - notifies the driver when positional awareness cannot be maintained.	-Test to confirm that system rejects GPS output indicating impossible changes in location. -Test to confirm that system reacts correctly to GPS failures. -Test to confirm system rejects inter-vehicle messages that fail to comply with the defined interface, are corrupted, or are deleted, erroneously transmitted (inserted), out of order, or outdated. -Test to confirm that HMI displays are accurate. -Confirm that HMI meets user expectations and is readable and understandable.
2.3	Enforce roadway curvature of the ODD	● Positional information (e.g., GPS, digital mapping) - GPS provides the location of the vehicle in coordination, while the digital map provides a reference location. ● EMS ECU - interfaces with the GPS antenna and received and the digital map file. ● EMS ECU Software - executes the digital map file with the GPS input to determine the roadway grade where the platoon is located. The ESC algorithm is also executed on the Brake ECU. ● HMI - notifies the driver when positional awareness cannot be maintained.	-Test to confirm that system rejects GPS output indicating impossible changes in location. -Test to confirm that system reacts correctly to GPS failures. -Test to confirm system rejects inter-vehicle messages that fail to comply with the defined interface, are corrupted, or are deleted, erroneously transmitted (inserted), out of order, or outdated. -Test to confirm that HMI displays are accurate. -Confirm that HMI meets user expectations and is readable and understandable.
2.4	Enforce roadway or infrastructure features of the ODD	● Positional information (e.g., GPS, digital mapping) - GPS provides the location of the vehicle in coordination, while the digital map provides a reference location. ● V2I communication - the system will receive over-the-air updates in regions where temporary changes are being made to the infrastructure (e.g., work zones) ● Driver monitoring system - monitors the drivers attentiveness and fatigue. ● EMS ECU - interfaces with the GPS antenna and received and the digital map file. ● EMS ECU Software - executes the digital map file with the GPS input to determine the roadway grade where the platoon is located.	-Test to confirm that system rejects GPS output indicating impossible changes in location. -Test to confirm that system reacts correctly to GPS failures. -Test to confirm system rejects V2I messages that fail to comply with the defined interface, are corrupted, or are deleted, erroneously transmitted (inserted), out of order, or outdated. -Test to confirm that driver monitoring system ensures accurate entry of start and stop times, attentiveness monitoring does adversely impact other system functions, and does not produce false alerts/alarms. -Test to confirm system rejects inter-vehicle messages that fail to comply with the defined interface, are

Sub function #	Goal of Intended Platooning Function	Platooning System Components and Elements and Their Function	Validation Activities
		● HMI - notifies the driver when the driver is not being attentive or is fatigued. The HMI also notifies the driver when there is an upcoming roadway or infrastructure feature is ahead and when the platoon is dissolved until the feature is no longer in the path of travel.	corrupted, or are deleted, erroneously transmitted (inserted), out of order, or outdated. -Test to confirm that HMI displays are accurate. -Confirm that HMI meets user expectations and is readable and understandable.
2.5	Enforce pavement conditions of the ODD	● EMS ECU - interfaces with the GPS antenna and received and the digital map file. ● EMS ECU Software - executes to detect wet pavement conditions. ● HMI - notifies the driver when the driver is not being attentive or is fatigued. The HMI also notifies the driver when there are wet pavement conditions and when the platoon is dissolved.	-Test to confirm system rejects inter-vehicle messages that fail to comply with the defined interface, are corrupted, or are deleted, erroneously transmitted (inserted), out of order, or outdated. -Test to confirm that HMI displays are accurate. -Confirm that HMI meets user expectations and is readable and understandable.
2.6	Enforce weather conditions of the ODD	● Sensors - detects precipitation in-front of and around the vehicle ● V2I communication - enables over-the-air updates to receive periodic weather updates ● EMS ECU - interfaces with the GPS antenna and received and the digital map file. ● EMS ECU Software - executes the weather detection algorithm to determine when HMI notifications should be issued. ● HMI - notifies the driver of current and upcoming weather conditions that are restricted by the ODD.	-Test to confirm system reacts correctly to sensor or camera failures. -Test to confirm system rejects V2I messages that fail to comply with the defined interface, are corrupted, or are deleted, erroneously transmitted (inserted), out of order, or outdated. -Test to confirm system rejects inter-vehicle messages that fail to comply with the defined interface, are corrupted, or are deleted, erroneously transmitted (inserted), out of order, or outdated. -Test to confirm that HMI displays are accurate. -Confirm that HMI meets user expectations and is readable and understandable.
3.1	Monitor and enforce driver's hours-of-service	● ELD - monitors the driver's hours-of-service ● Inter-vehicle communication devices - communicates hours-of-service between drivers when one driver exceeds the hours of service limit ● EMS ECU - serves as the interface between the ELD and the EMS ECU software. ● EMS ECU Software - integrated with the ELD, the hours-of-service algorithm uses the input from the ELD in all vehicles to determine which notifications should be given and to which drivers. ● HMI - notifies the drivers of the hours-of-service limit	-Test to confirm that driver monitoring system ensures accurate entry of start and stop times, attentiveness monitoring does adversely impact other system functions, and does not produce false alerts/alarms. -Test to confirm system rejects inter-vehicle messages that fail to comply with the defined interface, are corrupted, or are deleted, erroneously transmitted (inserted), out of order, or outdated. -Test to confirm that HMI displays are accurate. -Confirm that HMI meets user expectations and is readable and understandable.
3.2	Ensure the drivers are operating the platoon with full attentiveness	● Driver monitoring system - monitors the drivers' attentiveness and fatigue. ● Steering wheel sensors (e.g., grip strength detection) - detects the driver's grip on the steering wheel ● Inter-vehicle communication devices - communicates driver attentiveness and fatigue status to other vehicle in the platoon ● EMS ECU - serves as the interface for collecting input data from the driver monitoring system and steering wheel sensors for the EMS ECU software. The EMS ECU is also the interface between the inter-vehicle communication devices in platooning vehicles. ● EMS ECU Software - algorithms for ensuring driver alertness. ● HMI - notifies the drivers of inattentiveness and fatigue	-Test to confirm that driver monitoring system ensures accurate entry of start and stop times, attentiveness monitoring does adversely impact other system functions, and does not produce false alerts/alarms. -Test to confirm system reacts correctly to sensor or camera failures. -Test to confirm system rejects inter-vehicle messages that fail to comply with the defined interface, are corrupted, or are deleted, erroneously transmitted (inserted), out of order, or outdated. -Test to confirm that HMI displays are accurate. -Confirm that HMI meets user expectations and is readable and understandable.
4.1	Ensures the vehicle's tire pressure is acceptable for platooning conditions.	● Tire pressure monitoring sensors - detect tire pressure in vehicles ● Inter-vehicle communication devices - communicate tire pressure information between all vehicles in the platoon ● EMS ECU - serves as the interface between the tire pressuring monitoring sensors and the software. The EMS ECU also interfaces with the inter-vehicle communication devices and processes the messages. ● EMS ECU Software - executes the tire pressure	-Test to confirm system reacts correctly to sensor failures. -Test to confirm system rejects inter-vehicle messages that fail to comply with the defined interface, are corrupted, or are deleted, erroneously transmitted (inserted), out of order, or outdated. -Test to confirm that HMI displays are accurate. -Confirm that HMI meets user expectations and is readable and understandable.

Sub function #	Goal of Intended Platooning Function	Platooning System Components and Elements and Their Function	Validation Activities
		notification algorithm to determine if a notification should be issued. ● HMI - notifies the driver of the current state of the tire pressure	
4.2	Ensures the driver is not being exposed to excessive amounts of exhaust fumes	● Exhaust fume monitoring equipment - monitor exhaust fumes being exposed to the drivers of the FVs in the platoon. ● Inter-vehicle communication devices - communicate exhaust fume levels of exposure between all vehicles in the platoon ● EMS ECU - serves as the interface between the exhaust fume monitoring equipment and the EMS ECU software. The EMS ECU also interfaces with the inter-vehicle communication devices and processes the messages. ● EMS ECU Software - processes data from exhaust fume monitoring to ensure adequate spacing is maintained. ● HMI - notifies the driver when an unsafe level of exhaust fumes has been exposed to the driver	-Test to confirm system reacts correctly to sensor failures. -Test to confirm system rejects inter-vehicle messages that fail to comply with the defined interface, are corrupted, or are deleted, erroneously transmitted (inserted), out of order, or outdated. -Test to confirm that HMI displays are accurate. -Confirm that HMI meets user expectations and is readable and understandable.
5.1	To allow manual override by any of the drivers in the platoon at any time while platooning	● Accelerator actuator - activates the accelerator when commanded by the EMS ECU ● Brake actuator - activates the brakes when commanded by the EMS ECU ● Inter-vehicle communication devices - ● EMS ECU - transmits messages indicating that platoon is being deactivated. ● EMS ECU Software - executes algorithms to cease platooning. ● HMI - Indicates platooning status, allows for cessation of platooning.	-Test to confirm operator can immediately take over operation at any point (normal operation, on startup, after cessation of platooning), and that takeover control inputs override the platooning system until the user reestablishes the platoon. -Test to confirm system rejects inter-vehicle messages that fail to comply with the defined interface, are corrupted, or are deleted, erroneously transmitted (inserted), out of order, or outdated. -Test to confirm that HMI displays are accurate. -Confirm that HMI meets user expectations and is readable and understandable.

APPENDIX D: Fault Tree Analysis

The following sections describe each of the four hazards selected for the FTA.

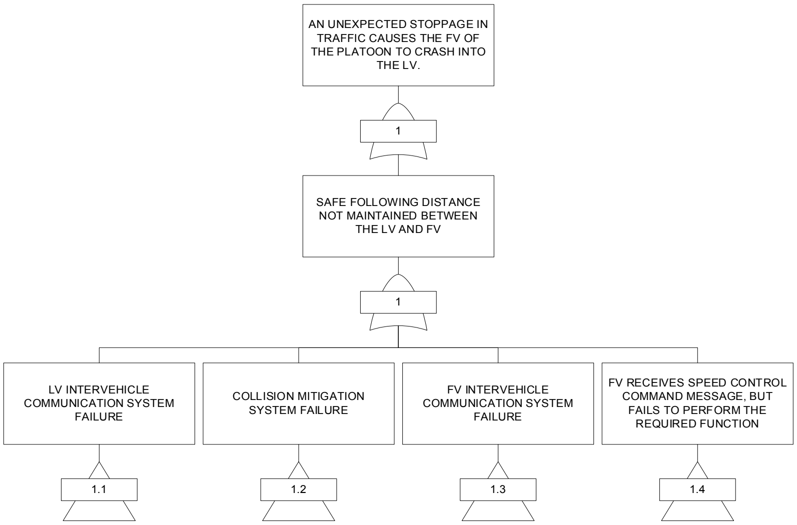
Fault Tree 1 – An Unexpected Stoppage in Traffic Causes the FV of the Platoon to Crash into the LV.

Table 21 summarizes each of the events that comprise of Fault Tree 1. The architecture of the high-level events that may cause the FV of the platoon to crash into the LV in the event of an unexpected stoppage in traffic are shown in **Figure 8**. The lower level events for this fault tree are illustrated in **Figure 9**, **Figure 10**, and **Figure 11**.

Table 21. Event Descriptions for Fault Tree 1

Fault Tree Event ID	Fault Tree Event Description
1	An unexpected stoppage in traffic causes the FV of the platoon to crash into the LV.
1	Safe following distance is not maintained between the LV and FV.
1.1	LV inter-vehicle communication system failure
1.1.1	Internal ECU component failure in LV
1.1.2	Software fails to generate speed control command message (to be sent to FV)
1.1.3	Software fails to transmit speed control command message to the FVs
1.1.4	Inter-vehicle communication device fails to transmit message to FV inter-vehicle communication device
1.2	CMS failure
1.2.1	Radar failure
1.2.2	CMS processor failure
1.2.3	CMS software failure
1.2.4	EMS failure
1.2.4.1	EMS software failure
1.2.4.2	Speed control failure
1.2.4.3	Engine brake failure
1.2.5	Brake system failure
1.2.5.1	Brake system software failure
1.2.5.2	Foundation brake failure
1.3	FV inter-vehicle communication system failure
1.3.1	Internal ECU component failure in FV
1.3.2	Inter-vehicle communication device fails to receive speed command message sent from LV
1.3.3	Inter-vehicle communication device fails to transmit steering command message to ECU

Fault Tree Event ID	Fault Tree Event Description
1.3.4	Software fails to decode steering command message sent from LV
1.4	FV receives speed control command from LV, but fails to act in response
1.4.1	Message is never transmitted to ECU
1.4.2	ECU hardware failure
1.4.3	EMS failure
1.4.3.1	EMS software failure
1.4.3.2	Speed control failure
1.4.3.3	Engine brake failure
1.4.4	Brake system failure
1.4.4.1	Brake system software failure
1.4.4.2	Foundation brake failure

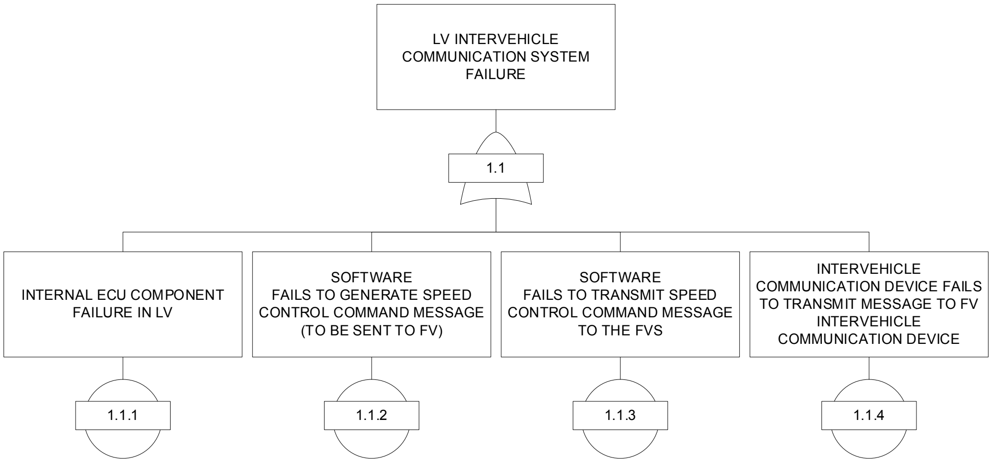

AN UNEXPECTED STOPPAGE IN TRAFFIC CAUSES THE FV OF THE PLATOON TO CRASH INTO THE LV.
1
SAFE FOLLOWING DISTANCE NOT MAINTAINED BETWEEN THE LV AND FV
1
LV INTERVEHICLE COMMUNICATION SYSTEM FAILURE
COLLISION MITIGATION SYSTEM FAILURE
FV INTERVEHICLE COMMUNICATION SYSTEM FAILURE
FV RECEIVES SPEED CONTROL COMMAND MESSAGE, BUT FAILS TO PERFORM THE REQUIRED FUNCTION
1.1
1.2
1.3
1.4

Source: Battelle

Figure 8. There Is an Unexpected Stoppage in Traffic (1).

Figure 8 illustrates the top logic gate for the first hazard considered – "*There is an unexpected stoppage in traffic (1.0)*". The end result of this hazard is that a FV of the platoon would crash into the LV. The main fault leading to this hazard fault would be that a safe following distance was not maintained between the LV and FV. This fault was broken into four second-level events.

LV INTER-VEHICLE COMMUNICATION SYSTEM FAILURE (1.1)


LV INTERVEHICLE COMMUNICATION SYSTEM FAILURE
1.1
INTERNAL ECU COMPONENT FAILURE IN LV
SOFTWARE FAILS TO GENERATE SPEED CONTROL COMMAND MESSAGE (TO BE SENT TO FV)
SOFTWARE FAILS TO TRANSMIT SPEED CONTROL COMMAND MESSAGE TO THE FVS
INTERVEHICLE COMMUNICATION DEVICE FAILS TO TRANSMIT MESSAGE TO FV INTERVEHICLE COMMUNICATION DEVICE
1.1.1
1.1.2
1.1.3
1.1.4

Source: Battelle

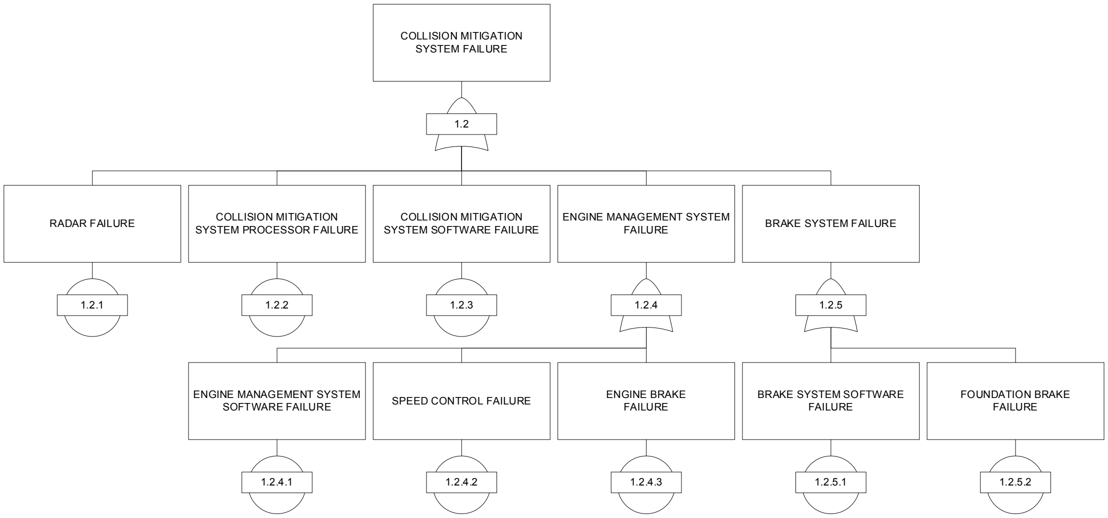
Figure 9. LV Inter-vehicle Communication System Failure (1.1).

Both the LV and FV, as part of their platooning subsystem, communicate with each other via an inter-vehicle communication system. This system is made up of hardware for creating, sending and receiving messages between the two vehicles. Data shared between the platooning vehicles includes speed and positional data, which is used by the ACC system to maintain a safe following distance. A failure of the communication system will lead to the FV's inability to maintain a safe following distance, resulting in the potential top-level hazard of a collision with the LV during an unexpected stoppage in traffic.

Failure of the LV inter-vehicle communication system can be caused by the following events shown in **Figure 9**:

- Internal ECU component failure
- Software fails to generate speed control command message (sent to FVs)
- Software fails to transmit speed control command message (sent to FVs)
- Communication device failure (fails to transmit message to FVs' communication devices)

CMS FAILURE (1.2)


COLLISION MITIGATION SYSTEM FAILURE
1.2
RADAR FAILURE
COLLISION MITIGATION SYSTEM PROCESSOR FAILURE
COLLISION MITIGATION SYSTEM SOFTWARE FAILURE
ENGINE MANAGEMENT SYSTEM FAILURE
BRAKE SYSTEM FAILURE
1.2.1
1.2.2
1.2.3
1.2.4
1.2.5
ENGINE MANAGEMENT SYSTEM SOFTWARE FAILURE
SPEED CONTROL FAILURE
ENGINE BRAKE FAILURE
BRAKE SYSTEM SOFTWARE FAILURE
FOUNDATION BRAKE FAILURE
1.2.4.1
1.2.4.2
1.2.4.3
1.2.5.1
1.2.5.2

Source: Battelle

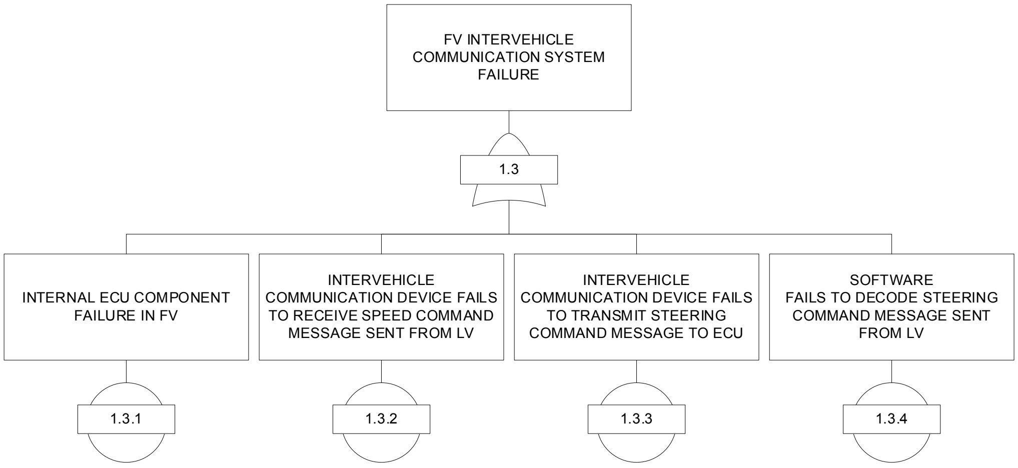
Figure 10. CMS Failure (1.2).

CMSs are forward-looking, radar-based systems comprised of collision warning and adaptive cruise control with active braking. The failure of the CMS can be due to collision warning detection failure, component failure and ACC (engine and/or brake control) failure. ACC failure is made up of a number of tertiary-level events.

Failure of the CMS can be caused by the following events shown in **Figure 10**:

- Radar failure
- CMS processor or electronic component failure
- CMS software failure
- Engine Management System failure caused by:
  - Engine Management System software failure
  - Speed control failure
  - Engine brake failure
- Brake system failure caused by
  - Brake system software failure
  - Foundation brake failure

FV INTER-VEHICLE COMMUNICATION SYSTEM FAILURE (1.3)

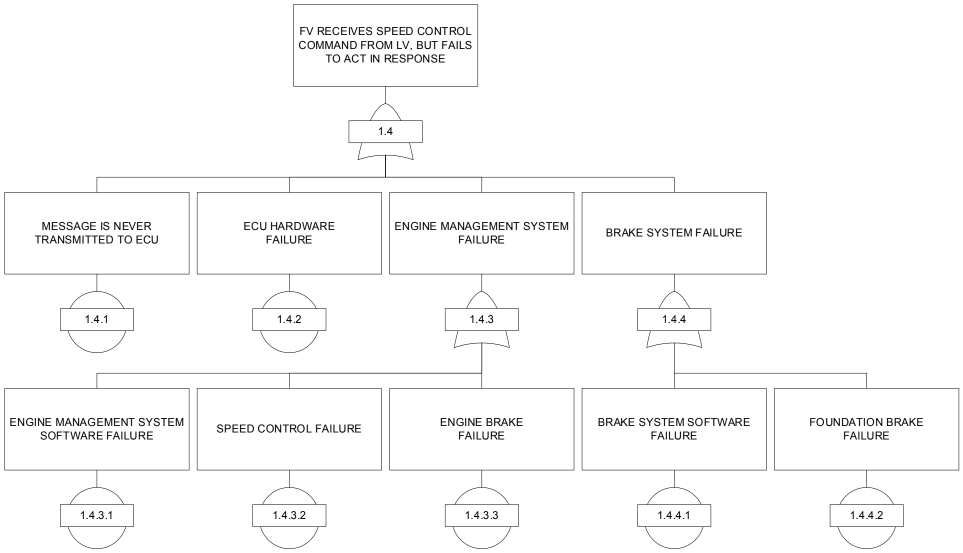

FV INTERVEHICLE COMMUNICATION SYSTEM FAILURE
1.3
INTERNAL ECU COMPONENT FAILURE IN FV
INTERVEHICLE COMMUNICATION DEVICE FAILS TO RECEIVE SPEED COMMAND MESSAGE SENT FROM LV
INTERVEHICLE COMMUNICATION DEVICE FAILS TO TRANSMIT STEERING COMMAND MESSAGE TO ECU
SOFTWARE FAILS TO DECODE STEERING COMMAND MESSAGE SENT FROM LV
1.3.1
1.3.2
1.3.3
1.3.4

Source: Battelle

Figure 11. FV Inter-vehicle Communication System Failure (1.3).

See section LV INTER-VEHICLE COMMUNICATION SYSTEM FAILURE (1.1) above.

FV RECEIVES SPEED CONTROL COMMAND MESSAGE, BUT FAILS TO PERFORM THE REQUIRED FUNCTION (1.4)


FV RECEIVES SPEED CONTROL COMMAND FROM LV, BUT FAILS TO ACT IN RESPONSE
1.4
MESSAGE IS NEVER TRANSMITTED TO ECU
ECU HARDWARE FAILURE
ENGINE MANAGEMENT SYSTEM FAILURE
BRAKE SYSTEM FAILURE
1.4.1
1.4.2
1.4.3
1.4.4
ENGINE MANAGEMENT SYSTEM SOFTWARE FAILURE
SPEED CONTROL FAILURE
ENGINE BRAKE FAILURE
BRAKE SYSTEM SOFTWARE FAILURE
FOUNDATION BRAKE FAILURE
1.4.3.1
1.4.3.2
1.4.3.3
1.4.4.1
1.4.4.2

Source: Battelle

Figure 12. FV Receives Speed Control Command Message, but Fails to Perform the Required Function (1.4).

This event is the result of all other platooning subsystems performing as designed – communication systems operating normally, CMS operating normally and at the point of the FV receiving a new speed control command message but then failing to perform whichever function is required (apply braking due to LV speed reduction, for example). Failure to perform a commanded function by the FV can also result in the top-level hazard of a collision with the LV during an unexpected stoppage in traffic.

There are two subsystem faults that could occur that lead to the 1.4 fault, the engine management system (EMS) fails or the brake system fails. These have tertiary-level events that could lead to their failure that will be enumerated below.

Failure to perform the required speed control function can be caused by the following events shown in **Figure 12**:

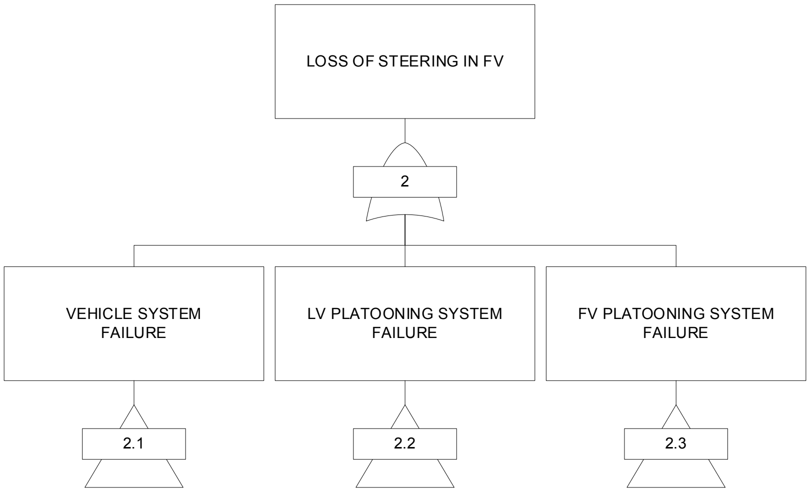
- Message is never transmitted to ECU
- ECU hardware failure
- EMS failure due to one of the following events:
    - EMS software failure
    - Speed control failure
    - Engine brake failure
- Brake system failure due to one of the following events:
    - Brake system software failure
    - Foundation brake failure

Fault Tree 2 – There Is a Loss of Steering in the FV.

Table 22 summarizes each of the events that comprise of Fault Tree 2. The architecture of the high-level events that may cause a loss of steering in the FV are shown in **Figure 13**. The lower level events for this fault tree are illustrated in **Figure 14**, **Figure 15**, and **Figure 16**.

Table 22. Event Descriptions for Fault Tree 2

Fault Tree Event ID	Fault Tree Event Description
2	Loss of steering in FV
2.1	Vehicle system failure
2.1.1	Steering column failure
2.1.1.1	Inadequate maintenance and inspection
2.1.1.2	Component failure
2.1.2	Steering tire blowout
2.1.2.1	Inadequate maintenance and inspection
2.1.2.2	Tire pressure sensor failure
2.1.2.3	Tire mechanical failure
2.1.3	Brake system failure
2.1.3.1	Inadequate maintenance and inspection
2.1.3.2	Component failure
2.2	LV platooning system failure
2.2.1	Internal ECU component failure
2.2.2	Software fails to generate steering command message
2.2.3	Software fails to transmit steering command message
2.2.4	Inter-vehicle communication device fails to transmit message to FV inter-vehicle communication device
2.3	FV platooning system failure
2.3.1	Internal ECU component failure
2.3.2	Inter-vehicle communication device fails to receive steering command message sent from LV
2.3.3	Inter-vehicle communication device fails to transmit steering command message to ECU
2.3.4	Software fails to decode steering command message sent from LV
2.3.5	Steering actuator fails to implement steering command message from LV

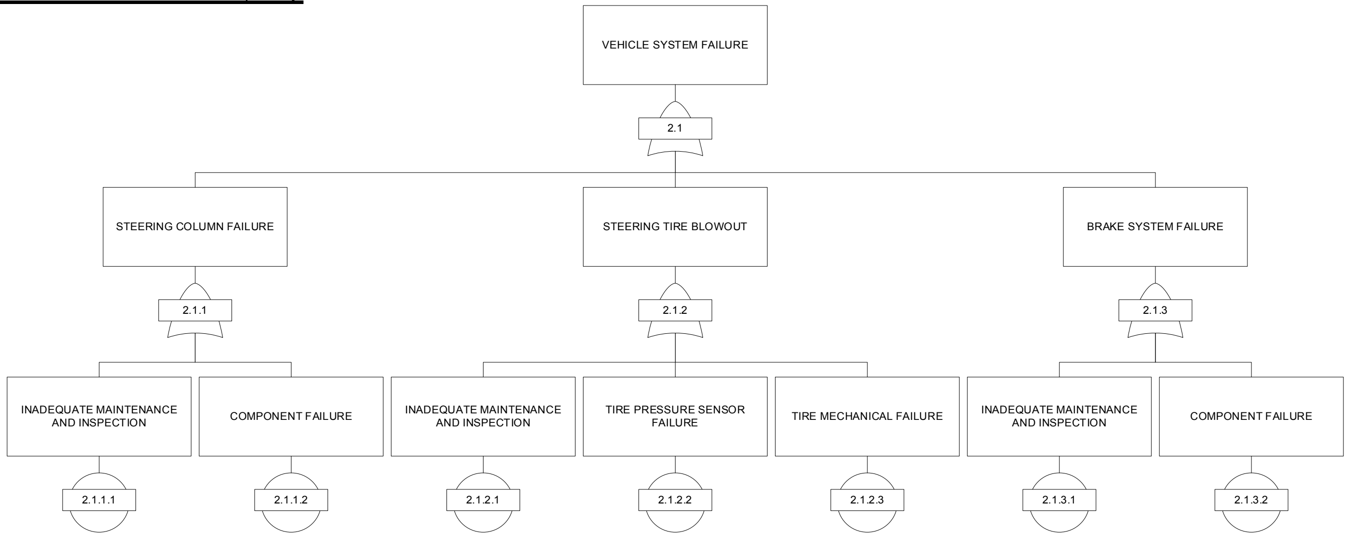


Source: Battelle

Figure 13. There Is a Loss of Steering Control in the FV (2).

Figure 13 shows the top logic gate for the next hazard considered – "*There is a loss of steering control in the FV*." This particular hazard only applies to the 3VL2 platooning system where there is both speed and steering control performed by the platooning system. The end results of this hazard are numerous but include a potential crash situation of the FV due to lack of steering. That crash could be a collision with the LV, with road infrastructure, or with another non-platooning vehicle. This fault was decomposed into three second-level faults described in the next section.

VEHICLE SYSTEM FAILURE (2.1)



Source: Battelle

Figure 14. Vehicle System Failure (2.1).

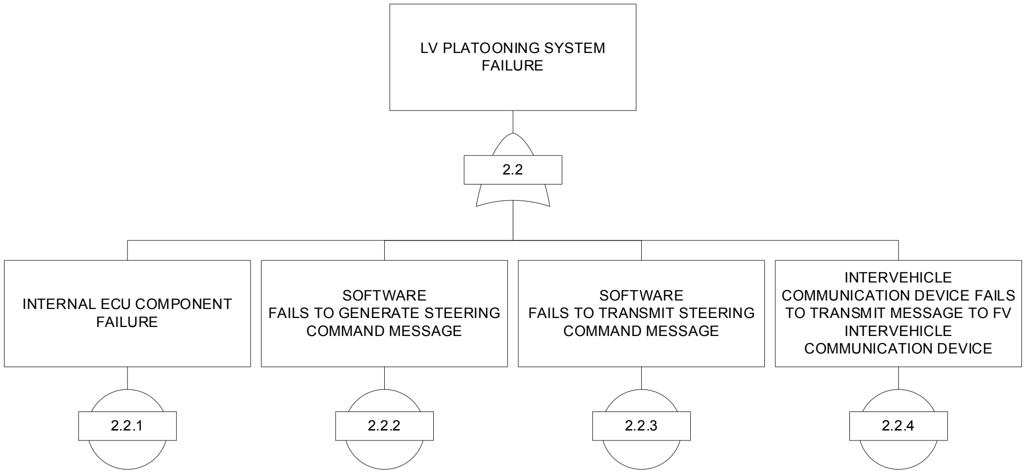
This fault is a roll-up of various truck subsystems that could fail and lead to the loss of steering control in the FV. While these subsystems are not a part of the platooning system under consideration, they are still necessary for the system to implement steering commands.

Vehicle System Failure can be caused by the following events shown in **Figure 14**:

- Steering column failure due to one of the following events:
  - Inadequate maintenance and inspection
  - Component failure (mechanical failure of actual steering column, for example)
- Steering tire blowout:
  - Inadequate maintenance and inspection
  - Tire pressure sensor failure
  - Tire mechanical failure

- Brake system failure:
    - Inadequate maintenance and inspection
    - Component failure (mechanical failure of brake pad, for example)

LV PLATOONING SYSTEM FAILURE (2.2)


LV PLATOONING SYSTEM FAILURE
2.2
INTERNAL ECU COMPONENT FAILURE
SOFTWARE FAILS TO GENERATE STEERING COMMAND MESSAGE
SOFTWARE FAILS TO TRANSMIT STEERING COMMAND MESSAGE
INTERVEHICLE COMMUNICATION DEVICE FAILS TO TRANSMIT MESSAGE TO FV INTERVEHICLE COMMUNICATION DEVICE
2.2.1
2.2.2
2.2.3
2.2.4

Source: Battelle

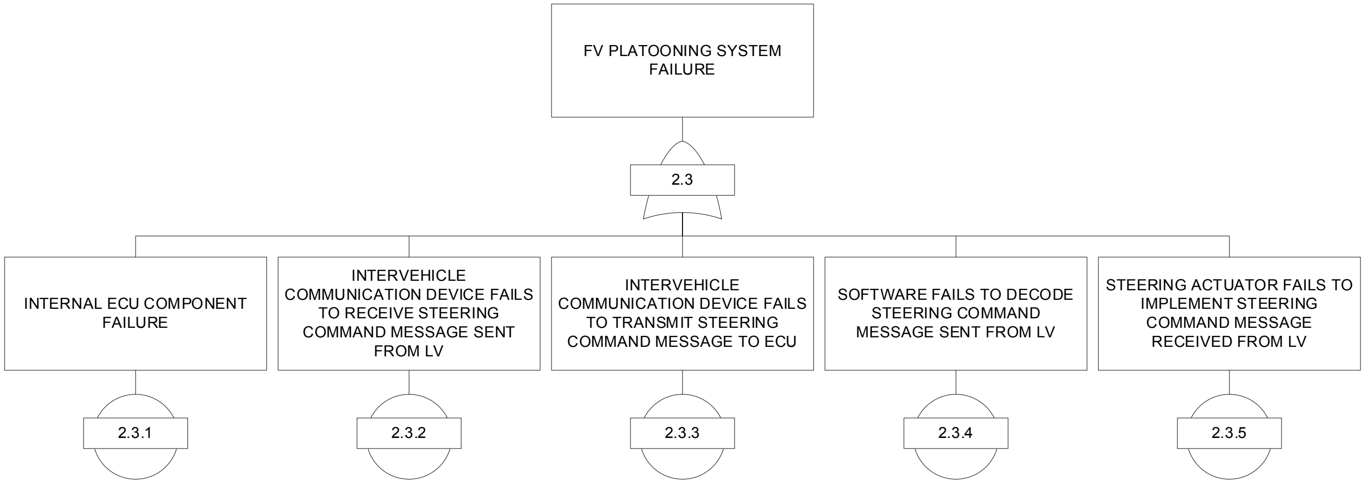
Figure 15. LV Platooning System Failure (2.2).

This fault considers the failures that could occur on the LV during the course of normal operation of the platoon. These failures are specifically concerned with the interaction between platooning vehicles during an event that would necessitate the FV to perform some type of steering function to maintain the platoon.

Failure to perform the required speed control function can be caused by the following events shown in **Figure 15**:

- Internal ECU component failure
- Platooning software fails to generate steering command message to send to the FV
- Software fails to send steering command message
- Inter-vehicle communication device fails to transmit message to FV inter-vehicle communication device

FV PLATOONING SYSTEM FAILURE (2.3)


FV PLATOONING SYSTEM FAILURE
2.3
INTERNAL ECU COMPONENT FAILURE
INTERVEHICLE COMMUNICATION DEVICE FAILS TO RECEIVE STEERING COMMAND MESSAGE SENT FROM LV
INTERVEHICLE COMMUNICATION DEVICE FAILS TO TRANSMIT STEERING COMMAND MESSAGE TO ECU
SOFTWARE FAILS TO DECODE STEERING COMMAND MESSAGE SENT FROM LV
STEERING ACTUATOR FAILS TO IMPLEMENT STEERING COMMAND MESSAGE RECEIVED FROM LV
2.3.1
2.3.2
2.3.3
2.3.4
2.3.5

Source: Battelle

Figure 16. FV Platooning System Failure (2.3).

This fault is similar to the 2.2 fault described earlier, only this fault is caused by failures on the FV that result in the inability to perform steering functions received from the LV, preventing the FVs from maintaining their position within the platoon.

Failure to perform the required speed control function can be caused by the following events shown in **Figure 16**:

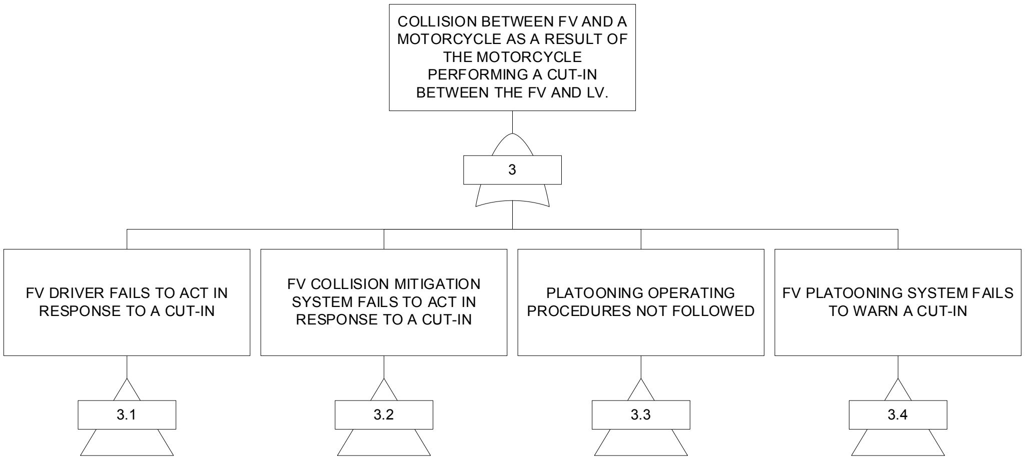
- Internal ECU component failure
- Inter-vehicle communication device fails to receive steering command message sent from LV
- Inter-vehicle communication device fails to transmit steering command message to ECU
- Software fails to decode steering command message sent from LV
- Steering actuator fails to implement steering command message received from LV

Fault Tree 3 – There Is a Collision Between the FV and a Motorcycle as a Result of the Motorcycle Performing a Cut-In Between the FV and the LV.

Table 23 summarizes each of the events that comprise of Fault Tree 3. The architecture of the high-level events that may cause a collision between the FV and a motorcycle as a result of the motorcycle performing a cut-in between the FV and the LV are shown in **Figure 17**. The lower level events for this fault tree are illustrated in **Figure 18**, **Figure 19**, **Figure 20**, and **Figure 21**.

Table 23. Event Descriptions for Fault Tree 3

Fault Tree Event ID	Fault Tree Event Description
3	Collision between FV and a motorcycle as a result of the motorcycle performing a cut-in between the FV and LV
3.1	FV driver fails to act in response to a cut-in
3.1.1	Lack of driver's training
3.1.1.1	Driver fails to identify a cut-in
3.1.1.2	Driver fails to disengage platoon
3.1.2	Distracted driving
3.1.3	Driver is inattentive
3.1.4	Driver is incapacitated
3.2	FV CMS fails to act in response to a cut-in
3.2.1	Radar failure
3.2.2	CMS processor failure
3.2.3	CMS software failure
3.2.4	EMS failure
3.2.4.1	EMS software failure
3.2.4.2	Speed control failure
3.2.4.3	Engine brake failure
3.2.5	Brake system failure
3.2.5.1	Brake system software failure
3.2.5.2	Foundation brake failure
3.3	Platooning operating procedures not followed
3.3.1	The vehicle with the best braking capability was in the LV position
3.4	FV platooning system fails to warn non-platooning vehicles of the platooning operations
3.4.1	Failure of the visible strobe on the platooning vehicle

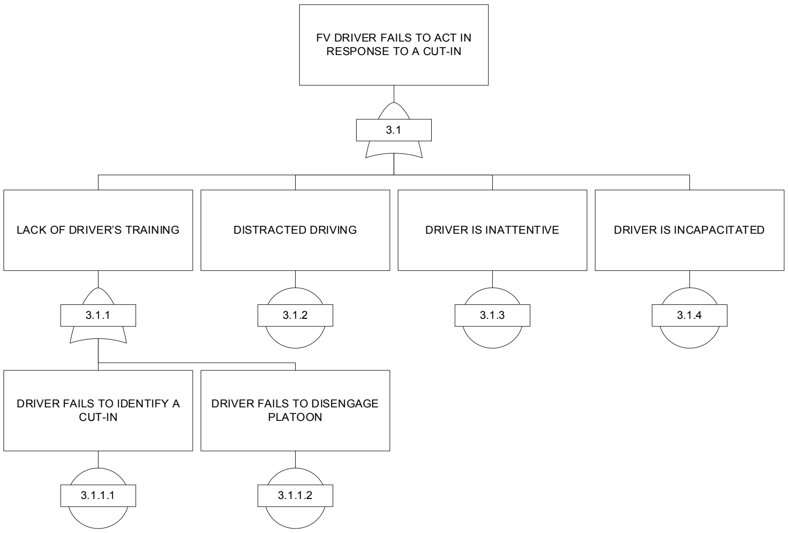

COLLISION BETWEEN FV AND A MOTORCYCLE AS A RESULT OF THE MOTORCYCLE PERFORMING A CUT-IN BETWEEN THE FV AND LV.
3
FV DRIVER FAILS TO ACT IN RESPONSE TO A CUT-IN
FV COLLISION MITIGATION SYSTEM FAILS TO ACT IN RESPONSE TO A CUT-IN
PLATOONING OPERATING PROCEDURES NOT FOLLOWED
FV PLATOONING SYSTEM FAILS TO WARN A CUT-IN
3.1
3.2
3.3
3.4

Source: Battelle

Figure 17. A Motorcycle Performs a Cut-In Between Two Platooning Vehicles (3)

Figure 17 shows the top logic gate for the next hazard considered – "*A motorcycle performs a cut-in between two platooning vehicles.*" The end result of this hazard is that the FV of the platoon would collide with a motorcycle. This fault was broken into four second-level faults described in the next section.

FV DRIVER FAILS TO ACT IN RESPONSE TO A CUT-IN (3.1)


FV DRIVER FAILS TO ACT IN RESPONSE TO A CUT-IN
3.1
LACK OF DRIVER'S TRAINING
DISTRACTED DRIVING
DRIVER IS INATTENTIVE
DRIVER IS INCAPACITATED
3.1.1
3.1.2
3.1.3
3.1.4
DRIVER FAILS TO IDENTIFY A CUT-IN
DRIVER FAILS TO DISENGAGE PLATOON
3.1.1.1
3.1.1.2

Source: Battelle

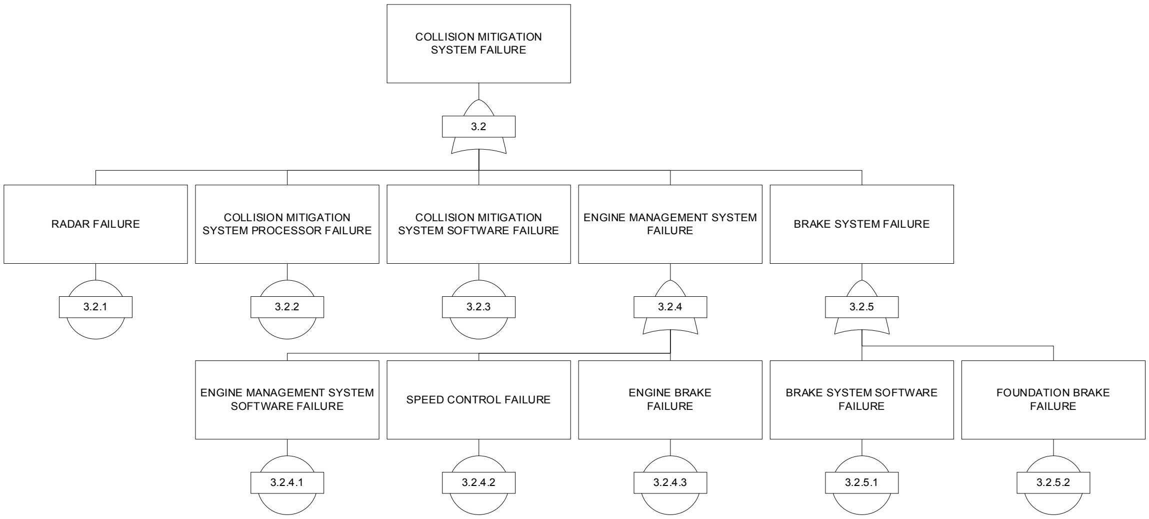
Figure 18. FV Driver Fails to Act in Response to a Cut-In (3.1).

This fault identifies the different scenarios that the driver of the FV can in a situation where they fail to respond to a cut-in upon a CMS failure.

Failure to respond to a cut-in can be caused by the following events shown in **Figure 18**:

- Lack of driving training, consisting of driver failure to:
  - Identify a cut-in
  - To disengage
- Distracted driving
- Driver is inattentive
- Driver is incapacitated

<u>FV CMS FAILS TO ACT IN RESPONSE TO A CUT-IN (3.2)</u>


COLLISION MITIGATION SYSTEM FAILURE
3.2
RADAR FAILURE
COLLISION MITIGATION SYSTEM PROCESSOR FAILURE
COLLISION MITIGATION SYSTEM SOFTWARE FAILURE
ENGINE MANAGEMENT SYSTEM FAILURE
BRAKE SYSTEM FAILURE
3.2.1
3.2.2
3.2.3
3.2.4
3.2.5
ENGINE MANAGEMENT SYSTEM SOFTWARE FAILURE
SPEED CONTROL FAILURE
ENGINE BRAKE FAILURE
BRAKE SYSTEM SOFTWARE FAILURE
FOUNDATION BRAKE FAILURE
3.2.4.1
3.2.4.2
3.2.4.3
3.2.5.1
3.2.5.2

Source: Battelle

Figure 19. FV CMS Fails to Act in Response to a Cut-In (3.2).

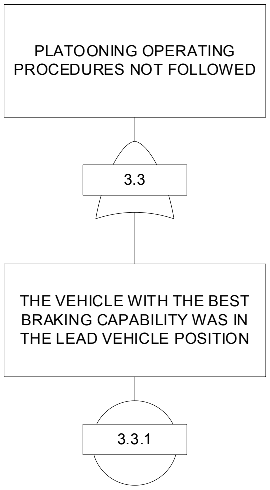
Refer to section CMS FAILURE (1.2) above for description. Events listed here for completeness.

Failure of the CMS can be caused by the following events shown in **Figure 19**:

- Radar failure
- CMS processor/electronic component failure
- CMS software failure
- Engine Management System failure caused by:
  - Engine Management System software failure
  - Speed control failure
  - Engine brake failure
- Brake system failure caused by

- Brake system software failure
- Foundation brake failure

PLATOONING OPERATING PROCEDURES NOT FOLLOWED (3.3)

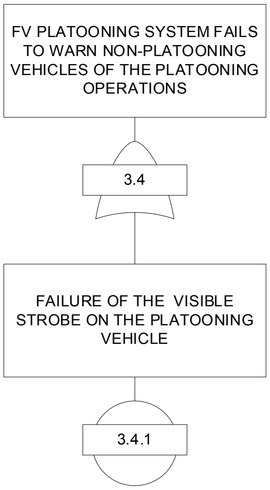

PLATOONING OPERATING PROCEDURES NOT FOLLOWED
3.3
THE VEHICLE WITH THE BEST BRAKING CAPABILITY WAS IN THE LEAD VEHICLE POSITION
3.3.1

Source: Battelle

Figure 20. Platooning Operating Procedures Not Followed (3.3).

This fault is the result of one event – a case where the operating procedures were not followed. It was identified in the preliminary hazard analysis that after an inspection of braking capability of each truck in the platoon, the truck with the best braking capability is placed in the last position in the platoon. This is done in case a sudden braking event occurs – the truck at the rear of the platoon needs better braking power to avoid collision with any LVs. For this particular hazard, if the FV does not have the best braking capability, it may be unable to stop in the event of a motorcycle (or other vulnerable road user) cuts into the platoon.

FV PLATOONING SYSTEM FAILS TO WARN OF A CUT-IN (3.4)


FV PLATOONING SYSTEM FAILS TO WARN NON-PLATOONING VEHICLES OF THE PLATOONING OPERATIONS
3.4
FAILURE OF THE VISIBLE STROBE ON THE PLATOONING VEHICLE
3.4.1

Source: Battelle

Figure 21. FV Platooning System Fails to Warn of a Cut-In (3.4).

This fault is also the result of one event. It was identified in the hazard analysis that each platooning vehicle should be outfitted with some form strobe or signage to alert non-platooning vehicles that a platoon is in formation. This fault occurs if that alert (in this case, a visible strobe) has failed. Failure to alert other vehicles on the road could lead to a situation where a motorcycle in an adjacent lane tries to perform a cut in, leading to the top-level hazard of a collision between the FV and the LV due to a motorcycle cut-in.

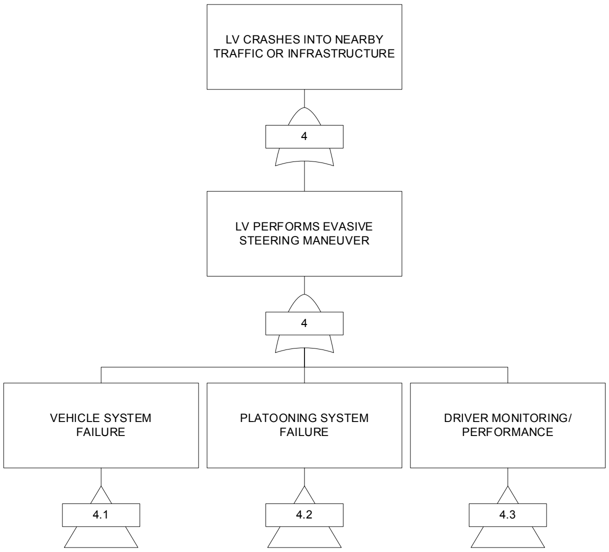
Fault Tree 4 – The LV Crashes into Nearby Traffic or Infrastructure.

Table 24 summarizes each of the events that comprise of Fault Tree 4. The architecture of the high-level events that may cause the LV to crash into nearby traffic or infrastructure are shown in **Figure 22**. The lower level events for this fault tree are illustrated in **Figure 23**, **Figure 24**, and **Figure 25**.

Table 24. Event Descriptions for Fault Tree 4

Fault Tree Event ID	Fault Tree Event Description
4	LV crashes into nearby traffic or infrastructure
4	LV performs evasive steering maneuver
4.1	Vehicle system failure
4.1.1	Steering column failure
4.1.1.1	Inadequate maintenance and inspection
4.1.1.2	Component failure
4.1.2	Steering tire blowout

Fault Tree Event ID	Fault Tree Event Description
4.1.2.1	Inadequate maintenance and inspection
4.1.2.2	Tire pressure sensor failure
4.1.2.3	Tire mechanical failure
4.1.3	Brake system failure
4.1.3.1	Inadequate maintenance and inspection
4.1.3.2	Component failure
4.2	Platooning system failure
4.2.1	CMS failure
4.2.1.1	Radar failure
4.2.1.2	CMS processor failure
4.2.1.3	CMS software failure
4.2.1.4	EMS failure
4.2.1.4.1	EMS software failure
4.2.1.4.2	Speed control failure
4.2.1.4.3	Engine brake failure
4.2.1.5	Brake system failure
4.2.1.5.1	Brake system software failure
4.2.1.5.2	Foundation brake failure
4.2.2	Sensor failure
4.2.2.1	Forward looking camera failure
4.2.2.2	Forward looking radar failure
4.2.3	HMI failure
4.2.3.1	Inaccurate notification to the driver of current conditions
4.2.3.2	Failure to notify the driver of current conditions
4.2.3.3	Untimely notification to the driver of current conditions
4.3	Driver monitoring/performance
4.3.1	Driver becomes incapacitated
4.3.2	Driver makes a late attempt to merge
4.3.3	Approaching an unknown work zone

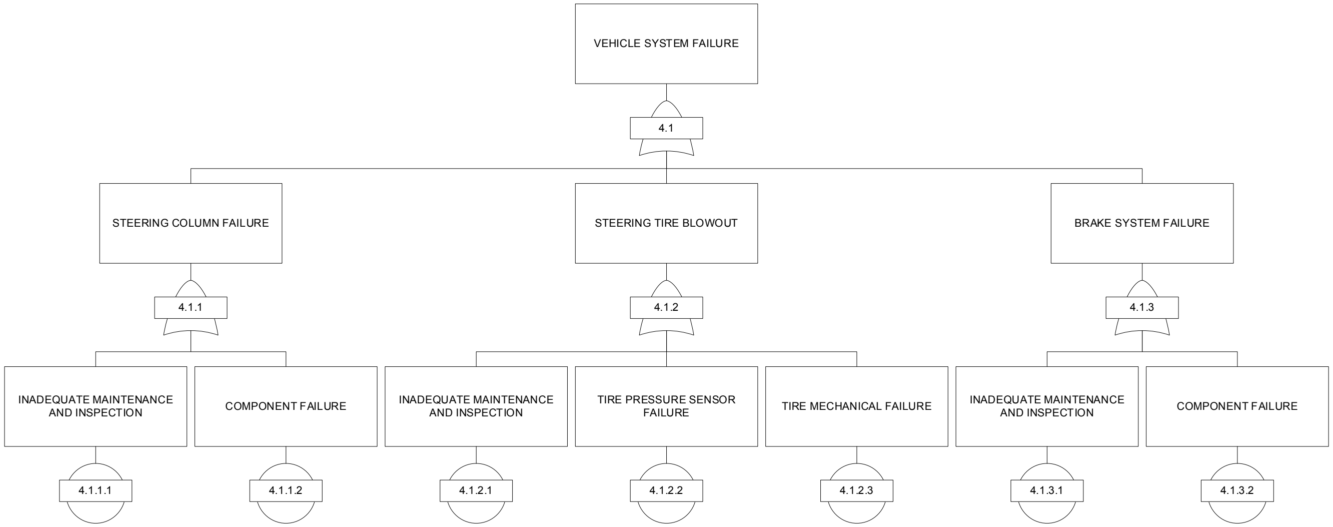

LV CRASHES INTO NEARBY TRAFFIC OR INFRASTRUCTURE
4
LV PERFORMS EVASIVE STEERING MANEUVER
4
VEHICLE SYSTEM FAILURE
PLATOONING SYSTEM FAILURE
DRIVER MONITORING/ PERFORMANCE
4.1
4.2
4.3

Source: Battelle

Figure 22. The Driver of the LV Performs an Evasive Maneuver (4).

Figure 22 shows the top logic gate for the last hazard considered – "*The driver of the LV performs an evasive maneuver.*" The end result of this hazard is that due to an unforeseen circumstance, the driver of the LV was forced to perform drastic steering of their vehicle, causing an unsafe condition and ultimately crashing into another vehicle in traffic or road infrastructure. This fault was broken into three second-level faults described in the next section.

VEHICLE SYSTEM FAILURE (4.1)



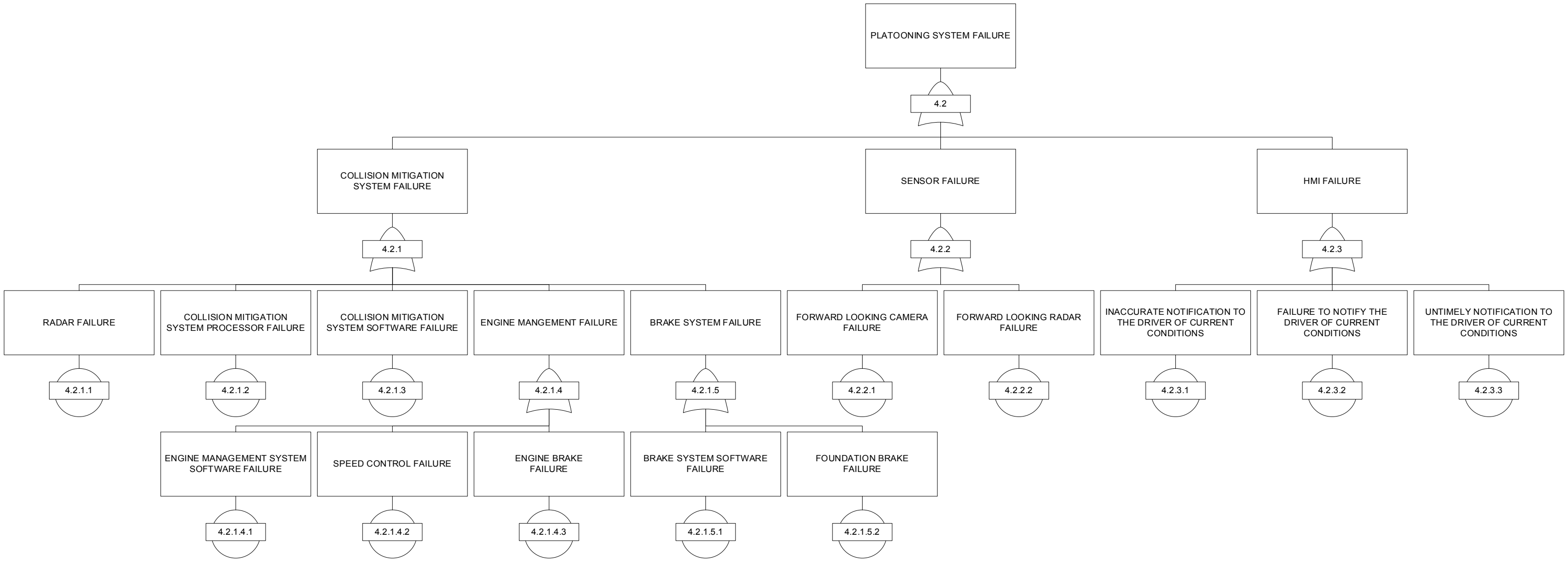
Source: Battelle

Figure 23. Vehicle System Failure (4.1).

Similar to Hazard 34, this fault is a roll-up of various truck subsystems that could fail and lead to the loss of steering control in the FV. While these subsystems are not a part of the platooning system under consideration, they are still necessary for the system to implement steering commands. Loss of any of the subsystems could lead to a situation where the driver is forced into take drastic steering measures to regain control of the vehicle. This rollup includes shown in **Figure 23**:

- Steering column failure due to one of the following events:
  - Inadequate maintenance and inspection
  - Component failure (mechanical failure of actual steering column, for example)
- Steering tire blowout
  - Inadequate maintenance and inspection
  - Tire pressure sensor failure
  - Tire mechanical failure
- Brake system failure
  - Inadequate maintenance and inspection
  - Component failure (mechanical failure of brake pad, for example)

PLATOONING SYSTEM FAILURE (4.2)


PLATOONING SYSTEM FAILURE
4.2
COLLISION MITIGATION SYSTEM FAILURE
SENSOR FAILURE
HMI FAILURE
4.2.1
4.2.2
4.2.3
RADAR FAILURE
COLLISION MITIGATION SYSTEM PROCESSOR FAILURE
COLLISION MITIGATION SYSTEM SOFTWARE FAILURE
ENGINE MANGEMENT FAILURE
BRAKE SYSTEM FAILURE
FORWARD LOOKING CAMERA FAILURE
FORWARD LOOKING RADAR FAILURE
INACCURATE NOTIFICATION TO THE DRIVER OF CURRENT CONDITIONS
FAILURE TO NOTIFY THE DRIVER OF CURRENT CONDITIONS
UNTIMELY NOTIFICATION TO THE DRIVER OF CURRENT CONDITIONS
4.2.1.1
4.2.1.2
4.2.1.3
4.2.1.4
4.2.1.5
4.2.2.1
4.2.2.2
4.2.3.1
4.2.3.2
4.2.3.3
ENGINE MANAGEMENT SYSTEM SOFTWARE FAILURE
SPEED CONTROL FAILURE
ENGINE BRAKE FAILURE
BRAKE SYSTEM SOFTWARE FAILURE
FOUNDATION BRAKE FAILURE
4.2.1.4.1
4.2.1.4.2
4.2.1.4.3
4.2.1.5.1
4.2.1.5.2

Source: Battelle

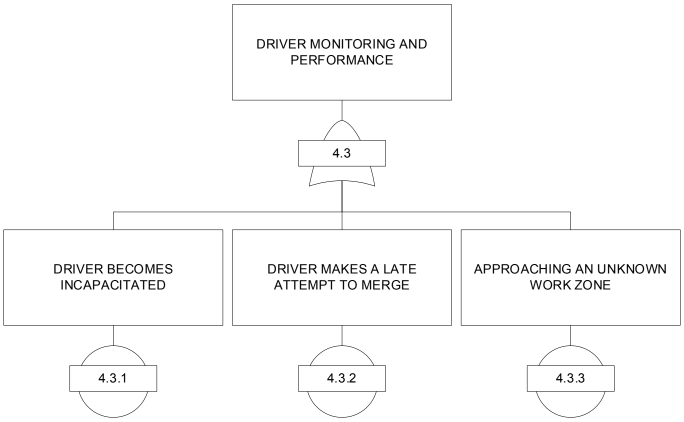
Figure 24. Platooning System Failure (4.2).

This fault combines the loss of the different subsystems that make up the platooning system. They include CMS, sensor failure and HMI failure.

Failure of the platooning system can be caused by the following tertiary-level events shown in in **Figure 24**:

- CMS failure caused by:
    - Radar failure
    - CMS processor/electronic component failure
    - CMS software failure
    - Engine Management System failure caused by:
        - Engine Management System software failure
        - Speed control failure
        - Engine brake failure
    - Brake system failure caused by
        - Brake system software failure
        - Foundation brake failure
- Sensor failure caused by:
    - Forward looking camera failure
    - Forward looking radar failure
- HMI failure caused by
    - Inaccurate notification to the driver of current conditions
    - Failure to notify driver of current conditions
    - Untimely notification to the driver of current conditions

DRIVER MONITORING AND PERFORMANCE (4.3)


DRIVER MONITORING AND PERFORMANCE
4.3
DRIVER BECOMES INCAPACITATED
DRIVER MAKES A LATE ATTEMPT TO MERGE
APPROACHING AN UNKNOWN WORK ZONE
4.3.1
4.3.2
4.3.3

Source: Battelle

Figure 25. Driver Monitoring and Performance (4.3).

Failure of the driver monitoring and performance can result in a situation where the driver is forced into drastic steering measures, resulting in the top-level crash condition.

Failure of the driver monitoring and performance can be caused by the following events shown in **Figure 25**:

- Driver becomes incapacitated
- Driver makes a late attempt to merge
- Driver approaches an unknown work zone

APPENDIX E: Safety Mitigations

Table 25. Safety Mitigations From Hazard Analysis and Risk Assessment

Safety Mitigation Number	Safety Mitigation Description	Safety Mitigation Type
1	The platooning vehicles are outfitted with run-flat tires.	Design
2	Sensor data is received and evaluated for integrity prior to executing commands sent from the LV.	Design
3	Forward and side-facing sensors will detect static road debris and alert the driver.	Design
4	Platooning software limits the upper bound of the maximum acceleration rate.	Design
5	A visible strobe or signal indicates that the vehicles are platooning.	Design
6	The HMI provides periodic driver engagement such as an alerter button (i.e., dead man switch).	Design
7	The platoon safely disengages and alerts the driver if there is a failure to engage with the HMI.	Design
8	The FVs monitor exhaust fume inhalation.	Design
9	The platoon disengages if any truck receives a detection flag.	Design
10	Drivers must be aware of passing space for vehicles ahead in the platoon.	Operations
11	The front-facing camera and sensors detect moving objects approaching the front and sides of the vehicle and alert the driver.	Design
12	Driver must be aware of other trucks and platoons, and always ensure there is a safe following distance between other trucks.	Operations
13	The vehicles are loaded according to operational policies and constraints.	Operations
14	The vehicle with the best braking capability takes the last following position of the platoon.	Operations
15	Each vehicle's load is independently verified (twice) prior to operating in platooning mode.	Operations
16	Train drivers on the proper use of the system.	Training
17	The driver will receive warnings from lane-keep assist system.	Design
18	Drivers must be trained to maintain lateral control when platooning.	Training

Safety Mitigation Number	Safety Mitigation Description	Safety Mitigation Type
19	Driver must be prepared to take over the system and brake.	Training
20	The Collision Mitigation System on FVs activates during a communication failure.	Design
21	Test all sensors and positioning system on all platoon-enabled vehicles prior to platooning.	Operations
22	The platoon disengages on data mismatch between information sources.	Design
23	Test platooning vehicle's communication subsystem prior to platooning.	Operations
24	The Collision Mitigation System activates upon surpassing safe following distance, alerting the driver, braking and disengaging the platoon.	Design
25	The driver of the FV can override the longitudinal control functionality (i.e., speed control).	Design
26	The communication system's redundant communication channels verify the integrity of the messages sent and received.	Design
27	The driver of the FV can override the lateral control functionality (i.e., steering control).	Design
28	The platoon disengages if the FV's acceleration is greater than the LV's acceleration (unless resuming safe distance).	Design
29	Platoon system must ensure FVs have shorter braking distance based on model, load, and performance.	Design
30	The system disengages from platooning mode upon a communication failure.	Design
31	Total Productive Maintenance ensures that platooning vehicles are for safe operation.	Maintenance
32	Operating procedures include a complete vehicle inspection and review of the platooning vehicle's maintenance logs prior to platooning.	Operations
33	The driver of the LV or FV can disengage the platoon at any time.	Design
34	All intervehicle communication messages are assigned a priority for every combination of messages received.	Design
35	The system software always acts upon the highest priority message received.	Design
36	The system software receives weather updates based on its geographical position.	Design

Safety Mitigation Number	Safety Mitigation Description	Safety Mitigation Type
37	The system sensors detect precipitation/icy conditions and notify the driver of changing weather conditions.	Design
38	The driver disengages platooning mode when low road surface friction conditions are registered by the electronic stability control system.	Training
39	Driver training includes how to identify low visibility conditions.	Training
40	The driver does not operate in platooning mode during low visibility conditions.	Operations
41	Drivers disengage platooning mode upon encountering a work zone.	Training
42	Drivers disengage platooning mode if they cannot visually identify lane markings.	Training
43	The system software is designed with high security credentials to prohibit cyber-attacks.	Design
44	Drivers report areas of degraded lane markings to the system.	Operations
45	The system safely disengages platooning mode and notifies the driver if the vehicle loses its positional awareness.	Design
46	The system maintains a safe distance from the infrastructure.	Design
47	A safe following distance regarding driver inhalation of exhaust fumes is determined.	Design
48	The system alerts the driver when platooning on grade that is not within the grade boundaries defined by the ODD.	Design
49	The system alerts the driver when platooning around a sharp curve that is not within the curvature boundaries defined by the ODD.	Design
50	Each FV has an HMI that provides a live-video feed from the LV's front facing camera.	Design
51	The system automatically disengages platooning mode when any of the platooning vehicles are outside the geographic ODD.	Design
52	The system alerts the driver when approaching an ODD roadway boundary, i.e., tunnel, border, bridge.	Design
53	The driver of the FV disengages platooning mode in high winds.	Operations
54	The driver of the LV must communicate with the driver of the FV over a defined frequency.	Operations

Safety Mitigation Number	Safety Mitigation Description	Safety Mitigation Type
55	The driver monitoring system monitors the driver's attentiveness and fatigue.	Design
56	The status of each platooning vehicle's driver must be indicated to other drivers in the platoon.	Design
57	The vehicle's Electronic Stability Control (ESC) system registers a slippery road condition and notifies the driver.	Design
58	Driver training includes accident mitigation.	Training
59	The system alerts the driver of the FV when the exhaust fume inhalation threshold has been met.	Design
60	The LV is equipped with ACC.	Design
61	The FV can monitor the condition of the tires in the LV.	Design
62	The platooning system will disengage upon the detection of a tire blowout.	Design
63	Each driver in the platoon is aware of the other driver's hours of service.	Operations
64	System will take accepted reaction time limits into consideration for design of following distances.	Design
65	Platooning system disengages during lane changes.	Design
66	The communication system between drivers uses a hands-free design (i.e., brake pedal).	Design
67	Platooning system notifies the drivers prior to the system disengaging.	Design
68	Platooning system will disengage upon an evasive steering maneuver (i.e., lateral acceleration limit).	Design
69	Blind spot detection sensors notify the driver of a detected object.	Design
70	Platooning system disengages when lane position is not maintained.	Design
71	When performing a lane change, the last FV initiates the change, allowing room for vehicles ahead of it to make the change in front of them.	Operations

APPENDIX F: References

Altan, O. (2017, March 22). *Vehicle and infrastructure communications* (PowerPoint presentation). Talking Freight Webinar, Federal Highway Administration. https://www.fhwa.dot.gov/Planning/freight_planning/talking_freight/march_2017/talking freight3_22_2017oa.pdf.

American Trucking Associations. (2020). *About.ATA* (Web page). www.trucking.org/ About.aspx.

Channel NewsAsia. (2017, January 9). Singapore to Start Trials of Driverless Trucks for Port Transport. In Channel NewsAsia. Retrieved from www.channelnewsasia.com/news /singapore/singapore-to-start-trials-of-driverless-trucks-for-port-transpor-7558490.

Commercial Vehicle Safety Alliance. (2020). About the Alliance. https://cvsa.org/about-us-page/about-cvsa/overview-of-cvsa/about-the-alliance/.

Concept Draw. (n.d.). Design elements - Fault tree analysis diagrams. www.ConceptDraw.com. https://conceptdraw.com/a183c3/preview.

Costlow, T. (2018, June 28). Volvo Trucks, FedEx Demonstrate 3-Truck Platoon on North Carolina Highway. https://www.sae.org/news/2018/06/volvo-fedex-truck-platooning.

Cuerden, R. (2018). Helm UK: Advanced Platooning Trials.

Klinedinst, D. (2020, May). *Cybersecurity best practices for integration/retrofit of telematics and aftermarket electronic systems into heavy vehicles* (Report No. FMCSA-RRT-19-013). Federal Motor Carrier Safety Administration. Available at https://rosap.ntl.bts.gov/view/dot/49248

Kotte, J. (2016, December 30). International Automotive Congress 2016: Platooning History and Current Activities in Europe.

Kuhn, B. T., Lukuc, M. R., Poorsartep, M., Wagner, J., Balke, K. N., Middleton, D. R., Songchitruksa, P., Wood, N., & Moran, M. (2017, August). *Commercial truck platooning demonstration in Texas - Level 2 automation* (Technical Report 0-6836-1). Texas A&M Transportation Institute. http://tti.tamu.edu/documents/0-6836-1.pdf.

International Standards Organization. (2019). Road vehicles — Safety of the intended functionality (2019-First ed., pp. 1-62). Switzerland: ISO.

Peloton Technology. (2018, December 4). Driver-Assistive Truck Platooning - Commercial Deployment Outlook.

Research Institutes of Sweden. (2012, May 30). The SARTRE Project. www.sp.se/sv/index /research/dependable_systems/Documents/The%20SARTRE%20project.pdf.

SAE International. (2014, January 16). *Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems, J3016_201401*. www.sae.org/standards /content/j3016_201401/.

SAE International. (2019, January 7). SAE J3016 Levels of Driving Automation. www.sae.org /news/2019/01/sae-updates-j3016-automated-driving-graphic.

Tsugawa, S. (2012, July 25). *Energy ITS: What we learned and what we should learn* (PowerPoint presentation). 2012 Road Vehicle Automation Workshop, Irvine, California. http://onlinepubs.trb.org/onlinepubs/conferences/2012/Automation/presentations/Tsugawa.pdf.

U.S. Department of Transportation. (2018, December 3). *Preparing for the future of transportation: Automated vehicles 3.0.* Retrieved from www.transportation.gov /sites/dot.gov /files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf.

DOT HS 813 065
May 2021

U.S. Department
of Transportation

**National Highway
Traffic Safety
Administration**

NHTSA