THESIS

COMPREHENSIVE CONCEPT-PHASE SYSTEM SAFETY ANALYSIS FOR HYBRID-ELECTRIC VEHICLES UTILIZING AUTOMATED DRIVING FUNCTIONS

Submitted by Matthew David Knopf Department of Mechanical Engineering

In partial fulfillment of the requirements For the Degree of Master of Science Colorado State University Fort Collins, Colorado Summer 2019

Master's Committee:

Advisor: Thomas Bradley

Daniel Olsen Sudeep Pasricha Copyright by Matthew David Knopf 2019

All Rights Reserved

ABSTRACT

COMPREHENSIVE CONCEPT-PHASE SYSTEM SAFETY ANALYSIS FOR HYBRID-ELECTRIC VEHICLES UTILIZING AUTOMATED DRIVING FUNCTIONS

Automotive system safety (SS) analysis involving automated driving functions (ADFs) and advanced driver assistance systems (ADAS) is an active subject of research but highly proprietary. A comprehensive SS analysis and a risk informed safety case (RISC) is required for all complex hybrid-vehicle builds especially when utilizing ADFs and ADAS. Industry standard SS procedures have been developed and are accessible but contain few detailed instructions or references for the process of completing a thorough automotive SS analysis. In this work, a comprehensive SS analysis is performed on an SAE-Level 2 autonomous hybrid-vehicle architecture in the concept phase which utilizes lateral and longitudinal automated corrective control actions. This paper first outlines a proposed SS process including a cross-functional SS working group procedure, followed by the development of an item definition inclusive of the ADFs and ADAS and an examination of 5 hazard analysis and risk assessment (HARA) techniques common to the automotive industry that were applied to 11 vehicle systems, and finally elicits the safety goals and functional requirements necessary for safe vehicle operation. The results detail functional failures, causes, effects, prevention, and mitigation methods as well as the utility of, and instruction for completing the various HARA techniques. The conclusion shows the resulting critical safety concerns for an SAE Level-2 autonomous system can be reduced through the use of the developed list of 116 safety goals and 950 functional safety requirements.

ii

ACKNOWLEDGEMENTS

I would like to thank my thesis advisor Dr. Bradley and my committee members Dr. Olsen and Dr. Pasricha for the opportunity to perform this work and the guidance while doing so. I would also like to thank my lab group and fellow Graduate Research Assistants Gabe Di Domenico, Troy Johnson, and David Trinko for their support and encouragement over the past two years. Finally, I would like to give a special thanks to my wife Leann and daughter Ava for their commitment and sacrifice while in pursuit of this degree.

TABLE OF CONTENTS

ABSTRACT	ii
ACKNOWLEDGEMENTSi	ii
LIST OF TABLES v	ii
LIST OF FIGURES i	Х
1 INTRODUCTION	1
1.1 The Importance of Systems Safety within the Automotive Industry	1
2 BACKGROUND	3
2.1 ISO 26262 Road Vehicles – Functional Safety	3
2.1.1 ISO 26262 Management of Functional Safety	5
2.1.2 ISO 26262 Concept Phase and System Development	6
2.1.3 ISO 26262 Product Development at the System, Hardware and Software-level	7
2.1.4 ISO 26262 Deficiencies	8
2.2 NASA System Safety Handbook	9
2.3 GM System Safety Process 1	1
2.4 Hazard Analysis and Risk Assessment (HARA) 1	3
2.4.1 HARA Definitions	4
2.4.2 HARA Types and Techniques	5
2.4.3 HARA – Preliminary Hazard Analysis (PHA) 1	8
2.4.4 HARA – Design Failure Mode and Effects Analysis (DFMEA) 1	8
2.4.5 HARA – System Element Fault Analysis (SEFA) 1	9
2.4.6 HARA – System Theoretic Process Analysis (STPA)	0
2.4.7 HARA – Hazard and Operability Study (HazOP) 2	0
2.5 Colorado State University	1
2.5.1 Colorado State University - EcoCAR	1
2.5.2 Colorado State University – Toyota	3
3 OBJECTIVES	6
4 RESULTS	8
4.1 Safety Plan	8
4.1.1 Safety Activities throughout the System Safety Lifecycle	8
4.1.2 Cross-Functional Safety Procedure	1

4.1.3 Ro	les and Responsibilities	. 33
4.1.4 Ev	idence of Competence	. 34
4.1.5 Ev	idence of Quality Management	. 34
4.1.6 Ev	idence of a Good Safety Culture	. 35
4.2 Item De	efinition	. 37
4.3 Applica	ation of HARA	. 42
4.3.1 HA	ARA applied using PHA	. 45
4.3.2 HA	ARA applied using DFMEA	. 47
4.3.3 HA	ARA applied using SEFA	. 55
4.3.3 HA	ARA applied using HazOP	. 60
4.3.4 HA	ARA applied using STPA	. 67
4.4 Safety	Goals and the Elicitation of Functional Requirements	. 72
4.4.1 La	ne Keeping Assist System Safety Goals and Functional Requirements	. 73
4.4.2 Ad	aptive Cruise Control System Safety Goals and Functional Requirements	. 76
4.4.3 CA	Vs Safety Goals and Requirements	. 80
4.4.4 CS	MS Safety Goals and Functional Requirements	. 84
4.4.5 PS	I HV & Mechanical Safety Goals and Functional Requirements	. 87
5 CONCLUS	ION	. 92
5.1 Contrib	putions	. 92
5.2 Future	Work	. 94
REFERENCES .		. 95
Appendix 1	Management of Functional Safety – Complete Documentation	. 98
Appendix 1.1	Safety Activities throughout the System Safety Lifecycle	. 98
Appendix 1.2	Cross-Functional Safety Procedure	. 99
Appendix 1.3	Roles and Responsibilities	123
Appendix 1.4	Evidence of Competence	125
Appendix 1.5	Evidence of Quality Management	125
Appendix 1.6	Evidence of a Good Safety Culture	126
Appendix 2 I	tem Definition – Complete Documentation	128
Appendix 2.1	CAVs Item Definition	128
Appendix 2.2	CSMS Item Definition	130
Appendix 2.3	PSI HV Item Definition	133

Appendix 2.4	PSI Mechanical Item Definition	134
Appendix 3 H	ARA – Complete Documentation	139
Appendix 3.01	HARA CAVs / CSMS ACC DFMEA	139
Appendix 3.02	HARA CAVs / CSMS LKA DFMEA	162
Appendix 3.03	HARA CAVs / CSMS LKA STPA	178
Appendix 3.04	HARA CAVs PHA	202
Appendix 3.05	HARA CSMS DFMEA	234
Appendix 3.06	HARA PSI HV DFMEA	263
Appendix 3.07	HARA PSI HV HazOP	285
Appendix 3.08	HARA PSI Mechanical Controls Hardware HazOP	289
Appendix 3.09	HARA PSI Mechanical DFMEA	292
Appendix 3.10	HARA PSI Mechanical HazOP	336
Appendix 3.11	HARA PSI SEFA	341
Appendix 4 S	afety Goals and Functional Requirements – Complete Documentation.	361
Appendix 4.1	ACC Safety Goals and Functional Requirements	361
Appendix 4.2	CAVs Safety Goals and Functional Requirements	366
Appendix 4.3	CSMS Safety Goals and Functional Requirements	381
Appendix 4.4	LKA Safety Goals and Functional Requirements	390
Appendix 4.5	PSI HV Safety Goals and Functional Requirements	404
Appendix 4.6	PSI Mechanical Safety Goals and Functional Requirements	414
LIST OF ABBRE	EVIATIONS	429

LIST OF TABLES

Table 1. Example of "Roles and responsibilities"	. 33
Table 2. Example of "Evidence of Competence"	. 34
Table 3. Example of "Evidence of a Good Safety Culture"	
Table 4. Example of the Item definition for the CAVs system using the Intel Mobil Eye 6	
Camera	. 40
Table 5. Example of the CSMS Item Definition using the HSC as the item	. 41
Table 6. Template used to perform the PHA	
Table 7. Example of a corrective/preventative measure and the associated requirement	. 47
Table 8. Template used to perform the DFMEA	. 48
Table 9. Severity rating scale with descriptions and associated criteria [30]	. 50
Table 10. Occurrence rating scale with descriptions and associated criteria [30]	
Table 11. Detection rating scale with descriptions and associated criteria [30]	. 53
Table 12. Forming the requirement from the DFMEA prevention mode and failure type	. 54
Table 13. Template 1 of 2 used to perform the SEFA	. 56
Table 14. Template 2 of 2 used to perform the SEFA	. 56
Table 15. Example of SEFA template 1 of 2 with analysis using the PSI subsystem and a P3	
architecture	. 58
Table 16. Example of SEFA template 2 of 2 with analysis using the PSI subsystem and a P3	
architecture	. 60
Table 17. Template used to perform the process parameter chart of the HazOP	. 61
Table 18. Template used to perform the HazOP	. 62
Table 19. Key process parameters and their associated systems	. 63
Table 20. Process parameter and guide word chart for a HV system (X indicates a relevant	
guideword and process parameter combination)	. 64
Table 21. Partial HazOP analysis when a temperature stimulus is applied to a HV system	. 66
Table 22. Template used to perform the STPA	. 67
Table 23. Example of a STPA on the LKA system	. 71
Table 24. Safety goals of the LKA system	. 74
Table 25. Number of requirements for lateral control using the EBCM vs. the EPS	
Table 26. Example of LKA system safety goals and their associated functional requirements	. 76
Table 27. Safety goals of the ACC system	. 77
Table 28. Number of requirements produced for the LKA vs. the ACC system using select	
HARA techniques	
Table 29. Example of the ACC system safety goals and functional requirements	. 80
Table 30. Example of CAVs safety goals	. 81
Table 31. Example of the CAVs safety goals and functional requirements	
Table 32. Example of the CSMS safety goals	
Table 33. Common CSMS failure causes and their associated prevention and mitigation metho	
	. 87

Table 34. Example of the PSI HV safety goals	. 88
Table 35. Example of the PSI HV safety goals and their functional requirements	. 89
Table 36. Example of the PSI-Mechanical safety goals	. 90
Table 37. Example of the PSI-Mechanical safety goals and their functional requirements	. 91

LIST OF FIGURES

Figure 1. The management of functional safety throughout the product lifecycle [ISO 26262].	5
Figure 2. Overview of NASA system safety processes in flowchart format [NASA]	. 10
Figure 3. General Motors' System Safety Process [GM]	. 12
Figure 4. Relationship among cause and effect for various HARA techniques	. 17
Figure 5. Colorado State University System Safety Process	. 29
Figure 6. Flow chart describing a method for completing the Item Definition	. 39

1 INTRODUCTION

1.1 The Importance of Systems Safety within the Automotive Industry

Systems safety is a disciplined and comprehensive engineering approach to identify, eliminate, and control safety related risks through the use of a structured analysis and assessment methods. The system safety approach is widely used across a variety of industries whose products are complex systems that involve potential risk to the operator, environment, or property.

For many large industries, such as aerospace, military, and automotive industries, system safety is a critical component to the structure of the systems lifecycle process, and is an active and evolving field of research [1]. Because these industries use advanced technologies and due to competition within and among industries, the systems safety processes within each OEM is largely unique and proprietary [2]. One key challenge that is derived from the proprietary nature of system safety processes are the problems of safety culture building, workforce development for system safety engineering and sharing best practices. At present, there is no publicly available comprehensive system safety example or reference, which could be used to help engineering teams to develop these shared, effective, and safety-critical analyses and practices.

This is particularly true for the automotive industry. The automotive industry is one of the largest in the world utilizing advanced technologies and implementing operator assist features in an effort to reduce operator error and system failures [3] [4]. This industry is unique because of the number and complexity of advanced technology systems that are available to and

operable by the untrained public every day.¹. The implementation of advanced driver assistance systems (ADAS) and automated driving functions (ADF) in vehicles is increasing rapidly [5] [6]. This stems from a desire to reduce the negative externalities associated with vehicles including driver-caused accidents, fuel consumption, road congestion, and emissions. ADAS and ADF's (which include adaptive cruise control, lane keeping assist, and other embedded systems) aim to improve the ease-of-use and the safety of transportation through less demanding human machine interfaces, a decrease in the operator requirements, and an increase in the vehicles' awareness of safety and safety-relevant behaviors [7] [8]. Despite these goals, the engineering of ADAS and ADF's carry safety concerns, both critical and nominal, which must be developed during the concept and requirements engineering phase and should be monitored and amended throughout the systems engineering lifecycle.

In response to these challenges, this thesis seeks to develop a set of relevant documentation, processes, and outcomes (requirements) for a system safety process as applied to University vehicle design projects. By documenting a system safety engineering process, this thesis seeks to begin to build a relevant knowledge-base, processes, and cultural basis to enable system safety considerations in University vehicle design/build/test projects.

¹ 1.2 billion cars and trucks [1] are on the road globally, which can be compared to 39,000 aircraft that fly globally. This speaks to the orders of magnitude higher public risk that is incurred through land vehicle design than is incurred through aircraft design. [https://www.telegraph.co.uk/travel/travel-truths/how-many-planes-are-there-in-the-world/]

2 BACKGROUND

There are many methods that have been developed for analyzing the safety of a complex systems. Key references that will be reviewed to provide some background into the state of the art in system safety engineering include the NASA System Safety Handbook, General Motors' Introductory Materials for EcoCAR System Safety (authored by Mark Vernacchia), and ISO 26262.

NASA has developed a holistic and systematic approach to the analysis of risks resulting from hazards that can affect humans, the environment, and mission assists [9]. The uniqueness of NASA's system safety process is the use of a holistic practice which references supplemental approaches to traditional forms of risk management. For example NASA considers measures of aggregate safety risk to include risk to the operator, environment, mission, and equipment. Specific to the automotive industry, GM has produced a proprietary and evolving system safety approach using a waterfall model [10]. The waterfall model is generally linear and iterative with clearly defined tasks and phases. The automotive industry standard for systems safety is the ISO 26262 Road Vehicles Functional Safety. This standard generally follows the systems engineering "V"-model and is available to the public for purchase [11].

2.1 ISO 26262 Road Vehicles – Functional Safety

Safety is a key issue in the development of road vehicles internationally. To address the safety risks of the development and implementation of automotive embedded systems a publicly accessible International Standard was created to guide OEMs in this process. The standard that is entitled "ISO 26262 Road Vehicles – Functional Safety" is intended to be applied to safety

related systems that include one or more electrical and/or electronic (E/E) systems within passenger cars with a maximum vehicle mass up to 3500 kg [11]. ISO 26262 states that it addresses possible hazards caused by malfunctioning behaviors of E/E safety related systems and the interactions of these systems but does not address the hazards related to internally caused failure such as fire, smoke, heat, or external caused failures such as adverse road conditions, or poor weather conditions. ISO 26262 also does not address failures associated with operator error, which represents a significant weakness because operator errors are asserted to be responsible for >94% of vehicle accidents [12].

Although not a comprehensive study on all safety aspects of an automotive system, ISO 26262 presents the framework for applying a systems safety analysis which can be expanded to more thoroughly determine automotive systems safety requirements.

ISO 26262 defines *functional safety* as the aspects of the safety of a system that require automatic control and regulation to deliver the safety function. Analogous to the design of a system to achieve any other function, the design of functional safety requires a system for management of the system safety function/product over its lifecycle.

The structure of the functional safety management includes a set of processes documented in Figure 1. Under the Management of Functional Safety process, ISO 26262 describes the following phases:

- 1. Concept phase,
- 2. Product development at the system-level,
- 3. Product development at the hardware-level,
- 4. Product development at the software-level,
- 5. Production and operation.

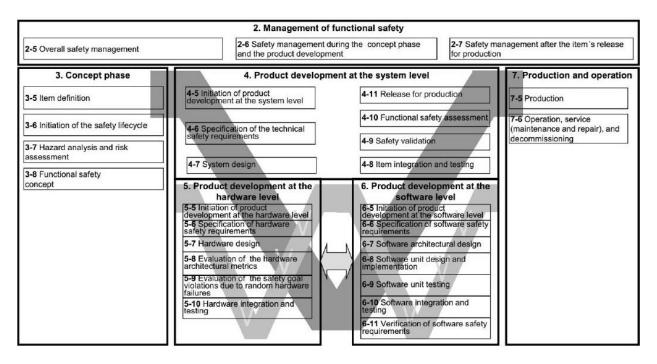


Figure 1. The management of functional safety throughout the product lifecycle [ISO 26262]

These phases are described in more detail in the following sections.

2.1.1 ISO 26262 Management of Functional Safety

The management of functional safety, ISO 26262-2, describes a framework for creating and implementing a safety culture. It identifies the roles and responsibilities in safety management throughout the project lifecycle which is clearly geared towards large companies who have many personnel working on the safety management team.

For smaller teams at the institutional level (more relevant for this university-based system safety exercise), ISO 26262-2 provides guidance as follows:

• The *work product* of a functional safety management process should be meeting the corresponding requirements of ISO 26262 and evidence of compliance with these safety requirements [13]. This means that a functional safety management work

product should result in meeting the requirements of the ISO, and should include evidence of meeting these requirements.

- Confirmation measures should be work products that are evaluated during subsequent activities. This means that work products should be confirmed and evaluated during and as part of their use in the tasks to which they are inputs.
- Functional safety assessments should be an evaluation of an item's functional safety achievement. The assessment of functional safety should be based on evaluation².

The safety case should provide a clear, comprehensive and defensible argument, supported by evidence, that an item is free from unreasonable risk. This means that the safety case is a document that makes the reasoned argument that the vehicle is safe to operate.

2.1.2 ISO 26262 Concept Phase and System Development

ISO 26262-3, "Concept Phase", is arguably the most critical part of this document particularly for smaller teams developing new systems and advanced components. It is with in the concept phase that hazards and risks can be identified and mitigated through a process of a detailed item definition and hazard analysis and risk assessment (HARA). From this HARA analysis a functional safety concept is derived.

Step 1 (ISO 26262 section 3-5) is to define the item.

The definition of the term *item* is a system or array of systems to implement a function at the vehicle level, to which ISO 26262 is applied [14].

The objectives of the item definition:

 $^{^{2}}$ Where assessment can be considered to be a determination of the quality of an item, and evaluation can be considered to be a systematic determination of a subject's enumerated or ranked merit.

- Describe the item, its functionality, dependencies on, and interaction with, the driver, the environment and other items at the vehicle level
- To support an adequate understanding of the item so that the activities in subsequent phases can be preformed

Next, the HARA is performed (ISO26262 section 3-7). The objectives of the HARA include:

- To identify and to classify the hazardous events caused by malfunctioning behavior of the item
- To formulate the safety goals (SGs) with their corresponding automotive safety integrity level (ASILs) related to the prevention or mitigation of the hazardous events, in order to avoid unreasonable risk

Together the item definition and HARA are used early in the development process to understand potential vulnerabilities within the system, and to help to define safety goals. Failure mode and effects analysis (FMEA) and a hazard and operability study (HazOP) are suitable techniques to support the HARA [14]. The result of these analyses will be a classification of the hazardous events using the ASIL rating system. A safety goal will be produced for each hazardous event with an ASIL exceeding quality managed (QM) ratings. The functional safety concept is a set of safety measures and mechanisms which support and lead to the enforcement of the safety goals, and is an output of the concept phase.

2.1.3 ISO 26262 Product Development at the System, Hardware and Software-level

At the product development phase at the system-level, detailed in ISO 26262-4, ISO 26262-5, and ISO 26262-6, specifications of the technical safety requirements are determined

and a system design is created. These work products feed the hardware and software development ultimately releasing the design for production and operation, detailed in ISO 26262-7. Because we seek to develop design requirements, phases 4 through 7 of the ISO 26262 safety lifecycle include activities beyond the scope of this thesis and will not be addressed in detail.

2.1.4 ISO 26262 Deficiencies

ISO 26262 gives guidance on how to perform a thorough system safety analysis but falls short on a few key issues during the concept phase for the purposes of this study. The deficiencies in ISO 26262 are understandable as it cannot possibly identify all potential hazards to all automotive architecture types, but there are key concept phase deficiencies which this study will attempt to elaborate:

- Lack of explanation and examples for how to perform the item definition task
- Lack of explanation and examples of how to perform a FMEA or HazOP in support of a HARA
- No comprehensive document or template to reference which aids in performing an item definition, HARA, or ASIL determination
- No list of the most critical safety concerns for any automotive architecture type
- No consideration of ADF or ADAS in the HARA activities [15]

In the production of the ISO 26262, comprehensive system safety analysis were conducted and documented to vet the developed process but the documentation of this process is not accessible. It would be significantly helpful as a comprehensive reference providing true examples of hazard analysis techniques at a system, hardware, and software-level and the associated analysis templates.

2.2 NASA System Safety Handbook

NASA has published a System Safety Handbook to serve as educational material and procedural documentation for its purposes. NASA System Safety Handbook addresses a wider breadth of safety concerns than does ISO 26262 to include human, environmental, equipment, and property safety. The inclusion of property, equipment and the depth of environmental concern used by NASA is an important supplement to the ISO 26262 description of safety, although these concerns are, by custom, not generally considered in automotive industry [Mark Vernacchia].

In the aerospace industry, equipment and property safety is of high importance because, when in operation, maintenance can be impossible and missions are often a one-attempt assignment. As systems become increasingly complex and the cost of designing, building, and operating becomes more important, the NASA system safety process presents a holistic approach to ensure hazards are identified and known risks are controlled [9]. Although not specifically tailored to the automotive industry, the NASA System Safety Handbook details a functional safety approach that can be viewed as broader than the ISO 26262 but with even fewer specifics and examples.

NASA's system safety framework illustrated in Figure 2 and begins with the definition of *key decision points* (KDPs) which are points of resolution along the system lifecycle. The KDPs define a set of phases, A through F, which include concept studies, technology development, design fabrication and completion, assembly and testing, operation and sustainment, and

closeout. The NASA system safety framework is broken into four phases and is performed in parallel to the KDPs [9].

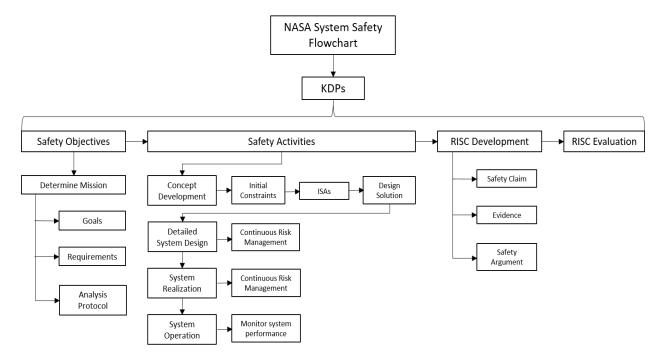


Figure 2. Overview of NASA system safety processes in flowchart format [NASA]

- 1. The *safety objectives phase* helps teams to understand the mission-level objectives, goals, requirements, and analysis protocols.
- 2. The system safety activity phase is further broken into four categories: concept development and early state system design, detailed system design, system realization, and system operation. This phase performs appropriate safety and risk analysis, assess safety management controls, and monitors system performance to identify risks/opportunities. During the safety and risk analysis an integrated safety analysis (ISA) is performed which is equivalent to the ISO 26262's HARA in that the principle outputs are:
 - A set of accident scenarios that can produce undesirable safety performance

- Identification and evaluation of the potential causes of these accident scenarios
- Identification and evaluation of existing controls associated with the scenarios
- Probability density functions
- Safety margins
- 3. The *risk-informed safety case (RISC) development and re-baselining phase* augments and evidences the RISC and safety claims. RISC is analogous to a functional safety concept in that it is a structured safety case, supported by a body of evidence that provides compelling analysis that a system will be adequately safe [9].
- 4. The *RISC evaluation phase* performs a final review of safety claims and determines if the systems is adequately safe.

2.3 GM System Safety Process

The GM system safety process is documented in a series of publicly available presentations, documents and personal correspondence with Mark Vernacchia, GM System Safety Engineering Fellow. The GM procedures document a robust and applied process, similar to and referencing the ISO 26262 process, but it differs in a few key ways. The GM process uses a "waterfall" model and divides the safety tasks in to four phases: concept, requirements, design, and final safety case [10]. A block diagram of GMs system safety process presented in Figure 3.

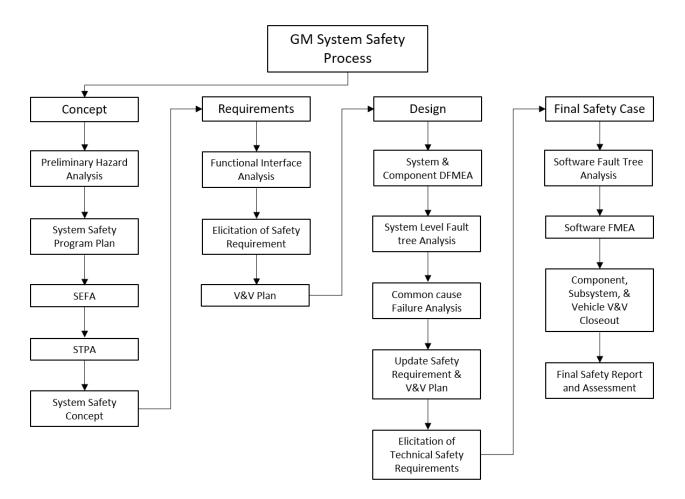


Figure 3. General Motors' System Safety Process [GM]

Key phases of the GM system safety process are:

- The *concept phase* involves a preliminary hazard analysis followed by the development of a safety program plan. Within this initial phase is the HARA, but GM prefers the use of a system element fault analysis (SEFA) and a system-theoretic process analysis (STPA). The conclusion of the concept phase is the creation of the system safety concept and a review of that concept.
- The *requirements phase* involves a functional interface analysis, the elicitation of the safety requirements, and the development of a safety verification and validation (V&V) plan.

- 3. The *design phase* involves a system/component design failure mode and effects analysis (DFMEA), system-level fault tree analysis (SLFTA), and a common cause failure analysis. Following these analyses, an update to the safety requirements and V&V plan is developed. Finally the system technical safety concept is created.
- During the *final safety case phase*, a software fault tree analysis and FMEA are performed. Component, subsystem, and vehicle V&V are closed out and a final safety report and assessment is documented.

Unlike the ISO 26262 process, GM does not require an item definition or impact analysis at the item level. This is perhaps justifiable because the items are well-defined in an engineered automobile, but ISO 26262 asserts that an item analysis is a crucial step to determining all items, sub-items, and the dependencies, interactions, and interfaces to one another [14].

2.4 Hazard Analysis and Risk Assessment (HARA)

An important component of each of the methods reviewed above is the HARA. A hazard analysis identifies the hazards associated with the equipment under control (including the equipment control systems), hazard effects, and the hazard causal factors. From these identified hazards, risk reduction measures will be applied and safety design actions will be implemented. A thorough hazard analysis systematically surveys the entirety of the system being developed, the subsystems, items, sub-items, personnel, software, and their interfaces and interaction.

The risk assessment aims to achieve a reduction in the associated hazard through applied safety functions. The application of a safety function can come in a variety of forms including software controls, redundancy verification method to monitor sensor data, or controls hardware

to decrease data latency or to improve visibility, or an additional piece of hardware such as an air bag.

HARA techniques continue to evolve as new methods are developed which broaden the capability of systems safety engineers to identify potential hazards and mitigation strategies earlier in the lifecycle process.

2.4.1 HARA Definitions

Across the spectrum of analysis types and techniques there is a common language used. The verbiage making up the systems safety language generally has similar definitions and it is important to note those. The following terms are regularly used within most HARA methods and the definitions described come from sources which define in reference to a systems safety application.

Failure: *The event when a required function is terminated or exceeded the acceptable limits* (JUS IEC 50).

Fault: The state of an item characterized by the inability to perform a required function, excluding the inability during preventative maintenance or other planned actions, or due to a lack of external resources (JUS IEC 50).

Error: A discrepancy between a computed, observed, or measured value or condition and the true, specified or theoretically correct value or condition (JUS IEC 50).

Hazard: A real or potential condition that could lead to an unplanned event or series of events (*i.e. mishap*) resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment (MIL-STD-882).

Mishap: An event or series of events resulting in unintentional death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. For the purposes of this Standard, the term "mishap" includes negative environmental impacts from planned events (MIL-STD-882).

Mitigation Measure: Action required to eliminate the hazard or when a hazard cannot be eliminated, reduce the associated risk by lessening the severity of the resulting mishap or lowering the likelihood that a mishap will occur (MIL-STD-882).

Safety: *Freedom from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment* (MIL-STD-882).

Risk: *A combination of the severity of the mishap and the probability that the mishap will occur* (MIL-STD-882).

Hazard Casual Factors: One or several mechanisms that trigger the hazard that may result in a mishap (MIL-STD-882).

Safety Requirement: A condition or series of conditions necessary for the system to prevent, detect, and mitigate potential hazards, faults, or failures.

2.4.2 HARA Types and Techniques

There are a wide variety of HARA types and techniques used to identify hazards and mitigate risk throughout the entirety of a projects lifecycle. Each technique examines a specific view of the system, and as a result, has an associated set of strengths and weaknesses [16]. HARA's are especially valuable early in the concept and development phases but can be utilized through a systems production, operation, and disposal. Popovich [17] notes that there are over 100 different hazard analysis techniques, many of which are minor variations of other

techniques. He outlines 22 unique analysis methods and places them on an engineering development lifecycle model to indicate when each method can provide the most utility at which stage of the systems engineering process.

Popovich further discusses the two primary categories of hazard analysis: *types* and *techniques*. The notable distinction between the two are the following:

Type:

- Establishes where, when, and what to analyze,
- Establishes a specific analysis task at a specific time in the projects lifecycle,
- Establishes what is desired from the analysis,
- Provides a specific design focus.

Technique:

- Establishes how to perform the analysis,
- Establishes a specific and unique analysis methodology,
- Provides the information to satisfy the intent of the analysis type.

In addition to the types and techniques of hazard analysis, these two can be further classified as being inductive, deductive, or exploratory methods. These terms can be confusing and are often incorrectly applied so it is important to understand how they fit into the context of hazard analysis and how they add value to the safety analyst [17]. Within the context of system safety analysis, inductive and deductive techniques are equivalent to bottom-up and top-down analysis methods while exploratory reasoning uses a middle-out approach [18]. The utility of these distinct methods derives from their potential to identify unique requirements from each. Of course, it is possible that an inductive method will identify some of the same requirements as an

exploratory method, but by including multiple methods, the systems safety engineer can hope to produce both exclusive and a comprehensive set of requirements.

An inductive analysis follows the path from specific to broad generalizations. This technique looks at "what if" scenarios and breaks down the system into individual components [17]. For example an inductive approach would initially identify the cause of a failure (flat tire), which through the appropriate analysis technique such as a failure mode and effects analysis will then lead to the possible effects (unintended longitudinal motion). An inductive approach can be difficult to apply to complex systems due to the large number of components to consider and the potential for compounding failure combinations

A deductive approach follows the path from general to specific. This technique looks at "how can" scenarios [17]. A deductive approach initially identifies the known effects of a failure (unintended longitudinal motion), then deduces possible causes (flat tire). This method of safety analysis is applicable for all sizes of systems and more easily identifies hazards caused by multiple or interacting failures.

The third technique is an exploratory method [10] which begins by identifying a single deviation to the system using guide words such as "function is required but not provided". From this, the system safety analysist can develop potential causes and effects of the failure. Figure 4 visualizes the paths taken for each analysis technique.

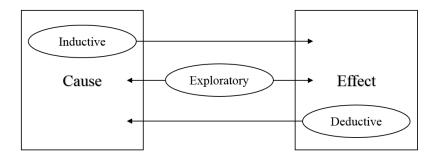


Figure 4. Relationship among cause and effect for various HARA techniques

Of the many HARA types and techniques, the automotive industry commonly uses a select few; preliminary hazard analysis, failure mode and effects analysis, system element fault analysis, system theoretic process analysis, and a hazard and operability study. All of which rely of expert judgement and knowledge of the system and components to assess potential hazards and the significance of the effects.

2.4.3 HARA – Preliminary Hazard Analysis (PHA)

A PHA is a type of inductive analysis used in the initial stages of the systems design. It is a broad technique focusing on identifying hazards, assessing the severity of the effects that would occur from that particular hazard, and identifying corrective and preventative measures [19]. The benefit of a PHA is that it allows for early recognition of weakness in the system concept, thus saving time and money that would be required during future discovery of the weakness.

The benefits and characteristics of the PHA are as follows:

- Provides early identification and high level hazard recognition,
- Elicits consistent safety requirements for both hardware and software systems,
- Applicable to any activity or system big and small,
- Elicits qualitative hazard descriptions and provides qualitative rankings of the hazardous situations which is used to prioritize hazard reduction tasks.

2.4.4 HARA – Design Failure Mode and Effects Analysis (DFMEA)

A DFMEA is an inductive analysis technique and one of the earliest developed methods for hazard analysis. Similar to all HARA techniques, the DFMEA aims to assess system and design risk, and develops strategies to detect and mitigate those risks. Unique to the FMEA is that the method ranks those risks based a risk priority classification. If it is completed very early in the concept stages of design, the DFMEA can provide valuable insight into potential hazards, the impact of those hazards, and the interfaces and interactions between subsystems [20] [21]. The benefits and characteristics of the DFMEA are as follows:

- Provides a deep-dive hazard analysis at the system, subsystem, and component level,
- Ranks potential hazards base on a risk priority number (RPN) to identify highest priority risks (*RPN = Severity * Occurance * Detection*),
- Intuitive and thorough analysis templates are available and used to identify potential failure modes, failure effects, causes of failure, and detection and mitigation methods.

2.4.5 HARA – System Element Fault Analysis (SEFA)

A SEFA is an inductive analysis technique used at the system-level to assess the consequence of system element faults. This analysis involves a methodical systems element review based on an already known system architecture and assists in recognition of systematic weaknesses of a design or architecture [10].

The benefits and characteristics of the SEFA are as follows:

- It must be completed after system architecture is defined and is used to compare multiple architectures,
- Allows for identification of component faults on the system as a whole,
- Clearly utilizes specific operating scenarios and associates component-to-component failures with hazards,

• Inclusion of the immediate resulting state after a failure leads to better hazard diagnostic and mitigation methods.

2.4.6 HARA – System Theoretic Process Analysis (STPA)

An STPA is an exploratory analysis technique used primarily from a controls perspective. STPA treats failures as controls problems, which can be useful in systems that are controlscentric [22] [23]. It is typically applied to control functions such as lane keeping assist systems and uses guide phrases to identify hazards and resulting hazard mitigation methods. This method delivers unique requirements that are not identified through other analysis techniques but the STPA's scope is limited to functional responses and does not easily pick up on elemental faults. The benefits and characteristics of the STPA are as follows:

- Specific to controls functions and software systems in particular,
- Identifies hazards through the use of unsafe control actions such as "function provided but incorrect timing",
- Elicits unique requirements from the use of causal factors and control constraints.

2.4.7 HARA – Hazard and Operability Study (HazOP)

A HazOP is also an exploratory technique of risk analysis which uses guide words and process parameters. These process parameters are dependent on the component and can be applied to system items resulting in partial or whole-system failures. Where the engine is the component, and a partial failure is possible, an example of this would be "only *part of* the requested *torque* is produced by the engine". This technique identifies system and component level hazards but also considers operability failures.

The benefits and characteristics of the HazOP are as follows:

- Far reaching scope to identify component and system-level requirements,
- Identifies potential failures through the use of function-deviating guide words such as "part of, more, less, late",
- Uses process parameters such as "torque, temperature, NVH" specific to the item of investigation.

2.5 Colorado State University

Colorado State University has long recognized the crucial role that the interplay of energy and mobility has around the globe and has pioneered research in this area. Colorado State University's (CSU) Engines and Energy Conversion Laboratory is an unparalleled network of researchers, centers and facilities focused on energy research, development and innovation. The Engines and Energy Conversion Laboratory is located at CSU's Energy Institute - Powerhouse Energy Campus which serves as a unifying hub for clean energy research, policy centers and start-up companies. Through its 13 affiliated centers, the Institute aims to increase collaboration with industry and governmental partners to solve real-world energy problems, and to accelerate the dissemination of CSU research and solutions.

2.5.1 Colorado State University - EcoCAR

One of the means by which CSU has built its research and workforce development program is through vehicle design/build/test programs. CSU has been a participant in the prestigious Advanced Vehicle Technology Competition (AVTC) "EcoCAR" since its inception with the primary objective of converting a conventional vehicle into a hybrid electric vehicle to meet the specific functional and technical requirements of the EcoCAR competition. The current EcoCAR competition is the fourth in this line of AVTCs. Each of the previous competitions had a unique set of rules which the teams must develop their systems around. These rules may be more performance driven, as was the case in EcoCAR 3, or more environmentally driven, as was the case in EcoCAR 2.

2019 begins the first of four years of the new "The EcoCAR Mobility Challenge (MC)" competition. The current competition tasks 13 North American universities to apply advanced propulsion systems, SAE Level 2 autonomy, Vehicle-2-X connectivity, and connected and automated vehicles (CAVs) to improve the energy consumption of a 2019 Chevrolet Blazer without compromising the vehicles emissions, drivability, utility, or safety [24]. A competition objective is to provide a real-world training ground for students to gain hands-on experience following a vehicle development process to design, build, and refine advanced technology vehicles [25].

In the case of EcoCAR MC, CAVs, which makes up 40% of the competition activities, includes systems such as adaptive cruise control (longitudinal autonomy), Vehicle-to-X-communication, lane keeping assist (limited lateral autonomy), and in-cabin augmented reality [26]. CAVs achieves a SAE Level 2 autonomy by implementing automated functions like acceleration and steering, but the driver must still remain engaged with the driving task and monitor the environment at all times. The addition of these embedded systems can have critical safety concerns, especially at the institutional level where manpower, time, and funding may be restricted compared to larger automotive companies. The development of an adequate functional safety concept is critical to the success of the project and safety of personnel, environment, and equipment.

The EcoCAR MC requires that the teams allocate a systems safety manager to address these issues, along with teams devoted to propulsion systems integration (PSI), controls systems modeling and simulation (CSMS), CAVs, and project management [26]. The vehicle will compete annually in a variety of events of which safety is the foundation. A few of these events include CAVs perception and longitudinal safety evaluation and propulsions system on-road safety evaluation. Successful completion of the evaluations will be an initial validation to the stakeholders that the system meets the safety requirements to perform the following rounds of evaluations. The systems safety manager is responsible for developing the system, functional, and technical requirements using a recommended General Motors (GM) system safety process outline previously.

2.5.2 Colorado State University – Toyota

Similar to EcoCAR, CSU has also been conducting research funded by Toyota Gasoline Hybrids Vehicles Research and Development to determine fuel economy impacts of predictive optimal energy management strategies [27]. Specifically, this project researches the application of pre-computed acceleration event controls as acceleration events provide particularly attractive opportunities for predictive optimal energy management because of their high energy cost and limited variability. This research also requires a full architectural redesign of a conventional vehicle into a hybrid electric vehicle. A thorough and documented safety analysis and testing plan is required and must be approved by the stakeholders.

The test vehicle platform (TVP) is a 2018 Toyota Tacoma. The objective of the TVP will be to demonstrate measurable fuel economy improvements using a predictive acceleration event (PAE) control strategy. Those improvements will be measured relative to a baseline control

strategy that does not use prediction. In order to get reliable data which can demonstrate the fuel economy improvements, the TVP team is implementing an autonomous switch activated drive cycle that is highly repeatable for both the PAE and baseline control strategies. The autonomous drive cycles command longitudinal movements only and leave lateral control in the hands of the operator. The predicative ability will come from a GPS signal accessible to the TVP's hybrid supervisory controller (HSC) [28]. The GPS signal will share the roads speed limit with the HSC which will then determine the optimal energy management strategy during acceleration events.

Regardless of the architecture type, from a hardware perspective the redesign will include the integration of an electric motor (EM) and a power source for that motor. This power source is often a high voltage battery pack built by the vehicle innovation team to meet the specific needs of the system. The addition of an EM involves reducing the length of the driveshaft and interfacing directly to the rear of the transmission in a P3 configuration. From a software perspective the redesign must include a hybrid supervisory controller which manages all other controllers including but not limited to the engine control module, transmission control module, and electric motor controller. The control strategies used by the HSC are original and independent to the redesigned vehicle. It is clear by the amount of modification to the Tacoma's hardware and controls systems that an early safety analysis and safety concept is going to guide the architecture design, component selection, and require a robust multi-phase test plan.

These vehicle innovation teams (VITs) are structured and preform in an equivalent manner to larger OEM's by categorizing sub-teams such as controls, powertrain, and highvoltage. Because the TVP's architectural redesign poses potentially severe safety risks to the operator, environment, and the vehicle platform its self, Toyota enforces strict standards for systems safety and requires CSU to incorporate a safety management team that is responsible for

the institutionalization a safety culture, development and execution of a hazard and risk analysis on the system, environment, and equipment, development of requirements, and ultimately ensuring safe production and operation. Toyota does not give guidance on the specifics of how to perform the safety analysis and test plan development so the safety management team has the availability to select from a range of analysis structures and techniques.

3 OBJECTIVES

The EcoCAR and Toyota projects are in development concurrently with the same management and system safety personnel working on both projects. The EcoCAR project requires a specific structure to part of the safety case analysis whereas the Toyota project has no requirement for structure of the safety case analysis. This allows the safety management team the opportunity to develop a structure that meets the needs of both projects. Because much of the redesign and additions are similar for both the EcoCAR and the TVP, the safety analysis will share many commonalities.

Colorado State University is consistently involved with vehicle innovation and the electrification of conventional vehicles. It would be ideal to have a comprehensive safety analysis to reference for future projects. Currently there is not a system that shares predecessor automotive safety work and for each new project the system safety manager has to start from the beginning with often little to no knowledge on the subject.

We seek to develop a set of objectives which contribute to provide answers to the following questions:

- Can a systems safety case be developed which addresses the concerns posed in the EcoCAR, Toyota, and future projects?
- What is an efficient and effective structure for performing a systems safety case?
- What is an efficient and effective method for performing a safety analysis during the HARA activity?
- What are critical safety concerns with implementing ADFs and ADAS

The objectives of this thesis are as follows:

Objective 1. *Provide a University-level automotive system safety process by determining the most effective ways to develop a risk informed safety case.*

Objective 2. Create a cross-functional safety working group procedure which will guide future safety managers, sub-team safety representatives, and provide requirements and testing traceability.

Objective 3. *Develop a comprehensive system safety analysis for a hybrid architecture advanced-vehicle build utilizing ADFs and ADAS.*

Objective 4. *Determine an efficient and effective HARA procedure for the various subsystems of a hybrid vehicle.*

Objective 5. *Determine critical safety concerns through the elicitation of safety goals and functional requirements.*

4 **RESULTS**

4.1 Safety Plan

A project plan defines the scope and high-level objectives of a project while the safety plan, defining high level safety concepts, is a compliment to this written report [13]. The safety plan cannot be thoroughly completed in the early stages of a project and is not intended to be inclusive of all safety elements because not all safety critical elements can be identified at this beginning stage of the project. This thesis's safety plan follows the ISO 26262 guidelines and therefore will include the following:

- Definition and plan of safety activities throughout the system safety lifecycle,
- Definition and assignment of roles and responsibilities regarding safety management and activities,
- Evidence of competence,
- Evidence of a good safety culture,
- Evidence of quality management,
- Cross-functional safety procedure.

4.1.1 Safety Activities throughout the System Safety Lifecycle

A well-structured systems safety process provides value through the entire engineering design, development, testing, and manufacturing phases of a systems process, and it provides early input to the system design by identifying potential hazards and determining the safety strategy. It then helps in the development of appropriate hardware, software and interface requirements ultimately leading to verification and validation of the system perforce to the defined requirements [13]. The system safety activity can have a significant impact on the systems content early in the development phases as the requirements that are allocated to major components can be vetted and traced to meet the system needs.

The structure and method of system safety activities determines the fidelity of the system safety case. A variety of widely used system safety processes have been outlined previously and all hold a very similar structure with differences only seen in term definitions and methods for analysis of individual safety activities.

To fulfill Objective 1 an initial Colorado State University System Safety Process was developed and later modified after completion of the concept phase functional requirements. The modified process can be seen in Figure 5 where the primary change to the layout was the elimination of the elicitation of ASIL ratings.

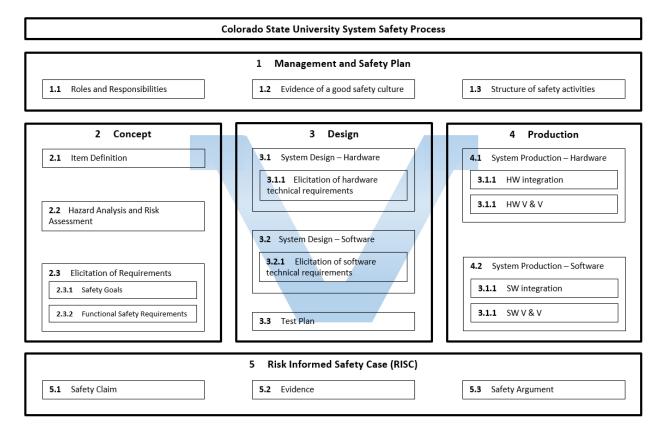


Figure 5. Colorado State University System Safety Process

After discussion with professional automotive system safety personnel at GM and Continental, it was recommended that the ASIL ratings not be used based on their subjective nature. This idea is reinforced by research documented by Khastgir [29] where the rule-set ASIL system was put to the test by conducting a workshop involving international functional safety experts as participants in an experiment where rules were provided for severity and controllability ratings. Khastgir states that based on the qualitative results and the variation seen, the rule-set was re-calibrated and a reduction in variation occurred. However, this experiment shows that ASIL ratings incur a large amount of variation of results, even among the automotive world's functional safety experts.

The general outline used in this system safety case aligns closely with ISO 26262 functional safety process with the following exceptions:

- Major phases are defined more closely matching a systems engineering V model
- ISO 26262 recommends using a HazOP and FMEA for the HARA activities. Instead a DFMEA, PHA, SEFA, HazOP, and STPA will be used here to elicit the safety goals and functional requirements
- In the definition and analysis of failure ISO 26262 does not include loss to the system or property. Instead a loss of property or systems will be included in this analysis (similar to NASA system safety process)
- NASA's Risk Informed Safety Case (RISC) method will be used to define the final safety case.

4.1.2 Cross-Functional Safety Procedure

A cross-functional safety procedure, fulfilling Objective 2 and fully documented in Appendix 1.2, is developed to facilitate the use of safety practices within the individual teams. For the purposes of University vehicle design projects, it is not possible for the system safety manager (SSM) to be completely involved in the technical low-level decision making of each team. In order to complete requirements, both technical and functional, and keep systems safety as a priority, the teams will follow this procedure when considering project scope and the implementation of systems.

The safety procedure requires that each team have a primary safety representative who will perform the steps to complete the safety objectives. These representatives should be identified very early in the project. The primary safety representative should be an individual with strong working knowledge of the low-level technical aspects of the team they are on. This individual will be the liaison between the safety manager and the specific team, tasked with translating system safety responsibilities and performing HARA activities. It is imperative that the safety representative set up times to allow for team collaboration in order to more thoroughly complete the safety activities.

The cross-functional safety procedure allows for the various teams working on a project to perform the appropriate safety analysis and provides guidance on how to do so. The document is easy to use and provides templates for each type of analysis. The teams can simple copy and paste the templates onto their own document and begin brainstorming. The SSM will guide and assist in ensuring the safety representatives have a thorough understand of how to complete the safety activities. It is critical that the individual teams perform their own analysis as they will undoubtedly present more unique and applicable safety concerns based on their subject matter

31

knowledge. But, the SSM should be an active participant in the individual teams HARA activities for the following reasons:

- The SSM has the most knowledge on how to perform the safety activities.
- The SSM can guide the teams on how to think about safety.
- The SSM will gain team specific low-level technical knowledge.
- The SSM will be the one compiling and presenting the information.
- The SSM must ensure oversight and that the work is being completed.

Often, the HARA activities can be intimidating to begin and the team specific safety representative may be unsure of how to respond to these tables. The objective of this procedure is not to be over-bearing with guidance and instruction but is to provide the necessities for completing the analysis with simple examples. It is important to encourage open-mindedness and reassure representatives that there are no poor considerations at the concept phase. Even if the idea has little potential to cause a hazard or failure, then it should be documented, evaluated and then discounted through this process. Because the team specific safety representative occasionally performs this duty as an additional role, the SSM should limit their individual scope and guide them to focus on components that are being added, modified, or interface and interact with the added and modified.

Each of the three vehicle design projects have utilized a similar team structure. The subteams outside of the managerial staff includes a propulsion system integration (PSI) team, a controls and system modeling & simulation (CSMS) team, and a connected and automated vehicles (CAVs) team. These teams will be instructed to perform specific tasks in the crossfunctional safety procedure based on requirements given by the project organizers. The structure of the team can be easily modified to suit the needs of any future project.

4.1.3 Roles and Responsibilities

Definition and assignment of roles and responsibilities regarding safety management and activities is the initial step to beginning the systems safety lifecycle. Roles shall be directed by the project manager and the safety management team shall be assigned based on project scope and individual expertise. The safety management team is a collection of team leads who have specific experience and will contribute at a technical level to the identification of potential hazards and mitigation solutions. Safety is a collaborative effort especially at the University projects where students' experience with system safety processes can be limited. Table 1 provides an example of the Roles and Responsibilities for the CSU-VIT

CSU VIT Roles and Responsibilities						
Role	Member	Responsibilities				
Project Manager	Dr. Thomas Bradley	Oversee high-level mission activities and operate in a supervisory capacity. Define project scope, and manage requirements, planning, schedule, budget, and stakeholder engagement.				
Powertrain Technical Manger	Gabriel Di Domenico Troy Johnson	Determine system/component requirements. Sourcing and procurement of component selection Integration of components and system build.				
Controls Technical Manager	David Trinko	Development of controls software. Determine system/component requirements through software simulation				
Systems Safety Manager	Matthew Knopf	Develop system safety case. Perform safety analysis and determine safety requirements. Develop test plan and V&V methods.				

Table 1. Example of "Roles and responsibilities"

4.1.4 Evidence of Competence

The project manager assigning the roles and responsibilities shall ensure those members

have sufficient skills, competencies, and qualifications in order to execute that assignment. Table

2 provides an example of the Evidence of Competence for CSU-VIT

Table 2. Example of "Evidence of Competence"

		CSU VIT Evidence of Competence
Member	Role	Evidence of Competence
Gabriel Di Domenico	Powertrain Technical Manager	Graduate research assistant involved in AVTC's for the previous 3 years. Currently also in role as PM for EcoCAR MC. Advanced study of hybrid electric vehicle architecture. Involved in the development and build of a hybrid Chevrolet Camaro
Troy Johnson	Powertrain Technical Manager	Graduate research assistant involved in FSAE as the PM role. Currently also in role as EM for EcoCAR MC. Advanced study of hybrid electric vehicle architecture.
David Trinko	Controls Technical Manager	Graduate research assistant involved in HEV development for previous 3 years. Advanced study of hybrid electric vehicle architecture. Integral part in the development of the controls for Toyota project.
Matthew Knopf	System Safety Manager	Graduate research assistant involved in AVTC's for the previous 2 years. Currently also in role as system safety manager for EcoCAR MC and acted in that role for EcoCAR 3. Involved in the development and build of a hybrid Chevrolet Camaro

4.1.5 Evidence of Quality Management

It is critical to institute and maintain a quality management system to support functional safety. Quality management, across all phases of the safety lifecycle, includes the university and facilities overall safety management, the project dependent safety management, and safety management regarding production, operation, service, and decommissioning [13].

Overall safety management ensures that those responsible for performing safety activities

in the safety lifecycle achieve the following objectives:

- Institute and maintain a top-down safety culture,
- Promotes effective communication across all disciplines,

- Institute and maintain adequate functional safety organizational rules and processes,
- Ensure training, guidance, a functional safety procedure is available for members,
- Ensure that the competence of the member is proportionate with their responsibilities.

Project dependent safety management ensures that during the concept development phase and at the system, hardware, and software-levels, the organization achieves the following objectives:

- Define safety activities for the system safety lifecycle,
- Plan, coordinate, and track the progress of safety activities,
- Create comprehensive safety cases in order to provide the argument for the achievement of functional safety,
- Decide at the end of development if the item achieves the minimum acceptable level of safety to be released for production and operation.

Safety management during the system lifecycle stages of production, operation, service, and decommissioning is a body of evidence, assembled from the previous work products, that justifies the system's level of safety during those phases of the product lifecycle.

4.1.6 Evidence of a Good Safety Culture

A good safety culture is a priority at the University level. Inexperience at any level of the systems engineering process can lead to severe safety implications. It is a requirement of the University, team, and individual to maintain functional safety and impose a commitment to integrity and excellence. It is important to note that a good safety culture requires management

35

buy-in then implementation throughout the facilities and working groups [13]. Table 3 provides

an example of the Evidence of a Good Safety Culture for CSU-VIT.

Table 3. Example of "Evidence of a Good Safety Culture"

Examples indicative of a poor safety culture	Examples indicative of a good safety culture
Accountability is not traceability	The process assures that accountability for decisions related to functional safety is documented and traceable
Cost and schedule take precedence over safety and quality	Safety is the highest priority
The reward system favors cost and schedule over safety and quality	The reward system supports and motivates the effective achievement of functional safety The reward system penalizes those who take short cuts that jeopardize safety or quality
Personnel assessing safety, quality, and their governing processes are influenced unduly by those responsible for executing the processes	 The process provides adequate checks and balances The appropriate level of independence in the safety, quality, verification, validation processes
 Passive attitude toward safety Heavy dependence on testing at the end of the product development cycle Management reacts only when there is a problem in the field 	 Proactive attitude towards safety Safety and quality issues are discovered and resolved from the earliest stage in the product lifecycle
The required resources are not planned or allocated in a timely manner	The required resources are allocated Skilled resources have the competence commensurate with the activity assigned
 "Groupthink" 'Stacking the deck" when forming review groups Dissenter is ostracized or labelled as "not a team player" Dissent reflects negatively on performance reviews "Minority dissenter" is labeled or treated as a "troublemaker", "not a team player", or a "whistleblower" Concerned employees fear repercussion 	 The process uses diversity to advantage Intellectual diversity is sought, valued, and integrated in all processes Behavior which counters the use of diversity is discouraged and penalized Supporting communication and decision-making channels exist and the management encourages their usage Self-disclosure is encouraged Disclosure of discovery by anyone else is encouraged The discovery and resolution process continues in the field
No systematic continuous improvement processes, learning cycles or other forms of "lessons learned" Processes are "ad hoc" or implicit	Continuous improvement is integral to all processes A defined traceable and controlled process followed a all levels, including - Management

- Engineering
- Development interfaces
- Verification
- Validation
- Functional safety audit
- Functional safety assessment

4.2 Item Definition

The definition of the term *item* is a system or array of systems to implement a function at the vehicle level that is able to cause harm to people inside or outside the vehicle [14]. In the early stages of concept development there are no concrete definitions of an item or system as these are confirmed from the development process but we can complete the item definition by anticipating which components will be used. The concept development phase begins with an item definition where the goal is to describe all items within a subsystem and their functionalities. Through this process the system safety analysist will begin to build an understanding of the item impact, interactions, interfaces and dependencies on other items and the system as a whole. ISO 26262 does recommend that the item definition include, in addition to the item, sub-items, and its functions, a written description of the dependencies on, and interactions with, the driver, the environment and other items at the vehicle level [14]. If not explicitly done during the item definition, dependencies, interactions, and interfaces will be investigated during the HARA activities. A procedure for performing the item definition is a follows:

- 1. Identify and group major vehicle systems,
- 2. Identify the items making up that system,
- 3. Identify the sub-items making up that item,
- 4. Determine a thorough list of the item functions focusing on the item inputs and outputs.

Identifying and grouping major vehicle systems can be accomplished by considering system boundaries. For hybrid vehicles the systems are PSI (mechanical, high-voltage), CSMS (controls hardware and software), and CAVs (semi-autonomous longitudinal and lateral control systems). Each of these has clearly defined boundaries and unique system functions.

Identifying the items making up the system will involve research and a greater understanding of the individual components involved in that system. These items can be viewed as subsystems because they provide a critical function to the vehicle and are comprised of sub-items. It is important to collaborate with the teams of the system you are working on since they will be knowledgeable of the items involved.

Identifying the sub-items will produce a thorough list of all components making up the item. It is the lowest level of the system component. Because of the intricacies of subsystems, research in conjunction with team collaboration, must be performed to accurately document all sub-items.

Determining a thorough list of the item functions is the final step in the item definition and illuminates the distinct roles of the item. The item function describes how the item contributes to the system, inputs to the item, interactions and interfaces, and outputs from the item. Like the previous steps, it can be helpful to research the item to identify the inputs and outputs. Table 8 shows the individual steps and how the item definition evolves.

38

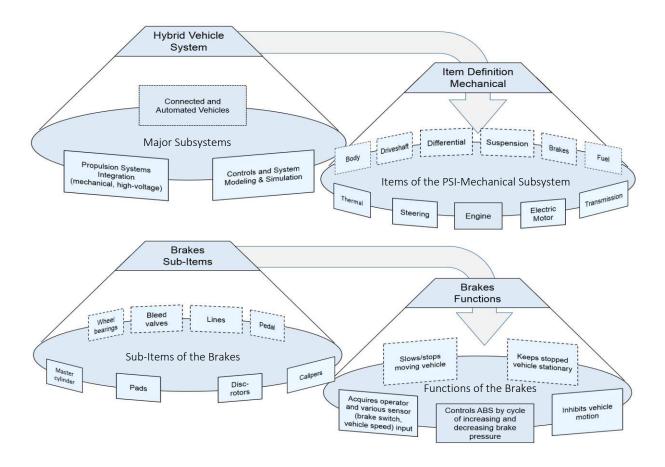


Figure 6. Flow chart describing a method for completing the Item Definition

The item definition is particularly useful in the investigation and documentation of some of the lesser understood items and functions such as CAVs, controls hardware, and controls software. This allows for the safety teams to list out all items and begin to formally document the potential functions of the items and sub-items. This process solidifies the decision making of which system owns which control functions and guides the team in determining constraints especially when software or functional ambiguity is present. Table 4 demonstrates the Item Definition for the CAVs system using the Intel Mobileye 6 camera as the item. The comprehensive CAVs Item Definition for the vehicle design project can be seen in Appendix 2.1.

CAVs Intel Mobileye 6 Item Definition					
Item	Sub-Item	Functional Behavior			
Intel Mobileye 6	Mount	- Performs multi-feature tracking			
	Wires	- Performs object and lane detection			
	Eye-Watch Display	- Performs forward collision warning			
	Senor	- Performs pedestrian collision warning			
		- Performs headway warning			
		- Performs traffic sign recognition			
		- Sends data to associated controller			
		- Provides a real-time display			

Table 4. Example of the Item definition for the CAVs system using the Intel Mobil Eye 6 Camera

As with many aspects of system safety analysis there is not a clearly defined comprehensive example of how to perform the Item Definition. The system safety analyst must use common sense and trial and error to determine the item, sub item, and functions of a system. For the propulsion systems integration (PSI) the items, sub-items, and functions are obvious. The item would be all major hardware systems such as the brakes, steering, engine etc... while the sub items would be the components making up those individual systems such as brake pads, lines, rotors etc... The functions of these items are also easy to identify especially when working in collaboration. It is still very beneficial to research articles on the functions of these items where more experienced professionals can better speak to the inputs and outputs. The comprehensive PSI Item Definition for the vehicle design project can be seen in Appendix 2.3 and Appendix 2.4.

Common sense and trial and error plays a role in the vehicle systems where the items and functions are less obvious. For example, during the analysis of the CSMS systems it was

challenging to decide if the controls hardware or the controls software was the item and what the specific functions would be. After producing both, it was easier to justify the controls hardware as the item because the hardware drew clearly defined boundaries around each item and its functions. Table 5 demonstrates an example from the CSMS Item Definition using the HSC as the item. The comprehensive CSMS Item Definition for the vehicle design project can be seen in Appendix 2.2.

Table 5. Example of the CSMS Item Definition using the HSC as the item

	CSMS HSC Item Definition							
Item	Sub-Item	Functional Behavior						
HSC	Connectors	- Acquires operator and various sensor inputs (APPS, gear, vehicle speed)						
	Mounts	- Controls all hybrid driving functions						
	Wire	 Controls torque via engine/EM torque split using rules-based or PAE control strategy 						
	Controller	- Maintains SOC at appropriate level						
		- Determines gear shifting						
		- Modifies stock signals						

It is important to account for and understand the item functions. These functions will be carried through and built upon during the course of the systems safety lifecycle and the HARA activities specifically. They will help determine hazards, failure modes and ultimately feed the safety goals and requirements. Typically during HARAs, the potential hazard or deviation is the failure of an item's function. For example, if one of the functions of the brakes is to: *inhibit vehicle motion* then the failure type would be that the brakes: *fail to inhibit vehicle motion*. During a DFMEA you would continue the analysis by saying a potential impact of this failure is: *unintended longitudinal motion* with a potential cause being: *brake pad/rotor failure*. The safety goal of this example could be that: *the brake system shall inhibit vehicle motion to match driver*

intent. In this example, we can see how an accurate description and awareness of the item's intended function is built upon and eventually results in a thorough understanding of failure types, the potential impact, causes, prevention, detection, and mitigation modes, and ultimately the safety goal and functional requirements.

A thorough analysis of the item definition will highlight item functions which clearly have a more critical risk association. This will be identified by the function's ability to potentially cause a loss of acceleration, braking, steering, or system failures that could cause the vehicle to decelerate or accelerate suddenly.

4.3 Application of HARA

As discussed in the background, there are many types and techniques of HARAs which can be applied throughout the system lifecycle. Because we are in the concept development stages of both the Toyota and the EcoCAR projects the HARA activities were focused on techniques which would provide safety goals, functional requirements, and guidance during this early design phase. We seek to know what techniques of HARA's will most effectively and efficiently produce potential hazards and provide detection and mitigation methods. The automotive industry routinely uses a common set of hazard identification methods [10] [17]. With this in mind the HARAs used during this activity were the PHA, DFMEA, SEFA, HazOP, and STPA.

For each team performing the HARA, a structured analysis is produced and followed. Each team performs a minimum of both an inductive and exploratory HARA technique. Based on some preliminary research, the general structure of the various analysis methods, and

42

discussions with systems safety representatives, specific techniques were chosen and performed for each team and subsystem.

CAVs is implementing a system of autonomous controls for lateral and longitudinal motion using a network of sensors and control strategies. The nature of this system is reliant on the recognition of vehicle deviation and the strategy for corrective action. Innately this would benefit from using an exploratory HARA technique and based on the template setup and type of analysis a STPA would likely produce the most complete and relevant set of safety goals and functional requirements. In an attempt to expand the investigation and further identify unique hazards of CAVs a DFMEA specific to the LKA and ACC systems was produced. The LKA and ACC systems control longitudinal and lateral motion so it would be beneficial to do an analysis specific to these two control strategies. A PHA was produced using the CAVs system as a whole in an effort to determine variances in between the PHA and DFMEA techniques.

CSMS is strictly a software system with arguably the greatest risk for potential hazards. CSMS controls all hybrid driving functions and subsystems. It is out of the CSMS that unintended vehicle behavior could most likely occur, including important safety considerations such as unintended accelerations, thermal runaway, and high voltage de-energizing. The LKA and ACC systems utilize aspects of both the CSMS and CAVs systems. Integration of CSMS controls hardware was determined to be a part of the PSI Mechanical team but the controls functionality is clearly within the CSMS domain.

The domain of PSI includes the largest amount of components and system interfaces and interactions. PSI is responsible for all mechanical/powertrain, HV, and controls hardware items. There are often clear "mechanical" and "component-level" distinctions between these systems which the DFMEA, SEFA and HazOP activities has the ability to address individually. A SEFA

43

is produced on the PSI system as a whole, while the HV components will be analyzed with a DFMEA and HazOP. The PSI Mechanical items will also be analyzed using a DFMEA and HazOP. In total, 5 individual HARA techniques will be used and 11 separate analysis will be performed to elicit safety goals and functional requirements. The techniques and their associated system of analysis are shown below.

- CAVs PHA
- CAVs / CSMS ACC System DFMEA
- CAVs / CSMS LKA System DFMEA, STPA
- CSMS DFMEA
- **PSI** SEFA
- **PSI HV** DFMEA, HazOP
- **PSI Mechanical** DFMEA, HazOP
- PSI / CSMS Controls Hardware HazOP

The HARA activities are often performed in a collaborative setting including contributions from the system safety manager, team-specific system safety representative, engineering manager, and team-specific safety representative. The systems safety manager normally leads this discussion and the team completes the analysis step by step until all HARA activities have been finalized.

There is not an available comprehensive resource or template guiding the safety analysist to perform the HARA activities. An important contribution of this thesis is the templates provided and the thoroughly documented safety analysis of each of the methods used.

4.3.1 HARA applied using PHA

The PHA was performed on the CAVs system as an initial method for determining a broad range of safety goals and functional requirements. The template used to complete the PHA can be seen in Table 6. The PHA moves through the analysis at the item level using the following steps:

- 1. Produce a block diagram of the relevant systems,
- 2. Identify potential hazards,
- 3. Identify causes of the hazard,
- 4. Identify major effects of the hazard,
- 5. Identify corrective and preventative measures of the hazard,
- 6. Determine and document the requirements.

Table 6. Template used to perform the PHA

PHA Template						
Item:						
Potential Hazard	Cause	Major Effect	Corrective/Preventative Measures	Requirement		

Producing a block diagram can be done at the item or system-level. Both will visualize the items interfaces and interactions with other components. This step allows the analyst to gain a better understanding of how the item assists the systems functionality

Identifying the potential hazards is an item level analysis which describes a failure of the items function that was documented in the item definition. An example using the item "brakes" would be a failure to slow or stop a moving vehicle, where slowing or stopping a moving vehicle is a function described in the item definition.

Identifying potential causes of the hazard relies on a very strong understanding of how the item acts. Considerations for this section are environmental causes, operator causes, or sub-item causes. Emphasis should be placed on causes which produce a critical system impact such as unintended vehicle motion. Common causes found during the analysis include:

- Wiring failures
- Unintended access or physical damage to the item
- Power failure
- Operation outside of min/max temperature range
- Sub-item failures
- Signal failures (latency, EMI, noise)
- Coding errors

Identifying the major effects of the hazard will highlight those effects which are more safety critical and guide the preventative measures. This step is more creative than the previous and can begin by asking "what if". It can also be useful research item impacts from a situations which may cause a hazard. This can be more difficult to do when analyzing software and electronic systems. Common critical effects found during the analysis include:

- Unintended longitudinal or lateral motion
- Loss or degradation of propulsion
- Operator and/or passenger injury
- Damage to or loss of property
- Damage to the environment
- Fire or thermal event

Identifying corrective and preventative measures of the hazard is done from understanding the cause and effect. This step can be completed in part by looking at the item manufactures specification sheet where they will describe installation and operating specifications. Less obvious and more creative prevention methods will also be identified especially if using a working group brainstorming approach. The measures identified here will directly lead to the item functional requirements.

Documenting the requirements that are a result of these system safety considerations is essentially a rewording of the corrective and preventative measures. The automotive system safety industry uses common and formal verbiage to describe a functional requirement through methods known as "shall statements". An example of the preventative measure and associated requirement are shown in Table 7.

Table 7. Example of a corrective/preventative measure and the associated requirement

CAVs Requirement Production					
Item: CAVs Intel Tank Computer					
Corrective/Preventative Measures Requirement					
To reduce computer signal input and output noise ensure wires are kept away from electrical machinery, are as short as possible, and use shielding	To reduce CAVs systems computer signal input and output noise the development team shall ensure wires are kept away from electrical machinery, are as short as possible, and use shielding				

ne 7. Example of a corrective/preventative measure and the associated requireme

4.3.2 HARA applied using DFMEA

The DFMEA is an item level hazard analysis which was performed on the CAVs / CSMS

LKA and ACC systems, CSMS, and the PSI Mechanical and HV systems. After performing this

analysis it was found that the template and requirements are very similar to those of the PHA.

The major difference between the two methods is that the DFMEA determines a risk priority

number (RPN) based on the severity, occurrence, and detection or the failure. The template used to complete the DFMEA can be seen in Table 8. The steps to completing the DFMEA include:

- 1. Produce a block diagram of the relevant system,
- 2. Document the function,
- 3. Identify the failure type,
- 4. Identify the potential impact and severity (S) involved,
- 5. Identify the potential causes and the likelihood of occurrence (O),
- 6. Identify the prevention modes, detection modes, and the ease at which the failure is detected (D),
- 7. Determine the risk priority number (RPN) using the formula,

RPN = *Severity* * *Occurance* * *Detection*

8. Determine and document the resulting requirements.

Table 8.	Template	used to	perform	the	DFMEA

	DFMEA Template									
Item:										
No. Function	Failure Type	Potential Impact	s	Potential Cause	0	Prevention Mode	Detection Mode	D	RPN	Requirement

Producing a block diagram can be done at the item or system-level, just like the PHAs block diagram, and provides a better understanding of the items interactions and interfaces with other components

Documenting the function is taken directly from the function, as determined and documented in the item definition. If an addition or update to the function occurs during the

DFMEA then it should also be updated in the item definition. This step will allow the safety analyst to easily state the failure type.

Identifying the failure type is a direct failure of the function of the item. For example if the function of the item "CAVs LKA" is to "*control lateral movement via electric power steering*", then the failure type would be "*failure to control lateral movement via electric power steering*".

Identifying the potential impact for a DFMEA is very similar to identifying the effects for a PHA. There are common high-level impacts which pose a critical safety risk. In addition to those mentioned in the effects column of the PHA, others found during the analysis include:

- Unintended acceleration
- Unintended exposure to toxic/flammable components
- Unintended exposure to HV

Determining the severity of a failure is subjective, especially when considering new or modified components, but a standard is available which is used to make this task more consistent. Table 9 describes the criteria and description for the severity rating.

Table 9. Severity rating scale with descriptions and associated criteria [30]

No.	Description	Criteria	
1	No effect	No discernible effect.	
2	Annoyance	Appearance or Audible Noise, vehicle operable, item does not conform. Defect noticed by discriminating customers (< 25%).	
3	Annoyance	Appearance or Audible Noise, vehicle operable, item does not conform. Defect noticed by many customers (50%).	
4	Annoyance	Appearance or Audible Noise, vehicle operable, item does not conform. Defect noticed by most customers (> 75%).	
5	Degradation of secondary function	Degradation of secondary function (vehicle operable, but comfort / convenience functions at reduced level of performance).	
6	Loss of secondary function	Loss of secondary function (vehicle operable, but comfort / convenience functions inoperable).	
7	Degradation of primary function	Degradation of primary function (vehicle operable, but at reduced level of performance).	
8	Loss of primary function	Loss of primary function (vehicle inoperable, does not affect safe vehicle operation).	
9	Safety and/or regulatory compliance	Potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulation with warning.	
10	Safety and/or regulatory compliance	Potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulation without warning.	

Severity Rating Scale

Identifying the potential causes of a failure during the DFMEA is identical to that step in the

PHA analysis and can be determined looking at the following:

- Environmental factors (debris, weather, NVH)
- Operational inputs (vehicle speed, gear selection, APP)
- Operational modes (PRNDL)
- Sub-item failures (line leaks, broken belt, component fatigue)

Determining the likelihood of occurrence is also subjective and a standard is available which

helps guide the analysist with consistent application. Table 10 describes the criteria and

description for the occurrence rating.

	Occurrence Rating Scale					
No.	Description	Criteria				
1	Very low	Failure is eliminated through preventative control.				
2	Low	No observed failures associated with almost identical design or in design simulation and testing.				
3	Low	Only isolated failures associated with almost identical design or in design simulation and testing.				
4	Moderate	Isolated failures associated with similar design or in design simulation and testing.				
5	Moderate	Occasional failures associated with similar designs or in design simulation and testing.				
6	Moderate	Frequent failures associated with similar designs or in design simulation and testing.				
7	High	Failure is uncertain with new design, new application, or change in duty cycle/operating conditions.				
8	High	Failure is likely with new design, new application, or change in duty cycle/operating conditions.				
9	High	Failure is inevitable with new design, new application, or change in duty cycle/operating conditions.				
10	Very high	New technology/new design with no history.				

Identifying the prevention mode involves a low-level understanding of the item and the cause of failure. Prevention methods can be hardware mitigation, software control strategies, or operational restrictions. Some hardware prevention methods can be found from the item manufacturer specification sheet where they describe mechanical constraints and installation requirements. Software control strategies may impose operational limits and actuate a

preventative action such as running a cooling system when a components temperature reaches a specified limit.

Identifying the detection mode will state the earliest time a failure can be detected and during what operational mode it can be detected in. It was found that in many cases detection can only occur while the vehicle is in an operation, which is inherently more dangerous than if it could be detected and vetted during the development phases, during diagnostics or while the vehicle was inoperable.

Determining the possible detectability of a failure can be equally as ambiguous as determining the severity and occurrence but a standard has been produced to assist in applying a consistent approach. Table 11 describes the criteria and description for the detection rating. Table 11. Detection rating scale with descriptions and associated criteria [30]

No.	Description	Criteria
1	Detection Not Applicable - Failure Prevention	Failure cause or failure mode cannot occur because it is fully prevented through design solutions (e.g. Proven design standard/best practice or common material, etc.).
2	Virtual Analysis - Correlated	Design analysis/detection controls have a strong detection capability. Virtual Analysis (e.g. CAE, FEA, etc.) is highly correlated with actual and/or expected operating conditions prior to design freeze.
3	Prior to Design Freeze	Product validation (reliability testing, development or validation tests) prior to design freeze using degradation testing (e.g. data trends, before/after values, etc.).
4	Prior to Design Freeze	Product validation (reliability testing, development or validation tests) prior to design freeze using test to failure (e.g. until leaks, yields, cracks, etc.).
5	Prior to Design Freeze	Product validation (reliability testing, development or validation tests) prior to design freeze using pass/fail testing (e.g. acceptance criteria for performance, function checks, etc.).
6	Post Design Freeze and Prior to Launch	Product verification/validation after design freeze and prior to launch with degradation testing (Subsystem or system testing after durability test e.g. Function check).
7	Post Design Freeze and Prior to Launch	Product verification/validation after design freeze and prior to launch with test to failure testing (Subsystem or system testing until failure occurs, testing of system interactions, etc.).
8	Post Design Freeze and Prior to Launch	Product verification/validation after design freeze and prior to launch with pass/fail testing (Subsystem or system testing with acceptance criteria e.g. Ride & handling, shipping evaluation, etc.).
9	Difficult to Detect	Design analysis/detection controls have a weak detection capability; Virtual Analysis (e.g. CAE, FEA, etc.) is not correlated to the expected actual operating conditions.
10	Absolute Uncertainty	No current design control; Cannot detect or is not analyzed.

Detection Rating Scale

Determining the risk priority number allows the analyst to easily identify which failure causes pose the greatest risk. Although the application of determining the severity, occurrence, and detection will seem subjective, at this stage in the analysis high risk items will stand out. To determine the RPN the analyst will multiple the severity, occurrence and detection numbers with the highest possible value being 1000. It is beneficial to perform the severity, occurrence, and detection ratings after all analysis has been complete and in one sitting so that the ratings will be applied more consistently and under a continual thought process.

Producing the requirements is the final step of the DFMEA template and is accomplished by rewording the failure type, potential cause, and prevention mode. This step requires the use of specific verbiage and sentence structure. It can be beneficial to word the prevention mode very similarly to how the requirement will be worded. This allows for easy documentation of the requirement. When writing the requirement, be specific. State what it is preventing, who will perform the prevention mitigation, and how it will be prevented. Table 12 shows a partial example of how this might look with select columns of the DFMEA omitted.

	DFMEA Applies to the LKA System							
Item: LKA system								
Failure Type	Potential Impact	Potential causes	Prevention Mode	Requirement				
Failure to performs lane- line, object detection and multi-feature tracking	Unintended lateral motion	Sensor visibility obstruction	To prevent a lane-line, object detection, or multi-feature tracking failure ensure sensors have clear field of view and are free of visibility obstructions	To prevent a lane-line, object detection, or multi-feature tracking failure the development team shall ensure sensors have a clear field of view and are free of visibility obstructions				

Table 12. Forming the requirement from the DFMEA prevention mode and failure type

The DFMEA uses the failure of the function of an item to determine potential impacts, causes, prevention, and detection modes. The prevention mode is often a translation and advancement of the cause of the failure which then becomes a requirement while the function is stated as a safety goal. The DFMEA method produced the largest set of safety goals and functional requirements but in our execution was especially repetitive in that it identified

requirements often related to the installation, operation, and maintenance of the item system being analyzed.

We can see that the PHA and DFMEA are similar in template setup, analysis method, and requirements elicitation, but the DMFEA is a slightly more thorough technique. The DFMEA forces the analysist to consider the severity, occurrence, and detectability of the failure which produces the RPN. This quantitative step helps visualize the critical nature of a failure as compared to all other failures. The DFMEA also allows for the analyst to consider detection modes which is the beginning of thinking about a testing procedure for the failure.

4.3.3 HARA applied using SEFA

The SEFA is system-level analysis technique performed by modeling the "failing" of a single element and analyzing its impact throughout other elements. The SEFA is not typically performed on software systems but is often conducted on actuators, motors, and other functional elements. For our analysis the SEFA was used on PSI systems. Table 13 and Table 14 show the templates used to complete the SEFA. The steps to completing the SEFA include:

- 1. Produce a system-level block diagram,
- 2. Identify systems operational states,
- 3. Name all elements within the system,
- 4. Identify the behavioral function of each element,
- 5. "Fail" each element individually,
- 6. Identify the impact of the element fault,
- 7. Identify the immediate resulting state prior to mitigation actions,
- 8. Identify the potential safety hazards,

- 9. Determine diagnostic methods,
- 10. Determine mitigation actions,
- 11. Identify the system state after mitigation action,
- 12. Determine and document requirements.

Table 13. Template 1 of 2 used to perform the SEFA

SEFA Template 1 of 2								
Multiple Range			-	perating				
Scenario		1	2	3	Impact of Item	Immediate		
(P,R,N,D)	Item Functions				Fault	Resulting State		
_	Range Operating	Range Operating Scenario	MultipleItenRangeStatOperating1	Multiple RangeItem No. Op StatesOperating Scenario112	Multiple RangeItem No. Operating StatesOperating Scenario1123	Multiple Range Item No. Operating States Operating 1 1 2 3 Impact of Item		

Table 14. Template 2 of 2 used to perform the SEFA

SEFA Template 2 of 2							
Item	Potential Safety	Diagnostic	Mitigation	System State After	Safety		
No.	Hazard	Method	Method	Mitigation	Requirement		

Producing a system-level block diagram helps identify element placement, interactions, and interfaces. It allows for a visualization of the system under analysis which better indicates potential element failures when performing the SEFA.

Identifying the operational states allows the analysist to perform the SEFA on multiple operating scenarios such as park, reverse, neutral, and drive. This will be used in understanding the immediate resulting state prior to and after mitigation methods are introduced.

Naming all elements in the system prepares the analysist for performing the "failure" section of the SEFA.

Identifying the behavioral function of the element should come directly from the item definition. If elemental functions are identified during the SEFA it should be updated in the item definition.

"Failing" each element individually is the first analytical step in this analysis and involves considering the impact on all other elements within the system. To fail the element, the analysist places a "0" in the associated "Item No. Operating State" column, then moves along the same row considering the state impact of each element listed. In this step, "0" means the element does not provide functionality to system as a whole and "1" mean the element does provide functionality to the system as a whole

Identifying the impact of the element fault simply states the system effects prior to any mitigation actions.

Identifying the immediate resulting state prior to mitigation actions helps to identify how the vehicle will perform after the failure is incurred. Table 15 shows an example thus far of how the SEFA is performed.

	Multiple Range Operating Scenario		Item No. Operating States				
Item No.	(P,R,N,D)	Item Functions	1	2	3	Impact of Item Fault	Immediate Resulting State
1	Driveshaft	Longitudinal shaft which transmits torque from engine/transmission to rear of vehicle	0	0	0	No torque transfer from engine/motor to differential	Vehicle decelerates to a stop Zero propulsive capability
2	Motor	Provides torque at user request by converting onboard stored electrical energy into rotational motion. Allows for energy regeneration and transfer to the battery during negative-torque events	1	0	1	Reduced power generation No torque generated from electrical energy transfer from ESS Vehicle runs on engine only	All operational states possible
3	Engine	Provide torque at request of operator by converting gasoline energy into kinetic motion	1	1	0	Reduced power generation No torque generation from stored energy in fuel tank Vehicle runs on motor only	All operational states possible

Table 15. Example of SEFA template 1 of 2 with analysis using the PSI subsystem and a P3 architecture

SEFA Applied to PSI Subsystem

• Unintended longitudinal or lateral motion,

• Loss or degradation of propulsion,

include:

• Operator and/or passenger injury,

Identifying the potential safety hazard is identical to the hazard step in the DFMEA and

PHA. The analysist should focus on hazards that pose a critical safety risk to the operator,

passengers, pedestrians, environment, or property. Commonly used critical safety hazards

- Unintended exposure to toxic/flammable components,
- Unintended exposure to HV.

Determining diagnostic methods allows the analyst to consider how the fault will be identified and assists in structuring the testing procedure. Because of the number of new and modified systems, the diagnostic methods will rarely come from the commonly used OBD II port but will often come from newly implemented software verification and validation checks which should then notify the operator when a system is functioning outside of normal limits.

Determining a mitigation action is particular to the fault and a product of the diagnostic method. In the ideal scenario, a software-identified corrective control action can provide an early diagnostic and mitigation action to prevent a safety hazard. If the unsafe control action cannot be diagnosed and mitigated from a controls perspective, then the operator would be required to perform the mitigation action. It was found that in any event, the operator must be allowed to override a corrective control action with minimal force and in short time.

Immediately following the mitigation method, the safety analyst should document the system state to identify the vehicle operational range. To describe a few examples, this would specify if (after the particular failure) the vehicle were stopped, capable of drive or reserve, or has any propulsive ability.

The final step in a SEFA analysis is determining and documenting the safety goals and functional requirements. This is similar to the safety goals and requirements step of the previously described HARA techniques but adds the diagnostic and mitigation wording into the requirement. The safety goal will restate the items function using the correct verbiage while the requirement will restate the failure of the function, impact of the fault, and the diagnostic and

59

mitigation method using correct verbiage. Table 16 describes an example of part 2 of the SEFA

template as a continuation from Table 15 above.

		SEFA A	pplied to the PSI Su	ıbsystem	
Item No.	Potential Safety Hazard	Diagnostic Method	Mitigation Method	System State After Mitigation	Safety Requirement
					Safety Requirement To prevent motor failure due to overheating the EMC shall actuate thermal controls to maintain motor temperature within a specified limit To prevent motor failure due to over- torque or over-speed, the HSC shall impose a governor to regulate to motor torque and speed to specified limits To prevent motor failure due to over- current the EMC shall impose a governor to regulate the flow of current within specified limits of the motor and battery pack
			motor, battery pack, or EMC exceeds specified current limits		To prevent motor failure the operator shall be provided real- time diagnostics and
			Allow operator override to discontinue motor operation		have the capability to discontinue motor operations

Table 16. Example of SEFA template 2 of 2 with analysis using the PSI subsystem and a P3 architecture

4.3.3 HARA applied using HazOP

The HazOP is both an item-level and system-level hazard analysis technique used, in our example, by the PSI team to determine human-caused and difficult-to-detect hazards. This

technique was used by the PSI team to analyze the mechanical, HV, and controls hardware systems. This is a two-part method using process parameters and guide words unique to the system being analyzed. Table 17 and Table 18 show the templates used to complete the HazOP. The steps to complete the HazOP are as follows:

- 1. Identify the item or system being analyzed,
- 2. Produce the process parameter and guide word chart,
 - a. Identify process parameters specific to the item,
 - b. Determine which guide words are applicable to the process parameter,
- 3. Complete the HazOP table using the specific process parameter and guide word,
 - a. Determine the deviation of the item,
 - b. Determine the consequences of the deviation,
 - c. Determine the causes of the deviation,
 - d. Determine safeguards to the deviation,
 - e. Determine and document the safety goal and requirement.

	Process Parameter Template											
	Guide Word											
Process Parameter	No	As well as	Part of	Reverse	Early	Late	Before	After	Faster	Slower	More	Less

Table 17.	Template used	to perform the	process parameter	chart of the HazOP
-----------	---------------	----------------	-------------------	--------------------

HazOP Template								
Process Parar	Process Parameter applied to Item:							
Guide Word Deviation Consequences Causes Safeguards Requirement								

Identification of the item or system being analyzed will come directly from the item definition. In our case, a system-level HazOP was performed. The difference being, for example, the analysis was applied to the high voltage energy storage system rather than the HV components (i.e. wiring harness, battery pack) individually.

The first step in producing the process parameter chart is to identify what process parameters apply to the specific system under analysis. For example, a high voltage system would have parameters such as temperature, current, voltage, clearance, or vibration while a controls software system would have signal, current, latency, noise, bandwidth, storage, or logic, to name a few. Table 19 describes the process parameters which can be used by each system while performing a HazOP. This can also be performed on specific system functions such as the LKA and ACC functions.

Major Subsystems and Associated Process Parameters				
PSI Mechanical	PSI High Voltage	PSI Controls Hardware	CAVs	CSMS
Vibration	Vibration	Vibration	Sensor Visibility	Signal Current
Torque	Temperature	Temperature	Signal Current	Signal Noise
Temperature	Current	Current	Signal Noise	Signal Bandwidth
Acceleration	Clearance	Clearance	Signal Bandwidth	Signal Latency
Deceleration	(maintenance, overheat, EMI)	(maintenance, overheat, EMI)	Signal Latency	Logic faults
Current	Unauthorized Access		Logic faults	Storage
Clearance	Voltage		Storage	Algorithm faults
(maintenance, overheat, EMI)			Algorithm faults	Clearance (EMI)
			Clearance (maintenance, overheat, EMI)	

Determining which guide words are applicable is relatively straight-forward but not all guide words will be used for a specific parameter. If the parameter can be applied in the way the guide word indicates and poses a potential safety risk then it should be used. The guide words should not be selected if there is no resulting hazardous event. The analyst should use best judgment and has the freedom to add parameters and guide words as necessary. Table 20 demonstrates an example of the process parameter and guide word combination chart for a HV system.

	Guide Word											
HV Process Parameter	No	As well as	Part of	Reverse	Early	Late	Before	After	Faster	Slower	More	Less
NVH									Х		Х	
Temperature											Х	Х
Current	Х		Х	Х	Х	Х					Х	Х
Voltage	Х		Х								Х	Х
Clearance											Х	Х
Unauthorized Access											Х	

Table 20. Process parameter and guide word chart for a HV system (X indicates a relevant guideword and process parameter combination)

Completing the HazOP table using the specific process parameters and guide words is the next step of this HARA activity. The table is very similar to the previous analysis methods in that the analysist identifies the deviation, consequence, causes, safeguards or mitigation methods, and requirements based on the application of the parameter and guide word.

Determining the deviation can be accomplished simply by stating the guide word and parameter in a way which describes a fault to the system or item under investigation. For example, the deviation could be, "No voltage to input terminal".

Determining the consequences of the deviation is identical to the effects columns of the PHA, DFMEA, and SEFA activities described previously. Commonly used safety-critical consequences are listed under the descriptions of the PHA and DFMEA and typically involve unintended movements and or injury to the operator or passengers.

Determining the causes of the deviation is not a restating of the guide word and parameter but rather a brainstorming as to the reasons for the guide word action. This describes how the deviation occurs and can be anything from hardware item failure, obstructed sensor view, or software failures. Assuming the causes of deviation is a critical step to determining safeguards and ultimately producing the requirement. Time should be allocated to discussion with subject matter experts to produce a comprehensive list of possibilities.

Determining safeguards to the cause of the deviation will have the greatest impact on the requirement. The safeguard is a description of the preventative and corrective measures used to identify and mitigate the hazard, either by producing a reduction in severity or occurrence. Broad examples of safeguards can be software control actions, implementation of manual emergency-stop switches, or an increase in the factor of safety for mechanical items.

Producing the requirement will be a restating of the deviation, cause, and safeguard using the common system safety verbiage. Table 21 shows a partial example of the HazOP table when temperature stimulus is applied to the HV system.

Guide Word	Deviation	Consequences	Causes	Safeguards	Requirement
More	High voltage system component temperatures exceed max	Failure of high voltage components Thermal runaway	High voltage component (battery pack, battery module, BMS, EMC) failure	All necessary high- voltage components will operate within specified temperature limits	To avoid operation outside of min/max temperature range all necessary high-voltage components shall operate within specified temperature limits
	operating temperature	Injury to operator and or passengers Loss or	High voltage thermal control (fans, coolant)	The high voltage system will be thermally controlled	To avoid operation outside of min/max temperature range the high voltage system shall be thermally controlled
		degradation of propulsion Unintended access to high voltage	failure Unintended access causing short circuit	The thermal control software will be validated during SIL, HIL, and closed course testing	To avoid operation outside of min/max temperature range the thermal control software shall be validated during SIL, HIL, and closed course testing
			Software controls program failure (logic, incorrect limit specification) Software controls signals failure	The high voltage harness will be as short as possible, have sufficient clearance from electrical machinery, twist wires, and use sufficiently fast signal transfer medium	To avoid software controls signal failure causing high voltage system operation outside of min/max temperature range the high voltage harness shall be as short as possible, have sufficient clearance from electrical machinery, and use sufficiently fast signal transfer medium
			(noise, EMI, wiring, sensitivity)	The high voltage system will provide real-time feedback to the operator	To avoid operation outside of min/max temperature range the high voltage system shall provide real-time feedback to the operator
				The operator will have a high voltage system emergency-power- off switch	To avoid operation outside of min/max temperature range the operator will have a high voltage system emergency- power-off switch

Table 21. Partial HazOP analysis when a temperature stimulus is applied to a HV system

4.3.4 HARA applied using STPA

The STPA is a system-level analysis, and was performed on the LKA system because of the large amount of controls impact on the vehicle. The STPA helps to develop a safer control structure by identifying unsafe control actions, causal factors, and control weaknesses. Table 22 shows the template used to complete the STPA. The steps to completing an STPA include:

- 1. Produce a block diagram of the relevant system,
- 2. Compete the STPA template of the desired system or item,
 - a. Identify control functions of the system,
 - b. Determine unsafe control actions (UCAs),
 - c. Identify potential hazards for each UCA,
 - d. Identify the causal factors,
 - e. Determine prevention and mitigation methods,
 - f. Document the requirements.

Table 22. Template used to perform the STPA

			STPA Template	e	
Item:					
Control Function	Unsafe Control Action	Potential Hazard	Causal Factors	Prevention/Mitigation	Requirements

Creating a block diagram is a critical step in the understanding of the control flow for software heavy systems. It assists in identifying potentially hazardous dependencies, interfaces, and interactions. It is important to emphasize that STPA should not be applied at the item-level, and this block diagram should document system-level interactions. This diagram should be a living document, modifiable as the STPA and control structure evolves.

Completing the STPA template requires a strong working knowledge of how the system functions under various operational states or UCAs. It is encouraged that this analysis be completed using a cross-functional safety working group. Those who have low-level technical knowledge of how the system functions and reacts to failures will provide insight for causal factors and possible prevention and mitigation methods.

Identifying the control functions of the system describes how the system works, inputs, outputs, dependencies, and interfaces. Determining functions can produce a large amount of variability and different analysts will produce different results. Think about the functions in the order that they occur and consider if it is reasonable to consolidate multiple functions into a single function. Using the example of an LKA system the functions may be the following:

- 1. The operator initiates the LKA system.
- 2. The LKA sensors perform lane-line, object detection, and multi-feature tracking.
- 3. The LKA sensors send gathered data to the LKA computer.
- The LKA computer performs sensor fusion data verification & validation using developed algorithms and NNs.
- The LKA computer determines and sends appropriate corrective control action to the supervisory controller.
- 6. The LKA system provides real-time feedback to the operator via haptic, audio, and visual stimuli.
- 7. The LKA system may control lateral movement via the EPS system.
- 8. The LKA system may control lateral movement via the EBCM system.

9. The operator disables the LKA system.

In the example above, the functions are described in the order that they occur beginning with the enabling of the LKA system and ending with the eventual disabling. But where does the extent of a function end? This can be difficult to determine. If the EPS is an item of the LKA system then could we have included the actions and interfaces of the EPS system? If so, function 7 from the above list may continue as so:

- 7.1 The supervisory controller sends corrective control action to the EPS.
- 7.2 The EPS controller verifies the steering and steering-torque sensor output.
- 7.3 The EPS controller sends a corrective control action torque request actuating the EPS motor.
- 7.4 The EPS motor resolver sensor sends motor rotational data to the EPS controller.
- 7.5 The EPS controller determines the corrective control action is met and halts actuation.

This amount of detail in a systems function is determined by the depth and breadth of the analysis and is not necessary for our purposes at the University level because the EPS system is stock and not modified in any way. In general, this step can be guided by or contribute to the block diagram in understanding functional flow. Typically, the block diagram will feed the understanding of the system functions and performing the "identifying functions" task will produce modifications to the block diagram.

Determining the UCAs can involve using the four common UCAs or developing unique UCAs that better fit the functions of the system under analysis. In the automotive industry the four common functional UCAs used are:

- 1. Required but not provided,
- 2. Provided but not required,
- 3. Provided but incorrect timing,
- 4. Provided but incorrect duration.

UCAs guide the analyst through an exploratory but controlled investigation of how functional deviations can occur. The analyst should maintain focus on the scope for the particular UCA. From the above list, UCA3 and UCA4 can have overlap and cause redundancies within the analysis. UCA3 is asking the analyst to consider that the function under investigation be provided late or early while UCA4 is asking to consider that the function under investigation be provided for too-long or too-short a period of time.

Identification of UCA-specific hazards is the point at which this unique HARA technique becomes like the HARA techniques mentioned previously. Similar to the previous techniques, the analyst should focus on hazards which may produce unintended vehicle movement, damage or injury to the operator, passengers, property, or the environment.

Identification of casual factors will inform the prevention and mitigation method. The STPA was performed on controls and software systems which produced a few common causal factors:

- Power failure,
- Signal corruption,
- Wiring failure (not proper gauge, installation or manufacturing failure),
- Operating system failure,
- Unintended access or physical damage (liquid, puncture),
- Algorithm, Neural Network, computational, or cyber-security failure,

• Sensor visibility obstruction or failure.

Along with some common casual factors, unique causal factors specific to the UCA and associated hazard were also identified. These eventually lead to a set of STPA-derived requirements not found by performing other HARA techniques.

Determining prevention and mitigation methods is a direct product of the function, hazard, and especially the causal factors. Generally, there is at least one prevention and mitigation method for each causal factor.

Documenting requirements is the final step in completing the STPA template. A requirement is often a rewording of the prevention and mitigation method. Similar to the previous HARA techniques, the automotive industry uses specific verbiage during this formal part of the analysis. The requirements list will be the document which is viewed by the development teams. A brief example of a partially completed STPA template for an LKA system is listed in Table 23.

	STPA applied to the LKA System				
Control Function	Unsafe Control Action	Potential Hazard	Causal Factors	Prevention / Mitigation	Requirements
Operator initiates LKA system	Required but not provided	The LKA system remains disabled	Operator aware that LKA system initiation is required but unaware of how to initiate	When the speed and operational environment allow, the LKA initiation procedure will be clearly defined to the operator via audio and visual alert with minimal required actions by the operator (single button initiation, voice activation)	To prevent a failure to initiate the LKA system, when the speed and operational environment allow, the LKA initiation procedure shall be clearly defined to the operator via audio and visual alert with minimal required actions by the operator (single button initiation, voice activation)

Table 23. Example of a STPA on the LKA system

This documented requirement demonstrates how the failure of the control function and the prevention and mitigation method are incorporated to define the specific functional requirement.

4.4 Safety Goals and the Elicitation of Functional Requirements

The elicitation of safety goals and functional requirements is the final work product to come out of the concept phase for the systems safety process. These requirements set the safety rules for the systems development teams. They are specific to the individual systems which were analyzed during the HARA activities and are traceable throughout the systems lifecycle. Safety goals are high-level safety requirements of the item. Similar to conventional functional requirements on the item function, these safety goals describe how the item or system safely behaves. Each system will have many safety goals and each safety goal will have at least one functional requirement. In addition to this, technical requirements and a verification and validation procedure will be developed for each functional requirement. The requirementspecific test plan will provide traceability and build evidence for the risk informed safety case presented at the end of the systems safety process.

During this thesis, safety goals and functional requirements were developed for the ACC, CAVs, CSMS, LKA, PSI HV, and PSI Mechanical systems. Through the analysis it was found that safety goals are a top-level, item-specific claim, which states that the item functions will operate safely and avoid unreasonable risk. In all the HARA techniques discussed in this paper, not one allows for a place to define a safety goal. Through the analysis, in an effort to create consistency among the various HARA activities, the safety goal would be derived primarily from the items function and in some cases through the fault or hazard of the function.

The requirements produced out of the HARA activity would become the functional requirements. These describe how the safety goal will be met, free from unreasonable risk. Although there are many unique safety-critical requirements which were found during the HARA activities some requirements may appear to be common sense or repetitive. Without these thoroughly documented, the development team may overlook a small but critical aspect effecting the items functionality. This could result in unnecessary hazards or eventual failures causing injury, redesign, wasted time, manpower, or money.

4.4.1 Lane Keeping Assist System Safety Goals and Functional Requirements

The LKA safety goals and functional requirements were produced from a DFMEA and STPA on the LKA system. The analysis elicited 8 safety goals and 189 unique functional requirements. The safety goals are a close derivative of the systems functions. These high-level goals seen in Table 24 dictate how the LKA system will safely operate. A comprehensive list of all LKA system safety goals and functional requirements can be found in Appendix 4.4.

Table 24. Safety goals of the LKA system

	LKA System Safety Goals					
SG No.	Safety Goal					
SGL01	The LKA system shall safely control lateral movement via the EBCM system					
SGL02	The LKA shall safely control lateral movement via the EPS system					
SGL03	The LKA shall perform lane-line, object detection and multi-feature tracking					
SGL04	The LKA sensors shall transmit data to the associated controller					
SGL05	The operator shall enable and disable the LKA system					
SGL06	The LKA system shall provide feedback to the operator (LKA status, haptic, visual, audio)					
SGL07	The LKA computer shall perform sensor fusion data verification & validation					
SGL08	The LKA computer shall send control action decisions to the associated controller					

Typically the LKA system controls lateral movement either by braking the wheel opposite of the lane deviation which uses the EBCM or by providing a torque to the steering system which uses the EPS. The DFMEA and the STPA analyzed both options and produced the results seen in Table 25. Controlling lateral movement via the EBCM is shown produce a greater potential for a fault. This is because the EBCM analysis produced a greater number of requirements and because the braking system has more interfacing and interacting components when compared to the EPS. The results state that the LKA system will provide corrective control actions through the EPS system.

LKA System Lateral Control Requirements					
	Using the EBCM	Using the EPS			
No. of Requirements	20	17			

Table 25. Number of requirements for lateral control using the EBCM vs. the EPS

Some requirements were developed which state how the sensors shall be installed to minimize potentially obstructive views. Some requirements state that the LKA system needs to alert the operator when the LKA system is not operational based on external environmental factors (operational speed, fog, poor lane-line visibility), or that the LKA system wiring will be installed according to manufacturer specification to include bend radii, heat shielding, EMI avoidance, proper gauge, and interfacing connections.

Less apparent requirements found through the analysis were that the LKA systems outward facing camera will be mounted on the interior of the windshield within the operational area of the windshield wipers. The LKA system will also have a secondary control of the windshield wipers because the operator may not be aware if the cameras field of view is obstructed by a small piece of debris. The LKA system will maintain a secondary control of the headlights in the scenario where a low-light event obstructs the sensors visibility. It was also found that the LKA feedback system should use at least two forms of feedback to alert the driver of lane deviation.

It was determined that the timing, duration, and level of feedback stimulus will be based on an assessment of operator engagement. Operator engagement will be determined by an onboard operator-monitoring camera. This camera will read and analyze the amount of head tilt, eye deviation, and hands-on-wheel engagement. Assessing driver responsiveness is a current subject of research with numerous questions outstanding. If the feedback stimulus is too great will the operator be startled and create a hazardous situation? What is the correct timing to provide feedback based on operator engagement, and at what audio, visual, or haptic levels? The answer is operator dependent but testing can be conducted, and a consensus formed, on levels and timing of feedback. There is also potential for the feedback system to learn the operator's

response times, possibly based on factors such as time of day, and adjust accordingly. Table 26

describes a partial list of the unique LKA system requirements.

	LKA System Safety Goals and Functional Requirements				
SG No.	Safety Goal	FSR No.	Functional Safety Requirement		
SGL02	The LKA system shall safely control lateral movement via the EPS system	FSRL02.02	The LKA EPS response system shall respond (feedback, lateral movement) more quickly in the event of less operator engagement (hands on wheel, head tilt, eye deviation)		
		FSRL02.04	The LKA EPS response system shall allow the operator to override automated controls with minimal steering engagement		
SGL03	The LKA shall perform lane- line, object detection and multi-feature tracking	FSRL03.02	The LKA system shall monitor the operators engagement to include head tilt, hands-on-wheel, and eye deviation		
		FSRL03.07	To avoid sensor visibility obstruction the LKA system shall have control of the wind shield wipers		
		FSRL03.08	To avoid sensor visibility obstruction the LKA system shall have control of the headlights		
SGL05	The operator shall initiate the LKA system	FSRL05.04	To prevent accidental disabling of the LKA system, the LKA system shall have a safeguard such as individual on/off buttons		
		FSRL05.09	Turn-indicator actuation shall be required for free movement out of lane, otherwise feedback will warn operator		
SGL06	The LKA system shall provide feedback to the operator (LKA status, haptic, visual, audio)	FSRL06.07	The LKA system audio feedback shall adjust to ambient volume (stereo system, excessive cabin noise)		

Table 26. Example of LKA system safety goals and their associated functional requirements

4.4.2 Adaptive Cruise Control System Safety Goals and Functional Requirements

The ACC safety goals and requirements were produced from a DFMEA. The analysis elicited 7 independent safety goals and 86 unique requirements. The high-level safety goals are

reflective of detailed ACC functions which are shown in Table 27. A comprehensive list of all

ACC system safety goals and functional requirements can be found in Appendix 4.1.

Table 27. Safety goals of the ACC system

ACC System Safety Goals					
SG No.	Safety Goal				
SGA01	The ACC system shall safely control longitudinal velocity via braking				
SGA02	The ACC system shall safely control longitudinal velocity via throttle position or APP				
SGA03	The ACC sensors shall observe surrounding traffic/object distance, velocity, size and position to include operator engagement				
SGA04	The ACC system shall transmit sensor data to associated controller				
SGA05	The Operator shall determine and set the ACC system velocity constraint				
SGA06	The Operator shall determine and set the ACC system distance constraint				
SGA07	ACC system shall provide feedback to the operator (ACC status, haptic, visual, audio)				

The ACC and LKA systems provide a corrective action for longitudinal and lateral movement respectively. These systems are similar in that they use CAVs sensors and computers for data gathering and validation, then determine and send a corrective control actions to the CSMS supervisory controller. The LKA analysis used a DFMEA and STPA while the ACC analysis used only a DFMEA. The value of the STPA can be seen in Table 28, the amount of unique requirements produced for the LKA system versus the amount for the ACC system.

Table 28. Number of requirements produced for the LKA vs. the ACC system using select HARA techniques

	LKA analysis	ACC analysis
	DFMEA & STPA	DFMEA
No. of Requirements	189	86

The difference in number of unique requirements for the two very similar LKA and ACC systems between the DFMEA and the STPA analysis methods is notable. It implies that the ACC system should undergo an STPA analysis to more thoroughly investigate the requirements elicitation.

The ACC system will require the control of both the accelerator pedal or throttle position and the braking system. It was determined in the LKA and PSI Mechanical analysis that the braking system provides a relatively great potential for fault but in this case there is no option but to use the EBCM system. As you will see in the PSI Mechanical analysis, because the braking system is largely unmodified the requirements to ensure safe operation are focused on proper installation and maintenance. In the case of the ACC system, requirements were found which can minimize the potential braking fault. An example of this is when a braking corrective control action is required, the system shall ensuring that the EBCM engages in a timely manner such that the controls do not put undue stress on the braking system and components. A timely braking control action will also ease operator and passenger discomfort. This can be done by ensuring brake lines are flooded early and are immediately able to be actuated in anticipation of a corrective action.

Through the analysis it was found that the operator shall be able to override the ACC automated controls with minimal braking or acceleration pedal engagement. Variations in the sensitivity of this override will need to be tested on a closed course and the program will need to be adjusted accordingly.

A primary safety concern discovered during the analysis was the distance and speed at which the ACC system should control a corrective braking action. If the program is not thoroughly vetted then the program can operate reliably but still put the vehicle in a hazardous

scenario. This is found to have serve safety implications to the operator, the vehicle, and the environment. It will require many iterations of controls testing to determine optimal braking actuation as a function of vehicle speed, vehicle load, distance from the object, and operator engagement.

A safety critical requirement can be seen in FSRA01.14 in Table 29. This describes that the corrective braking action needs to respond earlier in the event that there is less operator engagement. A harsher corrective braking response will startle the operator who may then make an immediate unsafe control decision such as slam on the brakes. Like the LKA system, operator engagement is measured by head tilt, eye deviation, and hands-on-wheel. Operator engagement will also determine the timeliness and level of feedback stimuli. Other unique ACC system requirements can be found in Table 29.

	ACC System Safety Goals and Functional Requirements					
SG No.	Safety Goal	FSR No.	Functional Safety Requirement			
SGA01	The ACC system shall safely control longitudinal velocity via braking	FSRA01.01	The ACC system shall allow operator to override automated controls with minimal braking engagement			
		FSRA01.14	The ACC brake response system shall respond (feedback, longitudinal movement) more quickly in the event of less operator engagement (hands on wheel, head tilt, eye deviation)			
SGA07	The ACC system shall provide feedback to the operator (ACC status, haptic,	FSRA07.03	The ACC system shall alert operator when deviation from set distance or velocity occurs			
	visual, audio)	FSRA07.08	The ACC system visual feedback shall adjust to ambient light (decrease during night, increase during day)			
SGA03	The ACC sensors shall observe surrounding traffic/objects distance, velocity, size and position to include operator engagement	FSRA03.10	The ACC system shall only be operational if sensor performance meets a minimum standard (communication speed, sensor availability or visibility)			

Table 29. Example of the ACC system safety goals and functional requirements

4.4.3 CAVs Safety Goals and Requirements

The CAVs safety goals and functional requirements were produced from a HazOP and

PHA. The analysis elicited 31 independent safety goals and 243 unique requirements. A sample

of the high-level safety goals are shown in Table 30. A comprehensive list of all CAVs safety

goals and requirements can be found in Appendix 4.2.

Table 30. Example of CAVs safety goals

	CAVs Safety Goals					
SG No.	Safety Goal					
SGC01.1	The Intel Tank Computer shall be responsible for blending various sensors (cameras, radars) data to achieve reliable, high-definition images					
SGC01.3	The Intel Tank Computer shall be responsible for determining if control action (EPS torque, braking, feedback) is required					
SGC02.2	The Intel Mobileye 6 camera shall perform multi-feature tracking					
SGC03.1	The Bosch Front, Rear, and Corner MRR Radars shall perform early front, rear, and corner speed detection					
SGC08.2	The Zed camera shall perform 6-axis positional tracking to sense space and motion					

The CAVs primary function is to determine potentially hazardous scenarios, such as lane deviation, and decide if a corrective control action is required. This is done through lateral and longitudinal control by the use of the LKA and ACC systems which were analyzed and described in the previous sections. The safety goals produced here pertain to the CAVs item functions and controls hardware itself. Those items include the Intel Tank computer, Intel Mobileye 6 camera, Bosch front and rear radar, Bosch medium range corner radars, Intel Movidius neural compute stick, KVaser, Niles operator-monitoring camera, real-time display, ZED depth perception camera, and the GPS module.

The requirements produced alert the development team to potential failures of the item functions and offer preventative measures. These include failure causes such as:

- wiring failures,
- unintended access or physical damage to the item,
- power failures,
- algorithm, neural network, computational, or cyber security failures,

- memory failures,
- over-heating,
- signal corruption.

The requirements developed relate directly to these failure causes and include software technical standards by which the CAVs development team should derive their program. Some of these technical standards include a sensors horizontal field of view, sensors speed accuracy, and cycle time. Other safety concerns were found in understanding and designing for signal latency, noise, quality, and bandwidth. This analysis also produced mounting, installation, and wiring requirements. Table 31 describes a brief example of the safety goals and a sample of the associated functional requirements.

CAVs Safety Goals and Functional Requirements			
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGC01.2	The Intel Tank Computer shall be responsible for performing sensor fusion data verification & validation using developed	FSRC01.06	The development team shall ensure the Intel Tank computer only makes corrective action decisions when fidelity of image meets minimum specified resolution
	algorithms and NNs	FSRC01.07	The development team shall ensure if the Intel Tank computer fails, it does not prevent vehicle from manual driving operations
		FSRC01.12	To prevent unintended access and physical damage the development team shall ensure the Intel Tank computer is inaccessible by passengers
		FSRC01.47	To prevent an Intel Tank computer operating system crash the development team shall ensure the program is developed such that it does not attempt to access an incorrect memory address leading to general protection fault
SGC03.1	Corner MRR Radars shall	FSRC03.19	To reduce radar signal noise the development team shall ensure the use of wire shielding and conduit
	safely perform early front, rear, and corner speed detection	FSRC03.27	The development team shall ensure the integrated program accounts for radar horizontal field of view and elevation ($\pm 6^{\circ}$ (160m), $\pm 6^{\circ}$ (100m), $\pm 10^{\circ}$ (60m), $\pm 25^{\circ}$ (36m), $\pm 42^{\circ}$ (12m))
SGC08.3	The Zed camera shall perform large-scale 3D mapping	FSRC08.14	To reduce ZED camera signal noise the development team shall ensure the use of automotive industry standard filtering techniques

Table 31. Example of the CAVs safety goals and functional requirements

The CAVs functions carry critical safety concerns to include determining and requesting automated corrective control actions which were mentioned in the LKA and ACC analysis. Being a student built vehicle without the expertise, time, manpower, equipment, and financial backing to thoroughly investigate the use of automated driving functions, the development team should err on the side of caution when implementing the timeliness and magnitude of a corrective control action request. The analysis determined that based on the university "skill level" the CAVs controls should, in typical operational scenarios such as routine driving on a

highway, provide preemptive control action requests and operator feedback. The CAVs development team will implement a data validation, distance, speed, and deviation buffer which ensures the vehicles control action decisions are truly corrective and accomplished in a manner which reduces the potential hazard. This can be completed by ensuring the Intel tank computer determines the fidelity of blended and non-blended images before deciding on control actions. The CAVs controls will implement minimum standards for sensor data resolution, quality, noise, and latency. The operator will always be aware of the "on/off" status of the CAVs controls. It is also imperative that the operator is capable of easily overriding a control action request either by actuation of the steering wheel, acceleration pedal, brake pedal, or turn signal.

4.4.4 CSMS Safety Goals and Functional Requirements

The CSMS safety goals and functional requirements were produced from a DMFEA and STPA. The analysis elicited 24 independent safety goals and 109 unique requirements. A sample of the high-level safety goals are shown in Table 32. A comprehensive list of all CSMS safety goals and functional requirements can be found in Appendix 4.3.

CSMS Safety Goals		
SG No.	Safety Goal	
SGS01.2	The HSC shall safely control engine/EM torque split	
SGS01.5	The HSC shall modify stock signals	
SGS02.1	The ECM shall safely control engine torque output as requested by the HSC through regulation of current	
SGS05.3	The BMS shall protect against over-current, over-voltage, under-voltage, and over-temperature	
SGS09.1	The APPS shall monitor the position of the accelerator pedal and transmit a torque request	
SGS10.1	The low voltage system shall control all auxiliary functions to include air bags, windshield wipers, instrument cluster, lights, entertainment system, turn signals, haptic feedback, security system, pumps, fans, controller and DAQ	

The primary function of CSMS is to safely control vehicle longitudinal and lateral motion by controlling all associated controllers from a hybrid supervisory controller (HSC). Longitudinal motion is controlled by the HSC through the use of a torque split between the EM and engine. Lateral motion is also controlled by the HSC through the use of the EPS. Additional functions of CSMS are energy management optimization and to manage auxiliary functions such as windshield wipers, fans, pumps, and the DAQ. The HSC is the primary controller determining all safety critical vehicle operations to include acceleration, deceleration, steering, braking, corrective control actions, HV controls, and thermal control systems. Items of CSMS include the HSC, ECM, TCM, EMC, EBCM, BMS, EPS, low-voltage systems, OBC, OBD II, CAN bus, and the APPS.

CSMS is the most safety critical system on the vehicle because of its ability to cause unintended longitudinal or lateral motion and the potential for a thermal control failure to cause HV thermal runaway. The HARA activities investigated CSMS item functions, control strategies, and hardware items. Some of the safety-critical requirements of CSMS are associated with:

- Controls software development and integration,
- Implementing a propulsive request in coordination with the TCM, ECM, EMC, EBCM, EPS, and the APPS,
- Implementing automated corrective control action requests.

To ensure safe vehicle control, the analysis determined that CSMS software and programing hazards can be prevented and mitigated through robust software modeling, simulation, and a V&V plan. The approach to safe vehicle functionality will be, in part, through iterative modeling and simulation activities. This iterative approach is designed to validate the controls software program and will be accomplished through the use of model in the loop, software in the loop, hardware in the loop, vehicle in the loop, closed course testing, and then open course testing.

Constraints of vehicle performance such as minimum 0-60 acceleration and emissions output provide additional safety concerns as the vehicle must be capable of open road certification. Safety analysis also found requirements for self-imposed constraints which must be implemented. These allow the vehicle to meet the open road certification constraints while operating in the safest possible manner. A few of the self-imposed constraints are shown below.

- Torque limitations on the EM and engine,
- Temperature limitations on the engine, EM, EMC, and battery pack,
- Speed limitations on the engine and EM,
- Current constraints on the EM, EMC, OBC, and battery pack.

Common failure causes of CSMS software were signals, algorithm, computation, or logic faults. Automotive programing and installation standards will be used to reduce the risk of these types of failures. A partial list of common causes of failure for CSMS controls and their associated prevention and mitigation requirements can be seen in Table 33.

Table 33. Common CSMS failure causes and their assoc	ciated prevention and mitigation methods
--	--

CSMS Failure Causes and Prevention/Mitigation Methods		
Cause Prevention/Mitigation Method		
Signals Failure (quality, latency, noise, bandwidth)	- Ensure use of high quality transmission medium and appropriate gauge to handle expected throughput (load)	
	- Ensure wires are efficiently routed and as short as possible	
	- Ensure wires are kept away from electrical machinery	
	- Ensure use of wire shielding and conduit	
	- Ensure use of proper wire grounding practices	
	- Ensure use of filtering	
	- Ensure security of wire and controller connection	
Algorithm, NN, Computational, or Logic Failure	- Ensure robust V&V plan (automotive industry standard is one defect per 1000 executable lines of code)	
Failure	- Ensure use of automotive software development standards	
	- Ensure use of multiple software scanning tools (Jarvis) to identify vulnerability and error in program code	
	- Ensure control of computational overflow and rounding errors	
	- Ensure use of data validity checks and redundancies	

4.4.5 PSI HV & Mechanical Safety Goals and Functional Requirements

PSI safety goals and functional requirements were produced from SEFA, PHAs,

DFMEAs, and HazOPs on the HV and mechanical systems. In total the PSI HARA activities

produced 39 individual safety goals and 529 unique requirements.

The PSI HV safety analysis created 20 individual safety goals and 314 unique requirements around the individual components and the HV energy system as a whole. HV components to which safety goals and requirements were developed include the battery pack, enclosure, junction box, wiring harness, BMS, OBC, EM, and the EMC. A sample of the high-level PSI HV safety goals are shown in Table 34. A comprehensive list of all PSI HV safety goals and requirements 4.5.

Table 34. Example of the PSI HV safety goals

PSI High Voltage Safety Goals		
SG No.	. Safety Goal	
SGH01	The HV battery pack shall safely store and supply energy to the EM	
SGH02	The HV enclosure shall safely contain enclosed components through the prevention of unintended horizontal or vertical movement and unauthorized access	
SGH05.2	The BMS shall safely monitor and report the data of the HV ESS voltage, temperature, SOC, and current	
SGH07.1	The EMC shall safely control the supply of current to the EM	
SGH08	The HV component clearance requirements shall be met to ensure safe vehicle operation	
SGH11	The magnitude of the current applied by the HV ESS when discharging shall match the current requested	

The HV system is developed and built in our labs at CSU to meet the specific requirements for the hybrid vehicle it will be a part of. The HV system provides critical safety concerns as a thermal runaway or unintended exposure to HV can cause risk to life, property, and the environment. Through the analysis, the primary sources of risk reduction was found to be proper training, installation, thermal control systems, and software controls limiting HV component temperatures, current, voltage, and torque.

The exploratory HazOP technique, when applied to the PSI HV system, produced safety

goals outside of the standard functional safety goals that were seen in the DFMEA. A brief

example of the unique safety goals and associated functional requirements can be seen in Table

35.

PSI High Voltage			
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGH01	The HV battery pack shall safely store and supply energy to the EM	FSRH01.02	To prevent the HV battery pack from operating outside of the max/min temperature range the development team shall ensure actuation of battery pack thermal control system (fans) when the temperature reaches specified limit
SGH02	The HV enclosure shall safely contain enclosed components through the prevention of unintended horizontal or vertical movement and unauthorized access	FSRH02.08	To prevent the HV enclosure failure from improper installation and mounting of components the development team shall ensure component mounting hardware is fire retardant
SGH04	The HV wiring harness shall safely transfer energy from the battery pack to the EM	FSRH04.09	To prevent HV wiring harness over-current failure the development team shall ensure relays and fuses are in place and functional to prevent over drawing of current

Table 35. Example of the PSI HV safety goals and their functional requirements

The PSI mechanical safety analysis produced 19 safety goals and 215 unique requirements. Particular focus was on the items and components which would be new or modified. The components to which safety goals and requirements were developed include the driveshaft, differential, engine, EM, transmission, vehicle body, suspension system, braking system, thermal system, power steering system, exhaust system, and the fuel system. A sample of the high-level PSI Mechanical safety goals are shown in Table 36. A comprehensive list of all PSI Mechanical safety goals and functional requirements can be found in Appendix 4.6.

Safety Goal		
The suspension system shall safely support the vehicle weight and absorb/reduce excess energy from road shock		
The braking system shall inhibit vehicle motion, slow or stop a vehicle in motion, and keep stationary vehicles stopped		
The thermal system shall detect and control cabin and component temperatures		
The exhaust system shall safely assist in the removal of toxic gases, fumes and noise reduction		
The applied torque magnitude shall match the torque magnitude requested		
The current applied to the EM shall not exceed maximum operating parameter		

PSI Mechanical Safety Goals

Many of the PSI Mechanical requirements produced include component specific installation and maintenance necessities. Maintenance requirements are listed in a vehicle technical inspection (VTI) which should be completed prior to vehicle operation. The VTI includes requirements such as ensuring proper fluid levels, no loose wiring, no leaks, no debris (snow, mud) build up, and low voltage auxiliary functionality. Common requirements found among the PSI Mechanical components which meeting the needs of safe installation practices include:

- Load bearing mount modeling
- Component shielding and enclosures to prevent unintended access or physical damage
- Accurate interface angles for drive line components
- Wire/tube bend radii and the security of their interface connections

Table 37 demonstrates and brief example of the PSI Mechanical system safety goals and functional requirements.

PSI Mechanical			
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGM05	The thermal system shall detect and control cabin and component temperatures	FSRM05.05	To avoid engine overheating the development teams shall ensure thermal system is designed such that there is sufficient air flow to cool engine components
SGM04	The braking system shall inhibit vehicle motion, slow or stop a vehicle in motion, and keep a stationary vehicle stopped	FSRM04.02	To avoid brake pad failure the development team shall ensure brake pad bolts and mounting hardware are securely fastened and free from potential loosening or unintended movement
SGM09	The applied torque magnitude shall match the torque magnitude requested	FSRM09.01	The engine and EM shall split the torque magnitude requested based on associated map

Table 37. Example of the PSI-Mechanical safety goals and their functional requirements

5 CONCLUSION

The system safety process is required by both the University and funding stakeholders for all advanced vehicle technology builds. Automotive systems safety procedures, analysis and findings are highly proprietary. While the structures of some safety procedures are publicly available, a comprehensive analysis is unavailable. In addition, there is a lack of continuity in the transfer of safety knowledge and analysis from build to build which this thesis has addressed and investigated.

5.1 Contributions

The intent of this work was to 1. Provide a University-level automotive system safety process by determining the most effective ways to develop a risk informed safety case 2. Create a crossfunctional safety working group procedure 3. Develop a comprehensive system safety analysis for a hybrid architecture advanced-vehicle build utilizing automated driving functions and advanced driver assistance systems 4. Determine an efficient and effective hazard analysis and risk assessment procedure for the various subsystems of a hybrid vehicle 5. Elicit safety goals and functional requirements. Through this investigative process a few notable contributions were made in the each of these areas.

A University-level automotive system safety process was created using an investigation
of various well established industry system safety procedures. This developed process
efficiently combines the most effective ways to develop a risk informed safety case. It
provides a detailed description of the safety activities to be performed throughout the
systems lifecycle.

- 2. A cross-functional safety working group procedure was created. This document outlines the way in which team-specific safety representatives will be selected, their duties within that role, and how they will incorporate a safety mindset into their specific team. It provides a delegation of HARA activities to include detailed templates, instructions for completing those templates, and examples to reference. Lastly, it gives guidance on documentation, traceability, and how to create a test plan.
- 3. A comprehensive systems safety analysis was performed for each subsystem using a variety of HARA techniques to include DFMEA, PHA, HazOP, SEFA, and a STPA. This analysis provides all associated templates for future use and guidance for completion of the HARA activity. The detailed analysis documents the item definition and the item functions. It provides a complete documentation of the HARA investigation to include failure types, potential impacts, causes, and prevention, detection, and mitigation methods.
- 4. Determining an efficient and effective HARA procedure for the specific subsystems was accomplished through an understanding of the comprehensive systems safety analysis. It provided comparisons of the inductive and exploratory approaches. This lead to the matching of specific HARA techniques to specific vehicle subsystems and the importance of at least one inductive and one exploratory approach for each subsystem. A key finding was that sub-teams should complete a DFMEA rather than a PHA. This is because the DFMEA investigates a detection mode and provides a risk priority number for easy identification of greater safety critical items. For exploratory techniques the STPA is ideal for software and control systems while the HazOP is superior when applied to mechanical or physical systems.

5. The elicitation of the safety goals and functional requirements specifies in detail how the development team should design, construct, install, and operate their system. It describes the method for deriving the safety goals and requirements from the item function, prevention, and mitigation methods.

5.2 Future Work

The results of this project fulfills the management and safety plan and concept phases of the CSU system safety process. Determining technical requirements is a necessary task which defines the detailed mechanics of the systems development. This requires manufacturer technical specifications and can be completed once the components have been selected. Once the technical requirements are documented the design and development will begin and a structured test plan for each requirement will be made and adhered to. When subsystems are validated and deemed safe for integration, the production phase will begin and whole-system testing will provide the last work products for the risk informed safety case.

A thorough investigation into the safety-critical feature of the timeliness and magnitude of automated control actions is required. The timeliness and magnitude of the control action and feedback will be a product of the vehicle speed, operator engagement, external environmental conditions, and surrounding object locations and trajectory. This will require robust software, hardware, and in vehicle verification and validation. Bench testing on operator responsiveness to various feedback types, times, and magnitudes should be analyzed based on the operators engagement. In vehicle testing will be required to modify the LKA and ACC control action decisions. This can only be completed once the vehicle is fully functional and should be evaluated on a closed course adhering to a well-developed iterative test plan.

REFERENCES

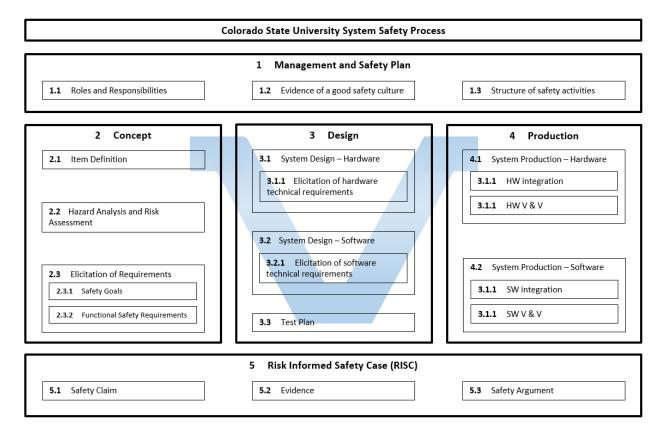
- H. Michalik and H. Dinse, "Electronic Automotive and Aerospace Systems a Master Programme on," *Proceedings of the 12th European Workshop on Microelectronics Education (EWME)*, pp. 75-77, 2018.
- [2] R. Van der Heijden and K. Van Wees, "Introducing Advanced Driver Assistance Systems: Some Legal Issues," *EJTIR*, pp. 309 - 326, 2001.
- M. T. R. Insights, "MIT Technology Review," 15 February 2019. [Online]. Available: https://www.technologyreview.com/s/612754/self-driving-cars-take-the-wheel/. [Accessed 5 April 2019].
- [4] J. Walker, "EMERJ," 19 February 2019. [Online]. Available: https://emerj.com/aiadoption-timelines/self-driving-car-timeline-themselves-top-11-automakers/. [Accessed 26 February 2019].
- [5] I. K. Harald Waschl, Control Strategies for Advanced Driver Assistance Systems and Autonomous Driving Functions, Switzerland: Springer International, 2019.
- [6] F. Biondi and D. Getty, "The Challenge of Advanced Driver Assistance Systems Assessment: A Scale for the Assessment of the Human–Machine Interface of Advanced Driver Assistance Technology," *Transportation Research Record*, 2018.
- [7] J. Tunnell, Z. Asher, S. Pasricha and T. Bradley, "Toward Improving Vehicle," *SAE Int J. of CAV*, vol. 1, no. 2, 2018.
- [8] J. Piao and M. McDonald, "Advanced Driver Assistance Systems from Autonomous to Cooperative Approach," *Transport Reviews*, vol. 28, no. 5, pp. 659-684, 2008.
- [9] H. Dezfuli, "System Safety Framework and Concepts for Implementation," *NASA System Safety Handbook*, vol. 1, 2011.
- [10] M. Vernacchia, L. Popma and J. Faucett, "System Safety Process & Concept Phase Overview," EcoCAR Mobility Challenge, Pontiac, 2018.
- [11] ISO_26262-10:2012(E), "Guideline on ISO 26262," Road Vehicles Functional Safety -Part 10, 2012.
- [12] U. D. o. Transportation, "Traffic Safety Facts Crash Stats," NHTSA's National Center for Statistics and Analysis, 2015.
- [13] ISO_26262-2:2018(E), "Management of Functional Safety," Road Vehilce Functional Safety - Part 2, 2018.

- [14] ISO_26262-3:2018(E), "Concept Phase," Road Vechicles Funtional Safety Part 3, 2018.
- [15] T. Schmid, "Safety Analysis for highly automated driving," *IEEE International Symposium* on Software Reliability Engineering Workshops, pp. 154-157, 2018.
- [16] S. Amberkar and B. Czerny, "A Comprehensive Hazard Analysis Technique for Safety-Critical Automotive Systems," *SAE Transactions*, vol. 110, no. 7, pp. 282-292, 2001.
- [17] V. Popovic and B. Vasic, "Review of Hazard Analysis Methods," *FME Transaction*, vol. 36, pp. 181-187, 2008.
- [18] E. Heil, "Professional Engineering for Industrial and Laboratory Safey," Abstraction Engineering, [Online]. Available: http://abstractionengineering.com/main/hazard-analysis/. [Accessed 15 February 209].
- [19] M. Rasusand, "Preliminary Hazard Analysis," System Reliability Theory, vol. 2, pp. 1-36, 2004.
- [20] T. Achatz, "Introduction to FMEA," 29 April 2009.
- [21] J. Bowles, "An Assessment of RPN Prioritization in a," *Annual Reliability and Maintainability Symposium*, pp. 380-386, 2003.
- [22] A. Abdulkhaleq and S. Wagner, "Using STPA in Compliance with ISO 26262 for Developing a Safe Architecture for Fully Automated Vehicles," *Automotive - Safety and Security*, 2017.
- [23] Q. Hommes, "Safety Analysis Approaches For Automotive Electronic Control Systems," *SAE International*, 15 January 2015.
- [24] "EcoCAR Mobility Challenge," U.S. Department of Energy, 2019. [Online]. Available: https://avtcseries.org/ecocar-mobility-challenge/. [Accessed 13 March 2019].
- [25] A. N. L, "EcoCAR Organization and Administration," *Launch Workshop Webinar Series*, 7 September 2018.
- [26] A. N. L, System Safety Working Group, 2018.
- [27] Z. Asher, D. Baker and T. Bradley, "Prediction error applied to hybrid electric vehicle optimal fuel economy," *IEEE Transactions on Control Systems Technology*, no. 99, pp. 1-14, 2017.
- [28] Z. Asher, J. Tunnell, D. Baker, R. Fitzgerald, D. Banaei-Kashani, S. Pasricha and T. Bradley, "Enabling Prediction for Optimal Fuel Economy Vehicle Control," in SAE World Congress Experience, Pontiac, 2018.

- [29] S. Khastgir, S. Birrell and G. Dhadyalla, "Towards increased reliability by objectification of Hazard Analysis and Risk Assessment (HARA) of automated automotive systems," *Safety Science*, vol. 99, pp. 166-177, 2017.
- [30] H. Prenscia, "Report Summary Rating Criteria and Classifications," *XFMEA Report Sample - Design FMEA*, pp. 1-6, 2017.

Appendix 1Management of Functional Safety – CompleteDocumentation

Appendix 1.1 Safety Activities throughout the System Safety Lifecycle



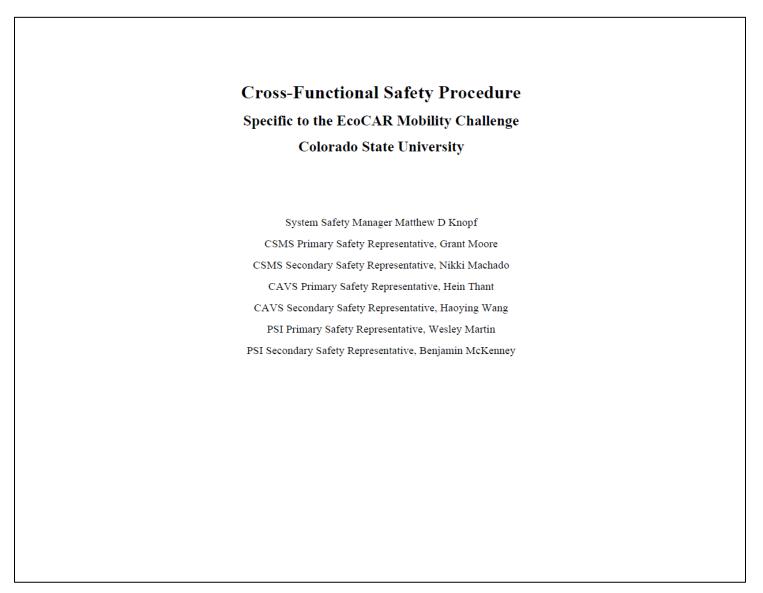


Table of Contents

1	Cro	oss-Functional Safety Procedure
2		nagement of Functional Safety
		Roles and Responsibilities
3	Iter	n Definition
4	Haz	zard Analysis and Risk Assessment (HARA)
	4.1	Preliminary Hazard Analysis (PHA)
	4.2	System Element Fault Analysis (SEFA)
	4.3	Systems Theoretic Process Analysis (STPA)
	4.4	Hazard and Operability Analysis (HazOP)
	4.5	Design Failure Mode and Effects Analysis (DFMEA)
5		citation of Safety Goals and Requirements
6	Tes	st Plan
Re	eferen	ces 22

1 Cross-Functional Safety Procedure

A cross-functional safety procedure is developed to facilitate the use of safety practices within the individual teams. It is not possible for the safety manager to be completely involved in the technical low-level decision making of each team. In order to complete requirements, both technical and functional, and keep systems safety as a priority, the teams will follow this procedure when considering project scope and the implementation of systems.

Consider the following when performing safety analysis:

- · PSI will compare the difference in architecture types initially perform Management, Item Definition, PHA and SEFA
- · CSMS initially perform Management, Item Definition, PHA, and either a SEFA or STPA
- CAVS initially perform Management, Item Definition, PHA, and STPA
- CSMS is responsible for controls software
- PSI is responsible for controls hardware
- · Limit the scope of your analysis to items and systems which will be added, modified, or interact with the added and modified
- · Use the verbiage from examples when writing requirements (operator, shall,), otherwise casual verbiage
- There are no stupid concerns write them down and they will be vetted
- Integrate your team into this process it will produce quicker and better results if the effort is collaborative
- This is a required objective take it seriously and do it to the best of your ability
- Analysis will be performed in MS Word complete block diagrams, templates, and brief description (one to two paragraphs at beginning of each analysis) of what was included, wasn't included and why (or anything you believe is worth mentioning)
- · Copy and paste necessary tables but DO NOT modify this document
- GET THIS DOCUMENT FROM T:\Projects\EcoCar_Mobility_Challenge\EcoCAR Mobility Challenge\Year 1\System Safety\System Safety Analysis
- The systems safety folder has good resources for you to reference

General Steps:

- 1. Management of Functional Safety
- 2. Item Definition
- 3. Preliminary hazard Analysis
- 4. System Element Fault Analysis
- 5. Systems Theoretic Process Analysis
- 6. Document Requirements
- 7. Document a Test Plan

2 Management of Functional Safety

This section describes requirements to satisfy the safety management category

2.1 Roles and Responsibilities

Definition and assignment of roles and responsibilities regarding safety management and activities is the initial step to beginning the systems safety lifecycle. Roles shall be directed by the project manager and the safety management team shall be assigned based on project scope and individual expertise. The safety management team is a collection of team leads who have skill specific experience and will contribute at a technical level to the identification of potential hazards and mitigation solutions. Safety is a collaborative effort especially at the University level where student experience can be limited. This is a single responsibility of the management of functional safety but it is the only activity unique to the individual teams.

1. Your requirement is to complete this table with all members of your team

Table 2.1 Roles and Responsibilities Template

Team:	2 2		
Role	Member	Responsibilities	

Table 2.2 Example of Roles and Responsibilities

Team: Management Role	Member	Responsibilities
	Member	
Project Manager	Dr. Thomas Bradley	Oversee high-level mission activities and operate in a supervisory capacity. Define project scope, and manage requirements, planning, schedule, budget, and stakeholder engagement.
Powertrain Technical Manger	Gabriel Di Domenico Troy Johnson	Determine system/component requirements. Sourcing and procurement of component selection Integration of components and system build.
Controls Technical Manager	David Trinko	Development of controls software. Determine system/component requirements through software simulation
Systems Safety Manager	Matthew Knopf	Develop system safety case. Perform safety analysis and determine safety requirements. Develop test plan and V&V methods.

3 Item Definition

The definition of the term item is a system or array of systems to implement a function at the vehicle level that is able to cause harm to people inside or outside the vehicle, to which ISO 26262 is applied. In the early stages of concept development there are no concrete definitions of an item or system as these are born from the development process. The concept development phase begins with an item definition where the goal is to describe the item, its functionality, dependencies on, and interactions with, the driver, the environment and other items at the vehicle level [1]. Within this analysis, focus is on items and functions which may potentially cause harm to the driver such as loss of acceleration, braking, steering, or system failures that could cause the vehicle to stop or accelerate suddenly.

1. Your requirement is to complete this table.

Table 3.0 Item Definition Template

Item	Sub-Item	Functional Behavior	
	j		

Table 3.1 Example of Item Definition of the Mechanical System

Item	Sub-Item	Functional Behavior
Driveshaft	Yokes	- Longitudinal shaft which transmits torque from
	U joint	engine/transmission to rear of vehicle
	Shaft	
	Bearings	1
	Clamps	7
	Rings]
	Axle beam	7
	Steering knuckle	1
	Rods	1
	Brake drum	
and CSMS syst software, a con	em can be tricky when thinking about CAVS ems. Is the item an actual controller, a piece of trol strategy? Think through this and do what use. Be able to defend your response if asked	Get the functional behavior correct. It carries throughout other analysis processes. AKA you're going to use it often Use Google, ex. "automotive driveshaft function".
about It		That will help fill this out accurately

4 Hazard Analysis and Risk Assessment (HARA)

There are a wide variety of HARA types and techniques used to identify hazards and mitigate risk throughout the entirety of a projects life cycle. HARA's are especially valuable early in the concept and development phases but can be utilized through a systems production, operation, and disposal. We will discuss those technique which you will be responsible for completing.

4.1 Preliminary Hazard Analysis (PHA)

A PHA is a type of inductive analysis used in the initial stages of the systems design. It is a broad technique focusing on identifying hazards, assessing the severity of the effects that would occur from that particular hazard, and identifies corrective and preventative measures. The benefit of a PHA is early recognition of weakness in the system concept, thus saving time and money that would be required during future discovery of the weakness.

The benefits and characteristics of the PHA are as follows:

- Provides early identification and high level hazard recognition
- Elicits consistent safety requirements for both hardware and software systems
- Applicable to any activity or system big and small
- Elicits qualitative hazard descriptions and provides qualitative rankings of the hazardous situations which is used to prioritize hazard reduction tasks
- 1. Your requirement is to complete this table.

Table 4.0 PHA template

Potential Hazard	Cause	Major Effect	Severity	Corrective/Preventative Measures	Requirement
------------------	-------	--------------	----------	-------------------------------------	-------------

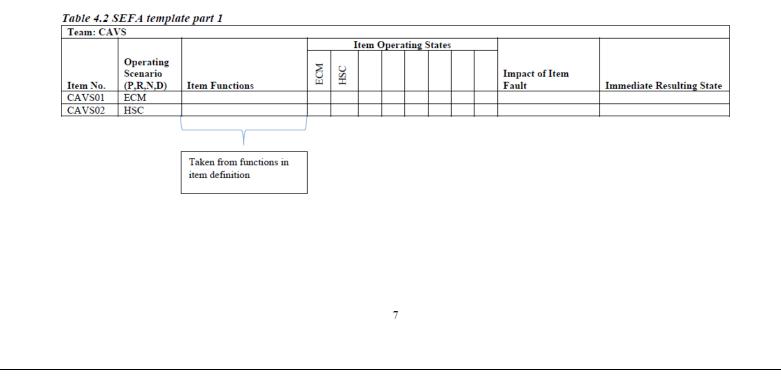
vehicle motion. Brakes fail to slow/stop moving vehicle Brakes fail to keep stopped vehicle stationary	Potential Hazard	Cause	Major Effect	Severity	Corrective/Preventative Measures	Requirement
This is the failure of the function from the Don't do this Use similar verbiage and make it sound professional. This will This is sort of the end goal of the analysis. Use similar	vehicle motion. Brakes fail to slow/stop moving vehicle Brakes fail to keep stopped vehicle	failure (overheating,	of longitudinal motion Operator and/or passenger injury Damage to or loss of property Damage to environment Unintended vehicle motion when stationary		installation of pads Ensure bolts and mounting hardware is securely fastened and free from potential loosening or movement Avoid adverse road conditions Routine maintenance and inspection for rust and corrosion	Development team shall ensure brake pad bolts and mounting hardware is securely fastened as free from potential loosening or unintended movement Operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH Operator shall perform routine inspection of brake system to check for rust, fatigue, and corrosion Operator shall avoid poor drivin
	the function from the	1			it sound professional. This will	This is sort of the end goal of the analysis. Use similar

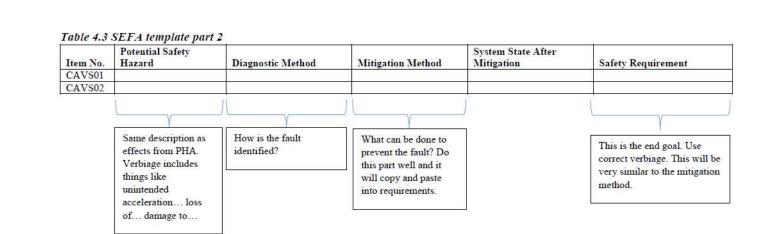
4.2 System Element Fault Analysis (SEFA)

SEFA is a system level exploratory analysis technique to evaluate the impact of system element faults upon the system as a whole and to determine if the system has sufficient content to detect and mitigate potential hazardous states created due to the fault. In the SEFA, a methodical review of the faults of system elements is conducted from which the consequences of each fault are identified. The analysis typically is performed based on a system's physical architecture design and assists in understanding flaws within the design or inadequacies in the design's ability to prevent, detect or respond appropriately to the impact of the faults of system elements [2].

Steps to completing a SEFA

- 1. Create system block diagram
- 2. Fill out SEFA template





SEFA Electric Vehicle Propulsion Example

A hybrid system architecture block diagram is provided below. This system contains two electric machines (EMs) that function either as a motor or a generator depending on driving conditions. These EMs are controlled by dedicated control processors (MCPA and MCPB) that use feedback from EM mounted resolvers. EM torque commands are determined by a hybrid control processor (HCP) that receives accelerator and brake pedal information from an engine control module (ECM) and an electric brake control module (EBCM) respectively. A transmission control module (TCM) selects different gear ratios based on ECM and transmission output speed sensor (TOSS) input. An internal mode switch (IMS) tells the system what range (Park, Reverse, Neutral, or Drive) the driver has selected. All of these entities constitute the system's elements [2].

Step 1. Create a Block Diagram

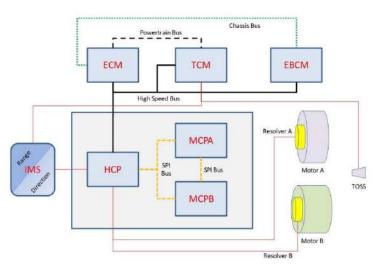


Figure 1. Hybrid Propulsion System Architecture [2]

			P	RIMA	RY Fai	ult	RESU	LTING	5 Faul	t					
ltem umber	Multiple Ranges (P,R,N,D)	Function(s) (Responsibilities)	ECM	HCP	MCP1	MCPZ	TCM	EBCM	Direction IMS	Range IMS	TOSS	M otorA Resolver	MotorB Resolver	Impact of Element Fault (Impact prior to any remedial or mitigation actions)	Immediate Resulting Stat (State of the syste prior to any remed or mitigation action
	Normal Operation	Provide Propulsion in an Electric Vehicle	1	1	1	1	1	1	1	1	1	1	1	NORMAL OPERATION	Selected Range
1	ECM	 * Read accelerator pedal inputs * Determine req'd torque based on driving condition and accel pedal input * Provide EBCM with Regen Braking Capacity * Performs plausiblity check btw HCP and TCM IMS inputs 	o	1	1	1	1	1	0	1	1	1	1	Engine not available or shuts <off></off>	Park - Park Reverse - Revers Neutral - Neutra Drive - Possible Acceleration
2	нср	* Determines torque and commands MCPs * Reads Motor Resolver inputs * Reads IMS Direction input * Provides IMS Direction to ECM	1	0	1	1	1	1	1	1	1	0	0	IMS info to HCP not evaluated Loss of Motor Resolver Info	Park - Park Reverse - Revers Neutral - Neutra Drive - Possible Acceleration
3	MCP1	* Commands torque to Motor A * Provides MPM function to HCP	1	1	0	1	1	1	1	1	1	0	1	Motor 1 shuts down	Park - Park Reverse - Possib Decel Neutral - No Issu Drive - Possible Acceleration
4	MCP2	* Commands torque to Motor B * Provides MPM function to HCP	1	1	1	0	1	1	1	1	1	1	0	Motor 2 shuts down	Park - Park Reverse - Possibi Accel Neutral - No Issu Drive - Possible Deceleration

Step 2. Fill out SEFA template

ltem Number	Multiple Ranges (P,R,N,D)	Potential Safety Hazard(s)	Diagnostic Method(s)	Mitigation Action(s)	System State After Mitigation	SAFETY Requirements
	Normal Operation	NONE	NONE	NONE	NONE	NONE
1	ECM	Loss of Propulsion	Lack of ECM communication detected by HCP and TCM	Set MIL light and go to reduced power	Reduced Propulsion	* System shall move to reduced propulsion when ECM fails * TCM and HCP shall detect ECM loss using CAN diagnostics
2	нср	Unintended Propulsion <or> Unintended Direction</or>	TCM and ECM detect loss of HCP. IMS info from TCM used for Driver Intent MCPs detect HCL loss.	Set MIL light and go to reduced power	Reduced Propulsion	* ECM shall set DTC and instruct BCM to display driver message * ECM shall default to TCM IMS info * MCPs shall limit mtr torques to RP * The system shall transition to RP without violating the Unintended Direction & Unintended Prop Engagement metric * The system shall provide ASIL D hardware design integrity
3	MCP1	Unintended Accel <or> Unintended Deceleration</or>	HCP and MCP2 detect loss of MCP1	Command TCM to go to Mode 2	Mode 2 (High Speed) Acceleration may be affected at low speeds or launch	 * System shall allow Motor A to free-wheel when MCP1 is lost * System shall tranistion to Mode 2 when MCP1 is lost without violating the Unintended Direction & Unintended Prop Engagement metric * HCP shall inform ECM of Mode 2 * ECM shall command BCM to display RP message * The system shall provide ASIL D hardware design integrity
4	MCP2	Unintended Accel <or> Unintended Deceleration</or>	HCP and MCP1 detect loss of MCP2	Command TCM to go to Mode 1	Mode 1 (Low Speed) Top speed may be loss than normal operation	* System shall allow Motor B to free-wheel when MCP2 is lost * System shall tranistion to Mode 1 when MCP2 is lost without violating the Unintended Direction & Unintended Prop Engagement metric * HCP shall Inform ECM of Mode 1 * ECM shall command BCM to display limited speed message * The system shall provide ASIL D hardware design integrity

4.3 Systems Theoretic Process Analysis (STPA)

STPA is a technique that represents the system content from a controls perspective, not a reliability point of view, and treats the system failures as control problems. It is used to evaluate failures associated with "functions" assigned to system elements and the impact of these failures on system behaviors during the defined operating scenarios. STPA determines unsafe controls actions created when each system element's functions fail according to a list of "misbehavior" guidewords; the possible causes that could lead to these unsafe control actions; and, finally, the constraints and/or requirements necessary to prevent or manage these causes to an acceptable risk level [2].

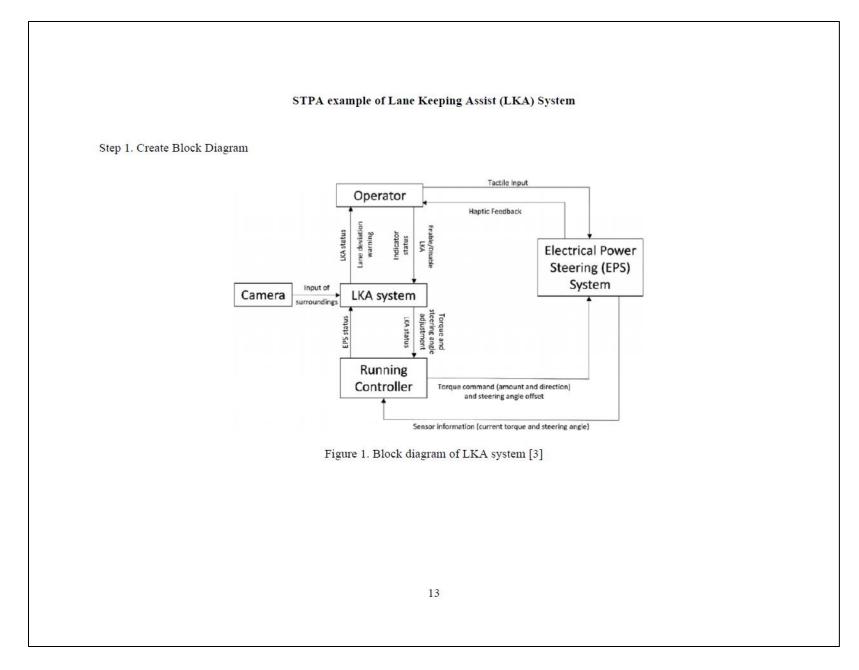
Steps to completing STPA:

- 1. Develop block diagram
- 2. Fill out STPA template

Table 4.4 STPA template

Control Function	Unsafe Control Action	Potential Hazard	Causal Factors	Constraints	Requirements
	Required but not provided				
	Provided but not required				
	Provided but incorrect timing				
	Provided but incorrect duration				
Copy and paste from functions column in item definition	This column always stays the same. Use these exact UCA's				This is the end goal. Use correct verbiage This will be very similar to the mitigation method.

12



Step 2. Fill out STPA template

Table 4.5 STPA example of LKA system [3]

Item: STPA Control	for Lane Keeping Unsafe	Potential Hazard	Causal Factors	Constraints	Requirements
Function	Control	Fotential Hazard	Causal Factors	Constraints	Requirements
runction	Action				
Torque and steering angle adjustment	Required but not provided	Torque request isn't transferred, while vehicle	Incorrect input from camera to LKA Misinterpreted lane marking	Camera check Accurate detection and	N/A
(from LKA to running		continues to drive out of lane	by LKA (system thinks vehicle is in lane)	processing of lane markings	
controller)			Incorrect turn-indicator status transmitted to LKA LKA is disabled		
	Provided but not required	Unexpected torque to the steering	LKA is enabled when it shouldn't be	Camera check Continuous communication of EPS	The running controller shall send the current EPS status signal to the LKA once the torque command has been implemented
			Incorrect camera input	status to LKA	-
				LKA refresh rate	The running controller shall update the LKA system if there is a mismatch between the sensor information from
			Electric power steering status not communicated to LKA		EPS and the EPS status stored in LKA
	Provided but	Controller sends	Incorrect input from camera	LKA processing time	The LKA system shall continuously
	incorrect timing	torque request at the wrong time	Incorrect processing of deviation by LKA	Incorrect refresh rate	monitor and verify the camera input with the current EPS status
			Turn-indicator malfunction Electric power steering status communication is delayed	Camera cycle rate	
	Provided but	Controller	Incorrect input from camera	LKA Processing time	The running controller shall refresh the
	incorrect	continues to send	LKA frozen	LIXA Processing time	LKA system if the LKA status is frozer
	duration	torque request	Electric power steering status not communicated to LKA	Camera cycle rate	LINA System II the LINA status is noted
				Continuous communication of EPS status to LKA	

4.4 Hazard and Operability Analysis (HazOP)

A HazOP is also an exploratory technique of risk analysis but uses guide words and process parameters. These process parameters are dependent on the component and can be applied to system items resulting in partial or whole-system failures. An example of this would be "only *part of* the requested *torque* is produced by the engine". This technique identifies system and component level hazards but also considers operability failures.

The benefits and characteristics of the HazOP are as follows:

- Far reaching scope to identify component and system level requirements
- · Identifies potential failures through the use of function-deviating guide words such as " part of, more, less, late"
- Uses process parameters such as "torque, temperature, NVH" specific to the item of investigation

Table 4.6 Process Parameter and Guide Word Combination Chart Template

Mechanical						Gu	ide Word						
Process	No	As well	Part of	Reverse	Other	Early	Late	Before	After	Faster	Slower	More	Less
Parameter		as											

Table 4.7 HazOP Template

FUNCTI	FUNCTION: Apply Torque Stimuli to EM							
Guide Word	Deviation	Consequences	Causes	Safeguards	Safety Goal			

Mechanical Guide Word													
Process	No	As well	Part of	Reverse	Other	Early	Late	Before	After	Faster	Slower	More	Less
Parameter		as											
NVH										Х	Х	Х	
Torque			Х	X		X	X					Х	X
Temperature												Х	X
Current	Х		Х	X		Х	Х					Х	X
Clearance												Х	Х
Angle												Х	

Table 4.8 Mechanical Process Parameter and Guide Word Combination Chart Example

Table 4.9 HazOP of the Mechanical System Example

Guide Word	Deviation	Consequences	Causes	Safeguards	Safety Goal
More	Torque applied is greater than intended	TVP accelerates faster than intended TVP collides with object TVP/operator damage/injury	Control software error. APPS error. Power supply error. EM/engine malfunction. Transmission controller error.	Controls software validation during SIL. Torque request magnitude/direction testing, APPS validation, and gear selection control testing during zero velocity and closed course phases	The applied torque magnitude shall match the torque request intended magnitude
Less	Torque applied is less than intended	TVP accelerates slower than intended	Control software error. APPS error. Power supply error. EM/engine malfunction. Transmission controller error.	Controls software validation during SIL. Torque request magnitude/direction testing, APPS validation, and gear selection control testing during zero velocity and closed course phases	

4.5 Design Failure Mode and Effects Analysis (DFMEA)

A DFMEA is an inductive analysis technique and one of the earliest developed method for hazard analysis [4]. Similar to all HARA techniques, the DFMEA aims to assess system and design risk and develop strategies to detect and mitigate those risks. Unique to the FMEA is that the method ranks those risks based a risk priority classification. If completed very early in the concept stages of design, the DFMEA can provide valuable insight into potential hazards, the impact of those hazards, and the interfaces and interactions between subsystems.

The benefits and characteristics of the DFMEA are as follows:

- · Provides a deep-dive hazard analysis at the system, subsystem, and component level
- Ranks potential hazards base on a risk priority number (RPN) to identify highest priority risks (*RPN = Severity * Occurance * Detection*)
- Intuitive and thorough analysis template used to identify potential failure modes, failure effects, causes of failure, and detection
 and mitigation methods

Table 4.10 FMEA Template

Iten	1: Brakes										
No.	Function	Failure Type	Potential Impact	s	Potential causes	0	Prevention Mode	Detection Mode	D	RPN	Requirement

No.	Function	Failure Type	Potential Impact	s	Potential causes	0	Prevention Mode	Detection Mode	D	RPN	Requirement
	Inhibits	Brakes fail	Unintended	9	Brake pad	5	Ensure proper	Vehicle	3	135	Development team shall
	vehicle	to Inhibit	loss of		fatigue or failure		mounting and	technical			ensure proper mounting
	motion.	vehicle	longitudinal		(overheating,		installation of	inspection will			and installation of pads
		motion.	motion		corrosion)		pads	identify if the			-
	Slows/stops				· · · ·		•	pads are free			Development team shall
	moving	Brakes fail	Operator				Ensure bolts	from fatigue or			ensure brake pad bolts
	vehicle	to	and/or				and mounting	corrosion			and mounting hardware
		slow/stop	passenger				hardware is				is securely fastened and
	Keeps	moving	injury				securely	Operator aware			free from potential
	stopped	vehicle					fastened and	during			loosening or unintende
	vehicle		Damage to or				free from	operation by			movement
	stationary	Brakes fail	loss of				potential	identifying			
		to keep	property				loosening or	unsettling smell,			Operator shall avoid
		stopped					movement	and vehicle			excessively adverse roa
		vehicle	Damage to					vibration			conditions (bumpy
		stationary	environment				Avoid adverse				terrain, excessive grade
							road conditions				which may cause a hig
			Unintended								NVH
			vehicle				Routine				
			motion when				maintenance				Operator shall perform
			stationary				and inspection				routine inspection of
			(rollaway)				for rust and				brake system to check
							corrosion				for rust, fatigue, and
											corrosion
							Avoid poor				
							drive behavior				Operator shall avoid po
											driving behaviors

Table 4.11 FMEA of the Mechanical System Example

5 Elicitation of Safety Goals and Requirements

The HARA has produced a list of safety goals and requirements which the system will be designed around. You will create a table of the safety goals and functional requirements.

Table 5.0 Safety Goals and Requirements Template

System: N	System: Mechanical							
SG No.	Safety Goal	FSR No.	Functional Safety Requirement	Failure Detection/Mitigation				

			Mechanical
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGM01	The driveshaft shall transmit torque from the engine and/or EM to the	FSRM01.01	To avoid driveshaft-EM interface failure the development team shall ensure proper mounting, installation, and manufacturing of modified driveshaft and its components
	rear of the vehicle	FSRM01.02	To avoid driveshaft-EM interface failure the development team shall ensure driveshaft bolts and mounting hardware is securely fastened and free from potential loosening or unintended movement
		FSRM01.03	To avoid driveshaft-EM interface failure the development team shall ensure driveshaft EM interface location is covered and free from potential unintended access or physical damage
		FSRM01.04	To avoid driveshaft-EM interface failure the development team shall ensure proper manufacturing and design for minimal driveshaft-EM interface angle
		FSRM01.05	To avoid driveshaft-EM interface failure the operator shall avoid adverse road condition which may produce NVH
		FSRM01.06	To avoid driveshaft-differential interface failure the development team shall ensure proper mounting, installation, and manufacturing of modified driveshaft and its components
		FSRM01.07	To avoid driveshaft-differential interface failure the development team shall ensure driveshaft bolts and mounting hardware is securely fastened and free from potential loosening or movement
		FSRM01.08	To avoid driveshaft-differential interface failure the development team shall ensure driveshaft-EM interface location is covered and free from potential unintended access or physical damage
		FSRM01.09	To avoid unintended access or physical damage of the driveshaft the development tear shall ensure driveshaft manufacturing and use of materials is sufficient to prevent unintended access and physical damage

Table 5.1 Example of Mechanical Safety Goals and Functional Safety Requirements

6 Test Plan

Use this table as a guideline to develop a test plan. The judgement criteria will determine the technical requirement by which the system will operate

Table 6.0 Test Plan template

FSR	Test Case Number (TCN)	Description	Expectation	Test	Judgement Criteria

Table 6.1 Example Test Plan and Technical Requirements

FSR	Test Case Number (TCN)	Description	Expectation	Test	Judgement Criteria
		E-stop use is an emergency action which halts functionality of the TVP's motor	Actuating E-stops should disconnect current flow from the battery to the motor	During zero velocity testing and while running an AE actuate E-stops	Deactivation of current flow should occur within 50 ms

References

- [1] ISO 26262- 3:2018 (en) Road Vehicles Functional Safety Part 3: Concept Phase
- [2] Vernacchia, Mark. "Delivering System Safety through Design Using Early Analysis Methods." Aug 2018. PowerPoint presentation
- [3] Mahajan, Haneet. "Application of systems theoretic process analysis to a lane keeping assist system." Reliability Engineering and System Safety. 167 (2017) 177-183
- [4] Achatz, Tom. "What is FMEA?" April 2009. PowerPoint presentation

	Management of Functional Safety						
Roles and Responsibilities							
Team: Management							
Role	Member	Responsibilities					
Faculty Advisors	Dr. Thomas Bradley	Oversee high-level mission activities and operate in a supervisory capacity. Define project scope, and manage requirements, planning, schedule,					
	Dr. Brett Windom Dr. Jason Quinn	budget, and stakeholder engagement.					
Project Manger	Gabriel Di Domenico	Determines scope of work and high-level technical and functional goals. Defines what work will be done and manages the development of the systems as a whole.					
Engineering Manager	Troy Johnson	Manages system-level requirements for CAVs CSMS and PSI teams. Determine system/component selection and implementation strategy. Over sees day-to-day concept, engineering, and development operations.					
Systems Safety Manager	Matthew Knopf	Develop system safety case through coordination with team system safety representatives. Performs safety analysis and determine safety requirements. Develop test plan and V&V methods.					
Team: CAVs							

Appendix 1.3Roles and Responsibilities

Role	Member	Responsibility
CAVs & CSMS Graduate Advisor	Vipin Kumar	Provide team guidance and assist with bridging CSMS and CAVs
GRA for Mechanical and CAVs	Aaron Rabinowitz	Assists with CAVs software and hardware implementation. Develop sensor validation methods.
CAVs Graduate Advisor	Joydeep Dey	Develop CAVs framework design, and manage CAVs software and hardware implementations.
CAVs Team Lead	Haoying Wang	Develop and integrate CAVs sensor architecture design, and CAVs software and hardware implementations
CAVs Systems Safety Representative	Hein Thant	Develop system safety case. Perform safety analysis and determine safety requirements. Develop test plan and V&V methods.
CAVs Vision Team Member	Hein Thant	Perform Matlab simulations, FOV scenarios, and DNN research.
CAVs Vision Team Member	Haoying Wang	Perform Matlab simulation, and FOV scenarios.

CAVs Engineer	Xinming Ye	Develop and implement sensor fusion algorithm simulation.
CAVs Controller Integration Engineer	Wes Taylor	Assist with controller in coordination with rest of CAVs system; Assist in judging CAVs controller capability
CAVs Mechanical team member	Abdulla Alghfeli	Perform wiring, CAD modeling, 3D printing, and mounting.
CAVs Mechanical team member	Abdulaziz Alshamsi	Perform wiring, CAD modeling, 3D printing, and mounting.
CAVs Engineer	JT Bovee	Perform CAVs software implementation.
CAVs Engineer	Shaolong Shi	Develop and simulate sensor fusion algorithm

Team: CSMS

Role	Member	Responsibilities
CSMS Team Lead	Nikki Machado	Oversee high-level mission activities and operate in a supervisory capacity. Define project scope, and manage requirements, planning, schedule, budget, and stakeholder engagement.
CSMS Technical Manager	Josh Urban	Development of controls software. Determine system/component requirements through software simulation
CSMS Systems Safety Representative	Grant Moore	Develop system safety case. Perform safety analysis and determine safety requirements. Develop test plan and V&V methods.

Team: PSI

	1	
Role	Member	Responsibilities
PSI Co-Team Lead	Nick Brunson- Williams	Provide high level technical advice, vendor communication, task development and delegation.
PSI Co-Team Lead	Brady Johnson	Provide high level technical advice, vendor communication, task development and delegation.
PSI System Safety Co- Representative	Ben Mckenney	Provide technical support for powertrain team functions including safety documentation and brainstorming
PSI System Safety Co- Representative	Wesley Martin	Provide technical support for mechanical team functions including safety documentation and brainstorming
PSI Team Members	Isaac Hellard Chris Huser	Provide technical support for mechanical team functions
	Grady Egan	
	Jesus Rodriguez	
	Michael Gaffney	

Appendix 1.4Evidence of Competence

CSU VIT Evidence of Competence		
Member	Role	Evidence of Competence
Gabriel Di Domenico	Powertrain Technical Manager	Graduate research assistant involved in AVTC's for the previous 3 years. Currently also in role as PM for EcoCAR MC. Advanced study of hybrid electric vehicle architecture. Involved in the development and build of a hybrid Chevrolet Camaro
Troy Johnson	Powertrain Technical Manager	Graduate research assistant involved in FSAE as the PM role. Currently also in role as EM for EcoCAR MC. Advanced study of hybrid electric vehicle architecture.
David Trinko	Controls Technical Manager	Graduate research assistant involved in hybrid controls development for previous 3 years. Advanced study of hybrid electric vehicle architecture. Integral part in the development of the controls for Toyota project.
Matthew Knopf	System Safety Manager	Graduate research assistant involved in AVTC's for the previous 2 years. Currently also in role as system safety manager for EcoCAR MC and acted in that role for EcoCAR 3. Involved in the development and build of a hybrid Chevrolet Camaro

Appendix 1.5 Evidence of Quality Management

It is critical to institute and maintain a quality management system to support functional safety.

Quality management, across all phases of the safety lifecycle, includes the university and facilities overall safety management, the project dependent safety management, and safety management regarding production, operation, service, and decommissioning.

Overall safety management ensures those responsible for performing safety activities in the safety lifecycle achieve the following objectives:

- Institute and maintain a safety culture,
- Promotes effective communication across all disciplines,

- Institute and maintain adequate functional safety organizational rules and processes,
- Ensure that the competence of the member is proportionate with their responsibilities.

Project dependent safety management ensures that during the concept development phase and at the system, hardware, and software-levels, the organization achieves the following objectives:

- Define safety activities for the system safety lifecycle,
- Plan, coordinate, and track the progress of safety activities,
- Create comprehensive safety cases in order to provide the argument for the achievement of functional safety,
- Decide at the end of development if the item achieves the minimum acceptable level of safety to be released for production and operation.

Safety management regarding production, operation, service, and decommissioning is a body of evidence, assembled from the previous work products, that justifies the systems level of safety.

Appendix 1.6Evidence of a Good Safety Culture

Management of Functional Safety Evidence of a Good Safety Culture		
Examples indicative of a poor safety culture Examples indicative of a good safety culture		
Accountability is not tractability	The process assures that accountability for decisions related to functional safety is documented and traceable	
Cost and schedule always take precedence over safety and quality	Safety is the highest priority	
The reward system favors cost and schedule over safety and quality	The reward system supports and motivates the effective achievement of functional safety The reward system penalizes those who take short cuts that jeopardize safety or quality	

Personnel assessing safety, quality, and their governing processes are influenced unduly by those responsible for executing the processes	 The process provides adequate checks and balances The appropriate level of independence in the safety, quality, verification, validation processes
 Passive attitude toward safety Heavy dependence on testing at the end of the product development cycle Management reacts only when there is a problem in the field 	 Proactive attitude towards safety Safety and quality issues are discovered and resolved from the earliest stage in the product lifecycle
The required resources are not planned or allocated in a timely manner	The required resources are allocated Skilled resources have the competence commensurate with the activity assigned
 "Groupthink" 'Stacking the deck" when forming review groups Dissenter is ostracized or labelled as "not a team player" Dissent reflects negatively on performance reviews "Minority dissenter" is labeled or treated as a "troublemaker", "not a team player", or a "whistleblower" Concerned employees fear repercussion 	 The process uses diversity to advantage Intellectual diversity is sought, valued, and integrated in all processes Behavior which counters the use of diversity is discouraged and penalized Supporting communication and decision-making channels exist and the management encourages their usage Self-disclosure is encouraged Disclosure of discovery by anyone else is encouraged The discovery and resolution process continues in the field
No systematic continuous improvement processes, learning cycles or other forms of "lessons learned"	Continuous improvement is integral to all processes
Processes are "ad hoc" or implicit	 A defined traceable and controlled process followed at all levels, including Management Engineering Development interfaces Verification Validation Functional safety audit Functional safety assessment

Appendix 2Item Definition – Complete Documentation

Appendix 2.1 CAVs Item Definition

CAVs Item Definition		
Item	Sub-Item	Functional Behavior
LKA system	 CAVs sensors and mounts Wiring Feedback system CSMS systems PSI systems 	 Operator initiates LKA system Performs lane-line, object detection and multi-feature tracking Sensors send data to associated computer Computer performs sensor fusion data verification & validation using developed algorithms and NNs Computer sends control action decision to associated controller Provides feedback to the operator (LKA status, haptic, visual, audio) Controls lateral movement via EBCM Controls lateral movement via EPS
ACC system	 CAVs sensors and mounts Wiring Feedback system CSMS systems PSI systems 	 Operator initiates ACC system and sets velocity and distance constraint Monitors surrounding traffic/object distance, velocity, size and position Monitors operator engagement Sensors send data to associated computer Computer sends control action decision to associated controller Provides feedback to the operator (ACC status, haptic, visual, audio) Controls longitudinal movement via EBCM Controls longitudinal movement via throttle position or APP

Intel Tank Computer	- Wires	- Blends various sensors (cameras, radars) data to achieve reliable, high-definition images
	- Fuses	- Performs sensor fusion data verification &
	- Mount	validation using developed algorithms and NNs
	- Sensor fusion algorithms and NNs	- Determines if control action (EPS torque, braking, feedback) is required
	- Computers	- Sends control action request to associated controller
		- Provides real-time functionalities
Intel Mobileye 6	- Mount	- Performs multi-feature tracking
0	- Wires	- Performs object and lane detection
	- Eye-Watch Display	- Performs forward collision warning
	- Sensor	- Performs pedestrian collision warning
		- Performs headway warning
		- Performs traffic sign recognition
		- Sends data to associated controller
		- Provides a real-time display
Bosch Front	- CAN bus	- Performs early front and rear speed detection
and Rear Radar	- Mount	- Performs early front and rear position detection
	- Radar	- Sends data to associated controller
Bosch MRR	- CAN bus	- Performs early corner speed detection
Corner Radar x2	- Mount	- Performs early corner position detection
	- Radar	- Sends data to associated controller
12 V CAVs	- Wires	- Powers all CAVs components
Power Supply	- Fuse	
	- Battery	
Intel Movidius Neural	- USB plug	 Performs vision processing tasks in assistance to Intel Tank computational capabilities
Compute Stick	- Sensor fusion algorithms	
	- NNs	- Assists in blending various sensors (cameras, radars) data to achieve reliable, high-definition images

		 Assists in performing sensor fusion data verification & validation Assists in determining if control action (EPS torque, braking, feedback) is required Offload DNN computation
KVaser	- Controller	- Interfaces CAN signals to USB
Niles CAM	- Wires	- Performs real-time monitoring of operator
	- Mount	- Sends data to associated controller
	- Camera	
CAVs real-time display	- Wires	 Acquires sensor fusion images from associated controller
	MountDisplay	- Displays sensors fusion images in real-time
ZED Camera	- USB cable	- Performs high-resolution depth perception
	- Mount	- Performs 6-axis positional tracking to sense space and motion
	- Camera	- Performs large-scale 3D mapping
GPS module	- Wires	- Receives GPS data
	- Mount	- Provides GPS data to associated controller

Appendix 2.2 CSMS Item Definition

	CSMS Item Definition		
Item	Sub-Item	Functional Behavior	
HSC	 Connectors Mounts Line Controller 	 Acquires operator and various sensor inputs (APPS, gear, vehicle speed) Controls all hybrid driving functions Controls torque via engine/EM torque split using rules-based or PAE control strategy Maintains SOC at appropriate level Determines gear shifting Modifies stock signals 	

ECM	- Connectors	- Controls engine torque output
	- Mounts	- Controls engine temperature
	- Line	- Controls A/F ratio
	- Controller	- Controls idle speed
		- Controls electronic valve
ТСМ	- Connectors	 Receives inputs from HSC, ECM, and various sensors (vehicle speed, wheel speed, throttle
	- Mounts	position)
	- Line	- Controls gear shifting
	- Controller	- Monitors and regulates transmission thermal control system
EMC	- Connectors	- Regulates supply of current to EM
	- Mounts	- Convert DC to AC
	- Line	- Controls direction of current
	- Controller	- Monitor and regulates EM temperature
ВСМ	- Connectors	 Powers auxiliary low-voltage systems to include power windows, power mirrors, and air
	- Mounts	conditioning
	- Line	
	- Controller	
EBCM	- Connectors	- Acquires operator and various sensor (wheel speed, brake switch) inputs
	Mounts	
	- Line	 Actuates and controls the automatic braking system by a cycle of increasing and decreasing brake pressure
	- Controller	brake pressure
BMS	- Connectors	- Ensure safe ESS operating conditions
	- Mounts	- Monitor ESS state (voltage, temperature, SOC, and
	- Line	current)
	- Controller	- Protects against over-current, over-voltage, under- voltage, and over-temperature
		- Reporting data
		- Controls/balances ESS environment

EPS	 Steering angle sensor Torque sensor Motor Vehicle speed sensor Wires Controller 	 Determines assisting steering power based on various inputs (driver steering torque request, steering wheel position, and vehicle speed) Actuates motor to rotate steering gear which reduces torque required by the driver
	- Mount	
Low Voltage	 Air bag Windshield wipers Instrument cluster Lights Entertainment system Turn signals Security system Keyless entry Power windows Power mirrors Power locks 	 Acquires inputs from the operator, environment, and various sensors Controls all auxiliary functions to include air bags, windshield wipers, instrument cluster, lights, entertainment system, turn signals, haptic feedback, security system, pumps, fans, controller and DAQ Controls thermal components Controls data acquisition
	PumpsFansDAQ	
OBC	- Connectors	- Controls charging to the HV battery pack
	MountsLine	
	- Controller	

OBD II	- Connectors	- Provides list of vehicle parameters to monitor
	- Mounts	
	- Line	
	- Controller	
CAN bus	Wiring harnessControllers	- Transfers necessary signals such as EM speed, EM torque, EM temperature, EMC temperature, SOC, current, voltage, battery temperature, and OBC
		temperature
Accelerator Pedal Position Sensor (APPS)	- Sensors	- Monitors the position of the accelerator pedal and transmit a torque request

Appendix 2.3 PSI HV Item Definition

PSI HV Item Definition			
Item	Sub-Item	Functional Behavior	
HV battery pack	ModuleLinesMounts	- Store and supply energy to EM	
Enclosure	 Mounts Thermal control/fans Wiring ports - Nema components 	 Contain HV components Prevent horizontal and vertical free movement of HV components Prevent unauthorized access to HV components 	
Junction box	 Mounts Relays Lines Nema components 	- Ease use for maintenance and consolidation of HV wire connections and relays	
Wiring	 Mounts Thermal protection Connectors Clamps 	- Transfer energy and signals	

BMS	 Connectors Mounts Line Controller 	 Ensure safe ESS operating conditions Monitor ESS state (voltage, temperature, SOC, and current) Reporting data Controls/balances ESS environment
OBC	 Connectors Mounts Port Controller 	- Controls charging to the HV battery pack
EMC	 Connectors Mounts Line Controller 	 Regulates supply of current to EM Convert DC to AC Control direction of current

Appendix 2.4 PSI Mechanical Item Definition

PSI Mechanical Item Definition			
Item	Sub-Item	Functional Behavior	
Driveshaft	- Yokes	- Longitudinal shaft which transmits torque from engine/transmission to rear of vehicle	
	- U joint	engine/transmission to rear or venicie	
	- Shaft		
	- Bearings		
	- Clamps		
	- Rings		
	- Axle beam		
	- Steering knuckle		
	- Rods		
	- Brake drum		

Differential	- Gears	- Provides power from driveshaft to wheels and
	- Cover	allows wheels to rotate at different speeds
	- Gasket	
Suspension	- Spring	- Provides dynamic energy absorption of vertical
	- Knuckle	force exerted on wheels by the change in road conditions
	- Upper arm	
	- Stabilization bar	
	- Radius rod	
	- Driveshaft boot	
	- Strut mount	
	- Ball joint	
	- Sway bar	
	- Tires	
Brakes	- Caliper	- Inhibits vehicle motion
	- Pads	- Slows/stops moving vehicle
	- Disc-rotor	- Keeps stopped vehicle stationary
	- Wheel bearing	
	- Bleed valves	
	- Lines	
	- Pedal	
	- Master cylinder	
Thermal	- Radiator	- Detects and controls cabin/component
	Hoses	temperatures
	- Fan	
	- Water pump	
	- Transmission cooler	
	- Reserve tank	
	- Heater core	
	- Thermostat/sensors	

Steering	- Wheel	- Controls lateral movement of the vehicle
	- Gearbox	
	- Arms/rods	
	- Column	
	- Pump	
	- Fluid reservoir	
	- Lines	
Exhaust	- Catalysts	- Removal of toxic gases/fumes and noise
	- Muffler	
	- Tubing	
	- Manifold	
	- Sensors	
	- Hanger/clamps	
Engine	Cylinder head cover	- Provide torque at request of operator
	- Intake/exhaust manifold	
	- Oil filter	
	- Water pump	
	- Timing belt/gears	
	- Oil pan/gasket	
	- Engine block	
	- Distributer/spark plugs	
	- Crankshaft	
	- Starter motor	
	- Air intake	
	- Furl rail/pump	
	- Engine control module	

Motor	- Fully assembled	- Provide torque at request of operator
	- Through shaft	 Allows for energy regeneration and transfer to the battery during negative torque events
	- Housing	buttery during negative torque events
	- Electric motor controller	
Transmission	- Through shaft input/output	- Transfers power from engine to driveshaft
	- Oil pump	- Gears change drive-wheel speed and torque in relation to engine speed and torque
	- Torque converter	
	Housing	
	- Transmission control module	
Clutch	- Through shaft input/output	- Enable smooth vehicle movement by transmitting torque from the engine to drivetrain
	- Disc	torque nom die engine to unvertain
	- Flywheel	
	- Pressure plate	
	- Housing	
F 1	- Indicator pin	
Fuel	- Tank/sensor gauge	- Store and supply fuel to engine
	- HP pump	
	- Port	
	- Hoses	
	- Injectors	
	- Filter	
	- Rail	
	- Emissions canister	
Body	- Hood	- Allows access to and protects components in
	- Grill	engine compartment
	- Headlights	- Allows operator to see in low light scenarios
	- Fenders	 Prevent debris from being thrown into air by rotating tire
	- Doors	 Allows access to/from cabin and protects operator from environment and debris
	- Bumpers	 Absorb impact of minor collision

 Tail lights Trunk cover Mirrors Windows 	 Signals turning and braking Allows for operator to have surrounding view
--	---

Appendix 3HARA – Complete Documentation

Appendix 3.01 HARA CAVs / CSMS ACC DFMEA

				CAVs / CS	MS A	CC DFMEA				
Function	Failure Type	Potential Impact	S	Potential Cause	0	Prevention Mode	Detection Mode	D	RPN	Functional Requirement
Control longitudinal velocity via braking	Failure to control longitudinal velocity via braking	Unintended acceleration Unintended longitudinal motion Operator and/or passenger injury Damage to or loss of	10	Wiring and/or signal failure (not proper gauge, installation or manufacturing failure)	7	Ensure wiring is securely installed using manufacturer installation specifications Ensure wire bend radii are adhered to	Vehicle technical inspection will identify wiring fatigue or failure Operator aware during operation by identifying eventual failure of vehicle	8	560	The ACC system shall be wired and installed according to manufacturer specifications to include bend radii, heat shielding, EMI avoidance, sheathing, proper gauge, and interface connections
		Damage to environment		Brake pad fatigue or failure (overheating, corrosion)	5	Ensure proper mounting and installation of pads Ensure bolts and mounting hardware is securely fastened and free from potential loosening or movement	componentsVehicletechnicalinspection willidentify if thepads are freefrom fatigue orcorrosionOperator awareduringoperation byidentifyingunsettlingsmell, andvehiclevibration	3	150	ACC brake system shall engage in timely manner such that brake pad fatigue and passenger discomfort is minimized Development teams shall ensure proper mounting and installation of brake pads Development teams shall ensure brake pad bolts and mounting

			Avoid adverse road conditions Routine maintenance and inspection for rust and corrosion Avoid poor driving behaviors				hardware are securely fastened and free from potential loosening or movement Operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH Operator shall avoid poor driving behaviors
	Brake rotor fatigue or failure (overheating, corrosion)	4	Ensure proper mounting and installation of rotors Ensure bolts and mounting hardware are securely fastened and free from potential loosening or movement Avoid adverse road conditions Routine maintenance and inspection for rust and corrosion Avoid poor drive behavior	Vehicle technical inspection will identify if the rotors are free from fatigue or corrosion Operator aware during operation by identifying unsettling smell, and vehicle vibration	3	120	ACC brake system shall engage in timely manner such that brake rotor fatigue and passenger discomfort is minimized Development teams shall ensure proper mounting and installation of brake rotors Development teams shall ensure brake rotor bolts and mounting hardware are securely fastened and free from potential loosening or movement Operator shall avoid excessively adverse road conditions (bumpy terrain,

						excessive grade) which may cause a high NVH Operator shall avoid poor driving behaviors
Debris (snow, mud) build-up on brake syster	3 n	Ensure brake system is free of build-up and debris prior to use	Vehicle technical inspection will identify if the brake system is free from build- up Operator aware during	6	180	Operator shall ensure brake system is free of build-up (snow, mud) and debris prior to use
			operation by identifying vehicle NVH			
Adverse road conditions (bumpy terrain excessive grade)	, 2	Avoid adverse road condition which may produce NVH and damage suspension	Operator aware prior to or during operation. Increased NVH	4	80	Operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH
Calipers get stuck	2	Avoid adverse road conditions Routine maintenance and inspection for rust and corrosion Avoid poor drive behavior	Operator aware during operation by identifying unsettling smell, vehicle vibration, and partial or total loss of functionality	6	120	Operator shall avoid excessively adverse road conditions which may cause a high NVH Operator shall ensure routine inspection for caliper rust and corrosion Operator shall avoid
Brake fluid line failure (leak, ai in line)		Ensure proper bleeding, mounting,	Operator aware during operation by	5	100	poor driving behaviors ACC brake system shall engage in timely manner such that brake

				its functionality	technical inspection will		shall ensure proper bleeding, mounting, installation, and
				Ensure bolts	inspection will identify leaks		installation, and routine maintenance
				and mounting hardware is			and inspection of brake line hardware and its
				securely fastened and			functionality
				free from potential			Development team shall ensure bolts and
				loosening or			mounting hardware are
				unintended movement			securely fastened and free from potential
							loosening or unintended movement
			Other				ACC system shall
							allow operator to override automated
							controls with minimal
							braking engagement
	Potential		Potential	Prevention	Detection		Functional
	Impact	S				RPN	Requirement

Control longitudinal velocity via throttle position or APP	Failure to control longitudinal velocity via throttle position	Unintended acceleration Unintended longitudinal motion Operator and/or passenger injury Damage to or loss of property Damage to environment	10	Wiring and/or signal failure (not proper gauge, installation or manufacturing failure)	7	Ensure wiring is securely installed using manufacturer installation specifications Ensure wiring gauge is sufficient to carry max operational current with factor of safety Ensure wire bend radii are adhered to	Vehicle technical inspection will identify wiring fatigue or failure Operator aware during operation by identifying eventual failure of vehicle components	8	560	The ACC system shall be wired and installed according to manufacturer specifications to include bend radii, heat shielding, EMI avoidance, sheathing, proper gauge, and interface connections
				Engine failure - Fuel filter failure (clogged, leak)	4	Ensure proper mounting, installation, and manufacturing of the fuel filter Ensure the permeable material is clean and the fuel filter is free of physical damage and leaks while under pressure	Vehicle technical inspection will identify if the filter is free of leaks or physical damage Operator aware during operation by identifying a lack of engine power, stalling, or misfire	6	240	Development team shall ensure proper mounting, installation, and manufacturing of the fuel filter Development team shall ensure the fuel filter permeable material is clean and the is free of physical damage and leaks while under pressure
				Engine failure - Fuel injection failure (clogged, leak)	4	Ensure proper installation of the fuel injectors	Operator aware during operation by identifying a partial or total	6	240	Development team shall ensure proper installation of the fuel injectors

			Ensure injector mounting hardware is securely fastened and free from potential loosening or movement Ensure adequate fuel level and type Ensure use of fuel system cleaners when	loss of engine functionality Clogged injector will produce surges of power			Development team shall ensure injector mounting hardware is securely fastened and free from potential loosening or movement Operator shall ensure adequate fuel level and type Operator shall ensure use of fuel system cleaners when recommended
	Engine failure - Fuel pump failure	4	recommended Ensure proper mounting and installation of fuel pump Ensure fuel pump mounting hardware is securely fastened and free from potential loosening or movement Ensure fuel adequate fuel level and type	Operator aware during operation by identifying a partial or total loss of engine functionality, rising temperature, surging, and decreased mpg	6	240	Development teams shall ensure proper mounting and installation of fuel pump Development teams shall ensure fuel pump bolts and mounting hardware are securely fastened and free from potential loosening or movement Operator shall ensure adequate fuel level and type

Po	ngine failure - 2 oor fuel uality		Verify fuel quality prior to filling	Operator aware during operation by identifying a partial or total loss of engine functionality, surging, and decreased mpg	6	120	Operator shall ensure fuel quality prior to filling
Im lul fil	ngine failure - 5 nproper ıbrication (oil lter/pump ilure)		Ensure proper mounting, installation, and manufacturing of the oil filter and pump Ensure bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from leaks and potential loosening or movement. Ensure frequent oil changes, clean oil, and that the oil filter is not ballooned or deformed	Vehicle technical inspection will identify deformation to filter and unclean oil Operator aware during operation by identifying loss of vehicle functionality, Sputtering, engine grinding, dirty exhaust, or a drop in pressure smell of exhaust fumes, or increased noise	8	400	Development teams shall ensure proper mounting, installation, and manufacturing of oil filter and pump Development team shall ensure bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from leaks and potential loosening or movement Operator shall ensure frequent oil changes, clean oil, and that the oil filter is not ballooned or deformed
Im	ngine failure - 1 nproper fuel ctane number	L	Verify prior to filling tank	Combustion failure will lead to loss of	4	40	Operator shall ensure proper fuel octane number prior to filling tank

	1		vehicle			
	1		functionality.			
Engine failure -	4	Ensure thermal	Sensors signal	8	320	Operator shall ensure
Excessive		system	to ECM	-		thermal system
heating		components				components (radiator,
(radiator,		(radiator,	Operator aware			coolant level, fans,
coolant leak,		coolant level,	during			water pump,
water pump,		fans) are	operation.			thermostat) are
fan, or		functional and	-			functional and
thermostat		sufficient to	Operator views			sufficient to cool the
failure)		cool the engine	engine temp in			engine
			cabin.			
	1	Ensure the fans				Development team
	1	are free from	Error message			shall ensure the fans
	1	potential	displayed.			are free from potential
		physical				physical damage
		damage				
						Development team
		Ensure				shall ensure fans pull
		enclosure fans				air from a cool source
		pull air from a				
		cool source				Development team
		Energy engine				shall ensure engine ventilation is sufficient
		Ensure engine ventilation is				
		sufficient to				to provide appropriate air movement through
		provide				engine bay
		appropriate air				engine bay
		movement				Development team
		through engine				shall ensure thermal
		bay				system is designed
		cuj				such that there is
		Ensure thermal				sufficient air flow to
	1	system is				cool engine
		designed such				components
	1	that there is				· ·
		sufficient air				Development team
		flow to cool				shall ensure proper
	1	engine				mounting, installation,
		components				and manufacturing of

		Ensure proper mounting, installation, and manufacturing of thermal system and its components Ensure bolts and mounting hardware are securely fastened and free from potential loosening or movement Ensure the ECM controls and mitigates overheating Operator drives appropriately to ensure engine temp is stable				thermal system and its components Development team shall ensure bolts and mounting hardware are securely fastened and free from potential loosening or movement Development team shall ensure the ECM controls and mitigates engine overheating
Engine failure - Head gasket failure	4	Ensure proper mounting, installation, and manufacturing of intake manifold and its components Ensure bolts, interface components (seals, gaskets),	Vehicle technical inspection will identify fluid leaks Operator aware during operation by identifying displayed engine high	6	240	Development team shall ensure proper mounting, installation, and manufacturing of intake manifold and its components Development team shall ensure bolts, interface components (seals, gaskets), and mounting hardware are

		and mounting hardware are securely fastened and free from leaks and potential loosening or movement Ensure thermal system is functional	temperatures, decrease in power, misfires, stalling, or gases venting in the engine bay			securely fastened and free from leaks and potential loosening or movement Operator shall ensure thermal system is functional
Engine failure - Engine misfire (ECM, sparkplug, ignition system valve/spring failure)	4	Ensure proper mounting, installation, and manufacturing of the sparkplugs, fuel injectors, and air intake system Ensure bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from leaks and potential loosening or movement Ensure proper A/F ratio and functioning O2 sensor	Vehicle technical inspection will identify fluid leaks Operator aware during operation by identifying hesitated power delivery, error message, reduced mpg, and increased emissions	8	320	Development team shall ensure proper mounting, installation, and manufacturing of the sparkplugs, fuel injectors, and air intake system Development team shall ensure bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from leaks and potential loosening or movement Development team shall ensure proper A/F ratio and functioning O2 sensor Development team shall ensure vacuum lines and manifold gasket are free from

			Ensure vacuum lines and manifold gasket are free from cracks and physical damage Ensure properly functioning timing belt Ensure properly functioning EGR valve		2	100	cracks and physical damage Development team shall ensure properly functioning timing belt Development team shall ensure properly functioning EGR valve
	Engine failure - Excessive load and improper driving	6	Ensure proper vehicle operation (reduce engine speed/load)	Vehicle technical inspection will identify tire wear, leaks, and brake component fatigue Operator aware during operation by identifying progressive loss of engine functionality	3	180	Operator shall ensure proper vehicle operation (reduce engine speed/load)
	Engine failure - Exhaust gas recirculation system (A/F ratio, O2 sensor failure)	2	Ensure proper mounting, installation, and manufacturing of EGR system and its components	Operator aware during operation by identifying progressive loss of engine functionality, rough idling, smell of fuel,	3	60	Development team shall ensure proper mounting, installation, and manufacturing of EGR system and its components Development team shall ensure bolts,

			Ensure bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from leaks and potential loosening or movement Ensure proper functionality of exhaust gas recirculation (EGR) valve and O2 sensor	poor mpg, error message			interface components (seals, gaskets), and mounting hardware are securely fastened and free from leaks and potential loosening or movement Development team shall ensure proper functionality of exhaust gas recirculation (EGR) valve and O2 sensor
	Motor failure - Over-current	7	Ensure software (HSC) limits the magnitude of current to the EM Ensure relays and fuses are in place and functional to prevent over drawing of current	Operator aware during operation by vehicle response to torque request, potential EM over-heat or failure	7	490	Development team shall ensure software (HSC) limits the magnitude of current to the EM Development team shall ensure relays and fuses are in place and functional to prevent over drawing of current
	Contamination (EM housing or coolant system failure)	7	Ensure proper mounting, installation, and manufacturing of the EM and housing	Vehicle technical inspection will identify leaks or physical damage	8	560	Development team shall ensure proper mounting, installation, and manufacturing of the EM and housing Development team shall ensure bolts,

		Ensure bolts, interface components, and mounting hardware are securely fastened and free from leaks and potential loosening or movement. Ensure cooling system and its components are functioning, proper coolant levels, and hoses running to and from the motor are leak free	Operator aware during operation by identifying loss of motor functionality			interface components, and mounting hardware are securely fastened and free from leaks and potential loosening or movement. Development team shall ensure cooling system and its components are functioning, proper coolant levels, and hoses running to and from the motor are leak free
Motor failure - Overheating (coolant failure)	8	Ensure thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the EM Ensure the fans are free from potential physical damage	Operator aware during operation by identifying high EM temperature and loss of motor functionality	8	640	Development team shall ensure thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the EM Development team shall ensure the fans are free from potential physical damage Development team shall ensure fans pull air from a cool source

1		Ensure fans pull				Development team
		air from a cool				shall ensure proper
		source				mounting, installation,
						and manufacturing of
		Ensure proper				coolant system and its
		mounting,				components
		installation, and				· · · · · · · · · · · · · · · · · · ·
		manufacturing				Development team
		of coolant				shall ensure bolts,
		system and its				hoses and mounting
		components				hardware are securely
		components				fastened and free from
		Ensure bolts,				potential loosening or
	1	hoses and				movement
		mounting				movement
	1	hardware are				Development team
		securely				shall ensure the HSC
		fastened and				controls and mitigates
		free from				e
						overheating
		potential				0
		loosening or				Operator shall avoid
		movement				poor driving behaviors
		E 1 100				
		Ensure the HSC				
		controls and				
		mitigates				
		overheating				
		Operator drives				
		appropriately to				
	1	ensure EM				
	L	temp is stable				
Motor failure -	7	Ensure thermal	Operator aware	8	560	Development team
Low resistance	1	system	during			shall ensure thermal
due to		components	operation by			system components
insufficient		(radiator,	identifying			(radiator, coolant level,
isolation		coolant level,	high motor			fans) are functional
between		fans) are	temperature			and sufficient to cool
windings		functional and	and loss of			the EM
(corrosion or	1	1	1		1	

physical damage)		sufficient to cool the EM Ensure bolts, hoses and mounting hardware are securely fastened and free from potential loosening or movement Ensure the HSC controls and mitigates overheating	motor functionality			Development team shall ensure bolts, hoses and mounting hardware are securely fastened and free from potential loosening or movement Development team shall ensure the HSC controls and mitigates overheating
Motor failure - Internal component failure (stator, rotor, bearings, or shaft)	3	Avoid adverse road condition which may produce NVH and damage EM internal components Ensure thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the EM	Operator aware during operation by identifying partial or total functionality failure	8	240	Operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH Development team shall ensure thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the EM
EM-driveshaft interface failure	8	Ensure proper mounting, installation, and manufacturing	Vehicle technical inspection will identify if the	9	720	Development team shall ensure proper mounting, installation, and manufacturing of

of EM, interface is free	EM, driveshaft, and its
driveshaft, and of	interfacing components
its interfacing manufacturing	internet ing components
components or installation	Development team
fatigue or	shall ensure bolts and
Ensure bolts failure	mounting hardware is
and mounting	securely fastened and
hardware is Operator aware	free from potential
securely during	loosening or
fastened and operation by	unintended movement
free from identifying	unintended movement
potential partial or total	Development team
loosening or functionality	shall ensure EM-
unintended failure	driveshaft interface
movement	location is covered and
movement	free from potential
Ensure EM-	unintended access or
driveshaft	physical damage
interface	physical damage
location is	Development team
covered and	shall ensure proper
free from	EM-driveshaft
potential	alignment
unintended	angiment
access or	Development team
	shall ensure EM-
physical	driveshaft interface
damage	
Ensura propar	angle is minimized
Ensure proper EM-driveshaft	Operator shall avoid
	Operator shall avoid
alignment	excessively adverse
Ensure EM	road conditions
Ensure EM-	(bumpy terrain,
driveshaft	excessive grade) which
interface angle	may cause a high NVH
is minimized	
Avoid adverse	
road condition	
which may	

	1	1		1	1 1 1 1 1 1 1 1			1	1
					produce NVH				
					and damage				
					EM-driveshaft				
					interface				
			EM-	8	Ensure proper	Vehicle	9	720	Development team
			transmission		mounting,	technical			shall ensure proper
			failure		installation, and	inspection will			mounting, installation,
					manufacturing	identify if the			and manufacturing of
					of EM,	interface is free			EM, transmission, and
					transmission,	of			its interfacing
					and its	manufacturing			components
					interfacing	or installation			1
					components	fatigue or			Development team
					r	failure			shall ensure EM-
					Ensure bolts				transmission bolts and
					and mounting	Operator aware			mounting hardware is
					hardware is	during			securely fastened and
					securely	operation by			free from potential
					fastened and	identifying			loosening or
					free from	partial or total			unintended movement
					potential	functionality			unintended movement
						failure			Development to one
					loosening or unintended	Tallure			Development team shall ensure EM-
					movement				transmission interface
									location is covered and
					Ensure EM-				free from potential
					transmission				unintended access or
					interface				physical damage
					location is				
					covered and				Development team
					free from				shall ensure proper
					potential				EM-transmission
					unintended				alignment
					access or				
					physical				Operator shall avoid
					damage				excessively adverse
					-				road conditions
					Ensure proper				(bumpy terrain,
					EM-				excessive grade) which
									may cause a high NVH
L	1		1		1	1	l	1	ing cause a ingit () II

	Accelerator Pedal (AP) and/or Accelerator Pedal Position Sensor (APPS) failure	3	transmission alignment Avoid adverse road conditions which may produce NVH and damage EM- transmission interface Ensure the AP and APPS mounting hardware are secure, free from unintended movement, and sufficient for open road conditions Ensure software limits current rates and ranges Ensure relays and fuses are in place and functional to prevent over drawing of current	Vehicle technical inspection will identify if AP and APPS are free of manufacturing or installation fatigue or failure Operator aware during operation by identifying immediate or eventual failure of vehicle components and loss of functionality	2	60	Development team shall ensure the AP and APPS mounting hardware are secure, free from unintended movement, and sufficient for open road conditions Development team shall ensure software limits current rates and ranges Development team shall ensure relays and fuses are in place and functional to prevent over drawing of current
							allow operator to override automated controls with minimal AP engagement

		Potential		Potential		Prevention	Detection			Functional
Function	Failure Type	Impact	S	Cause	0	Mode	Mode	D	RPN	Requirement
Sensors observe	Failure of	Unintended	5	Wiring and/or	5	Ensure wiring	Vehicle	4	100	The ACC sensors shall
surrounding	sensors to	longitudinal		signal failure		is securely	technical			be wired and installed
traffic/object	observe	motion		(not proper		installed using	inspection will			according to
distance,	surrounding			gauge,		manufacturer	identify wiring			manufacturer
velocity, size	traffic/object	ACC system		installation or		installation	fatigue or			specifications to
and position to	distance,	shutdown		manufacturing		specifications	failure			include bend radii, heat
include operator	velocity, size			failure)			_			shielding, EMI
engagement	and position to			D 0.11		Ensure wiring	Operator aware			avoidance, sheathing,
	include			Power failure		gauge is	during			proper gauge, and
	operator			a		sufficient to	operation by			interface connections
	engagement			Communication		carry max	identifying			
				failure		operational current with	eventual failure of vehicle			ACC system shall alert
						factor of safety				operator prior to and when shutdown occurs
						factor of safety	components			when shutdown occurs
						Ensure wire				ACC system shall only
						bend radii are				be operational if sensor
						adhered to				performance meets a
						uunerea to				minimum standard
										(communication speed,
										sensor availability or
										visibility)
										ACC communications
										shall operate
										independently and be
										free from external
				XX 1 1	7	F	X7.1.1	4	1.40	manipulation
				Unintended	7	Ensure sensor	Vehicle	4	140	Development team
				access and		enclosure	technical			shall ensure sensor
				physical		manufacturing and use of	inspection will			enclosure
				damage (debris, puncture)		and use of materials is	identify if sensors are free			manufacturing and use of materials is
				puncture)		sufficient to	of physical			sufficient to prevent
						prevent	damage			unintended access and
						unintended	Gamage			physical damage
						access and	Operator aware			physical damage
						access and	during			
	1			1			uuring			

		physical damage Ensure bolts and mounting hardware is securely fastened and free from potential loosening or unintended movement	operation by identifying functionality failure			Development team shall ensure sensor and sensor enclosure bolts and mounting hardware is securely fastened and free from potential loosening or unintended movement
Sensor visibility obstruction	7	Ensure sensors have clear field of view and are free of visibility obstruction	Vehicle technical inspection will identify if sensors are free of obstruction Operator aware during operation by identifying functionality failure	3	105	Operator shall ensure ACC system sensors have clear field of view and are free of visibility obstructions ACC system shall only be operational if sensor performance meets a minimum standard (communication speed, sensor availability or visibility)
Minimum operational speed	10	ACC sensors require a minimum vehicle speed to be operational	Operator aware during operation by identifying vehicle speed	1	50	ACC system shall require minimum vehicle speed based on sensor requirements
Other						ACC system shall function according to operator engagement ACC system shall respond (feedback, acceleration, deceleration) more

										quickly in the event of less operator engagement (hands on wheel, head tilt, eye deviation) ACC system shall respond (feedback, acceleration, deceleration) less quickly in the event of more operator engagement (hands on wheel, head tilt, eye deviation)
		Potential		Potential		Prevention	Detection			Functional
Function	Failure Type	Impact	S	Cause	0	Mode	Mode	D	RPN	Requirement
Sensor data	Failure of	Unintended	3	Wiring and/or	3	Ensure wiring	Vehicle	3	27	The ACC sensors shall
transmits to	sensor data	longitudinal		signal failure		is securely	technical			be wired and installed
controller	transmission	motion		(not proper		installed using	inspection will			according to
	to controller	1.00		gauge,		manufacturer	identify wiring			manufacturer
		ACC system		installation or		installation	fatigue or			specifications to
		shutdown		manufacturing failure)		specifications	failure			include bend radii, heat shielding, EMI
						Ensure wiring	Operator aware			avoidance, sheathing,
				Power failure		gauge is	during			proper gauge, and
						sufficient to	operation by			interface connections
				Communication		carry max	identifying			
				failure		operational	eventual failure			ACC system shall alert
						current with	of vehicle			operator prior to and
						factor of safety	components			when shutdown occurs
						Ensure wire				ACC system shall only
						bend radii are				be operational if sensor
						adhered to				performance meets a
										minimum standard
										(communication speed,
										sensor availability or
										visibility)

		Potential		Potential		Prevention	Detection			ACC communications shall operate independently and be free from external manipulation (malicious intrusion, EMI) Functional
Function	Failure Type	Impact	S	Cause	0	Mode	Mode	D	RPN 10	Requirement
Operator sets velocity constraint	Failure of operator to set velocity constraint	ACC system shutdown	1	Operator unaware of responsibility to set velocity constraint	10	Ensure system provides warning to operator that velocity input constraint is required	N/A	1	10	ACC system shall provide warning to operator that velocity input constraint is required ACC system shall operate within a specified velocity range
		Potential	G	Potential		Prevention	Detection	Б	DDN	Functional
Function Operator sets separation distance constraint	Failure Type Failure of operator to set separation distance constraint operator to set	Impact ACC system shutdown	S 1	Cause Operator unaware of responsibility to set distance constraint	O 10	Mode Ensure system provides warning to operator that distance input constraint is required	Mode N/A	D	RPN 10	RequirementACC system shallprovide warning tooperator that distanceinput constraint isrequiredThe ACC system shalloperate within aspecified distancerange
Function	Failure Type	Potential Impact	s	Potential Cause	0	Prevention Mode	Detection Mode	D	RPN	Functional Requirement
ACC provides feedback to the	Failure for ACC to	Unintended longitudinal	9	Wiring and/or signal failure (not proper	6	Ensure wiring is securely installed using	Vehicle technical inspection will	1	54	The ACC sensors shall be wired and installed according to

hapti	ic, visual,		manufacturing		fatigue or	shielding, EMI
audio	0)	Operator	failure)	Ensure wiring	failure	avoidance, sheathing,
		unaware of		gauge is		proper gauge, and
		potential	Power failure	sufficient to	Operator aware	interface connections
		hazard		carry max	during	
			Communication	operational	operation by	ACC system shall alert
			failure	current with	identifying	operator prior to and
				factor of safety	eventual failure	when shutdown occurs
			Audio or visual		of vehicle	
			system failure	Ensure wire	functions	ACC system shall alert
			2	bend radii are		operator when
				adhered to		deviation from set
						distance or velocity
				Ensure ACC		occurs
				alters operator		
				when deviation		ACC feedback system
				from set		shall function
				distance or		according to operator
				velocity occurs		engagement
				5		00
				Ensure ACC		ACC system shall
				system alerts		provide audio, visual,
				operator prior		and haptic feedback
				to and when		1
				shutdown		ACC system shall
				occurs		provide feedback in
						manner that does not
				Ensure ACC		startle the operator and
				system provides		cause greater potential
				audio, visual,		for hazard (not overly
				and haptic		loud or bright)
				feedback		
						ACC system audio
				Ensure ACC		feedback shall adjust to
				system provides		ambient volume (stereo
				feedback in		system, excessive
				manner that		cabin noise)
				does not startle		,
				the operator and		ACC system visual
				cause greater		feedback shall adjust to

potential for hazard (not overly loud or bright)Ensure ACC system audio and visual feedback adjust to ambient volume and light	ambient light (decrease during night, increase during day) ACC system shall only be operational if feedback performance meets a minimum standard (communication speed, audio, visual, haptic functionality)
	ACC communications shall operate independently and be free from external manipulation (malicious intrusion, EMI)

Appendix 3.02 HARA CAVs / CSMS LKA DFMEA

CAVs / CSMS LKA DFMEA										
Item: Lane Keeping Assist										
		Potential				Prevention				Functional
Function	Failure Type	Impact	S	Potential Cause	0	Mode	Detection Mode	D	RPN	Requirement
Controls lateral	Failure to	Unintended	10	Wiring and/or	7	Ensure wiring is	Vehicle technical	8	560	The LKA system
movement via	control lateral	lateral motion		signal failure (not		securely installed	inspection will			shall be wired and
EBCM	movement			proper gauge,		using	identify wiring			installed according to
	via brakes	Operator		installation or		manufacturer	fatigue or failure			manufacturer
		and/or		manufacturing		installation	•			specifications to
		passenger		failure)		specifications	Operator aware			include bend radii,
		injury				-	during operation			heat shielding, EMI

Damage to or loss of property			Ensure wire bend radii are adhered to	by identifying eventual failure of vehicle components			avoidance, sheathing, proper gauge, and interface connections
Damage to environment	Brake pad fatigue or failure (overheating, corrosion)	5	Ensure proper mounting and installation of pads Ensure bolts and mounting hardware is securely fastened and free from potential loosening or movement Avoid adverse road conditions Routine maintenance and	Vehicle technical inspection will identify if the pads are free from fatigue or corrosion Operator aware during operation by identifying unsettling smell, and vehicle vibration	3	150	LKA brake system shall engage in timely manner such that brake pad fatigue and passenger discomfort is minimized Development teams shall ensure proper mounting and installation of brake pads Development teams shall ensure brake pad bolts and mounting hardware are securely fastened
			inspection for rust and corrosion				and free from potential loosening or movement
			Avoid poor driving behaviors				Operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH
							Operator shall avoid poor driving behaviors
	Brake rotor fatigue or failure	4	Ensure proper mounting and	Vehicle technical inspection will	3	120	LKA brake system shall engage in

(overheating, corrosion)		installation of rotors Ensure bolts and mounting hardware are securely fastened and free from potential loosening or movement Avoid adverse road conditions Routine maintenance and inspection for rust and corrosion Avoid poor drive behavior	identify if the rotors are free from fatigue or corrosion Operator aware during operation by identifying unsettling smell, and vehicle vibration			timely manner such that brake rotor fatigue and passenger discomfort is minimized Development teams shall ensure proper mounting and installation of brake rotors Development teams shall ensure brake rotor bolts and mounting hardware are securely fastened and free from potential loosening or movement Operator shall avoid excessively adverse road conditions
						road conditions (bumpy terrain, excessive grade) which may cause a high NVH Operator shall avoid poor driving behaviors
Debris (snow, mud) build-up on brake system	3	Ensure brake system is free of build-up and debris prior to use	Vehicle technical inspection will identify if the brake system is free from build- up	6	180	Operator shall ensure brake system is free of build-up (snow, mud) and debris prior to use

Adverse road conditions (bumpy terrain, excessive grade)	2	Avoid adverse road condition which may produce NVH and damage suspension	Operator aware during operation by identifying vehicle NVH Operator aware prior to or during operation. Increased NVH	4	80	Operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH
Calipers get stuck	2	Avoid adverse road conditions Routine maintenance and inspection for rust and corrosion Avoid poor drive behavior	Operator aware during operation by identifying unsettling smell, vehicle vibration, and partial or total loss of functionality	6	120	Operator shall avoid excessively adverse road conditions which may cause a high NVH Operator shall ensure routine inspection for caliper rust and corrosion Operator shall avoid poor driving behaviors
Brake fluid line failure (leak, air in line)	2	Ensure proper bleeding, mounting, installation, and routine maintenance and inspection of hardware and its functionality Ensure bolts and mounting hardware is securely fastened	Operator aware during operation by identification of degrading performance Vehicle technical inspection will identify leaks	5	100	LKA brake system shall engage in timely manner such that brake lines are immediately able to actuated Development team shall ensure proper bleeding, mounting, installation, and routine maintenance and inspection of

					and free from potential loosening or unintended movement				brake line hardware and its functionality Development team shall ensure bolts and mounting hardware are securely fastened and free from potential loosening or unintended movement
			Other						LKA system shall allow operator to override automated controls with minimal braking engagement LKA system shall brake the front wheel opposite to the side of deviation
Failure Type	Potential	S	Detential Cause	0	Prevention Mode	Detection Mode	n	DDN	Functional Requirement
Failure Type Failure to control lateral movement via electrical power steering	Unintended lateral motion Operator and/or passenger injury Damage to or loss of property Damage to environment	10	Contamination of power steering fluid (old, air)	1	Ensure proper mounting, installation, and manufacturing of hoses, clamps, and their components Ensure interface components	Operator aware during operation by identifying a loss in steering functionality Vehicle technical inspection will identify a lack of, or	3	<u>30</u>	Development team shall ensure proper mounting, installation, and manufacturing of EPS hoses, clamps, and their components Development team shall ensure interface components
	control lateral movement via electrical power	Failure TypeImpactFailure toUnintendedcontrol laterallateral motionmovementOperatorvia electricalOperatorpowerand/orsteeringpassengerinjuryDamage to orloss ofpropertyDamage toDamage to	Failure TypeImpactSFailure toUnintended10control laterallateral motionmovementOperatorvia electricalOperatorpowerand/orsteeringpassengerinjuryDamage to orloss ofpropertyDamage toDamage to	Failure TypePotential ImpactSPotential CauseFailure to control lateral movement via electrical power steering10Contamination of power steering fluid (old, air)power steeringOperator passenger injury10Contamination of power steering fluid (old, air)Damage to or loss of propertyLLLDamage to Damage toLLLDamage to Damage toLLLDamage toLLLD	Failure TypePotential ImpactSPotential CauseOFailure to control lateral movement via electrical power steering10Contamination of power steering fluid (old, air)1Damage to or loss of propertyDamage to or loss of propertyIIDamage toIIIDamage toIII <t< td=""><td>Failure TypePotential hand movementpotential lossening or unintended movementFailure TypePotential ImpactOtherIFailure TypeImpactSPotential CauseOFailure TypeUnintended interded ocorrol lateral movement10 of power steeringContamination of power steering fluid (old, air)1Ensure proper mounting, installation, and/or propertyDamage to or loss of propertyDamage to or loss of propertyIIEnsure interface</td><td>Failure to control lateral movementPotential hosening or unintended movementpotential lossing or unintended movementFailure to control lateral movementOtherIPrevention HomePrevention ModeFailure to control lateral movement via electricial power steeringUnintended to injury10Contamination of power steering fluid (old, air)1Prevention ModeDetection ModeFailure to control lateral movement via electricial power steering10Contamination of power steering fluid (old, air)1Ensure proper manufacturing installation, operation by identifying a manufacturing iof hoses, of hoses, steeringDamage to or loss of property1Ensure injuryIoss in steering fluid (old, air)Ios in steering fluid identifying a manufacturing iof hoses, of hoses, steering fluid their infunctionality their infunctionality their infunctionality their infunctionality instellation, openation by infunctionality infunctionality their infunctionality in</td><td>Failure TypePotential Law indexApotential Lossening or unintended movementJpotential Lossening or unintended movementJFailure TypeImpactSPotential CauseOPreventionJJFailure to control lateral movementUnintended attract of power steering10Contamination of power steering fluid (old, air)DPreventionDDDamage to environment10Contamination of power steering fluid (old, air)1Ensure mounting, aware during operation by attract installation, operation by and/or steering fluid (old, air)1Ensure mounting, installation, operation by and identifying a loss in steering0Damage to environment15Finance inspection will installation, inspection will inspection will inspection will inspection will installation, inspection will1</td><td>Failure TypePotential ImpactSPotential causeOPreventionImpactImpactSFailure TypeImpactSPotential CauseOModeDetection ModeDRPNFailure TypeImpactSPotential CauseOModeDetection ModeDRPNFailure TypeUnintended lateral motion rownent10Contarmination of power steering fluid (old, air)1Ensure proper mounting, installation, and of boses, clamps, and functionality their components330Damage to environmentDamage to environmentImpactImpactImpactImpactImpactImpactDamage to environmentImpactImpactImpactImpactImpactImpactImpactImpactImpactDamage to environmentImpactImpactImpactImpactImpactImpactImpactImpactImpactDamage to environmentImpactImpactImpactImpactImpactImpactImpactImpactImpactImpactDamage to environmentImpactImpactImpactImpactImpactImpactImpactImpactImpactImpactImpactDamage to environmentImpactImpactImpactImpactImpactImpactImpactImpactImpactDamage to environmentImpactImpactImpactImpactImpactImpactImpactImpact</td></t<>	Failure TypePotential hand movementpotential lossening or unintended movementFailure TypePotential ImpactOtherIFailure TypeImpactSPotential CauseOFailure TypeUnintended interded ocorrol lateral movement10 of power steeringContamination of power steering fluid (old, air)1Ensure proper mounting, installation, and/or propertyDamage to or loss of propertyDamage to or loss of propertyIIEnsure interface	Failure to control lateral movementPotential hosening or unintended movementpotential lossing or unintended movementFailure to control lateral movementOtherIPrevention HomePrevention ModeFailure to control lateral movement via electricial power steeringUnintended to injury10Contamination of power steering fluid (old, air)1Prevention ModeDetection ModeFailure to control lateral movement via electricial power steering10Contamination of power steering fluid (old, air)1Ensure proper manufacturing installation, operation by identifying a manufacturing iof hoses, of hoses, steeringDamage to or loss of property1Ensure injuryIoss in steering fluid (old, air)Ios in steering fluid identifying a manufacturing iof hoses, of hoses, steering fluid their infunctionality their infunctionality their infunctionality their infunctionality instellation, openation by infunctionality infunctionality their infunctionality in	Failure TypePotential Law indexApotential Lossening or unintended movementJpotential Lossening or unintended movementJFailure TypeImpactSPotential CauseOPreventionJJFailure to control lateral movementUnintended attract of power steering10Contamination of power steering fluid (old, air)DPreventionDDDamage to environment10Contamination of power steering fluid (old, air)1Ensure mounting, aware during operation by attract installation, operation by and/or steering fluid (old, air)1Ensure mounting, installation, operation by and identifying a loss in steering0Damage to environment15Finance inspection will installation, inspection will inspection will inspection will inspection will installation, inspection will1	Failure TypePotential ImpactSPotential causeOPreventionImpactImpactSFailure TypeImpactSPotential CauseOModeDetection ModeDRPNFailure TypeImpactSPotential CauseOModeDetection ModeDRPNFailure TypeUnintended lateral motion rownent10Contarmination of power steering fluid (old, air)1Ensure proper mounting, installation, and of boses, clamps, and functionality their components330Damage to environmentDamage to environmentImpactImpactImpactImpactImpactImpactDamage to environmentImpactImpactImpactImpactImpactImpactImpactImpactImpactDamage to environmentImpactImpactImpactImpactImpactImpactImpactImpactImpactDamage to environmentImpactImpactImpactImpactImpactImpactImpactImpactImpactImpactDamage to environmentImpactImpactImpactImpactImpactImpactImpactImpactImpactImpactImpactDamage to environmentImpactImpactImpactImpactImpactImpactImpactImpactImpactDamage to environmentImpactImpactImpactImpactImpactImpactImpactImpact

Power steering low fluid and fluid	2	(seals, gaskets), and mounting hardware are securely fastened and free from potential loosening or movement Ensure functionality of pump and check for hose deterioration Ensure proper mounting, installation,	discolored steering fluid Increased friction and interference with hydraulic characteristics.	3	60	(seals, gaskets), and mounting hardware are securely fastened and free from potential loosening or movement Development team shall ensure functionality of EPS pump and check for hose deterioration Development team shall ensure proper mounting,
leaks		and manufacturing of hoses, clamps, and their components Ensure interface components (seals, gaskets), and mounting hardware are	identify low fluid level, and leaks Operator aware during operation by identifying a loss in steering functionality			installation, and manufacturing of EPS hoses, clamps, and their components Development team shall ensure interface components (seals, gaskets), and mounting hardware are securely fastened

	Broken belt which energizes power steering pump	3	securely fastened and free from potential loosening or movement Ensure the correct type of fluid is used, proper fluid levels, and check for leaks prior to operation Ensure proper mounting, installation, and manufacturing of the belt (tension, torque specs) and its components Ensure bolts, interface components,	Vehicle technical inspection will identify belt functionality Operator aware during operation by identifying a loss in steering functionality	5	150	and free from potential loosening or movement Development team shall ensure the correct type of fluid is used, proper fluid levels, and check for leaks prior to operation Development team shall ensure proper mounting, installation, and manufacturing of the belt (tension, torque specs) and its components The development teams hall ensure bolts, interface components, and mounting
			interface	e			components, and

Pump failure	2	free from potential loosening or unintended movement Ensure proper mounting, installation, and manufacturing of pump and its components Ensure bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from potential loosening or	Vehicle technical inspection will identify pump functionality Operator aware during operation by identifying a loss in steering functionality and audible increase in pump noise	5	100	loosening or unintended movement Development team shall ensure proper mounting, installation, and manufacturing of pump and its components components team shall ensure bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from potential loosening or movement
Electronic power steering failure	2	movement Ensure proper mounting, installation,	Operator aware during operation by	8	160	Development team shall ensure proper mounting,
Tanuie		and manufacturing of power	identifying a loss in			installation, and manufacturing of power steering

	steering system and its componentssteering functionality	system and its components Development
	Ensure bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from potential	team shall ensure bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from potential loosening or movement
	loosening or movement Ensure operator drives appropriately to prevent damage to steering rack Ensure power steering motor is functional	Operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH Development team shall ensure power steering motor is functional
Wiring and/or signal failure (not proper gauge, installation or	7 Ensure wiring is securely installed using manufacturer Vehicle technical sinspection will identify wiring fatigue or failure 8	560 The LKA system shall be wired and installed according to manufacturer specifications to

[<u> </u>	1			1		
				manufacturing		installation	Operator aware			include bend radii,
				failure)		specifications	during operation			heat shielding, EMI
							by identifying			avoidance, sheathing,
						Ensure wire bend	eventual failure			proper gauge, and
						radii are adhered	of vehicle			interface connections
						to	components			
				Other						LKA system shall
										function according to
										operator engagement
										1 00
										LKA system shall
										respond (feedback,
										lateral movement)
										more quickly in the
										event of less operator
										engagement (hands
										on wheel, head tilt,
										eye deviation)
										cyc ucviation)
										LKA system shall
										respond (feedback,
										lateral movement)
										less quickly in the
										event of more
										operator engagement
										(hands on wheel,
										head tilt, eye
										deviation)
										LKA system shall
										allow operator to
										override automated
										controls with
										minimal steering
										engagement
		Potential				Prevention				Functional
Function	Failure Type	Impact	S	Potential Cause	0	Mode	Detection Mode	D	RPN	Requirement
Performs lane-	Failure to		6	Wiring and/or	7	Ensure wiring is	Vehicle technical	8	336	The LKA sensors
line, object	performs			signal failure (not		securely installed	inspection will			shall be wired and
detection and	lane-line,			proper gauge,		using				installed according to

multi-feature tracking	object detection and multi-feature tracking	Unintended lateral motion LKA system shutdown	installation or manufacturing failure) Power failure Communication failure		manufacturer installation specifications Ensure wiring gauge is sufficient to carry max operational current with factor of safety Ensure wire bend radii are adhered to	identify wiring fatigue or failure Operator aware during operation by identifying eventual failure of vehicle components			manufacturer specifications to include bend radii, heat shielding, EMI avoidance, sheathing, proper gauge, and interface connections LKA system shall alert operator prior to and when shutdown occurs LKA system shall only be operational if sensor performance meets a minimum standard (communication speed, sensor availability or visibility) LKA communications shall operate independently and be free from external
			Unintended access and physical damage (debris, puncture)	6	Ensure sensor enclosure manufacturing and use of materials is sufficient to prevent unintended access and	Vehicle technical inspection will identify if sensors are free of physical damage	4	144	manipulation Development team shall ensure sensor enclosure manufacturing and use of materials is sufficient to prevent unintended

			physical damage Ensure bolts and mounting hardware is securely fastened and free from potential loosening or unintended movement	Operator aware during operation by identifying functionality failure			access and physical damage Development team shall ensure sensor and sensor enclosure bolts and mounting hardware are securely fastened and free from potential loosening or unintended movement
	Sensor visibility obstruction	7	Ensure sensors have clear field of view and are free of visibility obstruction	Vehicle technical inspection will identify if sensors are free of obstruction Operator aware during operation by identifying functionality failure	3	126	Operator shall ensure LKA system sensors have clear field of view and are free of visibility obstructions LKA system shall only be operational if sensor performance meets a minimum standard (communication speed, sensor availability or visibility) LKA system shall have control wind shield wipers

							LKA system shall have control of front lights
	Minimum operational speed	10	ACC sensors require a minimum vehicle speed to be operational	Operator aware during operation by identifying vehicle speed	1	60	LKA system shall require minimum vehicle speed based on sensor requirements and lane-line visibility
	Other						LKA system shall function according to operator engagement LKA system shall
							respond (feedback, acceleration, deceleration) more quickly in the event of less operator engagement (hands on wheel, head tilt, eye deviation)
							LKA system shall respond (feedback, acceleration, deceleration) less quickly in the event of more operator engagement (hands on wheel, head tilt, eye deviation)
							Development team shall impose criteria for deviation and corrective action

Function LKA sensors transmit data to associated controller	Failure Type Failure of LKA sensors transmit data to associated controller	Potential Impact Unintended lateral motion LKA system shutdown	<u>s</u> 6	Potential Cause Wiring and/or signal failure (not proper gauge, installation or manufacturing failure) Power failure Communication failure	<u>0</u> 5	Prevention Mode Ensure wiring is securely installed using manufacturer installation specifications Ensure wiring gauge is sufficient to carry max operational current with factor of safety Ensure wire bend radii are adhered to	Detection Mode Vehicle technical inspection will identify wiring fatigue or failure Operator aware during operation by identifying eventual failure of vehicle components	D 4	<u>RPN</u> 120	Development team shall impose criteria for deviation and corrective action Functional Requirement The LKA sensors shall be wired and installed according to manufacturer specifications to include bend radii, heat shielding, EMI avoidance, sheathing, proper gauge, and interface connections LKA system shall alert operator prior to and when shutdown occurs LKA system shall only be operational if sensor performance meets a minimum
										only be operational if
Function	Failure Type	Potential Impact	s	Potential Cause	0	Prevention Mode	Detection Mode	D	RPN	Functional Requirement

Operator initiates the LKA system	Failure of operator to set the LKA system	LKA system shutdown	1	Operator unaware of responsibility to initiate the LKA system	10	Ensure system provides warning to operator that LKA requires manual initiation		1	10	LKA system shall provide warning to operator that manual initiation is required LKA system shall operate within a specified velocity range Turn-indicator actuation shall be required for free movement out of lane, otherwise feedback will warn
		Potential				Prevention				operator Functional
Function	Failure Type	Impact	S	Potential Cause	0	Mode	Detection Mode	D	RPN	Requirement
LKA system provides feedback to the operator (LKA status, haptic, visual, audio)	Failure of LKA system to provide feedback to the operator (LKA status, haptic, visual, audio)	Unintended lateral motion LKA system shutdown Operator unaware of potential hazard	8	Viring and/or signal failure (not proper gauge, installation or manufacturing failure)Power failureCommunication failureAudio or visual system failure	5	Ensure wiring is securely installed using manufacturer installation specifications Ensure wiring gauge is sufficient to carry max operational current with factor of safety Ensure wire bend radii are adhered to Ensure LKA alerts operator	Vehicle technical inspection will identify wiring, audio, or visual fatigue or failure Operator aware during operation by identifying eventual failure of vehicle functions	3	120	The LKA sensors shall be wired and installed according to manufacturer specifications to include bend radii, heat shielding, EMI avoidance, sheathing, proper gauge, and interface connections LKA system shall alert operator prior to and when shutdown occurs LKA system shall alert operator when deviation occurs

	when deviation	LKA feedback
	from set distance	system shall function
	or velocity	according to operator
	occurs	engagement
	Ensure LKA	LKA system shall
	system alerts	provide audio, visual,
	operator prior to	and haptic feedback
	and when	
	shutdown occurs	LKA system shall
		provide feedback in
	Ensure LKA	manner that does not
	system provides	startle the operator
	audio, visual,	and cause greater
	and haptic	potential for hazard
	feedback	(not overly loud or
		bright)
	Ensure LKA	
	system provides	LKA system audio
	feedback in	feedback shall adjust
	manner that does	to ambient volume
	not startle the	(stereo system,
	operator and	excessive cabin
	cause greater	noise)
	potential for	
	hazard (not	LKA system visual
	overly loud or	feedback shall adjust
	bright)	to ambient light
		(decrease during
	Ensure LKA	night, increase
	system audio and	during day)
	visual feedback	
	adjust to ambient	LKA system shall
	volume and light	only be operational if
		feedback
		performance meets a
		minimum standard
		(communication
		speed, audio, visual,
		haptic functionality)

						LKA communications shall operate independently and be free from external manipulation (malicious intrusion, EMI)
--	--	--	--	--	--	---

Appendix 3.03 HARA CAVs / CSMS LKA STPA

			CAVs / CSMS	S LKA STPA	
Control Function	Unsafe Control Action	Potential Hazard	Causal Factors	Prevention/Mitigation	Functional Requirement
Operator initiates LKA system	Required but not provided	LKA system remains disabled	Operator unaware that LKA system initiation is required Operator aware that LKA system initiation is required	When the speed and operational environment allow, the LKA system will alert the operator that the LKA system requires operator initiation When the speed and operational environment allow, the LKA	When the speed and operational environment allow, the LKA system shall alert the operator that the LKA system requires operator initiation When the speed and operational environment allow, the LKA
			but unaware of how to initiate Wiring failure	initiation procedure will be clearly defined to the operator via audio and visual alert with minimal required actions by the operator (single button	initiation procedure shall be clearly defined to the operator via audio and visual alert with minimal required actions by the operator
			Operating system failure	 initiation) Wiring will be installed according to manufacturer specifications to include EMI avoidance, gauge, and bend radii If LKA operating system fails, the LKA system will alert the operator via audio and visual feedback 	(single button initiation) Wiring shall be securely installed according to manufacturer specifications to include EMI avoidance, connections, gauge, and bend radii

Provided but not required	LKA System remains disabled	LKA system requires a minimum speed, reasonable lane-line tracking, and object detection to enable Operator has previously initiated the LKA system	When the speed and operational environment allow, the LKA system will alert the operator that the LKA system requires operator initiation When the speed and operational environment allow, the LKA initiation procedure will be clearly defined to the operator via audio and visual alert with minimal required actions by the operator (single button initiation)	If LKA operating system fails, the LKA system shall alert the operator via audio and visual feedback When the speed and operational environment allow, the LKA system shall alert the operator that the LKA system requires operator initiation When the speed and operational environment allow, the LKA initiation procedure shall be clearly defined to the operator via audio and visual alert with minimal required actions by the operator (single button initiation)
			To prevent accidental disabling of the LKA system, the LKA system will have individual on/off buttons	To prevent accidental disabling of the LKA system, the LKA system shall have individual on/off buttons
Provided but incorrect timing	Operator believes the LKA system is enabled when it is not	Signal corruption Operating system failure Operator initiates the LKA system when desired	Ensure LKA system signal transfers through appropriate medium (type, gauge of wiring) and adheres to automotive wiring standards (twisted wires, EMI avoidance, shielding) Ensure the LKA system limits time of actuating once the operator initiates LKA system (ex. close loop after 500ms) Ensure LKA system alters operator once LKA system has been enabled The operator will be allowed to choose when LKA system will be enabled	The development team shall ensure the LKA system signal transfers through an appropriate medium (type, gauge of wiring) and adheres to automotive wiring standards (twisted wires, EMI avoidance, shielding) The development team shall ensure the LKA system limits time of actuation once the operator initiates LKA system (ex. close loop after 500ms) The development team shall ensure the LKA system alerts the operator once the LKA system has been enabled

	Provided but incorrect duration	LKA system becomes disabled	Operator holds LKA system initiation button too long	Ensure that if the LKA system "on" button is actuated, the LKA system enables, regardless of time pressed Ensure the LKA system "on" button is of the a reasonable quality to reduce bounce error	The operator shall be allowed to choose when LKA system will be enabled The development team shall ensure that if the LKA system "on" button is actuated, the LKA system enables, regardless of pressed time duration The development team shall ensure the LKA system "on" button is of the a reasonable quality to reduce bounce error
Control Function	Unsafe Control Action	Potential Hazard	Causal Factors	Prevention/Mitigation	Functional Requirement
Performs lane-line, object detection and multi-feature tracking	Required but not provided	LKA system is disabled LKA system operates on poor sensor data	Sensor visibility failure (obstruction, poor lane-line quality) Power failure Wiring failure Signal corruption Operating system failure	Ensure the LKA system sensors are placed in a location which minimizes potential visibility failures Ensure LKA system radars and cameras are of the quality which can produce true data during reasonably poor operational conditions (rain, fog, snow, dirt, poor lane-line quality) Ensure LKA system radars and cameras are mounted in location free from visibility obstruction Ensure the LKA system wiring will be installed according to manufacturer specifications to include EMI avoidance, gauge, and bend radii If LKA operating system fails, the LKA system will alert the operator via audio and visual feedback	The development team shall ensure the LKA system sensors are placed in a location which minimizes potential visibility failures The development team shall ensure LKA system radars and cameras are of the quality which can produce true data during reasonably poor operational conditions (rain, fog, snow, dirt, poor lane-line quality) The development team shall ensure LKA system radars and cameras are mounted in location free from visibility obstruction The development team shall ensure the LKA system wiring will be installed according to manufacturer specifications to include EMI avoidance, gauge, and bend radii

Provided but not required	There no LKA system operational state which does not require lane-line, object detection and multi-feature tracking	Computational overload	Ensure the LKA system is capable of processing the required amount of data	If LKA operating system fails, the LKA system shall alert the operator via audio and visual feedback The development team shall ensure the LKA system is capable of processing the required amount of data
Provided but incorrect timing	Unintended lateral movement Vehicle continues lane deviation Operator, passenger, or property damage and injury	Wiring failure Signal corruption Operating system failure	 Wiring will be installed according to manufacturer specifications to include EMI avoidance, gauge, and bend radii Ensure the LKA system signal transfers through appropriate medium (type, gauge of wiring) and adheres to automotive wiring standards (twisted wires, EMI avoidance, shielding) If the LKA operating system fails, the LKA system will alert the operator via audio and visual feedback The computer will be aware of signal latency and the LKA program will actuate a control action accordingly 	LKA system wiring shall be installed according to manufacturer specifications to include EMI avoidance, gauge, and bend radii The development team shall ensure the LKA system signal transfers through appropriate medium (type, gauge of wiring) and adheres to automotive wiring standards (twisted wires, EMI avoidance, shielding) If the LKA operating system fails, the LKA system shall alert the operator via audio and visual feedback The computer shall be aware of signal latency and the LKA program will actuate a control action accordingly
Provided but incorrect duration (sensor signal stops mid corrective control action)	Unintended lateral movement Vehicle continues lane deviation	Wiring failure Signal corruption Operating system failure	If sensor signal stops in during a corrective control action the LKA system will immediately disable and alert operator via visual, audio, and haptic feedback	If sensor signal stops in during a corrective control action the LKA system shall immediately disable and alert operator via visual, audio, and haptic feedback

		Operator, passenger, or property damage and injury		 Wiring will be installed according to manufacturer specifications to include EMI avoidance, gauge, and bend radii Ensure the LKA system signal transfers through appropriate medium (type, gauge of wiring) and adheres to automotive wiring standards (twisted wires, EMI avoidance, shielding) 	The development team shall ensure the LKA system wiring will be installed according to manufacturer specifications to include EMI avoidance, gauge, and bend radii The development team shall ensure the LKA system signal transfers through appropriate medium (type, gauge of wiring) and adheres to automotive wiring standards (twisted wires, EMI avoidance, shielding)
Control	Unsafe Control				
Function Sensors send	Action Required but not	Potential Hazard LKA system is	Causal Factors Wiring failure	Prevention/Mitigation If the LKA operating system fails,	Functional Requirement If the LKA operating system fails,
data to	provided	disabled	winng fanure	the LKA system will alert the	the LKA system shall alert the
associated	F		Signal corruption	operator via audio and visual	operator via audio and visual
computer			Power failure	feedback	feedback
				 Wiring will be installed according to manufacturer specifications to include EMI avoidance, gauge, and bend radii Ensure the LKA system signal transfers through appropriate medium (type, gauge of wiring) and adheres to automotive wiring standards (twisted wires, EMI avoidance, shielding) 	The development team shall ensure the LKA system wiring will be installed according to manufacturer specifications to include EMI avoidance, gauge, and bend radii The development team shall ensure the LKA system signal transfers through appropriate medium (type, gauge of wiring) and adheres to automotive wiring standards (twisted wires, EMI avoidance,
	Provided but not	LKA system	Operator believes	The LKA system will have constant	shielding) The LKA system shall have
	required	enabled when operator believes it is disabled	the LKA system is disabled when it is enabled	enabled/disabled form of feedback (light) indicated to the operator	constant enabled/disabled form of feedback (light) indicated to the operator
		Unintended lateral movement			

Provided but incorrect timing	LKA system engages in correct control actions to the operators surprise Unintended (late, early) lateral movement	Wiring failure Signal corruption	If the LKA operating system fails, the LKA system will alert the operator via audio and visual feedback Wiring will be installed according to manufacturer specifications to include EMI avoidance, gauge, and bend radii Ensure the LKA system signal transfers through appropriate medium (type, gauge of wiring) and adheres to automotive wiring standards (twisted wires, EMI avoidance, shielding)	If the LKA operating system fails, the LKA system shall alert the operator via audio and visual feedback The development team shall ensure the LKA system wiring will be installed according to manufacturer specifications to include EMI avoidance, gauge, and bend radii The development team shall ensure the LKA system signal transfers through appropriate medium (type, gauge of wiring) and adheres to automotive wiring standards (twisted wires, EMI avoidance, shielding) The computer shall be aware of signal latency and the LKA program will actuate a control action accordingly
Provided but incorrect duration	Sensor signal stops mid corrective control action Unintended lateral movement Vehicle continues lane deviation	Wiring failure Signal corruption Sensor visibility failure (obstruction, poor lane-line quality)	If the LKA operating system fails, the LKA system will alert the operator via audio and visual feedback Wiring will be installed according to manufacturer specifications to include EMI avoidance, gauge, and bend radii	If the LKA operating system fails, the LKA system shall alert the operator via audio and visual feedback The development team shall ensure the LKA system wiring will be installed according to manufacturer specifications to include EMI avoidance, gauge, and bend radii

		Operator, passenger, or property damage and injury		Ensure the LKA system signal transfers through appropriate medium (type, gauge of wiring) and adheres to automotive wiring standards (twisted wires, EMI avoidance, shielding)	The development team shall ensure the LKA system signal transfers through appropriate medium (type, gauge of wiring) and adheres to automotive wiring standards (twisted wires, EMI avoidance, shielding)
				Ensure the LKA system sensors are placed in a location which minimizes potential visibility failures Ensure LKA system radars and cameras are of the quality which can produce true data during reasonably poor operational conditions (rain, fog, snow, dirt, poor lane-line quality)	The computer shall be aware of signal latency and the LKA program will actuate a control action accordingly The development team shall ensure the LKA system sensors are placed in a location which minimizes potential visibility failures
				Ensure LKA system radars and cameras are mounted in location free from visibility obstruction	The development team shall ensure LKA system radars and cameras are of the quality which can produce true data during reasonably poor operational conditions (rain, fog, snow, dirt, poor lane-line quality)
Control Function	Unsafe Control Action	Potential Hazard	Causal Factors	Prevention/Mitigation	The development team shall ensure LKA system radars and cameras are mounted in location free from visibility obstruction Functional Requirement

Computer	Required but not	LKA system stays	Algorithm, NN,	Ensure wiring is securely installed	To avoid wiring failure of the intel
performs	provided	or becomes	computational, or	using manufacturer installation	tank computer the development
sensor fusion	1	disabled	cyber-security	specifications	team shall ensure wiring is securely
data	Provided but	albuolea	failure	specifications	installed using manufacturer
verification &	incorrect timing	Unintended lateral	Turfure	Ensure wiring gauge is sufficient to	installation specifications
validation	medirect unning		Power failure	carry max operational current with	instantion specifications
	D., 1.11.4	movement	rower failure		The second states for the second
using	Provided but		XX 1 1	factor of safety	To avoid wiring failure of the intel
developed	incorrect		Unintended access	Ensure wire bend radii are adhered to	tank computer the development
algorithms	duration		or physical damage		team shall ensure wiring gauge is
and NNs			(liquid, puncture)	Ensure computer alerts operator that	sufficient to carry max operational
				corrective action decisions are	current with factor of safety
			Wiring failure (not	disabled stating "LKA and ACC	
			proper gauge,	systems disabled" "No corrective	To avoid wiring failure of the intel
			installation or	action will be made"	tank computer the development
			manufacturing		team shall ensure wire bend radii
			failure)	Determine fidelity of non-blended	are adhered to
			,	image and decide if corrective action	
			Memory failure	should be applied	The development team shall ensure
					the computer alerts operator that
			Over-heating	Ensure computer only makes	corrective action decision is
			over heating	corrective action decisions when	disabled
			On anoting system	fidelity of image meets minimum	uisableu
			Operating system crash		The development teem shell ensure
			crash	specified resolution	The development team shall ensure
					the computer determines fidelity of
				Ensure if computer system fails, it	non-blended image and decide if
				does not prevent vehicle from manual	corrective action should be applied
				driving operations	
					The development team shall ensure
				Ensure manufacturing and	the computer only makes corrective
				installation is sufficient to prevent	action decisions when fidelity of
				unintended access and physical	image meets minimum specified
				damage	resolution
				Ensure use of covering at wire-	The development team shall ensure
				computer interface to prevent	if computer system fails, it does not
				unintended access	prevent vehicle from manual
				Avoid adverse road condition which	driving operations
					unving operations
				may produce NVH and damage	The development (
				computer	The development team shall ensure
					manufacturing and installation is

Ensure computer installation is inside	sufficient to prevent unintended
cabin in a dry debris-proof location	access and physical damage to the
	computer
Ensure computer is inaccessible by	
passengers	To prevent unintended access and
	physical damage to the development
See wiring and unintended access	team shall ensure use of coverings
requirements	at wire-computer interface to
*	prevent unintended access
Ensure the power supplied to the	1
computer is within manufacturer	To prevent physical damage to the
operational range	computer the operator shall avoid
Ensure computer NN model is	adverse road conditions which may
thoroughly defined and highly	produce NVH
sensitive to small variations in inputs	
sensiti e to sinuir vuriations in inputs	To prevent unintended access and
Ensure computer NN is thoroughly	physical damage the development
tested and validate prior to	team shall ensure computer
implementation	installation is inside cabin in a dry
Implementation	debris-proof location
Ensure computer NN imposes limits	debris-proof location
on output to not exceed boundaries	To prevent unintended access and
on output to not exceed boundaries	physical damage the development
Ensure computer NNs use of hidden	team shall ensure computer is
layers and neurons does not over-fit	inaccessible by passengers
training data and is sufficient to fit	maccessible by passengers
new and unseen data	To prevent power failure the
new and unseen data	development team shall ensure the
Ensura computar program codo is	power supplied to the computer is
Ensure computer program code is thoroughly vetted (Auto industry	within manufacturer operational
	1
standard is one defect per 1000	range
executable lines of code)	The development term shall see a
En la companya de la	The development team shall ensure
Ensure computer program is	the computer NN model is
developed using automotive coding	thoroughly defined and highly
standards	sensitive to small variations in
	inputs
Ensure use of multiple software	
scanning tools to identify	The development team shall ensure
vulnerability and error in computer	the computer NN is thoroughly

program code (industry uses Jarvis	tested and validate prior to
which analyses the binary executable	implementation
action and not the mistakes in the	
code)	The development team shall ensure
	the computer NN imposes limits on
Ensure control of computational	output to not exceed boundaries
overflow and compounding rounding	
errors	The development team shall ensure
	the computer NNs use of hidden
Ensure understanding of computer	layers and neurons does not over-fit
input and output signal quality, noise,	training data and is sufficient to fit
latency, and bandwidth accounting	new and unseen data
for measurement and control action	
error	The development team shall ensure
	the computer program code is
To reduce computer signal input and	thoroughly vetted (Auto industry
output latency, ensure use of high-	standard is one defect per 1000
quality transmission medium	executable lines of code)
quality transmission meaturn	
To prevent computer signal input and	The development team shall ensure
output bandwidth faults, ensure	the computer program is developed
transmission medium gauge is	using automotive coding standards
sufficient to handle expected	using automotive county standards
throughput (load) with factor of	The development team shall ensure
safety	the use of multiple software
salety	scanning tools to identify
Ensure understanding of time	vulnerability and error in computer
required to analyze and route	program code (industry uses Jarvis
computer signal data	which analyses the binary
computer signal data	
	executable action and not the
To reduce computer signal input and	mistakes in the code)
output noise ensure wires are as short	
as possible	The development team shall ensure
	the control of computational
To reduce computer signal input and	overflow and compounding
output noise ensure wires are kept	rounding errors
away from electrical machinery	
	The development team shall ensure
	the understanding of computer
	input and output signal quality,

r				
			To reduce computer signal input and	noise, latency, and bandwidth
			output noise it is recommended to	accounting for measurement and
			use twisted together wires	control action error
			To reduce internal computer signal	The development team shall reduce
			input and output noise ensure thermal	computer signal input and output
			effects on amplifiers are minimized	latency, ensure use of high-quality
			encets on unpriners are minimized	transmission medium
			To reduce computer signal input and	
			output noise, if possible, ensure	To prevent computer signal input
				To prevent computer signal input
			amplifier bandwidth matches input	and output bandwidth fault the
			signal bandwidth	development team shall ensure
				transmission medium gauge is
			To reduce computer signal input and	sufficient to handle expected
			output noise ensure use of proper	throughput (load) with factor of
			filtering techniques	safety
				-
			To reduce computer signal input and	The development team shall ensure
			output noise ensure use of wire	an understanding of time required to
			shielding and conduit	analyze and route computer signal
			sinclaing and conduct	data
			To reduce computer signal input and	uata
				To and the commentant signal in mut
			output noise ensure understanding of	To reduce computer signal input
			ground loops and impose proper	and output noise the development
			grounding practices	team shall ensure wires are as short
				as possible
			To ensure true data measurement test	
			the collection with the computer	To reduce computer signal input
			operating at the same temperature	and output noise the development
			that it will be operating at in real-	team shall ensure wires are kept
			world scenarios	away from electrical machinery
			Ensure understanding of potential	To reduce computer signal input
			computer signal input and output	and output noise it is recommended
			storage delays	to use twisted together wires
			Ensure the use of software safety and	To reduce internal computer signal
			that the system is free from external	input and output noise the
			unintended malicious control	development team shall ensure
L L		1		

1	
Ensure system software updates are	thermal effects on amplifiers are
performed over land-line and not	minimized
through the air	
C	To reduce computer signal input
Ensure computer is capable of storing	and output noise, if possible, the
and processing the expected amount	development team shall ensure the
of data with a factor of safety	amplifier bandwidth matches input
of data with a factor of safety	signal bandwidth
T	signal bandwidth
To prevent memory failure ensure	To an desce commenter signal in such
program is developed such that	To reduce computer signal input
information that is too large cannot	and output noise the development
be written into a memory buffer that	team shall ensure use of proper
is too small to contain it	filtering techniques
To prevent over-heating ensure	To reduce computer signal input
computer is mounted such that there	and output noise the development
is proper clearance and sufficient air	team shall ensure use of wire
flow to cool the computer	shielding and conduit
To prevent over-heating ensure	To reduce computer signal input
computer fans pull air from cool and	and output noise the development
dry source	team shall ensure understanding of
dry source	ground loops and impose proper
To prevent over-heating ensure	grounding practices
	grounding practices
computer imposes thermal self-	
regulation	To ensure true data measurement
	the development team shall test the
To prevent over-heating ensure	collection with the computer
computer operates within specified	operating at the same temperature
temperature range	that it will be operating at in real-
	world scenarios
To prevent operating system crash	
ensure system does not over heat	The development team shall ensure
	the understanding of potential
To prevent operating system crash	computer signal input and output
ensure computer is mounted such	storage delays
that there is proper clearance and	
sufficient air flow to cool the	
computer	The development team shall ensure
	the use of software safety and that
	the use of software safety and that

1	
To prevent operating system crash	the system is free from external
ensure computer fans pull air from	unintended malicious control
cool and dry source	
	To prevent computer memory
To prevent operating system crash	failure the development team shall
ensure computer imposes thermal	ensure the computer is capable of
self-regulation	storing and processing the expected
	amount of data with a factor of
To prevent operating system crash	safety
ensure computer operates within	
specified temperature range	To prevent computer memory
	failure ensure the program is
To prevent operating system crash	developed such that information
ensure program is developed such	that is too large cannot be written
that it does not attempt to access an	into a memory buffer that is too
incorrect memory address leading to	small to contain it
general protection fault	
	To prevent over-heating the
To prevent operating system crash	development team shall ensure the
ensure program is developed such	computer is mounted such that there
that the OS does not enter an infinite	is proper clearance and sufficient
loop	air flow to cool the computer
To prevent operating system crash	To prevent over-heating the
ensure program is developed such	development team shall ensure the
that information that is too large	computer fans pull air from cool
cannot be written into a memory	and dry source
buffer that is too small to contain it	
	To prevent over-heating the
To prevent operating system crash	development team shall ensure the
ensure program is developed such	computer imposes thermal self-
that deadlock is prevented (multiple	regulation
programs having control some	
resource another program needs)	To prevent over-heating the
	development team shall ensure the
To prevent operating system crash	computer operates within specified
ensure program performs shutdown	temperature range
operations	

		To prevent operating system crash the development team shall ensure the system does not over heat
		To prevent operating system crash the development team shall ensure the computer is mounted such that there is proper clearance and sufficient air flow to cool the computer
		To prevent operating system crash the development team shall ensure the computer fans pull air from cool and dry source
		To prevent operating system crash the development team shall ensure the computer imposes thermal self- regulation
		To prevent operating system crash the development team shall ensure the computer operates within specified temperature range
		To prevent operating system crash the development team shall ensure the program is developed such that it does not attempt to access an incorrect memory address leading to general protection fault
		To prevent operating system crash the development team shall ensure the program is developed such that the OS does not enter an infinite loop

required	enabled when operator believes it is disabled Unintended lateral movement LKA system engages in correct control actions to the operators surprise	the LKA system is disabled when it is enabled	enabled/disabled form of feedback (light) indicated to the operator	constant enabled/disabled form of feedback (light) indicated to the operator
Action	Potential Hazard	Causal Factors	Prevention/Mitigation	Functional Requirement
Required but not provided Provided but not required	Unintended lateral movement Vehicle continues lane deviation	Operator believes the LKA system is enabled when it is disabled	The LKA system will have constant enabled/disabled form of feedback (light) indicated to the operator Ensure wiring is securely installed	The LKA system shall have constant enabled/disabled form of feedback (light) indicated to the operator To avoid wiring failure of the intel
]	Required but not provided Provided but not	it is disabledit is disabledUnintended lateral movementLKA system engages in correct control actions to the operators surpriseUnsafe Control ActionPotential HazardRequired but not providedUnintended lateral movementProvided but not Provided but notVehicle continues	it is disabledenabledUnintended lateral movementUnintended lateral movementLKA system engages in correct control actions to the operators surprise	it is disabledenabledit is disabledenabledUnintended lateral movementILKA system engages in correct control actions to the operators surpriseUnsafe Control ActionPotential HazardCausal FactorsPrevention/MitigationRequired but not providedUnintended lateral movementVehicle continues lane deviationOperator believes the LKA system is enabled when it is disabledProvided but not requiredVehicle continues lane deviation

I	Provided but	Operator,	Unintended access		team shall ensure wiring is securely
i	incorrect	passenger, or	or physical damage	Ensure wiring gauge is sufficient to	installed using manufacturer
0	duration	property damage and injury	(liquid, puncture)	carry max operational current with factor of safety	installation specifications
I	Provided but	J. J. J.	Wiring failure (not	Ensure wire bend radii are adhered to	To avoid wiring failure of the intel
i	incorrect timing	LKA system	proper gauge,		tank computer the development
		enabled when	installation or	Ensure computer alters operator that	team shall ensure wiring gauge is
		operator believes	manufacturing	corrective action decisions are	sufficient to carry max operational
		it is disabled	failure)	disabled stating "LKA and ACC systems disabled" "No corrective	current with factor of safety
			Over-heating	action will be made"	To avoid wiring failure of the intel
					tank computer the development
			Operating system	Ensure computer only makes	team shall ensure wire bend radii
			crash	corrective action decisions when fidelity of image meets minimum	are adhered to
			Sensor malfunction	specified resolution	The development team shall ensure
			Sensor manufaction	specified resolution	the computer alerts operator that
			Operator believes	Ensure if computer system fails, it	corrective action decision is
			the LKA system is	does not prevent vehicle from manual	disabled
			disabled when it is	driving operations	
			enabled		The development team shall ensure
				Ensure manufacturing and	the computer only makes corrective
				installation is sufficient to prevent	action decisions when fidelity of image meets minimum specified
				unintended access and physical damage	resolution
				uanage	resolution
				Ensure use of covering at wire-	The development team shall ensure
				computer interface to prevent	if computer system fails, it does not
				unintended access	prevent vehicle from manual
				Avoid adverse road condition which	driving operations
				may produce NVH and damage	The development to an aball second
				computer	The development team shall ensure manufacturing and installation is
				Ensure computer installation is inside	sufficient to prevent unintended
				cabin in a dry debris-proof location	access and physical damage to the
				·····	computer
				Ensure computer is inaccessible by	*
				passengers	To prevent unintended access and
					physical damage to the development
					team shall ensure use of coverings

See wiring and unintended access	at wire-computer interface to
requirements	prevent unintended access
Ensure the power supplied to the	To prevent physical damage to the
computer is within manufacturer	computer the operator shall avoid
operational range	adverse road conditions which may
oporational range	produce NVH
To reduce computer signal input and	
output latency, ensure use of high-	To prevent unintended access and
quality transmission medium	physical damage the development
1	team shall ensure computer
To prevent computer signal input and	installation is inside cabin in a dry
output bandwidth faults, ensure	debris-proof location
transmission medium gauge is	r · · · · · · · · · · · · · · · · · · ·
sufficient to handle expected	To prevent unintended access and
throughput (load) with factor of	physical damage the development
safety	team shall ensure computer is
	inaccessible by passengers
Ensure understanding of time	
required to analyze and route	To prevent power failure the
computer signal data	development team shall ensure the
	power supplied to the computer is
To reduce computer signal input and	within manufacturer operational
output noise ensure wires are as short	range
as possible	
	The development team shall ensure
To reduce computer signal input and	the understanding of computer
output noise ensure wires are kept	input and output signal quality,
away from electrical machinery	noise, latency, and bandwidth
	accounting for measurement and
To reduce computer signal input and	control action error
output noise it is recommended to	
use twisted together wires	The development team shall reduce
	computer signal input and output
To reduce internal computer signal	latency, ensure use of high-quality
input and output noise ensure thermal	transmission medium
effects on amplifiers are minimized	The second se
To address comments a signalized of the	To prevent computer signal input
To reduce computer signal input and	and output bandwidth fault the
output noise, if possible, ensure	development team shall ensure

	mission medium gauge is
	cient to handle expected
	ghput (load) with factor of
To reduce computer signal input and safet	y
output noise ensure use of proper	
filtering techniques The	development team shall ensure
an ur	iderstanding of time required to
	ze and route computer signal
output noise ensure use of wire data	
shielding and conduit	
To re	duce computer signal input
	output noise the development
	shall ensure wires are as short
1 0	ssible
grounding practices	
	duce computer signal input
	output noise the development
	shall ensure wires are kept
	from electrical machinery
that it will be operating at in real-	
	duce computer signal input
	output noise it is recommended
	e twisted together wires
computer signal input and output	2
	educe internal computer signal
	and output noise the
	lopment team shall ensure
	hal effects on amplifiers are
	mized
Ensure computer is capable of storing To re	duce computer signal input
	output noise, if possible, the
	lopment team shall ensure the
	ifier bandwidth matches input
	l bandwidth
program is developed such that	
	educe computer signal input
	output noise the development
	shall ensure use of proper
	ing techniques
Inter	ing wenniques

	I
To prevent over-heating ensure	
computer is mounted such that there	To reduce computer signal input
is proper clearance and sufficient air	and output noise the development
flow to cool the computer	team shall ensure use of wire
	shielding and conduit
To prevent over-heating ensure	
computer fans pull air from cool and	To reduce computer signal input
dry source	and output noise the development
	team shall ensure understanding of
To prevent over-heating ensure	ground loops and impose proper
computer imposes thermal self-	grounding practices
regulation	
	To ensure true data measurement
To prevent over-heating ensure	the development team shall test the
computer operates within specified	collection with the computer
temperature range	operating at the same temperature
To prevent operating system crash	that it will be operating at in real-
ensure system does not over heat	world scenarios
To prevent operating system crash	The development team shall ensure
ensure computer is mounted such	the understanding of potential
that there is proper clearance and	computer signal input and output
sufficient air flow to cool the	storage delays
computer	storage delays
computer	
To prevent operating system crash	The development team shall ensure
ensure computer fans pull air from	the use of software safety and that
cool and dry source	the system is free from external
	unintended malicious control
To prevent operating system crash	Liniterated marterous control
ensure computer imposes thermal	To prevent computer memory
self-regulation	failure the development team shall
sen-regulation	ensure the computer is capable of
To prevent operating system crash	storing and processing the expected
ensure computer operates within	amount of data with a factor of
specified temperature range	
specified temperature range	safety
To provent operating system cresh	To provent computer memory
To prevent operating system crash	To prevent computer memory
ensure program is developed such	failure ensure the program is
that it does not attempt to access an	developed such that information

 1				7
			incorrect memory address leading to	that is too large cannot be written
			general protection fault	into a memory buffer that is too
				small to contain it
			To prevent operating system crash	
			ensure program is developed such	To prevent over-heating the
			that the OS does not enter an infinite	development team shall ensure the
			loop	computer is mounted such that there
			1	is proper clearance and sufficient
			To prevent operating system crash	air flow to cool the computer
			ensure program is developed such	1
			that information that is too large	To prevent over-heating the
			cannot be written into a memory	development team shall ensure the
			buffer that is too small to contain it	computer fans pull air from cool
				and dry source
			To prevent operating system crash	
			ensure program is developed such	To prevent over-heating the
			that deadlock is prevented (multiple	development team shall ensure the
			programs having control some	computer imposes thermal self-
			resource another program needs)	regulation
			resource unother program needs)	regulation
			To prevent operating system crash	To prevent over-heating the
			ensure program performs shutdown	development team shall ensure the
			operations	computer operates within specified
			I	temperature range
				I BAR BAR
				To prevent operating system crash
				the development team shall ensure
				the system does not over heat
				To prevent operating system crash
				the development team shall ensure
				the computer is mounted such that
				there is proper clearance and
				sufficient air flow to cool the
				computer
				L
				To prevent operating system crash
				the development team shall ensure
				the computer fans pull air from cool
				and dry source
 1	1	l		und dry source

rr	
	To prevent operating system crash the development team shall ensure the computer imposes thermal self- regulation
	To prevent operating system crash the development team shall ensure the computer operates within specified temperature range
	To prevent operating system crash the development team shall ensure the program is developed such that it does not attempt to access an incorrect memory address leading to general protection fault
	To prevent operating system crash the development team shall ensure the program is developed such that the OS does not enter an infinite loop
	To prevent operating system crash the development team shall ensure the program is developed such that information that is too large cannot be written into a memory buffer that is too small to contain it
	To prevent operating system crash the development team shall ensure the program is developed such that deadlock is prevented (multiple programs having control some resource another program needs)
	To prevent operating system crash the development team shall ensure

Control	Unsafe Control				the program performs shutdown operations The LKA system shall allow the operator to easily override the corrective control action via actuation of steering, braking or accelerating The LKA system shall temporarily disengage when the operator actuates turn signal
Function	Action	Potential Hazard	Causal Factors	Prevention/Mitigation	Functional Requirement
Provides feedback to the operator (LKA status, haptic, visual, audio)	Required but not provided	Operator unaware of lane deviation Unintended later movement	Failure of one or all of the feedback systems (visual, haptic, audio) Operator unable to see, hear, or feel feedback levels Power failure Wiring failure Signal corruption	The LKA feedback system will alert the operator using at least two forms of feedback The operator will have control of the level of LKA system feedback stimuli The LKA system will perform feedback checks and disable functionality if specified minimum standard is not met Ensure the LKA system wiring will be installed according to manufacturer specifications to include EMI avoidance, gauge, and bend radii	The LKA feedback system shall alert the operator using at least two forms of feedback The operator shall have control of the level of LKA system feedback stimuli The LKA system shall perform feedback checks and disable functionality if specified minimum standard is not met The development team shall ensure the LKA system wiring will be installed according to manufacturer specifications to include EMI avoidance, gauge, and bend radii
	Provided but not required	Operator alerted to false deviation Operator startled and makes spontaneous corrective action	Sensor malfunction or obstruction (dirt, debris stuck to sensor) Environmental conditions	The LKA system will check for sensor obstructions (validate wheel speed with sensor data) Ensure LKA system radars and cameras are of the quality which can produce true data during reasonably	The LKA system shall check for sensor obstructions (validate wheel speed with sensor data) The development team shall ensure LKA system radars and cameras are of the quality which can produce

Provided but incorrect timing	False positive Operator alerted to early or late of lane deviation Operator startled and makes spontaneous corrective action False positive or negative	Operator believes the LKA system is disabled when it is enabled Sensor malfunction or obstruction (dirt, debris stuck to sensor) Environmental conditions Operator believes the LKA system is disabled when it is enabled	 poor operational conditions (rain, fog, snow, dirt, poor lane-line quality) Ensure LKA system radars and cameras are mounted in location free from visibility obstruction The LKA system will have constant enabled/disabled form of feedback (light) indicated to the operator The LKA system will check for sensor obstructions (validate wheel speed with sensor data) Ensure LKA system radars and cameras are of the quality which can produce true data during reasonably poor operational conditions (rain, fog, snow, dirt, poor lane-line quality) Ensure LKA system radars and cameras are mounted in location free from visibility obstruction The LKA system will have constant enabled/disabled form of feedback (light) indicated to the operator 	true data during reasonably poor operational conditions (rain, fog, snow, dirt, poor lane-line quality) The development team shall ensure LKA system radars and cameras are mounted in location free from visibility obstruction The LKA system shall have constant enabled/disabled form of feedback (light) indicated to the operator The LKA system shall check for sensor obstructions (validate wheel speed with sensor data) The development team shall ensure LKA system radars and cameras are of the quality which can produce true data during reasonably poor operational conditions (rain, fog, snow, dirt, poor lane-line quality) The development team shall ensure LKA system radars and cameras are mounted in location free from visibility obstruction The LKA system shall have constant enabled/disabled form of feedback (light) indicated to the operator
duration	Annoyance to the operator Operator may believe corrective control action needs to be taken	environmental conditions	Ensure LKA system vin check for sensor obstructions (validate wheel speed with sensor data) Ensure LKA system radars and cameras are of the quality which can produce true data during reasonably	The development team shall ensure LKA system radars and cameras are of the quality which can produce

			LKA system program error	 poor operational conditions (rain, fog, snow, dirt, poor lane-line quality) Ensure LKA system radars and cameras are mounted in location free from visibility obstruction The operator will be capable of disenabling the LKA feedback system If LKA feedback system is disabled by the operator then the entire LKA system will disengage 	true data during reasonably poor operational conditions (rain, fog, snow, dirt, poor lane-line quality) The development team shall ensure LKA system radars and cameras are mounted in location free from visibility obstruction The operator shall be capable of disenabling the LKA feedback system If LKA feedback system is disabled by the operator then the entire LKA system shall disengage until the operator initiates it again
Control Function	Unsafe Control Action	Potential Hazard	Causal Factors	Prevention/Mitigation	Functional Requirement
Controls	Required but not	Operator	Contamination of	Ensure proper mounting,	Development team shall ensure
lateral	provided	anticipates	power steering fluid	installation, and manufacturing of	proper mounting, installation, and
movement	-	corrective control	(old, air)	hoses, clamps, and their components	manufacturing of EPS hoses,
via EPS	Provided but	action but none			clamps, and their components
	incorrect timing	occurs	Power steering low	Ensure interface components (seals,	
			fluid and fluid leaks	gaskets), and mounting hardware are	Development team shall ensure
	Provided but	Vehicle continues		securely fastened and free from	interface components (seals,
	incorrect	lane deviation	Broken belt which	potential loosening or movement	gaskets), and mounting hardware
	duration	Thinks de diter i	energizes power		are securely fastened and free from
		Unintended lateral movement	steering pump	Ensure functionality of pump and check for hose deterioration	potential loosening or movement
			Pump failure		Development team shall ensure
		Operator,	-	Ensure proper mounting,	functionality of EPS pump and
		passenger, or	Wiring failure	installation, and manufacturing of the	check for hose deterioration
		property damage		belt (tension, torque specs) and its	
		and injury	Signal corruption	components	Development team shall ensure
					proper mounting, installation, and
			EPS controls failure	Ensure proper mounting,	manufacturing of the EPS belt
				installation, and manufacturing of	(tension, torque specs) and its
				pump and its components	components

			Ensure power steering motor is functional	Development team shall ensure proper mounting, installation, and manufacturing of pump and its components Development team shall ensure power steering motor is functional
Provided but not required	LKA system enabled when operator believes it is disabled Unintended lateral movement LKA system engages in correct control actions to the operators surprise	Operator believes the LKA system is disabled when it is enabled	The LKA system will have constant enabled/disabled form of feedback (light) indicated to the operator	The LKA system shall have constant enabled/disabled form of feedback (light) indicated to the operator

Appendix 3.04 HARA CAVs PHA

	CAVs PHA
Item: Intel Tank Com	iter

			Corrective/Preventative	
Potential Hazard	Cause	Major Effect	Measure	Functional Requirement
Failure to blend various	Wiring failure (not	Wiring failure will	Ensure wiring is securely	To avoid wiring failure of the intel tank
sensors (cameras, radars)	proper gauge,	cause fault in	installed using manufacturer	computer the development team shall
data to achieve reliable, high-	installation or	computer leading to no	installation specifications	ensure wiring is securely installed using
definition images Failure to perform sensor	manufacturing failure)	corrective action decisions	Ensure wiring gauge is sufficient to carry max operational current	manufacturer installation specifications To avoid wiring failure of the intel tank
fusion data verification &		Operator unaware of	with factor of safety	computer the development team shall
validation using developed algorithms and NNs		system failure Computer, if	Ensure wire bend radii are adhered to	ensure wiring gauge is sufficient to carry max operational current with factor of safety
Failure to determines if control action (EPS torque, braking, feedback) is required		operational, operates on single point source information Less reliable image to	Ensure computer alters operator that corrective action decisions are disabled stating "LKA and ACC systems disabled" "No	To avoid wiring failure of the intel tank computer the development team shall ensure wire bend radii are adhered to
Failure to send control action request to associated controller		which the computer can determine deviations and control actions	corrective action will be made" Determine fidelity of non-blended image and decide if corrective	The development team shall ensure computer alerts operator when corrective action decision is disabled
Failure to provides real-time functionalities		Operator expects control action but none is taken	action should be applied Ensure computer only makes corrective action decisions when fidelity of image meets minimum	The development team shall ensure the system determines fidelity of non- blended image and decides if corrective action should be applied
		Unintended longitudinal motion Unintended lateral motion	specified resolution Ensure if computer system fails, it does not prevent vehicle from manual driving operations	The development team shall ensure the computer only makes corrective action decisions when fidelity of image meets minimum specified resolution
				The development team shall ensure if computer system fails, it does not prevent vehicle from manual driving operations

Unintended access	Failure of CAVs	Ensure manufacturing and	The development team shall ensure
or physical damage	computer and CAVs	installation is sufficient to prevent	manufacturing and installation is
(liquid, puncture)	systems	unintended access and physical	sufficient to prevent unintended access
	-)	damage	and physical damage to the computer
		Ensure use of covering at wire- computer interface to prevent unintended access Avoid adverse road condition which may produce NVH and damage computer Ensure computer installation is inside cabin in a dry debris-proof location Ensure computer is inaccessible by passengers	To prevent unintended access and physical damage to the development team shall ensure use of coverings at wire-computer interface To prevent physical damage to the computer the operator shall avoid adverse road condition which may produce NVH To prevent unintended access and physical damage the development team shall ensure computer installation is inside cabin in a dry debris-proof location
			To prevent unintended access and physical damage the development team shall ensure computer is inaccessible by passengers
Power failure		See wiring and unintended access requirements Ensure the power supplied to the computer is within manufacturer operational range	To prevent power failure the development team shall ensure the power supplied to the computer is within manufacturer operational range
Algorithm, NN, computational, or cyber-security failure	1	Ensure computer NN model is thoroughly defined and highly sensitive to small variations in inputs	To prevent CAVs failure the development team shall ensure the computer NN model is thoroughly defined and highly sensitive to small variations in inputs
		Ensure computer NN is thoroughly tested and validate prior to implementation	To prevent CAVs failure the development team shall ensure the

Ensure computer NN imposes limits on output to not exceed boundariesEnsure computer NNs use of hidden layers and neurons does not over-fit training data and is sufficient to fit new and unseen dataEnsure computer program code is thoroughly vetted (Auto industry standard is one defect per 1000 executable lines of code)Ensure computer program is developed using automotive coding standardsEnsure use of multiple software scanning tools to identify vulnerability and error in computer program code (industry uses Jarvis which analyses the binary executable action and not the mistakes in the code)Ensure control of computational overflow and compounding rounding errorsEnsure understanding of computer input and output signal quality, noise, latency, and	 computer NN is thoroughly tested and validate prior to implementation To prevent CAVs failure the development team shall ensure the computer NN imposes limits on output to not exceed boundaries To prevent CAVs failure the development team shall ensure the computer NNs use of hidden layers and neurons does not over-fit training data and is sufficient to fit new and unseen data To prevent CAVs failure the development team shall ensure the computer program code is thoroughly vetted (Auto industry standard is one defect per 1000 executable lines of code) To prevent CAVs failure the development team shall ensure the computer program is developed using automotive coding standards To prevent CAVs failure the development team shall ensure the computer program is developed using automotive coding standards To prevent CAVs failure the development team shall ensure the computer program is developed using automotive coding standards To prevent CAVs failure the development team shall ensure the use of multiple software scanning tools to identify vulnerability and error in computer program code (industry uses Jarvis which analyses the binary executable action and not the mistakes in the code)
rounding errors Ensure understanding of	identify vulnerability and error in computer program code (industry uses Jarvis which analyses the binary
measurement and control action error	To prevent CAVs failure the development team shall ensure the control of computational overflow and compounding rounding errors

To reduce computer signal input	To prevent CAVs failure the
and output latency, ensure use of	development team shall ensure the
high-quality transmission medium	understanding of computer input and
	output signal quality, noise, latency, and
To prevent computer signal input	bandwidth accounting for measurement
and output bandwidth faults,	and control action error
ensure transmission medium	
gauge is sufficient to handle	To prevent CAVs failure the
expected throughput (load) with	development team shall reduce computer
factor of safety	signal input and output latency, ensure
	use of high-quality transmission medium
Ensure understanding of time	
required to analyze and route	To prevent computer signal input and
computer signal data	output bandwidth fault the development
	team shall ensure transmission medium
To reduce computer signal input	gauge is sufficient to handle expected
and output noise ensure wires are	throughput (load) with factor of safety
as short as possible	
	To prevent CAVs failure the
To reduce computer signal input	development team shall ensure an
and output noise ensure wires are	understanding of time required to
kept away from electrical	analyze and route computer signal data
machinery	anaryze and route computer signar data
machinery	To reduce computer signal input and
To reduce computer signal input	output noise the development team shall
and output noise it is	ensure wires are as short as possible
recommended to use twisted	ensure wires are as short as possible
	To reduce computer signal input and
together wires	To reduce computer signal input and
To make a internal commuter	output noise the development team shall
To reduce internal computer	ensure wires are kept away from
signal input and output noise	electrical machinery
ensure thermal effects on	m 1
amplifiers are minimized	To reduce computer signal input and
	output noise it is recommended to use
To reduce computer signal input	twisted together wires
and output noise, if possible,	
ensure amplifier bandwidth	To reduce internal computer signal input
matches input signal bandwidth	and output noise the development team
	shall ensure thermal effects on
	amplifiers are minimized

	To reduce computer signal input	
	and output noise ensure use of	To reduce computer signal input and
	proper filtering techniques	output noise, if possible, the development team shall ensure the
	To reduce computer signal input	amplifier bandwidth matches input
	and output noise ensure use of	signal bandwidth
	wire shielding and conduit	
		To reduce computer signal input and
	To reduce computer signal input	output noise the development team shall
	and output noise ensure understanding of ground loops	ensure use of proper filtering techniques
	and impose proper grounding	To reduce computer signal input and
	practices	output noise the development team shall
	*	ensure use of wire shielding and conduit
	To ensure true data measurement	
	test the collection with the	To reduce computer signal input and
	computer operating at the same temperature that it will be	output noise the development team shall ensure understanding of ground loops
	operating at in real-world	and impose proper grounding practices
	scenarios	and impose proper grounding practices
		To ensure true data measurement the
	Ensure understanding of potential	development team shall test the
	computer signal input and output	collection with the computer operating
	storage delays	at the same temperature that it will be operating at in real-world scenarios
	Ensure the use of software safety	operating at in rear-world scenarios
	and that the system is free from	To prevent CAVs failure the
	external unintended malicious	development team shall ensure the
	control	understanding of potential computer
		signal input and output storage delays
	Ensure system software updates	To provent CAVe failure the
	are performed over land-line and not through the air	To prevent CAVs failure the development team shall ensure the use
	not anough the an	of software safety and that the system is
		free from external unintended malicious
		control
Memory failure	Ensure computer is capable of	To prevent computer memory failure the
	storing and processing the	development team shall ensure the
	expected amount of data with a factor of safety	computer is capable of storing and
	factor of safety	

	To prevent memory failure ensure program is developed such that information that is too large cannot be written into a memory buffer that is too small to contain it	processing the expected amount of data with a factor of safety To prevent computer memory failure ensure the program is developed such that information that is too large cannot be written into a memory buffer that is too small to contain it
Over-heating	To prevent over-heating ensure computer is mounted such that there is proper clearance and sufficient air flow to cool the computer	To prevent over-heating the development team shall ensure the computer is mounted such that there is proper clearance and sufficient air flow to cool the computer
	To prevent over-heating ensure computer fans pull air from cool and dry source To prevent over-heating ensure	To prevent over-heating the development team shall ensure the computer fans pull air from cool and dry source
	To prevent over-heating ensure computer imposes thermal self- regulation To prevent over-heating ensure computer operates within	To prevent over-heating the development team shall ensure the computer imposes thermal self- regulation
	specified temperature range	To prevent over-heating the development team shall ensure the computer operates within specified temperature range
Operating system crash	To prevent operating system crash ensure system does not over heat	To prevent operating system crash the development team shall ensure the system does not over heat
	To prevent operating system crash ensure computer is mounted such that there is proper clearance and sufficient air flow to cool the computer	To prevent operating system crash the development team shall ensure the computer is mounted such that there is proper clearance and sufficient air flow to cool the computer
		To prevent operating system crash the development team shall ensure the

To prevent operating system crash ensure computer fans pull air from cool and dry source To prevent operating system crash ensure computer imposes thermal self-regulation	computer fans pull air from cool and dry source To prevent operating system crash the development team shall ensure the computer imposes thermal self- regulation
To prevent operating system crash ensure computer operates within specified temperature range	To prevent operating system crash the development team shall ensure the computer operates within specified temperature range
To prevent operating system crash ensure program is developed such that it does not attempt to access an incorrect memory address leading to general protection fault	To prevent operating system crash the development team shall ensure the program is developed such that it does not attempt to access an incorrect memory address leading to general protection fault
To prevent operating system crash ensure program is developed such that the OS does not enter an infinite loop	To prevent operating system crash the development team shall ensure the program is developed such that the OS does not enter an infinite loop
To prevent operating system crash ensure program is developed such that information that is too large cannot be written into a memory buffer that is too small to contain it	To prevent operating system crash the development team shall ensure the program is developed such that information that is too large cannot be written into a memory buffer that is too small to contain it
To prevent operating system crash ensure program is developed such that deadlock is prevented (multiple programs having control some resource another program needs)	To prevent operating system crash the development team shall ensure the program is developed such that deadlock is prevented (multiple programs having control some resource another program needs)

	To prevent operating system	To prevent operating system crash the
	crash ensure program performs	development team shall ensure the
	shutdown operations	program performs shutdown operations
Adverse	Ensure computer operates	To prevent control action decision
environmental	according to a specified minimum	failure the development team shall
conditions (poor	for sensor data quality	ensure the computer operates according
sensor output; dark,		to a specified minimum for sensor data
fog, poorly painted	Ensure computer disables	quality
or no lane lines)	corrective action decisions when	
	minimum standard for lane-line,	To prevent control action decision
	object, and traffic sign	failure the development team shall
	recognition is not met	ensure the computer disables the
		associated corrective action decisions
	Ensure computer operates	when minimum standard for lane-line,
	according to a specified minimum	object, and traffic sign recognition is not
	for lane-line recognition (lane	met
	dots, poorly painted lines, no	
	lines)	To prevent control action decision
		failure the development team shall
	Ensure computer operates	ensure the computer operates according
	according to a specified minimum	to a specified minimum for lane-line
	for low-light operations	recognition (lane dots, poorly painted
		lines, no lines)
	Ensure computer has control of	
	headlights	To prevent control action decision
		failure the development team shall
		ensure the computer operates according
		to a specified minimum for traffic sign
		recognition
		To prevent control action decision
		failure the development team shall
		ensure the computer operates according
		to a specified minimum for low-light
		operations
		To prevent control action decision
		failure the development team shall
		ensure the computer has control of
		headlights

	Other		Ensure system allows operator to increase or decrease feedback timing Ensure system allows operator to increase or decrease feedback volume Ensure system allows operator to increase or decrease feedback visual stimulation Ensure system allows operator to increase or decrease haptic feedback stimulation	The development team shall ensure the computer allows the operator to increase or decrease feedback timing The development team shall ensure the computer allows the operator to increase or decrease feedback volume The development team shall ensure the computer allows the operator to increase or decrease feedback visual stimulation The development team shall ensure the computer allows the operator to increase or decrease feedback visual stimulation
Item: Intel Mobileye 6				
Potential Hazard	Cause	Major Effect	Corrective/Preventative Measure	Functional Requirement
Failure to perform multi-	Wiring failure (not	Failure of CAVs	Ensure Intel Mobileye 6 camera	The development team shall ensure the
feature tracking	proper gauge, installation or	functionality	wiring is securely installed using manufacturer installation	Intel Mobileye 6 camera wiring is securely installed using manufacturer
Failure to perform object and lane-line detection	manufacturing failure)	Computer, if operational, operates	specifications	installation specifications
Failure to perform forward		on single point source information	Ensure Intel Mobileye 6 camera wiring gauge is sufficient to carry	The development team shall ensure the Intel Mobileye 6 camera wiring gauge is
collision warning		Operator unaware of	max operational current with factor of safety	sufficient to carry max operational current with factor of safety
Failure to perform pedestrian collision warning		system failure	Ensure Intel Mobileye 6 camera	The development team shall ensure the
C		Less reliable image to	wire bend radii are adhered to	Intel Mobileye 6 camera wire bend radii
Failure to perform headway warning		which the computer can determine	Ensure Intel Mobileye 6 camera	are adhered to
warming		deviations and control	alerts computer that system	The development team shall ensure the
Failure to perform traffic		actions	failure has occurred	Intel Mobileye 6 camera alerts the
sign recognition				computer when failure has occurred

	Unintended access	Unintended	Ensure Intel Mobileye 6 camera	The development team shall answer the
Failure to transmit data to	or physical damage	longitudinal motion	manufacturing and installation is	The development team shall ensure the Intel Mobileye 6 camera manufacturing
associated controller	(liquid, puncture)	ioligitudillai illotioli	sufficient to prevent unintended	and installation is sufficient to prevent
associated controller	(inquid, puncture)	Unintended lateral	1	unintended access and physical damage
Failure to provide real-time		motion	access and physical damage	unintended decess and physical damage
display			Ensure Intel Mobileye 6 camera is	The development team shall ensure the
unsprug			placed inside cabin and top-	Intel Mobileye 6 camera is placed inside
			center of wind shield within	cabin and top-center of wind shield
			operational area of windshield	within operational area of windshield
			wipers	wipers
			wipers	•
			Ensure use of covering at wire-	The development team shall ensure the
			Intel Mobileye 6 camera interface	use of covering at wire- Intel Mobileye 6
			to prevent unintended access	camera interface to prevent unintended
			-	access
			Avoid adverse road condition	
			which may produce NVH and	The development team shall ensure the
			damage or loosen the Intel	Intel Mobileye 6 camera installation is
			Mobileye 6 camera	inside cabin in a dry debris-proof
				location
			Ensure Intel Mobileye 6 camera	TT1
			installation is inside cabin in a dry	The operator shall avoid adverse road conditions which may produce NVH and
			debris-proof location	damage or loosen the Intel Mobileye 6
				camera
	Power failure		See wiring and unintended access	The development team shall ensure the
	I ower failure		requirements	power supplied to the Intel Mobileye 6
			requirements	camera is within manufacturer
			Ensure the power supplied to the	recommended operational range
			Intel Mobileye 6 camera is within	
			manufacturer operational range	
	Signal or cyber-	1	Ensure understanding of Intel	The development team shall ensure an
	security failure		Mobileye 6 camera signal quality,	understanding of Intel Mobileye 6
	-		noise, latency, and bandwidth	camera signal quality, noise, latency,
			accounting for measurement and	and bandwidth accounting for
			control action error	measurement and control action error
			To reduce Intel Mobileye 6	To reduce Intel Mobileye 6 camera
			camera signal latency, ensure use	signal latency the development team

of high-quality transmission medium	shall ensure the use of a high-quality transmission medium
To prevent Intel Mobileye 6 camera signal bandwidth faults, ensure transmission medium gauge is sufficient to handle expected throughput (load) with factor of safety	To prevent Intel Mobileye 6 camera signal bandwidth faults the development team shall ensure the transmission medium gauge is sufficient to handle expected throughput (load) with factor of safety
Ensure understanding of time required to analyze and route Inte Mobileye 6 camera signal data	The development team shall ensure an understanding of time required to analyze and route Intel Mobileye 6 camera signal data
To reduce Intel Mobileye 6 camera signal noise ensure wires are as short as possible	To reduce Intel Mobileye 6 camera signal noise the development team shall ensure the wires are as short as possible
To reduce Intel Mobileye 6 camera signal noise ensure wires are kept away from electrical machinery	To reduce Intel Mobileye 6 camera signal noise the development team shall ensure the wires are kept away from electrical machinery
To reduce Intel Mobileye 6 camera signal noise it is recommended to use twisted together wires	To reduce Intel Mobileye 6 camera signal noise it is recommended to use twisted together wires
To reduce internal Intel Mobileye 6 camera signal noise ensure thermal effects on amplifiers are minimized	To reduce internal Intel Mobileye 6 camera signal noise the development team shall ensure the thermal effects on amplifiers are minimized
To reduce Intel Mobileye 6 camera signal noise, if possible, ensure amplifier bandwidth matches input signal bandwidth	To reduce Intel Mobileye 6 camera signal noise, if possible, the development team shall ensure the amplifier bandwidth matches input signal bandwidth

	To reduce Intel Mobileye 6	To reduce Intel Mobileye 6 camera
	camera signal noise ensure use of	signal noise the development team shall
	proper filtering techniques	ensure the use of proper filtering techniques
	To reduce Intel Mobileye 6	teeninques
	camera signal noise ensure use of	To reduce Intel Mobileye 6 camera
	wire shielding and conduit	signal noise the development team shall
	_	ensure the use of wire shielding and
	To reduce Intel Mobileye 6	conduit
	camera signal noise ensure	
	understanding of ground loops	To reduce Intel Mobileye 6 camera
	and impose proper grounding	signal noise the development team shall
	practices	ensure the understanding of ground
		loops and impose proper grounding
	Ensure understanding of potential	practices
	Intel Mobileye 6 camera signal	
	storage delays	The development team shall ensure
		understanding of potential Intel
	Ensure the use of software safety	Mobileye 6 camera signal storage delays
	and that the Intel Mobileye 6	
	camera signal is free from	The development team shall ensure the
	external unintended malicious	use of software safety and that the Intel
	control	Mobileye 6 camera signal is free from
		external unintended malicious control
	Ensure Intel Mobileye 6 camera	
	system software updates are	The development team shall ensure Intel
	performed over land-line and not	Mobileye 6 camera system software
	through the air	updates are performed over land-line and
		not through the air
Capability	To prevent field of view failure	To prevent field of view failure the
limitations	ensure Intel Mobileye 6 camera is	development team shall ensure the Intel
	mounted in the operational area of	Mobileye 6 camera is mounted in the
Failure of field of	the wind shield wipers	operational area of the wind shield
view		wipers
	To prevent field of view failure	
Adverse	ensure Intel Mobileye 6 camera	To prevent field of view failure the
environmental	has control of wind shield wipers	development team shall ensure the Intel
conditions (dark,	(debris may impede camera view	Mobileye 6 camera has control of wind
fog, poorly painted	while operator is unaware)	shield wipers (debris may impede
or no lane lines)		camera view while operator is unaware)

			Ensure Intel Mobileye 6 camera is of high-quality to maintain operations during low-light, poorly painted lane lines, and adverse weather conditions Ensure Intel Mobileye 6 camera indicates to computer and operator when the system is unavailable	The development team shall ensure the Intel Mobileye 6 camera is of high- quality to maintain operations during low-light, poorly painted lane lines, and adverse weather conditions The development team shall ensure the Intel Mobileye 6 camera indicates to computer and operator when the system is unavailable
Item: Bosch Front, Rear, an	d Corner MRR Radars			
Potential Hazard	Cause	Major Effect	Corrective/Preventative Measure	Functional Requirement
Failure to perform early front, rear, and corner speed detection Failure to perform front, rear, and corner position detection Failure to send data to associated controller	Wiring failure (not proper gauge, installation or manufacturing failure)	Wiring failure will cause fault in computer leading to no corrective action decisions Operator unaware of system failure Computer, if operational, operates on single point source information Less reliable image to	Ensure radar wiring is securely installed using manufacturer installation specifications Ensure radar wiring gauge is sufficient to carry max operational current with factor of safety Ensure radar wire bend radii are adhered to Ensure radar alters computer that system failure has occurred	The development team shall ensure the radar wiring is securely installed using manufacturer installation specifications The development team shall ensure the radar wiring gauge is sufficient to carry max operational current with factor of safety The development team shall ensure the radar wire bend radii are adhered to The development team shall ensure the radar alters computer that system failure has occurred
	Unintended access or physical damage (liquid, puncture)	which the computer can determine	Ensure radar manufacturing and installation is sufficient to prevent unintended access and physical damage	The development team shall ensure the radar manufacturing and installation is sufficient to prevent unintended access and physical damage

deviations and control actionsEnsure use of covering at wire- radar interface to prevent unintended accessThe development team shall ensure the use of covering at wire- radar interface to prevent unintended accessThe development team shall ensure the use of covering at wire- radar interface to prevent unintended accessThe development team shall ensure the use of covering at wire- radar interface to prevent unintended accessPower failureUnintended longitudinal motionSee wiring and unintended access requirementsThe development team shall ensure the power supplied to the radar is within manufacturer operational rangeSignal or cyber- security failureSignal or cyber- security failureEnsure the power supplied to the radar is within manufacturer operational rangeThe development team shall ensure the understanding of radar signal quality, noise, latency, and bandwidth accounting for measurement and control action errorThe development team shall ensure the understanding of radar signal quality, noise, latency, and bandwidth faults, ensure transmission mediumThe development team shall ensure the understanding of radar signal quality, noise, latency, and bandwidth faults, ensure transmission mediumTo reduce radar signal latency, the development team shall ensure the such of high-quality transmission mediumFor greevent radar signal bandwidth faults, ensure transmission mediumTo reduce radar signal latency, the development team shall ensure the understanding of time required to andrige at frout camera signal dataTo reduce radar signal latency the development team shall ensure the wires are a short as possible	ГТ			
Power failure Operator expects control action but none is taken Avoid adverse road condition which may produce NVH and damage of losen the radar The operator shall avoid adverse road condition which may produce NVH and damage of losen the radar Power failure Unintended longitudinal motion See wiring and unintended access requirements The development team shall ensure the proper supplied to the radar is within manufacturer operational range The development team shall ensure the understanding of radar signal quality, noise, latency, and bandwidth accounting for radar signal quality, noise, latency, and bandwidth accounting for measurement and control action error The development team shall ensure the understanding of radar signal quality, noise, latency, and bandwidth accounting for measurement and control action error To reduce radar signal latency, transmission medium To reduce radar signal latency, transmission medium To reduce radar signal latency, transmission medium To revent radar signal bandwidth faults, ensure transmission medium To revent radar signal bandwidth faults, ensure transmission medium To prevent radar signal bandwidth faults, ensure transmission medium gauge is sufficient to handle expected throughput (load) with factor of safety safety The development team shall ensure the wires are a short as possible To reduce radar signal noise the development team shall ensure the wires are as short as possible				-
Operator expects Avoid adverse road condition The operator shall avoid adverse road condition which may produce NVH and damage or loosen the radar Power failure Unintended longitudinal motion Security failure Security failure Ensure the power supplied to the radar is within manufacturer operational range Signal or cyber-security failure Signal or cyber-security failure Ensure the power supplied to the radar is within manufacturer operational range The development team shall ensure the motion and pandwidth accounting for masurement and control action error Signal or cyber-security failure For educe radar signal latency, ensure use of high-quality transmission medium To reduce radar signal latency, ensure use of high-quality transmission medium To prevent radar signal latency, the development team shall ensure the use of high-quality transmission medium To prevent radar signal latency, ensure use of high-quality transmission medium To prevent radar signal latency, the development team shall ensure the use of safety To prevent radar signal latency errading of time required to analyze and route camera signal data To reduce radar signal noise the development team shall ensure the use of safety To reduce radar signal noise Ensure understanding of time required to analyze and route camera signal data To reduce radar signal noise To reduce radar signal noise the development team shall ensure the winderstanding of time required to analyze and route camera signal noise		actions	1	e
Power failurecontrol action but nome is takenAvoid adverse road condition which may produee NVH and damage of produe NVH and damage the radarThe operator shall avoid adverse road condition which may produee NVH and damage of neaderPower failureUnintended longitudinal motionSee wiring and unintended access requirementsThe development team shall ensure the power supplied to the radar is within manufacturer operational rangeThe development team shall ensure the power supplied to the radar is within manufacturer operational rangeSignal or cyber- security failureSignal or cyber- security failureEnsure the power supplied to the radar is within manufacturer operational rangeThe development team shall ensure the understanding of radar signal quality, noise, latency, and bandwidth accounting for measurement and control action errorNo reduce radar signal latency, ensure use of high-quality transmission mediumTo reduce radar signal latency, the development team shall ensure the use of high-quality transmission medium action errorTo prevent radar signal bandwidth faults, ensure transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyTo prevent radar signal noise the development team shall ensure the understanding of time required to analyze and route analyze a		Organistan avreata	unintended access	to prevent unintended access
Image: here is takenwhich may produce NVH and damage the radarcondition which may produce NVH and damage to rosen the radarPower failureUnintended longitudinal motionSee writing and unintended access requirementsThe development team shall ensure the power supplied to the radar is within manufacturer operational rangeThe development team shall ensure the power supplied to the radar is within manufacturer operational rangeSignal or cyber- security failureSignal or cyber- security failureEnsure the power supplied to the radar is within manufacturer operational rangeThe development team shall ensure the understanding of radar signal quality, noise, latency, and bandwidth accounting for measurement and control action errorTo reduce radar signal latency, ensure use of high-quality transmission mediumTo reduce radar signal latency, the development team shall ensure the use of high-quality transmission medium action errorTo prevent radar signal sufficient to handle expected throughput (load) with factor of safetyTo reduce radar signal loadid faults, the development team shall ensure the understanding of time required to analyze and route camera signal data To reduce radar signal noise the development team shall ensure the wires are ashort as possibleTo reduce radar signal noise the development team shall ensure the wires are ashort as possible		1 1	A . 1 . 1	
Power failureUnintended longitudinal motiondamage the radardamage or loosen the radarPower failureUnintended lateral motionSignal or cyber- security failureThe development team shall ensure the radar is within manufacturer operational rangeThe development team shall ensure the monufacturer operational rangeSignal or cyber- security failureFinare understanding of radar signal quality, noise, latency, and bandwidth accounting for ensure understanding of radar signal quality, noise, latency, and bandwidth faults, ensure transmission mediumThe development team shall ensure the understanding of radar signal quality, noise, latency, and bandwidth faults, ensure transmission mediumTo reduce radar signal latency, ensure use of high-quality transmission mediumTo requee radar signal bandwidth faults, ensure transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyTo prevent radar signal and you with factor of safetyTo reduce radar signal noise ensure use as short as possibleTo reduce radar signal noise the development team shall ensure the winderstanding of time radar signal noise the				
Power failureUnintended longitudinal motionSee wiring and unintended access requirementsThe development team shall ensure the power supplied to the radar is within manufacturer operational rangeSignal or cyber- security failureSignal or cyber- security failureEnsure the opwer supplied to the radar is within manufacturer operational rangeThe development team shall ensure the power supplied to the radar signal quality, noise, latency, and bandwidth accounting for measurement and control action errorTo reduce radar signal latency, the development team shall ensure the use of high-quality transmission mediumTo reduce radar signal bandwidth faults, ensure transmission mediumTo prevent radar signal bandwidth faults, ensure transmission medium gue is sufficient to handle expected throughput (load) with factor of safetyTo reduce radar signal bandwidth faults, the development team shall ensure the understanding of time ensure the cramera signal data To reduce radar signal noise the development team shall ensure the wires are as short as possible		is taken	• 1	
Forse inducelongitudinal motionSignal or cyber- security failureSignal or cyber- security failureEnsure the power supplied to the radar is within manufacturer operational rangeThe development team shall ensure the understanding of radar signal quality, noise, latency, and bandwidth accounting for measurement and control action errorThe development team shall ensure the understanding of radar signal quality, noise, latency, and bandwidth accounting for measurement and control action errorThe development team shall ensure the understanding of radar signal quality, noise, latency, and bandwidth accounting for measurement and control action errorTo reduce radar signal latency, ensure use of high-quality transmission mediumTo reduce radar signal bandwidth faults, ensure transmission mediumTo reduce radar signal bandwidth faults, ensure transmission mediumTo prevent radar signal bandwidth faults, the development team shall ensure the transmission mediumTo reduce radar signal bandwidth faults, ensure transmission mediumTo prevent radar signal bandwidth faults, the development team shall ensure the transmission mediumTo reduce radar signal data To reduce radar signal dataTo reduce radar signal noise the development team shall ensure the wires are as short as possible		Unintended		
Linitended lateral motionEnsure the power supplied to the radar is within manufacturer operational rangeInanufacturer operational rangeSignal or cyber- security failureSignal or cyber- security failureEnsure the power supplied to the radar is within manufacturer operational rangeThe development team shall ensure the understanding of radar signal quality, noise, latency, and bandwidth accounting for measurement and control action errorTo reduce radar signal latency, ensure use of high-quality transmission mediumTo reduce radar signal latency, ensure use of high-quality transmission mediumTo reduce radar signal latency, to reduce radar signal bandwidth faults, ensure transmission mediumTo prevent radar signal bandwidth faults, ensure transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyTo prevent radar signal ond ensure understanding of time required to analyze and route camera signal dataTo reduce radar signal noise the development team shall ensure the wires are as short as possibleTo reduce radar signal noise the development team shall ensure the wires are as short as possible	Power failure			
Unintended lateral motionEnsure the power supplied to the radar is within manufacturer operational rangeThe development team shall ensure the understanding of radar signal quality, noise, latency, and bandwidth accounting for measurement and control action errorThe development team shall ensure the understanding of radar signal quality, noise, latency, and bandwidth accounting for measurement and control action errorTo reduce radar signal latency, ensure use of high-quality transmission mediumTo reduce radar signal latency, ensure use of high-quality transmission mediumTo reduce radar signal bandwidth facuts, ensure ensure use of high-quality transmission mediumTo prevent radar signal bandwidth faults, ensure transmission medium guge is sufficient to handle expected throughput (load) with factor of safetyTo prevent radar signal bandwidth faults, the development team shall ensure the transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyTo reduce radar signal dataTo reduce radar signal noise ensure wires are as short as possibleTo reduce radar signal noise the development team shall ensure the wires are as short as possible		longitudinai motion	requirements	
motionListic power supplied to the radar is within manufacturer operational rangeThe development team shall ensure the understanding of radar signal quality, noise, latency, and bandwidth accounting for measurement and control action errorThe development team shall ensure the understanding of radar signal latency, ensure es of high-quality transmission medium transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyTo prevent radar signal bandwidth faults, ensure faults, the development team shall ensure the transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyTo prevent radar signal bandwidth faults, the development team shall ensure the transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyTo prevent radar signal noise ensure wires are as short as possibleTo reduce radar signal noise the development team shall ensure the winderstanding of time required to analyze and route camera signal noise the development team shall ensure the wires are as short as possibleTo reduce radar signal noise the development team shall ensure the wires are as short as possible		Unintended lateral	Ensure the neuron complicities the	manufacturer operational range
Signal or cyber- security failureEnsure understanding of radar signal quality, noise, latency, and bandwidth accounting for measurement and control action errorThe development team shall ensure the understanding of radar signal quality, noise, latency, and bandwidth accounting for measurement and control action errorTo reduce radar signal latency, ensure use of high-quality transmission mediumTo reduce radar signal latency, ensure use of high-quality transmission mediumTo reduce radar signal latency, ensure use of high-quality transmission mediumTo prevent radar signal bandwidth faults, ensure transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyTo prevent radar signal noise ensure understanding of time required to analyze and route camera signal dataTo reduce radar signal noise ensure wires are as short as possibleTo reduce radar signal noise the development team shall ensure the wires are as short as possible				
Signal or cyber- security failureEnsure understanding of radar signal quality, noise, latency, and bandwidth accounting for measurement and control action errorThe development team shall ensure the understanding of radar signal quality, noise, latency, and bandwidth accounting for measurement and control action errorTo reduce radar signal latency, ensure use of high-quality transmission mediumTo reduce radar signal bandwidth faults, ensure transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyTo prevent radar signal bandwidth faults, ensure transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyTo prevent radar signal noise the development team shall ensure the understanding of time required to analyze and route camera signal dataTo reduce radar signal noise throughput (load) with factor of safetyTo reduce radar signal noise throughput (load) with factor of safetyEnsure understanding of time required to analyze and route camera signal dataTo reduce radar signal noise the development team shall ensure the wires are as short as possible				
security failuresignal quality, noise, latency, and bandwidth accounting for measurement and control action errorunderstanding of radar signal quality, noise, latency, and bandwidth accounting for measurement and control action errorTo reduce radar signal latency, ensure use of high-quality transmission mediumTo reduce radar signal latency, ensure use of high-quality transmission mediumTo reduce radar signal latency, development team shall ensure the use of high-quality transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyTo prevent radar signal bandwidth faults, ensure transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyTo reduce radar signal noise ensure understanding of time required to analyze and route camera signal dataTo reduce radar signal noise the development team shall ensure the wires are as short as possible	Signal an arthur			The development teem shell ensure the
bandwidth accounting for measurement and control action errornoise, latency, and bandwidth accounting for measurement and control action errorTo reduce radar signal latency, ensure use of high-quality transmission mediumTo reduce radar signal latency, teams signal bandwidth faults, ensure transmission mediumTo revent radar signal bandwidth faults, ensure transmission mediumTo prevent radar signal bandwidth faults, ensure transmission mediumTo prevent radar signal bandwidth faults, ensure transmission mediumTo prevent radar signal bandwidth faults, ensure transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyTo prevent radar signal bandwidth faults, the development team shall ensure the transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyTo reduce radar signal noise ensure and route camera signal dataTo reduce radar signal noise ensure wires are as short as possibleTo reduce radar signal noise the development team shall ensure the wires are as short as possible			signal quality noise latency and	
measurement and control action erroraccounting for measurement and control action errorTo reduce radar signal latency, ensure use of high-quality transmission mediumTo reduce radar signal latency, ensure use of high-quality transmission mediumTo reduce radar signal latency, ensure use of high-quality transmission mediumTo reduce radar signal bandwidth faults, ensure transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyTo prevent radar signal of time required to analyze and route camera signal dataTo reduce radar signal noise ensure wires are as short as possibleTo reduce radar signal noise the development team shall ensure the wires are as short as possible	security failure			
erroraction errorTo reduce radar signal latency, ensure use of high-quality transmission mediumTo reduce radar signal latency, development team shall ensure the use of high-quality transmission mediumTo prevent radar signal bandwidth faults, ensure transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyTo prevent radar signal bandwidth faults, the development team shall ensure the transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyTo prevent radar signal bandwidth faults, the development team shall ensure the transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyThe development team shall ensure the understanding of time required to analyze and route camera signal dataTo reduce radar signal noise ensure wires are as short as possibleTo reduce radar signal noise ensure wires are as short as possibleTo reduce radar signal noise the development team shall ensure the wires are as short as possible				
To reduce radar signal latency, ensure use of high-quality transmission mediumTo reduce radar signal latency, the development team shall ensure the use of high-quality transmission mediumTo prevent radar signal bandwidth faults, ensure transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyTo prevent radar signal bandwidth faults, the development team shall ensure the transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyTo prevent radar signal bandwidth faults, the development team shall ensure the transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyTo reduce radar signal dataTo reduce radar signal noise ensure wires are as short as possibleTo reduce radar signal noise the development team shall ensure the wires are as short as possible				
ensure use of high-quality transmission mediumdevelopment team shall ensure the use of high-quality transmission mediumTo prevent radar signal bandwidth faults, ensure transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyTo prevent radar signal bandwidth faults, the development team shall ensure the transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyTo reduce radar signal noise ensure wires are as short as possibleTo reduce radar signal noise the development team shall ensure the wires are as short as possible			enor	
ensure use of high-quality transmission mediumdevelopment team shall ensure the use of high-quality transmission mediumTo prevent radar signal bandwidth faults, ensure transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyTo prevent radar signal bandwidth faults, the development team shall ensure the transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyTo reduce radar signal noise ensure wires are as short as possibleTo reduce radar signal noise the development team shall ensure the wires are as short as possible			To reduce radar signal latency	To reduce radar signal latency, the
transmission mediumof high-quality transmission mediumTo prevent radar signal bandwidth faults, ensure transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyTo prevent radar signal bandwidth faults, the development team shall ensure the transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyEnsure understanding of time required to analyze and route camera signal dataTo reduce radar signal noise ensure wires are as short as possibleTo reduce radar signal noise the development team shall ensure the wires are as short as possible				
To prevent radar signal bandwidth faults, ensure transmission medium gauge is sufficient to handle expected throughput (load) with factor of safety Ensure understanding of time required to analyze and route camera signal data To reduce radar signal noise ensure wires are as short as possible To reduce radar signal noise the				
bandwidth faults, ensure transmission medium gauge is sufficient to handle expected throughput (load) with factor of safety Ensure understanding of time required to analyze and route camera signal data To reduce radar signal noise ensure wires are as short as possible To reduce radar signal noise the development team shall ensure the understanding of time required to analyze and route camera signal data To reduce radar signal noise ensure wires are as short as possible To reduce radar signal noise the				of high quality transmission meanant
bandwidth faults, ensure transmission medium gauge is sufficient to handle expected throughput (load) with factor of safety Ensure understanding of time required to analyze and route camera signal data To reduce radar signal noise ensure wires are as short as possible To reduce radar signal noise the development team shall ensure the understanding of time required to analyze and route camera signal data To reduce radar signal noise ensure wires are as short as possible To reduce radar signal noise the			To prevent radar signal	To prevent radar signal bandwidth
transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyensure the transmission medium gauge is sufficient to handle expected throughput (load) with factor of safetyThe development team shall ensure the understanding of time required to analyze and route camera signal dataThe development team shall ensure the understanding of time required to analyze and route camera signal dataTo reduce radar signal noise ensure wires are as short as possibleTo reduce radar signal noise the development team shall ensure the wires are as short as possible				
sufficient to handle expected throughput (load) with factor of safety Ensure understanding of time required to analyze and route camera signal data To reduce radar signal noise ensure wires are as short as possible To reduce radar signal noise the development team shall ensure the wires are as short as possible To reduce radar signal noise the				
throughput (load) with factor of safetythroughput (load) with factor of safetyThe development team shall ensure the understanding of time required to analyze and route camera signal dataThe development team shall ensure the understanding of time required to analyze and route camera signal dataTo reduce radar signal noise ensure wires are as short as possibleTo reduce radar signal noise the are as short as possibleTo reduce radar signal noise theTo reduce radar signal noise the are as short as possible				
safety The development team shall ensure the understanding of time required to analyze and route camera signal data To reduce radar signal noise ensure wires are as short as possible To reduce radar signal noise the To reduce radar signal noise the development team shall ensure the wires are as short as possible To reduce radar signal noise the To reduce radar signal noise the the development team shall ensure the wires the development team shall ensur				
To reduce radar signal noise the ensure wires are as short as possible To reduce radar signal noise the intervention of the ensure the wires are as short as possible To reduce radar signal noise the intervention of the team shall ensure the wires are as short as possible To reduce radar signal noise the intervention of the team shall ensure the wires are as short as possible To reduce radar signal noise the intervention of the team shall ensure the wires are as short as possible To reduce radar signal noise the intervention of the team shall ensure the wires are as short as possible To reduce radar signal noise the intervention of the team shall ensure the wires are as short as possible the intervention of the team shall ensure the wires are as short as possible the intervention of the team shall ensure the wires are as short as possible the intervention of the team shall ensure the wires are as short as possible the intervention of the team shall ensure the wires are as short as possible the intervention of the team shall ensure the wires are as short as possible the intervention of the team shall ensure the wires are as short as possible the intervention of the team shall ensure the wires are as short as possible the intervention of the team shall ensure the wires are as short as possible the intervention of the team shall ensure the wires are as short as possible the intervention of the team shall ensure the wires are as short as possible the intervention of team shall ensure the wires are as short as possible the intervention of team shall ensure the wires are as short as possible the intervention of team shall ensure the wires are as short as possible the intervention of team shall ensure the wires are as short as possible the intervention of team shall ensure the wires are as short as possible the intervention of team shall ensure the wires are as short as possible the intervention of team shall ensure the wires are as short as possible the team shall ensure the wires are as short as possible the team sha				3 r ··· (···· ··· ··· ··· ··· ··· ··· ··· ···
Ensure understanding of time understanding of time required to required to analyze and route camera signal data To reduce radar signal noise the development team shall ensure the wires ensure wires are as short as possible To reduce radar signal noise the To reduce radar signal noise the are as short as possible To reduce radar signal noise the				The development team shall ensure the
required to analyze and route camera signal data To reduce radar signal noise ensure wires are as short as possible To reduce radar signal noise the development team shall ensure the wires are as short as possible To reduce radar signal noise the			Ensure understanding of time	
camera signal data To reduce radar signal noise the the the the the the the the the the				
To reduce radar signal noise ensure wires are as short as possible To reduce radar signal noise the development team shall ensure the wires are as short as possible To reduce radar signal noise the				
To reduce radar signal noise ensure wires are as short as possible To reduce radar signal noise are as short as possible To reduce radar signal noise the				To reduce radar signal noise the
ensure wires are as short as possible possible To reduce radar signal noise the			To reduce radar signal noise	
possible To reduce radar signal noise the				
To reduce radar signal noise the			possible	·
				To reduce radar signal noise the
development team shart ensure the writes				development team shall ensure the wires
are kept away from electrical machinery				are kept away from electrical machinery

To reduce radar signal noise	
	ar signal noise it is the
	eam shall ensure the to use
twisted togeth	
To reduce radar signal noise it is	
recommended to use twisted To reduce inte	rnal radar signal noise the
	eam shall ensure the s on amplifiers are
To reduce internal radar signal minimized	•
noise ensure thermal effects on	
amplifiers are minimized To reduce rad	ar signal noise, if possible,
	ent team shall ensure the
	lwidth matches input
possible, ensure amplifier signal bandwi	
bandwidth matches input signal	
	ar signal noise the
	eam shall ensure the use
	ring techniques
ensure use of proper filtering	
	ar signal noise the
	eam shall ensure the use
	ing and conduit
ensure use of wire shielding and	6
	ar signal noise the
	eam shall ensure the
	of ground loops and
	grounding practices
loops and impose proper	
	ent team shall ensure the
	of potential radar signal
Ensure understanding of potential storage delays	
radar signal storage delays	
	ent team shall ensure the
	e safety and that the radar
	rom external unintended
from external unintended malicious com	
malicious control	
	ent team shall ensure the
	re updates are performed
	and not through the air

	Ensure system software updates are performed over land-line and not through the air	
Capability limitations Failure of field of	To prevent field of view failure ensure radar is mounted such that the signal projects unimpeded	To prevent field of view failure The development team shall ensure the radar is mounted such that the signal projects unimpeded
Failure of field of view Adverse environmental conditions (dark, fog, poorly painted or no lane lines)	 Ensure radar is of high-quality to maintain operations during low-light, poorly painted lane lines, and adverse weather conditions Ensure radar indicates to computer and operator when the system is unavailable Ensure integrated program accounts for radar horizontal field of view and elevation (±6° (160m), ±6°(100m), ±10°(60m), ±25°(36m), ±42°(12m)) Ensure integrated program accounts for radars speed, distance, and angle measurement accuracy (0.11 m/s, 0.12 m, ±0,3°) Ensure integrated program accounts for radars speed, distance, and angle object separation capability (0.72 m/s, 0.66 0m, ±7°) 	unimpeded The development team shall ensure the radar is of high-quality to maintain operations during low-light, poorly painted lane lines, and adverse weather conditions The development team shall ensure the radar indicates to computer and operator when the system is unavailable The development team shall ensure the integrated program accounts for radar horizontal field of view and elevation $(\pm 6^{\circ} (160m), \pm 6^{\circ}(100m), \pm 10^{\circ}(60m), \pm 25^{\circ}(36m), \pm 42^{\circ}(12m))$ The development team shall ensure the integrated program accounts for radars speed, distance, and angle measurement accuracy (0.11 m/s, 0.12 m, $\pm 0.3^{\circ}$) The development team shall ensure the integrated program accounts for radars speed, distance, and angle object separation capability (0.72 m/s, 0.66 0m,
	Ensure integrated program accounts for radars cycle time (60 ms)	±7°) The development team shall ensure the integrated program accounts for radars cycle time (60 ms)

	Ensure integrate accounts for rad modulation	ars frequency integ	development team shall ensure the grated program accounts for radars hency modulation
	Ensure integrate accounts for rad number of detec	ars maximum integ	development team shall ensure the grated program accounts for radars imum number of detectable objects

Item: Intel Movidius Neural Compute Stick

			Corrective/Preventative	
Potential Hazard	Cause	Major Effect	Measure	Functional Requirement
Failure to perform vision	Power failure		Ensure compute stick is securely	The development team shall ensure the
processing tasks in assistance			input to the computer	compute stick is securely input to the
to Intel Tank computational				computer
capabilities	Algorithm, NN,		Ensure compute stick NN model	The development team shall ensure the
	computational, or		thoroughly defined and highly	compute stick NN model thoroughly
Failure to assist in blending	cyber-security		sensitive to small variations in	defined and highly sensitive to small
various sensors (cameras,	failure		inputs	variations in inputs
radars) data to achieve				
reliable, high-definition			Ensure compute stick NN is	The development team shall ensure the
images			thoroughly tested and validate	compute stick NN is thoroughly tested
			prior to implementation	and validate prior to implementation
Failure to assist in				
performing sensor fusion			Ensure compute stick NN	The development team shall ensure the
data verification & validation			imposes limits on output to not	compute stick NN imposes limits on
			exceed boundaries	output to not exceed boundaries
Failure to assist in				
determining if control action			Ensure compute stick NNs use of	The development team shall ensure the
(EPS torque, braking,			hidden layers and neurons does	compute stick NNs use of hidden layers
feedback) is required			not over-fit training data and is	and neurons does not over-fit training
			sufficient to fit new and unseen	data and is sufficient to fit new and
			data	unseen data
			Ensure compute stick program	The development team shall ensure the
			code is thoroughly vetted (Auto	compute stick program code is
				thoroughly vetted (Auto industry

industry standard is one defect per 1000 executable lines of code) standard is one defect per 1000 executable lines of code)
Ensure compute stick program is developed using automotive coding standards The development team shall ensure the using automotive coding standards
Ensure use of multiple software scanning tools to identify vulnerability and error in compute stick program code (industry uses Jarvis which analyses the binary executable action and not the mistakes in the code) The development team shall ensure the use of multiple software scanning tools to identify vulnerability and error in compute stick program code (industry uses Jarvis which analyses the binary executable action and not the mistakes in the code)
Ensure control of computational overflow and compounding rounding errors The development team shall ensure the control of computational overflow and compounding rounding errors
Ensure understanding of compute stick input and output signal quality, noise, latency, and bandwidth accounting for measurement and control action error
Ensure understanding of time required to analyze and route computer signal data
To reduce compute stick signal input and output noise ensure use of proper filtering techniques To reduce compute stick signal input and output noise the development team shall ensure the use of proper filtering techniques
Ensure understanding of potential compute stick signal input and output storage delays The development team shall ensure the understanding of potential compute stick signal input and output storage delays
Ensure the use of software safety and that the system is free fromThe development team shall ensure the use of software safety and that the

	external unintended malicious control	system is free from external unintended malicious control
System software	Ensure compute stick is capable	The development team shall ensure the
requirements not	of storing and processing the	compute stick is capable of storing and
met	expected amount of data with a	processing the expected amount of data
	factor of safety	with a factor of safety
	To prevent memory failure ensure program is developed such that information that is too large cannot be written into a memory buffer that is too small to contain it	To prevent memory failure the development team shall ensure the program is developed such that information that is too large cannot be written into a memory buffer that is too small to contain it
	Ensure compute stick and computer interface is compatible Ensure computer free storage	The development team shall ensure the compute stick and computer interface is compatible
	space is available to allow compute stick to operate	The development team shall ensure the computer free storage space is available to allow compute stick to operate

Item: KVaser

			Corrective/Preventative	
Potential Hazard	Cause	Major Effect	Measure	Functional Requirement
Failure to interface CAN	Unintended access		Ensure KVaser manufacturing	The development team shall ensure
signals to USB	or physical damage		and installation is sufficient to	KVaser manufacturing and installation is
	(liquid, puncture)		prevent unintended access and	sufficient to prevent unintended access
			physical damage	and physical damage to the computer
			Ensure use of covering at KVaser	To prevent unintended access and
			interfaces to prevent unintended	physical damage the development team
			access	shall ensure use of coverings at KVaser
				interfaces
			Avoid adverse road condition	
			which may produce NVH and	To prevent physical damage to the
			damage KVaser or loosen	KVaser the operator shall avoid adverse
			interfaces	road condition which may produce NVH

	Ensure KVaser installation is inside cabin in a dry debris-proof location	To prevent unintended access and physical damage the development team shall ensure KVaser installation is inside cabin in a dry debris-proof location
	Ensure KVaser is inaccessible by	
	passengers	To prevent unintended access and physical damage the development team shall ensure KVaser is inaccessible by passengers
Software failure	Ensure KVaser functionality prior to open-road operation	The development team shall ensure KVaser functionality prior to open-road operation
Capacity failure	Ensure the KVaser is capable of processing the expected amount pf data with a factor of safety	The development team shall ensure the KVaser is capable of processing the expected amount pf data with a factor of safety

Item: Niles Camera Monitoring Operator

			Corrective/Preventative	
Potential Hazard	Cause	Major Effect	Measure	Functional Requirement
Failure to perform real-time	Wiring failure (not	Failure of CAVs	Ensure Niles camera wiring is	The development team shall ensure the
monitoring of operator	proper gauge,	functionality	securely installed using	Niles camera wiring is securely installed
	installation or		manufacturer installation	using manufacturer installation
Failure to send data to	manufacturing	Computer, if	specifications	specifications
associated controller	failure)	operational, operates		
		on single point source	Ensure Niles camera wiring	The development team shall ensure the
		information	gauge is sufficient to carry max	Niles camera wiring gauge is sufficient
			operational current with factor of	to carry max operational current with
		Operator unaware of	safety	factor of safety
		system failure		
		x 11.1.1 .	Ensure Niles camera wire bend	The development team shall ensure the
		Less reliable image to	radii are adhered to	Niles camera wire bend radii are adhered
		which the computer		to
		can determine	Ensure Niles camera alerts	
			computer that system failure has	
			occurred	

Unintended access	deviations and control	Ensure Niles camera	The development team shall array (1)
or physical damage	actions and control	manufacturing and installation is	The development team shall ensure the Niles camera manufacturing and
(liquid, puncture)	actions		installation is sufficient to prevent
(inquia, puncture)	Unintended	sufficient to prevent unintended	unintended access and physical damage
	longitudinal motion	access and physical damage	unintended access and physical damage
	C	Ensure Niles camera is placed	The development team shall ensure the
	Unintended lateral motion	inside cabin and top-center of wind shield within operational area of windshield wipers	Niles camera is placed inside cabin and top-center of wind shield within operational area of windshield wipers
		area or windshield wipers	T T T T T T T T T T T T T T T T T T T
		Ensure use of covering at wire- Niles camera interface to prevent unintended access	The development team shall ensure the use of covering at wire- Niles camera interface to prevent unintended access
		Avoid adverse road condition which may produce NVH and damage Niles camera	The development team shall ensure the Niles camera installation is inside cabin in a dry debris-proof location
		Ensure Niles camera installation is inside cabin in a dry debris- proof location	The operator shall avoid adverse road conditions which may produce NVH and damage the camera
Power failure		See wiring and unintended access requirements	The development team shall ensure the power supplied to the Niles camera is within manufacturer recommended
		Ensure the power supplied to the Niles camera is within manufacturer operational range	operational range
Signal or cyber-		Ensure understanding of Niles	The development team shall ensure an
security failure		camera signal quality, noise, latency, and bandwidth accounting for measurement and control action error	understanding of Niles camera signal quality, noise, latency, and bandwidth accounting for measurement and control action error
		To reduce Niles camera signal latency, ensure use of high-	To reduce Niles camera signal latency the development team shall ensure the
		quality transmission medium	use of a high-quality transmission medium
		To prevent Niles camera signal bandwidth faults, ensure transmission medium gauge is	To prevent Niles camera signal bandwidth faults the development team

sufficient to handle expected	shall ensure the transmission medium
throughput (load) with factor of	gauge is sufficient to handle expected
safety	throughput (load) with factor of safety
Ensure understanding of time	The development team shall ensure an
required to analyze and route	understanding of time required to
Niles camera signal data	analyze and route Niles camera signal data
To reduce Niles camera signal	
noise ensure wires are as short as	To reduce Niles camera signal noise the
possible	development team shall ensure the wires are as short as possible
To reduce Niles camera signal	
noise ensure wires are kept away	To reduce Niles camera signal noise the
from electrical machinery	development team shall ensure the wires are kept away from electrical machinery
To reduce Niles camera signal	
noise it is recommended to use	To reduce Niles camera signal noise it is
twisted together wires	recommended to use twisted together wires
To reduce internal Niles camera	
signal noise ensure thermal	To reduce internal Niles camera signal
effects on amplifiers are minimized	noise the development team shall ensure the thermal effects on amplifiers are
mmmzed	minimized
To reduce Niles camera signal	
noise, if possible, ensure	To reduce Niles camera signal noise, if
amplifier bandwidth matches	possible, the development team shall
input signal bandwidth	ensure the amplifier bandwidth matches input signal bandwidth
To reduce Niles camera signal	
noise ensure use of proper	To reduce Niles camera signal noise the
filtering techniques	development team shall ensure the use of proper filtering techniques
To reduce Niles camera signal	
noise ensure use of wire shielding	To reduce Niles camera signal noise the
and conduit	development team shall ensure the use
	of wire shielding and conduit
To reduce Niles camera signal	
noise ensure understanding of	

		ground loops and impose proper	To reduce Niles camera signal noise the
		grounding practices	development team shall ensure the
			understanding of ground loops and
		Ensure understanding of potential	impose proper grounding practices
		Niles camera signal storage	
		delays	The development team shall ensure
			understanding of potential Niles camera
		Ensure the use of software safety	signal storage delays
		and that the Niles camera signal is	
		free from external unintended	The development team shall ensure the
		malicious control	use of software safety and that the Niles
			camera signal is free from external
		Ensure system software updates	unintended malicious control
		are performed over land-line and	
		not through the air	The development team shall ensure
			system software updates are performed
			over land-line and not through the air
Caj	pability	To prevent field of view failure	To prevent field of view failure the
lim	nitations	ensure Niles camera is mounted	development team shall ensure the
		in the location free of obstruction	camera is mounted in a location free of
Fai	ilure of field of		obstruction
vie	ew	Ensure camera is of high-quality	
		to maintain operations during	The development team shall ensure the
Ad	lverse	low-light	camera is of high-quality to maintain
env	vironmental		operations during low-light
cor	nditions (dark,	Ensure Niles camera indicates to	
	g, poorly painted	computer and operator when the	The development team shall ensure the
or	no lane lines)	system is unavailable	Niles camera indicates to computer and
			operator when the system is unavailable
tem: Real-Time Display			
ion. Real-Thic Display			
			1

			Corrective/Preventative	
Potential Hazard	Cause	Major Effect	Measure	Functional Requirement
Failure to acquire sensor	Wiring failure (not		Ensure display wiring is securely	The development team shall ensure the
fusion data from associated	proper gauge,		installed using manufacturer	display wiring is securely installed using
controller	installation or		installation specifications	manufacturer installation specifications
	manufacturing		L.	
Failure to display sensors	failure)		Ensure display wiring gauge is	The development team shall ensure the
fusion images in real-time			sufficient to carry max	display wiring gauge is sufficient to

	an another all assume that the for the for	
	operational current with factor of	carry max operational current with factor
	safety	of safety
	Ensure display wire bend radii are	The development team shall ensure the
	adhered to	display wire bend radii are adhered to
		display wire bend fault are adhered to
	Ensure display alters computer	
	that system failure has occurred	
Unintended access	Ensure display manufacturing and	The development team shall ensure the
or physical damage	installation is sufficient to prevent	camera manufacturing and installation is
(liquid, puncture)	unintended access and physical	sufficient to prevent unintended access
	damage	and physical damage
	C C	
	Ensure display is placed inside	The development team shall ensure the
	cabin within view of operator	display is placed inside cabin within
		view of the operator
	Ensure use of covering at wire-	
	display interface to prevent	The development team shall ensure the
	unintended access	use of covering at wire- display interface
	Avoid adverse road condition	to prevent unintended access
	which may produce NVH and	The development team shall ensure the
	damage or loosen display	display installation is inside cabin in a
		dry debris-proof location
	Ensure display installation is	ary deons-proof location
	inside cabin in a dry debris-proof	The operator shall avoid adverse road
	location	conditions which may produce NVH and
		damage or loosen the display
Power failure	See wiring and unintended access	The development team shall ensure the
	requirements	power supplied to the display is within
	_	manufacturer recommended operational
	Ensure the power supplied to the	range
	display is within manufacturer	
	operational range	
Signal or cyber-	Ensure understanding of display	The development team shall ensure an
security failure	signal quality, noise, latency, and	understanding of display signal quality,
	bandwidth accounting for	noise, latency, and bandwidth
	measurement and control action	accounting for measurement and control
	error	action error

To reduce display signal latency,	To reduce display signal latency the
ensure use of high-quality	development team shall ensure the use
transmission medium	of a high-quality transmission medium
	or a high quarty transmission moutum
To prevent display signal	To prevent display signal bandwidth
bandwidth faults, ensure	faults the development team shall ensure
transmission medium gauge is	the transmission medium gauge is
sufficient to handle expected	sufficient to handle expected throughput
throughput (load) with factor of	(load) with factor of safety
safety	
	The development team shall ensure an
Ensure understanding of time	understanding of time required to
required to analyze and route	analyze and route display signal data
display signal data	
	To reduce display signal noise the
To reduce display signal noise	development team shall ensure the wires
ensure wires are as short as	are as short as possible
possible	
	To reduce display signal noise the
To reduce display signal noise	development team shall ensure the wires
ensure wires are kept away from	are kept away from electrical machinery
electrical machinery	
	To reduce display signal noise it is
To reduce display signal noise it	recommended to use twisted together
is recommended to use twisted	wires
together wires	
	To reduce internal display signal noise
To reduce internal display signal	the development team shall ensure the
noise ensure thermal effects on	thermal effects on amplifiers are
amplifiers are minimized	minimized
To reduce display signal noise, if	To reduce display signal noise, if
possible, ensure amplifier	possible, the development team shall
bandwidth matches input signal	ensure the amplifier bandwidth matches
bandwidth	input signal bandwidth
To reduce display signal noise	To reduce display signal noise the
ensure use of proper filtering	development team shall ensure the use
techniques	of proper filtering techniques

To reduce display signal noise ensure use of wire shielding and conduit	To reduce display signal noise the development team shall ensure the use of wire shielding and conduit
To reduce display signal noise ensure understanding of ground loops and impose proper grounding practices	To reduce display signal noise the development team shall ensure the understanding of ground loops and impose proper grounding practices
Ensure the use of software safety and that the display signal is free from external unintended malicious control	The development team shall ensure the use of software safety and that the display signal is free from external unintended malicious control
Ensure system software updates are performed over land-line and not through the air	The development team shall ensure display system software updates are performed over land-line and not through the air

Item: ZED Camera

			Corrective/Preventative	
Potential Hazard	Cause	Major Effect	Measure	Functional Requirement
Failure to perform high-	Wiring failure (not	Failure of CAVs	Ensure ZED camera wiring is	The development team shall ensure the
resolution depth perception	proper gauge,	functionality	securely installed using	ZED camera wiring is securely installed
	installation or	-	manufacturer installation	using manufacturer installation
Failure to perform 6-axis	manufacturing	Computer, if	specifications	specifications
positional tracking to sense	failure)	operational, operates	specifications	L
space and motion	, ,	on single point source	Ensure ZED camera wiring gauge	The development team shall ensure the
		information	is sufficient to carry max	ZED camera wiring gauge is sufficient
Failure to perform large-scale		mornation	operational current with factor of	to carry max operational current with
3D mapping		Operator unaware of	safety	factor of safety
		system failure	Survey	
		5	Ensure ZED camera wire bend	The development team shall ensure the
		Less reliable image to	radii are adhered to	ZED camera wire bend radii are adhered
		which the computer		to
		can determine	Ensure ZED camera alters	
		deviations and control	computer that system failure has	
		actions	occurred	
	Power failure		See wiring and unintended access	The development team shall ensure the
			requirements	power supplied to the ZED camera is

	Unintended		within manufacturer recommended
	longitudinal motion	Ensure the power supplied to the	operational range
	XX	ZED camera is within	
	Unintended lateral	manufacturer operational range	
Signal or cyber- security failure	motion	Ensure understanding of ZED camera signal quality, noise, latency, and bandwidth accounting for measurement and control action error	The development team shall ensure an understanding of ZED camera signal quality, noise, latency, and bandwidth accounting for measurement and control action error
		To reduce ZED camera signal latency, ensure use of high- quality transmission medium	To reduce ZED camera signal latency the development team shall ensure the use of a high-quality transmission medium
		To prevent ZED camera signal bandwidth faults, ensure	To prevent ZED camera signal
		transmission medium gauge is sufficient to handle expected throughput (load) with factor of safety	bandwidth faults the development team shall ensure the transmission medium gauge is sufficient to handle expected throughput (load) with factor of safety
		salety	unoughput (load) with factor of safety
		Ensure understanding of time	The development team shall ensure an
		required to analyze and route ZED camera signal data	understanding of time required to analyze and route ZED camera signal data
		To reduce ZED camera signal	
		noise ensure wires are as short as possible	To reduce ZED camera signal noise the development team shall ensure the wires are as short as possible
		To reduce ZED camera signal	
		noise ensure wires are kept away from electrical machinery	To reduce ZED camera signal noise the development team shall ensure the wires are kept away from electrical machinery
		To reduce ZED camera signal	······································
		noise it is recommended to use	To reduce ZED camera signal noise it is
		twisted together wires	recommended to use twisted together wires
		To reduce internal ZED camera	
		signal noise ensure thermal	To reduce internal ZED camera signal noise the development team shall ensure

	effects on amplifiers are minimized	the thermal effects on amplifiers are minimized
	To reduce ZED camera signal noise, if possible, ensure amplifier bandwidth matches input signal bandwidth	To reduce ZED camera signal noise, if possible, the development team shall ensure the amplifier bandwidth matches input signal bandwidth
	To reduce ZED camera signal noise ensure use of proper filtering techniques	To reduce ZED camera signal noise the development team shall ensure the use of proper filtering techniques
	To reduce ZED camera signal noise ensure use of wire shielding and conduit	To reduce ZED camera signal noise the development team shall ensure the use of wire shielding and conduit
	To reduce ZED camera signal noise ensure understanding of ground loops and impose proper grounding practices	To reduce ZED camera signal noise the development team shall ensure the understanding of ground loops and impose proper grounding practices
	Ensure understanding of potential ZED camera signal storage delays	The development team shall ensure understanding of potential ZED camera signal storage delays
	Ensure the use of software safety and that the ZED camera signal is free from external unintended malicious control	The development team shall ensure the use of software safety and that the ZED camera signal is free from external unintended malicious control
	Ensure system software updates are performed over land-line and not through the air	The development team shall ensure system software updates are performed over land-line and not through the air
Capability limitations	To prevent field of view failure ensure ZED camera is mounted in the operational area of the wind	To prevent field of view failure the development team shall ensure the ZED camera is mounted in the operational
Failure of field of view	shield wipers	area of the wind shield wipers
	To prevent field of view failure ensure ZED camera has control of	To prevent field of view failure the development team shall ensure the ZED

	Adverse environmental conditions (dark, fog, poorly painted or no lane lines)		 wind shield wipers (debris may impede camera view while operator is unaware) Ensure ZED camera is of high-quality to maintain operations during low-light, poorly painted lane lines, and adverse weather conditions Ensure ZED camera indicates to computer and operator when the system is unavailable 	camera has control of wind shield wipers (debris may impede camera view while operator is unaware) The development team shall ensure the ZED camera is of high-quality to maintain operations during low-light, poorly painted lane lines, and adverse weather conditions The development team shall ensure the camera indicates to computer and operator when the system is unavailable
Item: GPS Potential Hazard	Cause	Major Effect	Corrective/Preventative Measure	Functional Requirement
Failure to receive GPS data Failure to provide GPS data to associated controller	Wiring failure (not proper gauge, installation or manufacturing failure)		IntersureEnsure GPS wiring is securely installed using manufacturer installation specificationsEnsure GPS wiring gauge is sufficient to carry max operational current with factor of safetyEnsure GPS wire bend radii are adhered toEnsure GPS alters computer that	The development team shall ensure the GPS wiring is securely installed using manufacturer installation specifications The development team shall ensure the GPS wiring gauge is sufficient to carry max operational current with factor of safety The development team shall ensure the GPS wire bend radii are adhered to

damage

Unintended access

or physical damage (liquid, puncture) system failure has occurred Ensure GPS manufacturing and

installation is sufficient to prevent unintended access and physical The development team shall ensure the GPS manufacturing and installation is sufficient to prevent unintended access,

loosening, and physical damage

	I	Ensure use of coursing a standard	The development to a set 1, 11, set of 4
		Ensure use of covering at wire-	The development team shall ensure the
		GPS interface to prevent	use of covering at wire-GPS interface to
		unintended access	prevent unintended access
		Avoid adverse road condition	The operator shall avoid adverse road
		which may produce NVH and	
		• 1	conditions which may produce NVH and
	D (1)	damage or loosen the GPS	damage or loosen the GPS
	Power failure	See wiring and unintended access	The development team shall ensure the
		requirements	power supplied to the GPS is within
			manufacturer recommended operational
		Ensure the power supplied to the	range
		GPS is within manufacturer	
	~	operational range	
	Signal or cyber-	Ensure understanding of GPS	The development team shall ensure an
	security failure	signal quality, noise, latency, and	understanding of GPS signal quality,
		bandwidth accounting for	noise, latency, and bandwidth
		measurement and control action	accounting for measurement and control
		error	action error
		To reduce GPS signal latency,	To reduce GPS signal latency the
		ensure use of high-quality	development team shall ensure the use
		transmission medium	of a high-quality transmission medium
		To prevent GPS signal bandwidth	To prevent GPS signal bandwidth faults
		faults, ensure transmission	the development team shall ensure the
		medium gauge is sufficient to	transmission medium gauge is sufficient
		handle expected throughput (load)	to handle expected throughput (load)
		with factor of safety	with factor of safety
		-	-
		Ensure understanding of time	The development team shall ensure an
		required to analyze and route GPS	understanding of time required to
		signal data	analyze and route GPS signal data
		-	
		To reduce GPS signal noise	To reduce GPS signal noise the
		ensure wires are as short as	development team shall ensure the wires
		possible	are as short as possible
		1	L ·
		To reduce GPS signal noise	To reduce GPS signal noise the
		ensure wires are kept away from	development team shall ensure the wires
		electrical machinery	are kept away from electrical machinery
L I			

[]		
	To reduce GPS signal noise it is recommended to use twisted together wires	To reduce GPS signal noise it is recommended to use twisted together wires
	To reduce internal GPS signal noise ensure thermal effects on amplifiers are minimized	To reduce internal GPS signal noise the development team shall ensure the thermal effects on amplifiers are minimized
	To reduce GPS signal noise, if possible, ensure amplifier bandwidth matches input signal bandwidth	To reduce GPS signal noise, if possible, the development team shall ensure the amplifier bandwidth matches input signal bandwidth
	To reduce GPS signal noise	
	ensure use of proper filtering techniques	To reduce GPS signal noise the development team shall ensure the use of proper filtering techniques
	To reduce GPS signal noise ensure use of wire shielding and conduit	To reduce GPS signal noise the development team shall ensure the use of wire shielding and conduit
	To reduce GPS signal noise	_
	ensure understanding of ground loops and impose proper grounding practices	To reduce GPS signal noise the development team shall ensure the understanding of ground loops and impose proper grounding practices
	Ensure understanding of potential GPS signal storage delays	The development team shall ensure understanding of potential GPS signal
	Ensure the use of software safety and that the GPS signal is free	storage delays
	from external unintended malicious control	The development team shall ensure the use of software safety and that the GPS signal is free from external unintended malicious control
Capability limitations	Ensure GPS is of high-quality to maintain operations during low- light, poorly painted lane lines, and adverse weather conditions	The development team shall ensure the GPS is of high-quality to maintain operations during low-light, poorly

Failure of field of			painted lane lines, and adverse weather
view		Ensure GPS indicates to computer	conditions
		and operator when the system is	
Adverse		unavailable	The development team shall ensure the
environmental			GPS indicates to computer and operator
conditions (dark,			when the system is unavailable
fog, poorly painte	1		
or no lane lines)			

Appendix 3.05 HARA CSMS DFMEA

CSMS DMFEA										
Item: HSC										
Function	Failure Type	Potential Impact	S	Potential Cause	0	Prevention Mode	Detection Mode	D	RPN	Functional Requirement
Control all hybrid functions Torque control via engine/EM torque split using a variety of control strategies Maintain SOC at appropriate level Control gear shifting Modify stock	Failure to control all hybrid functions Failure to control engine/EM torque split Failure to maintain SOC at appropriate level	Unintended acceleration Unintended longitudinal motion Loss or degradation of propulsion system Operator and/or passenger injury	10	Wiring failure (not proper gauge, installation or manufacturing failure)	7	Ensure wiring is securely installed using manufacturer installation specifications Ensure wiring gauge is sufficient to carry max operational current with factor of safety Ensure wire bend radii are	Vehicle technical inspection will identify wiring fatigue or failure Operator aware during operation by identifying eventual failure of vehicle components	8	560	To avoid HSC wiring failure the development team shall ensure wiring is securely installed using manufacturer installation specifications To avoid HSC wiring failure the development team shall ensure wiring gauge is sufficient to carry max operational current with factor of safety

Failure to control gear shifting Failure to modify stock signals	Damage to or loss of property Damage to environment							To avoid HSC wiring failure the development team shall ensure wire bend radii are adhered to and wiring is protected from heat sources
	Potential for overheating Unintended exposure to high voltage	Unintended access or physical damage (liquid, puncture)	5	Ensure manufacturing is sufficient to prevent unintended access and physical damage Ensure use of covering at wire-HSC interface to prevent unintended access Avoid adverse road condition which may produce NVH and damage the HSC	Vehicle technical inspection will identify if the HSC is free of unintended access Operator aware during operation by identifying eventual failure of vehicle components and loss of functionality	9	450	To avoid HSC unintended access or physical damage the development team shall ensure proper mounting, installation, and manufacturing of the HSC To avoid HSC unintended access or physical damage the development team shall ensure use of covering at wire-HSC interface To avoid HSC unintended access or physical damage the operator shall avoid adverse road conditions which may produce NVH
		Installation failure (wire, mounting)	7	Ensure HSC and mounting hardware are sufficient for max operational G- force with factor of safety	Vehicle technical inspection will identify if HSC is free of manufacturing or installation fatigue or failure	8	560	To avoid HSC installation failure the development team shall ensure the mounting hardware are sufficient for max operational G-force with factor of safety

		Ensure HSC and mounting hardware are secure and free from potential lessening or unintended movement	Operator aware during operation by identifying eventual failure of vehicle components and loss of functionality			To avoid HSC installation failure the development team shall ensure the mounting hardware is secure and free from potential lessening or unintended movement
Over-current	7	Ensure software limits current rates and ranges Ensure relays and fuses are in place and functional to prevent over drawing of current	Operator aware during operation by error signal and identifying eventual failure of vehicle components and loss of functionality	7	490	To avoid HSC over- current failure the development team shall ensure software limits current ranges To avoid HSC over- current failure the development team shall ensure relays and fuses are in place and functional
Over-heating	4	Ensure HSC is mounted such that there is proper clearance and sufficient air flow to cool the HSC	Vehicle technical inspection will identify if the HSC has proper clearance to allow for natural air flow cooling Operator aware during operation by identifying eventual failure of vehicle components	9	360	To avoid HSC over- heating failure the development team shall ensure the HSC is mounted such that there is proper clearance and sufficient air flow to cool the HSC

r		ſ	1		-	Γ		1	1		
							and loss of				
							functionality				
Item: ECM											
	Failure	Potential				Prevention	Detection			Functional	
Function	Туре	Impact	S	Potential Cause	0	Mode	Mode	D	RPN	Requirement	
Control engine	Failure to	Unintended	10	Wiring failure	7	Ensure wiring	Vehicle	8	560	To avoid ECM wiring	
torque output	control	acceleration		(not proper gauge,		is securely	technical			failure the	
	engine torque			installation or		installed using	inspection will			development team	
Control engine	output	Unintended		manufacturing		manufacturer	identify wiring			shall ensure wiring is	
temperature		longitudinal		failure)		installation	fatigue or			securely installed	
	Failure to	motion				specifications	failure			using manufacturer	
Control A/F	control									installation	
ratio	engine	Loss or				Ensure wiring	Operator aware			specifications	
	temperature	degradation of				gauge is	during				
Control idle	F 11	propulsion				sufficient to	operation by			To avoid ECM wiring	
speed	Failure to control A/F	system				carry max	identifying eventual failure			failure the	
Control	ratio	Omeneten				operational current with	of vehicle			development team shall ensure wiring	
electronic valve	ratio	Operator and/or				factor of safety				gauge is sufficient to	
electronic valve	Failure to	passenger				factor of safety	components			carry max operational	
	control idle	injury				Ensure wire				current with factor of	
	speed	nijury				bend radii are				safety	
	speed	Damage to or				adhered to				safety	
	Failure to	loss of				udifered to				To avoid ECM wiring	
	control	property								failure the	
	electronic	property								development team	
	valve	Damage to								shall ensure wire bend	
		environment								radii are adhered to	
										and wiring is protected	
		Potential for								from heat sources	
		overheating		Unintended	5	Ensure	Vehicle	9	450	To avoid ECM	
				access or physical		manufacturing	technical			unintended access or	
				damage (liquid,		is sufficient to	inspection will			physical damage the	
				puncture)		prevent	identify if the			development team	
						unintended	ECM is free of			shall ensure proper	
						access and	unintended			mounting, installation,	
						physical	access and			and manufacturing of	
						damage	physical			the ECM	
							damage				

		Ensure use of covering at wire-ECM interface prevent unintended access Avoid adverse road condition which may produce NVH and damage ECM	Operator aware during operation by identifying eventual failure of vehicle components and loss of functionality			To avoid ECM unintended access or physical damage the development team shall ensure use of covering at wire-ECM interface To avoid ECM unintended access or physical damage the operator shall avoid adverse road conditions which may produce NVH
Installation failure (wire, mounting)	7	Ensure ECM and mounting hardware are sufficient for max operational G- force with factor of safety Ensure ECM and mounting hardware are secure and free from unintended movement	Vehicle technical inspection will identify if ECM is free of manufacturing or installation fatigue or failure Operator aware during operation by identifying eventual failure of vehicle components and loss of functionality	8	560	To avoid ECM installation failure the development team shall ensure the mounting hardware are sufficient for max operational G-force with factor of safety To avoid ECM installation failure the development team shall ensure the mounting hardware is secure and free from potential lessening or unintended movement
Over-current	7	Ensure software limits current rates and ranges	Operator aware during operation by error signal and identifying	7	490	To avoid ECM over- current failure the development team shall ensure software limits current ranges

				Over-heating	2	Ensure relays and fuses are in place and functional to prevent over drawing of current Ensure ECM is mounted such that there is proper clearance and sufficient air flow to cool the ECM	eventual failure of vehicle components and loss of functionality Vehicle technical inspection will identify if the ECM has proper clearance to allow for natural air flow cooling Operator aware during operation by identifying eventual failure of vehicle components and loss of functionality	9	180	To avoid ECM over- current failure the development team shall ensure relays and fuses are in place and functional To avoid ECM over- heating failure the development team shall ensure the ECM is mounted such that there is proper clearance and sufficient air flow to cool the ECM
Item: TCM	D 1					D (*		[
Function	Failure Type	Potential Impact	S	Potential Cause	0	Prevention Mode	Detection Mode	D	RPN	Functional Requirement
Control gear	Failure to	Unintended	9	Wiring failure	7	Ensure wiring	Vehicle	8	5004	To avoid TCM wiring
shifting	control gear	longitudinal		(not proper gauge,		is securely	technical			failure the
Control	shifting	motion		installation or		installed using	inspection will			development team
Control	Esiluma ta	Lassar		manufacturing		manufacturer	identify wiring			shall ensure wiring is
transmission	Failure to	Loss or		failure)		installation	fatigue or			securely installed
temperature	control	degradation of				specifications	failure			using manufacturer
	transmission	propulsion				En anna antinir a	On english and and			installation
	temperature	system				Ensure wiring	Operator aware			specifications
						gauge is	during			

Operator and/or passenger injury Damage to or loss of property Damage to environment Potential for overheating			sufficient to carry max operational current with factor of safety Ensure wire bend radii are adhered to	operation by identifying eventual failure of vehicle components	9	107	To avoid TCM wiring failure the development team shall ensure wiring gauge is sufficient to carry max operational current with factor of safety To avoid TCM wiring failure the development team shall ensure wire bend radii are adhered to and wiring is protected from heat sources
	Unintended access or physical damage (liquid, puncture)	5	Ensure manufacturing is sufficient to prevent unintended access and physical damage Ensure use of covering at wire-TCM interface prevent unintended access Avoid adverse road condition which may produce NVH and damage TCM	Vehicle technical inspection will identify if the TCM is free of unintended access and physical damage Operator aware during operation by identifying eventual failure of vehicle components and loss of functionality	9	405	To avoid TCM unintended access or physical damage the development team shall ensure proper mounting, installation, and manufacturing of the TMC To avoid TCM unintended access or physical damage the development team shall ensure use of covering at wire-TMC interface To avoid TCM unintended access or physical damage the operator shall avoid adverse road conditions which may produce NVH

	Installation failure (wire, mounting)	7	Ensure TCM and mounting hardware are sufficient for max operational G- force with factor of safety Ensure TCM and mounting hardware are secure and free from unintended	Vehicle technical inspection will identify if TCM is free of manufacturing or installation fatigue or failure Operator aware during operation by identifying eventual failure	8	504	To avoid TCM installation failure the development team shall ensure the mounting hardware are sufficient for max operational G-force with factor of safety To avoid TCM installation failure the development team shall ensure the mounting hardware is secure and free from
	Over-current	7	Ensure	of vehicle components and loss of functionality Operator aware	7	441	potential lessening or unintended movement To avoid TCM over-
			software limits current rates and ranges Ensure relays and fuses are in place and functional to prevent over drawing of current	during operation by error signal and identifying eventual failure of vehicle components and loss of functionality			current failure the development team shall ensure software limits current ranges To avoid TCM over- current failure the development team shall ensure relays and fuses are in place and functional
	Over-heating	2	Ensure TCM is mounted such that there is proper clearance and sufficient air flow to cool the TCM	Vehicle technical inspection will identify if the TCM has proper clearance to allow for	9	162	To avoid TCM over- heating failure the development team shall ensure the TCM is mounted such that there is proper clearance and sufficient air flow to cool the TCM

Item: EMC							natural air flow cooling Operator aware during operation by identifying eventual failure of vehicle components and loss of functionality			
	Failure	Potential				Prevention	Detection			Functional
Function	Туре	Impact	s	Potential Cause	0	Mode	Mode	D	RPN	Requirement
Controls supply	Failure to	Unintended	10	Wiring failure	7	Ensure wiring	Vehicle	8	560	To avoid EMC wiring
of current to EM	control	acceleration	10	(not proper gauge,	,	is securely	technical	0	500	failure the
	current	www.		installation or		installed using	inspection will			development team
Convert DC to	supply to EM	Unintended		manufacturing		manufacturer	identify wiring			shall ensure wiring is
AC	11.2	longitudinal		failure)		installation	fatigue or			securely installed
	Failure to	motion		,		specifications	failure			using manufacturer
Control	control					-				installation
direction of	current	Loss or				Ensure wiring	Operator aware			specifications
current	direction	degradation of				gauge is	during			-
		propulsion				sufficient to	operation by			To avoid EMC wiring
Control EM	Failure to	system				carry max	identifying			failure the
temperature	control EM					operational	eventual failure			development team
	temperature	Operator				current with	of HV			shall ensure wiring
		and/or				factor of safety	components			gauge is sufficient to
		passenger								carry max operational
		injury				Ensure wire				current with factor of
		D				bend radii are				safety
		Damage to or				adhered to				
		loss of								To avoid EMC wiring failure the
		property								
		Damage to								development team shall ensure wire bend
		Damage to environment								radii are adhered to
	l	environment				l				raun are aunereu to

Potential for							and wiring is protected from heat sources
overheating	Unintended	5	Ensure	Vehicle	9	450	To avoid EMC
Unintended	access or physical damage (liquid,		manufacturing is sufficient to	technical inspection will			unintended access or physical damage the
exposure to	puncture)		prevent	identify the			development team
high voltage	r		unintended	EMC is free of			shall ensure proper
			access and	unintended			mounting, installation,
			physical damage	access			and manufacturing of the EMC
				Operator aware			
			Ensure use of	during			To avoid EMC
			covering at wire-EMC	operation by identifying			unintended access or physical damage the
			interface	eventual failure			development team
			prevent	of HV			shall ensure use of
			unintended	components			covering at wire- EMC
			access				interface
			Avoid adverse				To avoid EMC
			road condition				unintended access or
			which may				physical damage the
			produce NVH and damage				operator shall avoid adverse road
			EMC				conditions which may
							produce NVH
	Installation failure	7	Ensure EMC	Vehicle	8	560	To avoid EMC
	(wire, mounting)		and mounting	technical			installation failure the
			hardware are sufficient for	inspection will identify if			development team shall ensure the
			max	EMC is free of			mounting hardware are
			operational G-	manufacturing			sufficient for max
			force with	or installation			operational G-force
			factor of safety	fatigue or			with factor of safety
			Ensure EMC	failure			To avoid EMC
			and mounting	Operator aware			installation failure the
			hardware is	during			development team
			secure and free	operation by			shall ensure the
			from	identifying			mounting hardware is

	1	unintended	eventual failure			secure and free from
		movement	of HV			potential lessening or
	_		components			unintended movement
Over-current	7	Ensure	Operator aware	7	490	To avoid EMC over-
		software limits	during			current failure the
		current rates	operation by			development team
		and ranges	error signal and			shall ensure software
			identifying			limits current ranges
		Ensure relays	eventual failure			
		and fuses are in	of HV			To avoid EMC over-
		place and	components			current failure the
		functional to	-			development team
		prevent over				shall ensure relays and
		drawing of				fuses are in place and
		current				functional
Operation outside	8	Ensure	EMC monitors	8	640	To avoid EMC
of max/min		operation	and sends			operation outside of
temperature range		within	temperature			max/min temperature
(environmental or		specified EMC	data in real			range the development
coolant failure)		temp range	time			team shall ensure the
		F B				EMC has a thermal
		Actuate	Operator aware			controls system and
		thermal system	during			software forces
		when EMC	operation by			operation within
		reaches	identifying a			specified EMC
		specified	thermal event,			temperature range
		temperature	error message			temperature runge
		temperature	of overheating,			To avoid EMC
		Ensure thermal	or failure of			operation outside of
		system	HV			max/min temperature
		components	components			range the development
		(radiator,	components			team shall actuate
		coolant level,				cooling fans when
		fans) are functional and				EMC reaches specified
						temperature
		sufficient to				
		cool the EM				To avoid EMC
						operation outside of
		Ensure the fans				max/min temperature
		are free from				range the development

Item: BMS						potential physical damage Ensure bolts, hoses and mounting hardware are securely fastened and free from potential loosening or movement				team shall ensure thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the EMC To avoid EMC operation outside of max/min temperature range the development team shall ensure the fans are free from potential physical damage To avoid EMC operation outside of max/min temperature range the development team shall ensure bolts, hoses and mounting hardware are securely fastened and free from potential loosening or unintended movement
	Fellung	Dodon4:-1	1			D uonon4!	Da4a a4		1	Eurotional
Function	Failure Type	Potential Impact	S	Potential Cause	0	Prevention Mode	Detection Mode	D	RPN	Functional Requirement
Ensure safe ESS	Failure to	Unintended	10	Wiring failure	7	Ensure wiring	Vehicle	8	560	To avoid BMS wiring
operating	ensure safe	longitudinal		(not proper gauge,		is securely	technical			failure the
conditions	ESS	motion		installation or		installed using	inspection will			development team
	operating			manufacturing		manufacturer	identify wiring			shall ensure wiring is
Monitor ESS	conditions	Loss or		failure)		installation	fatigue or			securely installed
state (voltage,		degradation of				specifications	failure			using manufacturer
temperature,	Failure to	propulsion								installation

SOC, and current) Protects against over-current, over-voltage, under-voltage, and over- temperature Reporting data Controls and balances ESS environment	state (voltage, temperature, SOC, and current) Failure to protect against over- current, over- voltage, under- voltage, and over- temperature Failure to	Operator and/or passenger injury Damage to or loss of property Damage to environment Potential for overheating Unintended			Ensure wiring gauge is sufficient to carry max operational current with factor of safety Ensure wire bend radii are adhered to	Operator aware during operation by identifying eventual failure of HV components			To avoid BMS wiring failure the development team shall ensure wiring gauge is sufficient to carry max operational current with factor of safety To avoid BMS wiring failure the development team shall ensure wire bend radii are adhered to and wiring is protected from heat sources
	report data Failure to control and balance ESS environment	exposure to high voltage Short circuit Thermal event Inaccurate ESS state readings (voltage, temperature, SOC)	Unintended access or physical damage (liquid, puncture)	5	Ensure manufacturing is sufficient to prevent unintended access and physical damage Ensure use of covering at wire-BMS interface prevent unintended access Avoid adverse road condition which may produce NVH and damage BMS	Vehicle technical inspection will identify the BMS is free of unintended access and physical damage Operator aware during operation by identifying eventual failure of HV components	9	450	To avoid BMS unintended access or physical damage the development team shall ensure proper mounting, installation, and manufacturing of the BMS To avoid BMS unintended access or physical damage the development team shall ensure use of covering at wire- BMS interface To avoid BMS unintended access or physical damage the operator shall avoid adverse road

						conditions which may produce NVH
Installation failur	e 7	Ensure BMS	Vehicle	8	560	To avoid BMS
(wire, mounting)		and mounting	technical			installation failure the
		hardware are	inspection will			development team
		sufficient for	identify if			shall ensure the
		max	BMS is free of			mounting hardware are
		operational G-	manufacturing			sufficient for max
		force with	or installation			operational G-force
		factor of safety	fatigue or failure			with factor of safety
		Ensure BMS				To avoid BMS
		and mounting	Operator aware			installation failure the
		hardware is	during			development team
		secure and free	operation by			shall ensure the
		from	identifying			mounting hardware is
		unintended	eventual failure			secure and free from
		movement	of HV			potential lessening or
			components			unintended movement
Over-current	7	Ensure	Operator aware	7	490	To avoid BMS over-
		software limits	during			current failure the
		current rates	operation by			development team
		and ranges	error signal and			shall ensure software
			identifying			limits current ranges
		Ensure relays	eventual failure			
		and fuses are in	of HV			To avoid BMS over-
		place and	components			current failure the
		functional to				development team
		prevent over				shall ensure relays and
		drawing of				fuses are in place and
		current				functional
Over-heating	4	Ensure BMS is	Vehicle	9	360	To avoid BMS over-
		mounted such	technical			heating failure the
		that there is	inspection will			development team
		proper	identify if the			shall ensure the BMS
		clearance and	BMS has			is mounted such that
		sufficient air	proper			there is proper
		flow to cool	clearance to			clearance and
		the BMS	allow for			sufficient air flow to
						cool the BMS

Item: OBC							natural air flow cooling Operator aware during operation by identifying eventual failure of vehicle components and loss of functionality			
item. Obc	Failure	Potential				Prevention	Detection			Functional
Function	Туре	Impact	S	Potential Cause	0	Mode	Mode	D	RPN	Requirement
Controls charging to the HV battery pack	Failure to control charging to the HV battery pack	Potential for overheating Unintended exposure to high voltage Short circuit Thermal event Loss of motor functionality	10	Charging port failure	5	Ensure charging port cover is sufficient to provide freedom from unintended access or physical damage Ensure charging port is securely installed using manufacturer installation specifications Ensure wiring gauge is sufficient to carry max operational	Vehicle technical inspection will identify wiring fatigue or failure Operator aware during operation by identifying eventual failure of HV components	4	200	To avoid OBC wiring failure the development team shall ensure charging port cover is sufficient to provide freedom from unintended access or physical damage To avoid OBC wiring failure the development team shall ensure charging port is securely installed using manufacturer installation specifications To avoid OBC wiring failure the development team

		current with factor of safety Ensure wire bend radii are adhered to				shall ensure wiring gauge is sufficient to carry max operational current with factor of safety To avoid OBC wiring failure the development team shall ensure wire bend radii are adhered to
Wiring failure (not proper gauge, or installation)	7	Ensure wiring is securely installed using manufacturer installation specifications Ensure wiring gauge is sufficient to carry max operational current with factor of safety Ensure wire bend radii are adhered to	Vehicle technical inspection will identify wiring fatigue or failure Operator aware during operation by identifying eventual failure of HV components	8	560	To avoid OBC wiring failure the development team shall ensure wiring is securely installed using manufacturer installation specifications To avoid OBC wiring failure the development team shall ensure wiring gauge is sufficient to carry max operational current with factor of safety To avoid OBC wiring failure the development team shall ensure wire bend radii are adhered to and wiring is protected from heat sources
Unintended	5	Ensure	Vehicle technical	9	450	To avoid OBC
access or physical damage		manufacturing is sufficient to	inspection will			unintended access or physical damage the
(liquid, puncture)		prevent	identify the			development team

			unintended access and physical damage Ensure use of covering at wire-OBC interface prevents unintended access Avoid adverse road condition which may produce NVH and damage OBC Ensure charging port cover is sufficient to provide freedom from unintended access or physical	OBC is free of unintended access Operator aware during operation by identifying eventual failure of HV components			shall ensure proper mounting, installation, and manufacturing of the OBC To avoid OBC unintended access or physical damage the development team shall ensure use of covering at wire- OBC interface To avoid OBC unintended access or physical damage the operator shall avoid adverse road conditions which may produce NVH
	Installation failure (wire, mounting)	7	damage Ensure OBC and mounting hardware are sufficient for max operational G- force with factor of safety	Vehicle technical inspection will identify if OBC is free of manufacturing or installation fatigue or failure	8	560	To avoid OBC installation failure the development team shall ensure the mounting hardware are sufficient for max operational G-force with factor of safety

1		1 1	E ODC				T IODO
			Ensure OBC,	Operator aware			To avoid OBC
			charging port,	during			installation failure the
			and mounting	operation by			development team
			hardware are	identifying			shall ensure the
			secure and free	eventual failure			mounting hardware is
			from	of HV			secure and free from
			unintended	components			potential lessening or
			movement				unintended movement
	Over-current	7	Ensure	Operator aware	7	490	To avoid OBC over-
			software limits	during			current failure the
			current rates	operation by			development team
			and ranges	error signal and			shall ensure software
				identifying			limits current ranges
			Ensure relays	eventual failure			
			and fuses are in	of HV			To avoid OBC over-
			place and	components			current failure the
			functional to	_			development team
			prevent over				shall ensure relays and
			drawing of				fuses are in place and
			current				functional
		1	1		-	640	T LODG
	Operation outside	8	Ensure	OBC	8	640	To avoid OBC
	Operation outside of max/min	8	Ensure operation	OBC temperature	8	640	operation outside of
		8			8	640	
	of max/min	8	operation within	temperature	8	640	operation outside of max/min temperature
	of max/min temperature range	8	operation	temperature signal sends	8	640	operation outside of
	of max/min temperature range (environmental or	8	operation within specified OBC	temperature signal sends data in real	8	640	operation outside of max/min temperature range the development
	of max/min temperature range (environmental or	8	operation within specified OBC temperature	temperature signal sends data in real	8	640	operation outside of max/min temperature range the development team shall ensure the
	of max/min temperature range (environmental or	8	operation within specified OBC temperature	temperature signal sends data in real time Operator aware	8	640	operation outside of max/min temperature range the development team shall ensure the OBC has a thermal
	of max/min temperature range (environmental or	8	operation within specified OBC temperature range	temperature signal sends data in real time Operator aware during	8	640	operation outside of max/min temperature range the development team shall ensure the OBC has a thermal controls system and software forces
	of max/min temperature range (environmental or	8	operation within specified OBC temperature range Actuate thermal control	temperature signal sends data in real time Operator aware during operation by	8	640	operation outside of max/min temperature range the development team shall ensure the OBC has a thermal controls system and software forces operation within
	of max/min temperature range (environmental or	8	operation within specified OBC temperature range Actuate thermal control system when	temperature signal sends data in real time Operator aware during operation by identifying a	8	640	operation outside of max/min temperature range the development team shall ensure the OBC has a thermal controls system and software forces operation within specified OBC
	of max/min temperature range (environmental or	8	operation within specified OBC temperature range Actuate thermal control system when OBC reaches	temperature signal sends data in real time Operator aware during operation by identifying a thermal event,	8	640	operation outside of max/min temperature range the development team shall ensure the OBC has a thermal controls system and software forces operation within
	of max/min temperature range (environmental or	8	operation within specified OBC temperature range Actuate thermal control system when OBC reaches specified	temperature signal sends data in real time Operator aware during operation by identifying a thermal event, error message	8	640	operation outside of max/min temperature range the development team shall ensure the OBC has a thermal controls system and software forces operation within specified OBC temperature range
	of max/min temperature range (environmental or	8	operation within specified OBC temperature range Actuate thermal control system when OBC reaches	temperature signal sends data in real time Operator aware during operation by identifying a thermal event, error message of overheating,	8	640	operation outside of max/min temperature range the development team shall ensure the OBC has a thermal controls system and software forces operation within specified OBC temperature range To avoid OBC
	of max/min temperature range (environmental or	8	operation within specified OBC temperature range Actuate thermal control system when OBC reaches specified temperature	temperature signal sends data in real time Operator aware during operation by identifying a thermal event, error message of overheating, or failure of	8	640	operation outside of max/min temperature range the development team shall ensure the OBC has a thermal controls system and software forces operation within specified OBC temperature range To avoid OBC operation outside of
	of max/min temperature range (environmental or	8	operation within specified OBC temperature range Actuate thermal control system when OBC reaches specified temperature Ensure thermal	temperature signal sends data in real time Operator aware during operation by identifying a thermal event, error message of overheating, or failure of HV	8	640	operation outside of max/min temperature range the development team shall ensure the OBC has a thermal controls system and software forces operation within specified OBC temperature range To avoid OBC operation outside of max/min temperature
	of max/min temperature range (environmental or	8	operation within specified OBC temperature range Actuate thermal control system when OBC reaches specified temperature Ensure thermal system	temperature signal sends data in real time Operator aware during operation by identifying a thermal event, error message of overheating, or failure of	8	640	operation outside of max/min temperature range the development team shall ensure the OBC has a thermal controls system and software forces operation within specified OBC temperature range To avoid OBC operation outside of max/min temperature range the development
	of max/min temperature range (environmental or	8	operation within specified OBC temperature range Actuate thermal control system when OBC reaches specified temperature Ensure thermal system components	temperature signal sends data in real time Operator aware during operation by identifying a thermal event, error message of overheating, or failure of HV	8	640	operation outside of max/min temperature range the development team shall ensure the OBC has a thermal controls system and software forces operation within specified OBC temperature range To avoid OBC operation outside of max/min temperature range the development team shall actuate
	of max/min temperature range (environmental or	8	operation within specified OBC temperature range Actuate thermal control system when OBC reaches specified temperature Ensure thermal system components (radiator,	temperature signal sends data in real time Operator aware during operation by identifying a thermal event, error message of overheating, or failure of HV	8	640	operation outside of max/min temperature range the development team shall ensure the OBC has a thermal controls system and software forces operation within specified OBC temperature range To avoid OBC operation outside of max/min temperature range the development team shall actuate cooling fans when
	of max/min temperature range (environmental or	8	operation within specified OBC temperature range Actuate thermal control system when OBC reaches specified temperature Ensure thermal system components	temperature signal sends data in real time Operator aware during operation by identifying a thermal event, error message of overheating, or failure of HV	8	640	operation outside of max/min temperature range the development team shall ensure the OBC has a thermal controls system and software forces operation within specified OBC temperature range To avoid OBC operation outside of max/min temperature range the development team shall actuate

						functional and sufficient to cool the EM Ensure the fans are free from potential physical damage Ensure bolts, hoses and mounting hardware are securely fastened and				To avoid OBC operation outside of max/min temperature range the development team shall ensure thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the OBC To avoid OBC operation outside of max/min temperature
						free from potential loosening or movement				range the development team shall ensure the fans are free from potential physical damage
										To avoid OBC operation outside of max/min temperature range the development team shall ensure bolts, hoses and mounting hardware are securely fastened and free from potential loosening or unintended movement
Item: OBD II										
Function	Failure Type	Potential Impact	s	Potential Cause	0	Prevention Mode	Detection Mode	D	RPN	Functional Requirement
Provide requested vehicle	Failure to provide requested	Short Circuit	2	Wiring failure (not proper gauge, installation or	7	Ensure wiring is securely installed using	Vehicle technical inspection will	8	112	To avoid OBD II wiring failure the development team

parameters to monitor	vehicle parameters to monitor	Loss of DAQ functionality	manufacturing failure)		manufacturer installation specifications Ensure wiring gauge is sufficient to carry max operational current with factor of safety Ensure wire bend radii are adhered to	identify wiring fatigue or failure Operator aware during operation by identifying eventual failure of vehicle components and loss of DAQ			shall ensure wiring is securely installed using manufacturer installation specifications To avoid OBD II wiring failure the development team shall ensure wiring gauge is sufficient to carry max operational current with factor of safety To avoid OBD II wiring failure the development team shall ensure wire bend radii are adhered to
			Unintended access or physical damage to CAN bus (liquid, puncture)	5	Ensure manufacturing is sufficient to prevent unintended access and physical damage	Vehicle technical inspection will identify if the OBD II is free of physical damage Operator aware during operation by identifying eventual loss of DAQ Vehicle	9	90	and wiring is protected from heat sources To avoid OBD II unintended access or physical damage the development team shall ensure proper mounting, installation, and manufacturing of the OBD II
			(wire, mounting)		and mounting hardware are secure, free	technical inspection will identify if the			installation failure the development team shall ensure the

						from unintended movement, and sufficient for open road conditions with a factor of safety	OBD II is free of manufacturing or installation fatigue or failure Operator aware during operation by identifying eventual loss of DAQ			mounting hardware is secure, free from unintended movement, and sufficient for open road conditions with a factor of safety
				Over-current	7	Ensure software limits current rates and ranges Ensure relays and fuses are in place and functional to prevent over drawing of current	Operator aware during operation by error signal and eventual loss of DAQ	7	98	To avoid OBD II over- current failure the development team shall ensure software limits current ranges To avoid OBD II over- current failure the development team shall ensure relays and fuses are in place and functional
Item: CAN Bus									I	
Function	Failure Type	Potential Impact	S	Potential Cause	0	Prevention Mode	Detection Mode	D	RPN	Functional Requirement
Transfer	Failure to	Unintended	9	Wiring failure	7	Ensure wiring	Vehicle	8	504	To avoid CAN bus
necessary	transfer	longitudinal		(not proper gauge,		is securely	technical			wiring failure the
signals such as	necessary	motion		installation or		installed using	inspection will			development team
EM speed, EM	signals such			manufacturing		manufacturer	identify wiring			shall ensure wiring is
torque, EM	as EM speed,	Loss or		failure)		installation	fatigue or			securely installed
temperature,	EM torque,	degradation of		-		specifications	failure			using manufacturer
EMC	EM	propulsion				_				installation
temperature,	temperature,	system				Ensure wiring	Operator aware			specifications
SOC, current,	EMC	-				gauge is	during			-
voltage, battery	temperature,	Operator				sufficient to	operation by			To avoid CAN bus
temperature, and	SOĈ,	and/or				carry max	identifying			wiring failure the

OBC temperature	current, voltage, battery temperature, and OBC temperature	passenger injury Damage to or loss of property			operational current with factor of safety Ensure wire bend radii are	eventual failure of vehicle components and loss of DAQ			development team shall ensure wiring gauge is sufficient to carry max operational current with factor of safety
		Damage to environment Potential for overheating Short Circuit			adhered to Ensure wiring bus is properly protected				To avoid CAN bus wiring failure the development team shall ensure wire bend radii are adhered to and wiring is protected from heat sources
		Error messages Loss of communication between controllers and a loss of their functionality Loss of DAQ functionality	Unintended access or physical damage to CAN bus (liquid, puncture)	5	Ensure manufacturing is sufficient to prevent unintended access and physical damage Ensure use of CAN bus covering to prevent unintended access and physical damage	Vehicle technical inspection will identify the CAN bus is free of physical damage Operator aware during operation by identifying eventual failure of vehicle components and loss of DAQ	9	405	To avoid CAN bus unintended access or physical damage the development team shall ensure proper mounting, installation, and manufacturing of the CAN bus To avoid CAN bus unintended access or physical damage the development team shall ensure use of covering at wire- CAN bus interface To avoid CAN bus unintended access or physical damage the operator shall avoid adverse road conditions which may produce NVH
			Installation failure (wire, mounting)	7	Ensure CAN bus harness	Vehicle technical	8	504	To avoid CAN bus installation failure the
			(whe, mounting)	1	ous namess	ucilintai			instantation failure the

			and mounting hardware are secure, free from unintended movement, and sufficient for open road conditions with a factor of safety	inspection will identify if the CAN bus is free of manufacturing or installation fatigue or failure Operator aware during operation by identifying eventual failure of vehicle components and loss of DAQ			development team shall ensure the mounting hardware are sufficient for max operational G-force with factor of safety To avoid CAN bus installation failure the development team shall ensure the mounting hardware is secure and free from potential lessening or unintended movement
	Over-current	7	Ensure software limits current rates and ranges Ensure relays and fuses are in place and functional to prevent over drawing of current	Operator aware during operation by error signal and identifying eventual failure of vehicle components	7	441	To avoid CAN bus over-current failure the development team shall ensure software limits current ranges To avoid CAN bus over-current failure the development team shall ensure relays and fuses are in place and functional
	Over-heating	2	Ensure the CAN bus is mounted such that there is proper clearance and sufficient air flow to cool the CAN bus	Vehicle technical inspection will identify if the CAN bus has proper clearance to allow for natural air flow cooling	9	162	To avoid CAN bus over-heating failure the development team shall ensure the CAN bus is mounted such that there is proper clearance and sufficient air flow to cool the CAN bus

							Operator aware during operation by identifying eventual failure of vehicle components and loss of functionality			
	Failure	Potential		sition Sensor (APPS)		Prevention	Detection	D	DDM	Functional
Function Monitor the	Type Failure to	Impact Unintended	S	Potential Cause Wiring failure	0 2	Mode Ensure wiring	Mode Vehicle	D 8	RPN 160	Requirement To avoid AP/APPS
position of the accelerator pedal and transmit a torque request	monitor the position of the accelerator pedal and transmit a torque request	acceleration Unintended longitudinal motion Loss or degradation of propulsion system Operator and/or passenger injury Damage to or loss of property Damage to environment		(not proper gauge, installation or manufacturing failure)		is securely installed using manufacturer installation specifications Ensure wiring gauge is sufficient to carry max operational current with factor of safety Ensure wire bend radii are adhered to	technical inspection will identify wiring fatigue or failure Operator aware during operation by identifying error message and eventual failure of vehicle components	0		wiring failure the development team shall ensure wiring is securely installed using manufacturer installation specifications To avoid AP/APPS wiring failure the development team shall ensure wiring gauge is sufficient to carry max operational current with factor of safety To avoid AP/APPS wiring failure the development team shall ensure wire bend radii are adhered to and wiring is protected from heat sources

Potential for overheating	Unintended access or physical damage to pedal or senor (liquid, puncture)	2	Ensure manufacturing is sufficient to prevent unintended access and physical damage	Vehicle technical inspection will identify if the AP and APPS is free of unintended access and physical damage Operator aware during operation by identifying immediate or eventual failure of vehicle components and loss of functionality	9	180	To avoid AP/APPS unintended access or physical damage the development team shall ensure proper mounting, installation, and manufacturing of the AP/APPS To avoid AP/APPS unintended access or physical damage the development team shall ensure use of covering at wire- AP/APPS interface To avoid AP/APPS unintended access or physical damage the operator shall avoid adverse road conditions which may
	Installation failure (wire, mounting)	2	Ensure the AP and APPS mounting hardware are secure, free from unintended movement, and sufficient for open road conditions with a factor of safety	Vehicle technical inspection will identify if AP and APPS are free of manufacturing or installation fatigue or failure Operator aware during operation by identifying immediate or	8	160	produce NVH To avoid AP/APPS installation failure the development team shall ensure the mounting hardware are sufficient for max operational G-force with factor of safety To avoid AP/APPS installation failure the development team shall ensure the mounting hardware is secure and free from

			eventual failure of vehicle components and loss of functionality			potential lessening or unintended movement
Over-current	2	Ensure software limits current rates and ranges Ensure relays and fuses are in place and functional to prevent over drawing of current	Operator aware during operation by identifying immediate or eventual failure of vehicle components and loss of functionality	7	140	To avoid AP/APPS over-current failure the development team shall ensure software limits current ranges To avoid AP/APPS over-current failure the development team shall ensure relays and fuses are in place and functional
Over-heating	2	Ensure APPS is mounted such that there is proper clearance and sufficient air flow to cool	Vehicle technical inspection will identify if the APPS has proper clearance to allow for natural air flow cooling Operator aware during operation by identifying eventual failure of vehicle components and loss of functionality	9	180	To avoid AP/APPS over-heating failure the development team shall ensure the AP/APPS is mounted such that there is proper clearance and sufficient air flow to cool the AP/APPS

	Failure	Potential				Prevention	Detection			Functional
Function	Туре	Impact	S	Potential Cause	0	Mode	Mode	D	RPN	Requirement
Control of all	Failure to	Unintended	10	Wiring failure	3	Ensure wiring	Vehicle	8	240	To avoid low voltage
auxiliary	control of all	longitudinal		(not proper gauge,		is securely	technical			component wiring
functions to	auxiliary	motion		installation or		installed using	inspection will			failure the
include air bags,	functions to			manufacturing		manufacturer	identify wiring			development team
windshield	include air	Loss or		failure)		installation	fatigue or			shall ensure wiring is
wipers,	bags,	degradation of				specifications	failure			securely installed
Instrument	windshield	propulsion								using manufacturer
cluster, lights,	wipers,	system				Ensure wiring	Operator aware			installation
entertainment	Instrument					gauge is	during			specifications
system, turn	cluster,	Operator				sufficient to	operation by			
signals, haptic	lights,	and/or				carry max	identifying			To avoid low voltage
feedback,	entertainment	passenger				operational	error message			component wiring
security system,	system, turn	injury				current with	and eventual			failure the
pumps, fans,	signals,					factor of safety	failure of			development team
controllers, and	haptic	Damage to or					vehicle			shall ensure wiring
DAQ	feedback,	loss of				Ensure wire	components			gauge is sufficient to
	security	property				bend radii are				carry max operational
Controls thermal	system,					adhered to				current with factor of
components	pumps, fans,	Damage to								safety
	controller	environment								
Controls data	and DAQ									To avoid low voltage
acquisition		Potential for								component wiring
	Failure to	overheating								failure the
	control									development team
	thermal	Reduced or								shall ensure wire bend
	components	loss of								radii are adhered to
		visibility								and wiring is protected
	Failure to	-								from heat sources
	controls data	Driver		Unintended	2	Ensure	Vehicle	9	180	To avoid low voltage
	acquisition	unaware of		access or physical		manufacturing	technical			component unintended
		vehicle		damage (liquid,		is sufficient to	inspection will			access or physical
		operational		puncture)		prevent	identify if the			damage the
		data (velocity,				unintended	low voltage			development team
		RPM, engine				access and	components			shall ensure proper
		temperature)				physical	are free of			mounting, installation,
						damage	unintended			and manufacturing of
						-	access and			the low voltage
										systems

			physical damage Operator aware during operation by identifying immediate or eventual failure of vehicle components and loss of functionality			To avoid low voltage component unintended access or physical damage the development team shall ensure use of covering at wire-low voltage component interface To avoid low voltage component unintended access or physical damage the operator shall avoid adverse road conditions which may produce NVH
Installation failure (wire, mounting)	3	Ensure the low voltage components mounting hardware are secure, free from unintended movement, and sufficient for open road conditions with a factor of safety	Vehicle technical inspection will identify if low voltage components are free of manufacturing or installation fatigue or failure Operator aware during operation by identifying immediate or eventual failure of vehicle components and loss of functionality	8	240	To avoid low voltage component installation failure the development team shall ensure the mounting hardware are sufficient for max operational G-force with factor of safety To avoid low voltage component installation failure the development team shall ensure the mounting hardware is secure and free from potential lessening or unintended movement

Over-current	2	Ensure software limits current rates and ranges Ensure relays and fuses are in place and functional to prevent over drawing of current	Operator aware during operation by identifying immediate or eventual failure of vehicle components and loss of functionality	7	140	To avoid low voltage component over- current failure the development team shall ensure software limits current ranges To avoid low voltage component over- current failure the development team shall ensure relays and fuses are in place and functional
Over-heating	2	Ensure low voltage components are mounted such that there is proper clearance and sufficient air flow to cool	Vehicle technical inspection will identify if the low voltage components has proper clearance to allow for natural air flow cooling Operator aware during operation by identifying eventual failure of vehicle components and loss of functionality	9	180	To avoid low voltage over-heating failure the development team shall ensure the low voltage component is mounted such that there is proper clearance and sufficient air flow to cool the low voltage
Component failure (headlights, tail lights, windshield wipers,)	3	Ensure low voltage components are functional	Vehicle technical inspection will identify if low voltage	8	240	To avoid low voltage component failure the operator shall ensure low voltage components are

	Replace fatigued components	components are fatigued or have failed	functional and replace fatigued components
		Operator aware during operation by identifying eventual failure of vehicle components and loss of functionality	

Appendix 3.06 HARA PSI HV DFMEA

	PSI HV DFMEA										
Item: HV Battery Pack											
Function	Failure Type	Potential Impact	s	Potential Cause	0	Prevention Mode	Detection Mode	D	RPN	Functional Requirement	
Store and supply energy to EM	Failure to store and supply energy to EM matching operator request	Unintended Vehicle deceleration Unintended longitudinal motion Thermal runaway Unintended exposure to high voltage	10	Operation outside of max/min temp range (overheating, under-heat)	8	Operate vehicle within specified battery temp range Actuate cooling fans when battery pack reaches specified temperature Use manufacturer	BMS monitors and sends temperature data in real time Operator aware during operation by identifying a thermal event, error message of overheating, or failure of HV components	8	640	To prevent the HV battery pack from operating outside of the max/min temperature range the development team shall ensure specified temperature limits are controlled by the BMS To prevent the HV battery pack from operating outside of the max/min temperature	

Short circuit Operator and/or passenger injury Damage to or loss of property Loss of HV power Damage to environment	Operation while	7	recommended installation instructions (clearance, bend radii) Limit charge and discharge current to specified range BMS monitors	BMS monitors	6	420	range the development team shall ensure actuation of battery pack thermal control system (fans) when the temperature reaches limit To prevent the HV battery pack from operating outside of the max/min temperature range the development team shall ensure proper installation using manufacturer recommended specifications to include component clearances and wire bend radii To prevent the HV battery pack from operating outside of the max/min temperature range the development team shall ensure a limit to charging and discharging current to a specified range To prevent the HV
	undercharged		SOC. Controls software will only draw current at	and sends SOC data in real time	0	420	battery pack from operating while undercharged the development team shall ensure the BMS monitors and controls the SOC in real-time

			specified minimum SOC				To prevent the HV battery pack from operating while undercharged the development team shall ensure controls software will only draw current at specified minimum SOC
	Unintended access to HV battery pack (liquid, insect, bolt)	8	Ensure proper mounting, installation, and manufacturing of enclosure and HV components Ensure bolts and mounting hardware is securely fastened and free from potential loosening or movement Ensure all vents are covered with appropriate screening to prevent access from liquid, debris, dust, or insects Ensure fans are pulling air from	Vehicle technical inspection will identify authorized access Operator aware during operation by identifying failure of HV components	9	720	To prevent the HV battery pack from unintended access the development team shall ensure proper mounting, installation, and manufacturing of enclosure and HV components To prevent the HV battery pack from unintended access the development team shall ensure bolts and mounting hardware is securely fastened and free from potential loosening or movement To prevent the HV battery pack from unintended access the development team shall ensure solts and free from potential loosening or movement To prevent the HV battery pack from unintended access the development team shall ensure all HV enclosure vents are covered with appropriate screening to prevent access from liquid, debris, dust, or insects

		dry particulate- free source Ensure enclosure location is covered when vehicle is not in use				To prevent the HV battery pack from unintended access the development team shall ensure HV thermal control system fans are pulling air from dry particulate-free source To prevent the HV battery pack from unintended access the development team shall ensure the enclosure location is covered and free from the external environment when vehicle is not in use
Improper Installation (mounting, bend radii, clearance)	8	Use manufacturer recommended installation instructions (clearance, bend radii, and soldering) Ensure HV battery pack is securely installed to prevent unintended movement Ensure wires, bus bars, and all interfacing components are securely	Vehicle technical inspection will identify improper installation Operator aware during operation by identifying a failure of HV components	8	640	To ensure the HV battery pack is properly installed the development team shall ensure manufacturer recommended installation instructions (clearance, bend radii, and soldering) To ensure the HV battery pack is properly installed the development team shall ensure the wires, bus bars, and all interfacing components are securely mounted and adequate clearance used

	1	1	r			1	1	r	1	1
						installed and				
						adequate				
						clearance used				
				Excess charging	7	Ensure software	Operator aware	8	560	To prevent the HV
				or discharging		(HSC, OBC,	during			battery pack failure
				of current		EMC) limits	operation by			from excess charging or
						charging and	identifying a			discharging of current
						discharging	charging and			the development team
						rates and ranges	discharging			shall ensure software
						C	rates			(HSC, OBC, EMC)
						Ensure relays				limits charging and
						and fuses are in	OBC controls			discharging rates and
						place and	and mitigates			ranges
						functional to	charging while			Tungeo
						prevent over	vehicle is not in			To prevent the HV
						drawing of	operation			battery pack failure
						current	operation			from excess charging or
						eurient				discharging of current
										the development team
										shall ensure relays and
										fuses are in place and
										functional to prevent
										over drawing of current
										over drawing of current
Item: Enclosure	:									
	Failure	Potential		Potential		Prevention	Detection			Functional
Function	Туре	Impact	S	Cause	0	Mode	Mode	D	RPN	Requirement
Contain HV	Failure to	Unintended	10	Unintended	8	Ensure proper	Vehicle	9	720	To prevent the HV
components	contain HV	longitudinal		access to HV	_	mounting,	technical	-	-	enclosure failure from
1	components	motion		components		installation, and	inspection will			unintended access the
Prevent	r r			(liquid, insects,		manufacturing	identify			development team shall
horizontal and	Failure to	Failure any or		fingers,		of enclosure	unauthorized			ensure proper
vertical free	prevent	all HV		hardware)		(sealing, welds,	access			mounting, installation,
movement of HV	horizontal or	components				bolt holes)				and manufacturing of
components	vertical	policius					Operator aware			enclosure (sealing,
T T T T T T T T T T T T T T T T T T T	movement of	Thermal				Ensure bolts	during			welds, bolt holes)
Prevent	HV	runaway				and mounting	operation by			
unauthorized	components	1 and 1 ay				hardware is	identifying a			To prevent the HV
access to HV	Ponento					securely	failure of HV			enclosure failure from
components						fastened and	components			unintended access the
components	1	1		l		rasteneu anu	components		I	unintended access the

Failure to	Unintended			free from				development team shall
prevent	exposure to			potential				ensure bolts and
unauthorized	high voltage			loosening or				mounting hardware is
access to HV				movement				securely fastened and
components	Short circuit							free from potential
				Ensure all vents				loosening or movement
	Operator			are covered				
	and/or			with				To prevent the HV
	passenger			appropriate				enclosure from
	injury			screening				unintended access the
								development team shall
	Damage to or			Ensure fans are				ensure all vents are
	loss of			pulling air from				covered with
	property			dry particulate-				appropriate screening
				free source				
	Loss of HV							To prevent the HV
	power			Ensure				enclosure failure from
	-			enclosure				unintended access the
	Damage to			location is				development team shall
	environment			covered when				ensure the enclosure
				vehicle is not in				location is covered and
				use				free from the external
				use				environment when
								vehicle is not in use
		improper	7	Use existing	Vehicle	8	560	To prevent the HV
		mounting to	1	mount locations	technical	0	500	enclosure failure from
		vehicle frame		on vehicle	inspection will			improper mounting to
		(enclosure		frame to secure	identify frame			the vehicle frame the
		vibration)		enclosure	•			development team shall
		vioration)		enciosure	mounting			ensure the use of
				Enguno	fatigue or failures			
				Ensure	lanures			existing mount
				mounting				locations on vehicle
				hardware is	Operator aware			frame
				sufficient for	during			-
				max operational	operation by			To prevent the HV
				G-force with	identifying a			enclosure failure from
				factor of safety	failure of HV			improper mounting to
					components			the vehicle frame the
				Ensure proper				development team shall
				enclosure				ensure mounting

	Improper	7	manufacturing (welds, thread engagement) Ensure	Vehicle	8	560	hardware is sufficient for max operational G- force with factor of safety To prevent the HV enclosure failure from improper mounting to the vehicle frame the development team shall ensure proper enclosure manufacturing (welds, thread engagement) To prevent the HV
	installation and mounting of components (components within enclosure vibration)		component mounting hardware is sufficient for max operational G-force with factor of safety Ensure component mounting hardware is fire retardant Ensure component mounting hardware is secure and free from unintended movement	technical inspection will identify component installation fatigue or failures Operator aware during operation by identifying a failure of HV components	0	500	 To prevent the TV enclosure failure from improper installation and mounting of components the development team shall ensure To prevent the HV enclosure failure from improper installation and mounting of components the development team shall ensure component mounting hardware is fire retardant To prevent the HV enclosure failure from improper installation and mounting hardware is fire retardant To prevent the HV enclosure failure from improper installation and mounting of components the development team shall ensure component mounting hardware is

							secure and free from unintended movement
	Cooling failure	8	Ensure	Vehicle	9	720	To prevent a HV
	(fans, vents)	Ŭ	enclosure fans	technical	Ĺ		enclosure cooling
	(14116), (01106)		are operational	inspection will			failure the development
			and sufficient to	identify cooling			team shall ensure the
			cool that battery	fan fatigue or			enclosure fans are
			pack	failures			operational and
			pack	Tanuies			sufficient to cool that
			Ensure the	Operator aware			battery pack
			enclosure fans	during			battery pack
			are free from				To prevent a HV
				operation by			
			potential	identifying a			enclosure cooling
			physical	continued			failure the development
			damage	heating and			team shall ensure the
				eventual failure			enclosure fans are free
			Ensure	of HV			from potential physical
			enclosure fans	components			damage
			pull air from a				
			dry and				To prevent a HV
			particulate free				enclosure cooling
			source				failure the development
							team shall ensure the
			Ensure				enclosure fans pull air
			enclosure				from a dry and
			ventilation is				particulate free source
			sufficient to				
			cool HV				To prevent a HV
			components				enclosure cooling
							failure the development
			Ensure				team shall ensure the
			enclosure is				enclosure ventilation is
			designed such				sufficient to cool HV
			that there is				components
			sufficient air				-
			flow to cool				To prevent a HV
			HV				enclosure cooling
			components				failure the development
			and that the				team shall ensure the
			flow is free				enclosure is designed

	Adverse road conditions (NVH)	3	from interference Do not operate on roads which may produce high NVH	Operator aware during operation. Increased NVH	3	90	such that there is sufficient air flow to cool HV components and that the flow is free from interference To prevent a HV enclosure failure the operator shall not operate vehicle during adverse environmental conditions (excessively rough roads, NVH)
	Manufacturing failure (material, welds)	8	Ensure materials used in enclosure manufacturing are capable of withstanding high NVH Ensure proper enclosure manufacturing (welds, thread engagement) Ensure materials used in manufacturing of enclosure are fire retardant	Vehicle technical inspection will identify enclosure manufacturing fatigue or failure Operator aware during operation by identifying eventual failure of HV components	8	640	To prevent a HV enclosure manufacturing failure the development team shall ensure materials used in enclosure manufacturing are capable of withstanding high NVH To prevent a HV enclosure manufacturing failure the development team shall ensure proper enclosure manufacturing (welds, thread engagement) To prevent a HV enclosure failure the development team shall ensure materials used in manufacturing of enclosure are fire retardant

	Failure	Potential		Potential		Prevention	Detection			Functional
Function	Туре	Impact	S	Cause	0	Mode	Mode	D	RPN	Requirement
Ease use for	Failure to	Unintended	10	Wiring failure	7	Ensure wiring	Vehicle	8	560	To prevent junction box
maintenance and	provide	deceleration		(not proper		is securely	technical			wiring failure the
consolidation of	current			gauge,		installed using	inspection will			development team shall
HV wire		Unintended		installation or		manufacturer	identify			ensure wiring is
connections and		longitudinal		manufacturing		installation	junction box			securely installed using
relays		motion		failure)		specifications	wiring fatigue			manufacturer
							or failure			installation
		Loss or				Ensure wiring				specifications
		degradation				gauge is	Operator aware			
		of propulsion				sufficient to	during			To prevent junction box
		system				carry max	operation by			wiring failure the
						operational	identifying			development team shall
		Thermal				current with	eventual failure			ensure wiring gauge is
		event				factor of safety	of HV			sufficient to carry max
							components			operational current with
		Operator				Ensure wire				factor of safety
		and/or				bend radii are				
		passenger				adhered to				To prevent junction box
		injury								wiring failure the
										development team shall
		Damage to or								ensure wire bend radii
		loss of			_			_		are adhered to
		property		Unintended	5	Ensure box	Vehicle	9	450	To prevent junction box
		-		access and		manufacturing	technical			failure from unintended
		Damage to		physical		is sufficient to	inspection will			access the development
		environment		damage (liquid,		prevent	identify			team shall ensure the
		~		insect,		unintended	junction box is			box manufacturing is
		Short circuit		puncture)		access and	free of			sufficient to prevent
						physical	unintended			unintended access,
		Unintended				damage	access			loosening, and physical
		exposure to								damage
		high voltage				Ensure use of	Operator aware			
						grommets at	during			To prevent junction box
						wire-box	operation by			failure from unintended
						interface	identifying			access the development
			1	1	1	prevent	eventual failure	1	1	team shall ensure the

		unintanda d	of HV	1	r	use of geometric st
		unintended				use of grommets at wire-box interface
		access	components			
						prevent unintended
				_		access
Manufacturing	7	Ensure junction	Vehicle	8	560	To prevent junction box
or installation		box and	technical			failure the development
failure (wire,		mounting	inspection will			team shall ensure the
mounting)		hardware is	identify			junction box and
		sufficient for	junction box is			mounting hardware is
		max operational	free of			sufficient for max
		G-force with	manufacturing			operational G-force
		factor of safety	or installation			with factor of safety
			fatigue or			
		Ensure junction	failure			To prevent junction box
		box and				failure the development
		mounting	Operator aware			team shall ensure the
		hardware is fire	during			junction box and
		retardant	operation by			mounting hardware is
			identifying			fire retardant
		Ensure junction	eventual failure			
		box and	of HV			To prevent junction box
		mounting	components			failure the development
		hardware is	eomponents			team shall ensure the
		secure and free				junction box and
		from				mounting hardware is
		unintended				secure and free from
		movement				unintended movement
Over-current	7	Ensure software	On anot on aviana	7	490	To prevent junction box
Over-current	/		Operator aware during	/	490	over-current failure the
		(HSC, OBC,	0			
		EMC) limits	operation by			development team shall
		current	error signal and			ensure software (HSC,
		magnitude	identifying			OBC, EMC) limits
		_	eventual failure			current magnitude
		Ensure relays	of HV			
		and fuses are in	components			To prevent junction box
		place and				over-current failure the
		functional to				development team shall
		prevent over				ensure relays and fuses
		drawing of				are in place and
		current				

Item: Wiring H	arness			Environmental conditions outside of IP67 ratings	2	Ensure the environmental conditions do not exceed that specified by IP67 ratings	Operator aware prior to or during operation by identifying environmental conditions	2	40	functional to prevent over drawing of current To prevent junction box failure the development team shall ensure box minimum rating of IP67
	Failure	Potential		Potential		Prevention	Detection			Functional
Function	Туре	Impact	S	Cause	0	Mode	Mode	D	RPN	Requirement
Transfer energy	Failure to transfer energy	Unintended decelerationUnintended longitudinal motionLoss or degradation of propulsion systemThermal eventOperator and/or passenger injuryDamage to or loss of	10	Wiring failure (not proper gauge, installation or manufacturing failure)	7	Ensure wiring is securely installed using manufacturer installation specifications Ensure wiring gauge is sufficient to carry max operational current with factor of safety Ensure wire bend radii are adhered to	Vehicle technical inspection will identify wiring harness fatigue or failure Operator aware during operation by identifying eventual failure of HV components	8	560	To prevent HV wiring harness failure the development team shall ensure wiring is securely installed using manufacturer installation specifications To prevent HV wiring harness failure the development team shall ensure wiring gauge is sufficient to carry max operational current with factor of safety To prevent HV wiring harness failure the development team shall ensure wire bend radii are adhered to
		property Damage to environment		Unintended access or physical damage to	7	Ensure harness manufacturing is sufficient to prevent unintended	Vehicle technical inspection will identify if harness is free	9	630	To prevent HV wiring harness failure the development team shall ensure the harness manufacturing is

Short circuit	harness (liquid,		access and	of unintended			sufficient to prevent
Short circuit	debris)		physical	access or			unintended access and
Unintended	de0113)		damage	physical			physical damage
exposure to			Gamage	damage			physical damage
high voltage			Ensure use of	uanage			To prevent HV wiring
nigh voltage				On contra concern			harness failure the
			covers and	Operator aware			
			shielding to	during			development team shall
			prevent	operation by			ensure the use of covers
			unintended	identifying			and shielding to prevent
			access and	eventual failure			unintended access and
			physical	of HV			physical damage
			damage	components			
							To prevent HV wiring
			Avoid adverse				harness failure the
			road condition				operator shall avoid
			which may				adverse road condition
			project debris				which may project
			and damage				debris and damage
			harness				harness
	Installation	7	Ensure harness	Vehicle	8	560	To prevent HV wiring
	failure (wire,		and mounting	technical			harness installation
	mounting, bend		hardware is	inspection will			failure the development
	radii)		sufficient for	identify if			team shall ensure the
			max operational	harness is free			harness and mounting
			G-force with	of			hardware is sufficient
			factor of safety	manufacturing			for max operational G-
			factor of safety	or installation			force with factor of
			Ensure harness	fatigue or			safety
1 1	1	1			1		Sarcey
			and mounting	failure			
			and mounting	failure			To provent UV wining
			hardware are				To prevent HV wiring
				Operator aware			harness installation
			hardware are fire retardant	Operator aware during			harness installation failure the development
			hardware are fire retardant Ensure harness	Operator aware during operation by			harness installation failure the development team shall ensure the
			hardware are fire retardant Ensure harness and mounting	Operator aware during operation by identifying			harness installation failure the development team shall ensure the harness and mounting
			hardware are fire retardant Ensure harness and mounting hardware is	Operator aware during operation by identifying eventual failure			harness installation failure the development team shall ensure the harness and mounting hardware is secure and
			hardware are fire retardant Ensure harness and mounting hardware is secure and free	Operator aware during operation by identifying eventual failure of HV			harness installation failure the development team shall ensure the harness and mounting
			hardware are fire retardant Ensure harness and mounting hardware is secure and free from	Operator aware during operation by identifying eventual failure			harness installation failure the development team shall ensure the harness and mounting hardware is secure and
			hardware are fire retardant Ensure harness and mounting hardware is secure and free	Operator aware during operation by identifying eventual failure of HV			harness installation failure the development team shall ensure the harness and mounting hardware is secure and free from unintended

Ltore DMC				Over-current	7	Ensure software (HSC, OBC, EMC) limits current rates and ranges Ensure relays and fuses are in place and functional to prevent over drawing of current	Operator aware during operation by error signal and identifying eventual failure of HV components	7	490	To prevent HV wiring harness over-current failure the development team shall ensure software (HSC, OBC, EMC) limits current rates and ranges To prevent HV wiring harness over-current failure the development team shall ensure relays and fuses are in place and functional to prevent over drawing of current
Item: BMS	D 1		1	D () 1		D (*		1		
Function	Failure Type	Potential Impact	S	Potential Cause	0	Prevention Mode	Detection Mode	D	RPN	Functional Requirement
Ensure safe ESS	Failure to	Unintended	10	Wiring failure	7	Ensure wiring	Vehicle	8	560	To prevent BMS wiring
			10	U	/	U	technical	0	500	
operating	ensure safe ESS	longitudinal motion		(not proper		is securely				failure the development team shall ensure the
conditions		motion		gauge,		installed using	inspection will			
M ' EGG	operating	т		installation or		manufacturer	identify wiring			wiring is securely
Monitor ESS	conditions	Loss or		manufacturing		installation	fatigue or			installed using
state (voltage,		degradation		failure)		specifications	failure			manufacturer
temperature,	Failure to	of propulsion					_			installation
SOC, and	monitor ESS	system				Ensure wiring	Operator aware			specifications
current)	state					gauge is	during			
	(voltage,	Operator				sufficient to	operation by			To prevent BMS wiring
Protects against	temperature,	and/or				carry max	identifying			failure the development
over-current,	SOC, and	passenger				operational	eventual failure			team shall ensure the
over-voltage,	current)	injury				current with	of HV			wiring gauge is
under-voltage,						factor of safety	components			sufficient to carry max
and over-	Failure to	Damage to or								operational current with
temperature	protect	loss of				Ensure wire				factor of safety
	against over-	property				bend radii are				
Reporting data	current, over-					adhered to				To prevent BMS wiring
	voltage,	Damage to								failure the development
	under-	environment								team shall ensure wire

Controls/balances	voltage, and	Potential for							bend radii are adhered
Controls/balances ESS environment	voltage, and over- temperature Failure to report data Failure to control and balance ESS environment	Potential for overheating Unintended exposure to high voltage Short circuit Thermal event Inaccurate ESS state readings (voltage, temperature, SOC)	Unintended access or physical damage (liquid, puncture)	5	Ensure manufacturing is sufficient to prevent unintended access and physical damage Ensure use of covering at wire-BMS interface prevent unintended access	Vehicle technical inspection will identify the BMS is free of unintended access and physical damage Operator aware during operation by identifying eventual failure of HV	9	450	bend radii are adhered to To prevent BMS failure the development team shall ensure the manufacturing is sufficient to prevent unintended access and physical damage To prevent BMS unintended access or physical damage failure the development team shall ensure use of covering at wire-BMS interface prevent unintended access
		SOC)			Avoid adverse road condition which may produce NVH and damage BMS	components			To prevent BMS unintended access or physical damage failure the operator shall avoid adverse road condition which may produce NVH and damage BMS
			Installation failure (wire, mounting)	7	Ensure BMS and mounting hardware are sufficient for max operational G-force with factor of safety Ensure BMS and mounting hardware is secure and free from	Vehicle technical inspection will identify if BMS is free of manufacturing or installation fatigue or failure Operator aware during operation by identifying	8	560	To prevent BMS installation failure the development team shall ensure the BMS and mounting hardware are sufficient for max operational G-force with factor of safety To prevent BMS installation failure the development team shall ensure the BMS and mounting hardware is

				Over-current	7	Ensure software limits current rates and ranges Ensure relays	components Operator aware during operation by error signal and identifying	7	490	To prevent BMS over- current failure the development team shall ensure software limits current rates and ranges
						and fuses are in place and functional to prevent over drawing of current	eventual failure of HV components			To prevent BMS over- current failure the development team shall ensure relays and fuses are in place and functional to prevent over drawing of current
				Over-heating	4	Ensure BMS is mounted such that there is proper clearance and sufficient air flow to cool the BMS	Vehicle technical inspection will identify if the BMS has proper clearance to allow for natural air flow cooling	9	360	To prevent BMS over- heating failure the development team shall ensure the BMS is mounted such that there is proper clearance and sufficient air flow to cool the BMS
							Operator aware during operation by identifying eventual failure of TVP components and loss of			
Item: OBC							functionality			
Function	Failure Type	Potential Impact	s	Potential Cause	0	Prevention Mode	Detection Mode	D	RPN	Functional Requirement

Controls charging to the HV battery pack	Failure to control charging to the HV battery pack	Potential for overheating Unintended exposure to high voltage Short circuit Thermal event Loss of motor functionality	10	Charging port failure	5	Ensure charging port cover is sufficient to provide freedom from unintended access or physical damage Ensure charging port is securely installed using manufacturer installation specifications Ensure wiring gauge is sufficient to carry max operational	Vehicle technical inspection will identify wiring fatigue or failure Operator aware during operation by identifying eventual failure of HV components	4	200	To prevent OBC charging port failure the development team shall ensure the charging port cover is sufficient to provide freedom from unintended access or physical damage To prevent OBC charging port failure the development team shall ensure the charging port is securely installed using manufacturer installation specifications To prevent OBC charging port failure the development team shall ensure wiring gauge is sufficient to carry max operational current with
				Wiring failure (not proper gauge, or installation)	7	current with factor of safety Ensure wire bend radii are adhered to Ensure wiring is securely installed using manufacturer installation specifications Ensure wiring gauge is	Vehicle technical inspection will identify wiring fatigue or failure Operator aware during operation by identifying eventual failure	8	560	factor of safety To prevent OBC charging port failure the development team shall ensure wire bend radii are adhered to To prevent OBC wiring failure the development team shall ensure the wiring is securely installed using manufacturer installation specifications

			sufficient to carry max operational current with factor of safety Ensure wire bend radii are adhered to	of HV components			To prevent OBC wiring failure the development team shall ensure wiring gauge is sufficient to carry max operational current with factor of safety To prevent OBC wiring failure the development team shall ensure wire bend radii are adhered to
	Unintended access or physical damage (liquid, puncture)	5	Ensure manufacturing is sufficient to prevent unintended access and physical damage Ensure use of covering at wire-OBC interface prevents unintended access Avoid adverse road condition which may produce NVH and damage OBC Ensure	Vehicle technical inspection will identify the OBC is free of unintended access Operator aware during operation by identifying eventual failure of HV components	9	450	To prevent OBC failure the development team shall ensure manufacturing is sufficient to prevent unintended access and physical damage To prevent OBC unintended access or physical damage failure the development team shall ensure the use of covering at wire-OBC interface prevents unintended access To prevent OBC unintended access or physical damage failure the development team shall ensure charging port cover is sufficient to provide freedom from unintended access
			charging port cover is				or physical damage

 			CC				The second
			sufficient to				To prevent OBC
			provide				unintended access or
			freedom from				physical damage failure
			unintended				the operator shall avoid
			access or				adverse road condition
			physical				which may produce
			damage				NVH and damage OBC
	Installation	7	Ensure OBC	Vehicle technical	8	560	To prevent OBC
	failure (wire,		and mounting	inspection will			installation failure the
	mounting)		hardware are	identify if OBC			development team shall
			sufficient for	is free of			ensure the OBC and
			max operational	manufacturing or			mounting hardware are
			G-force with	installation			sufficient for max
			factor of safety	fatigue or failure			operational G-force
				-			with factor of safety
			Ensure OBC,	Operator aware			-
			charging port,	during operation			To prevent OBC
			and mounting	by identifying			installation failure the
			hardware are	eventual failure			development team shall
			secure and free	of HV			ensure the OBC,
			from	components			charging port, and
			unintended	1			mounting hardware are
			movement				secure and free from
							unintended movement
	Over-current	7	Ensure software	Operator aware	7	490	To prevent OBC over-
			limits current	during operation	-		current failure the
			rates and ranges	by error signal			development team shall
				and identifying			ensure software limits
			Ensure relays	eventual failure			current rates and ranges
			and fuses are in	of HV			and ranges
			place and	components			To prevent OBC over-
			functional to				current failure the
			prevent over				development team shall
			drawing of				ensure relays and fuses
			current				are in place and
			Current				functional to prevent
							over drawing of current
	Operation	8	Ensure	OBC	8	640	To prevent OBC over-
	outside of	0			0	040	heating failure the
			operation	temperature			
	max/min		within specified				development team shall

			1	tampagatuga	1	OBC	aignal canda data	1		ensure software limits
				temperature			signal sends data in real time			
				range		temperature	in real time			operation within
				(environmental		range	0			specified OBC
				or coolant		A	Operator aware			temperature range
				failure)		Actuate cooling	during operation			
						fans when OBC	by identifying a			-
						reaches	thermal event,			To prevent OBC over-
						specified	error message of			heating failure the
						temperature	overheating, or			development team shall
							failure of HV			ensure actuation of
						Use	components			thermal control system
						manufacturer				(fans) when OBC
						recommended				reaches specified
						installation				temperature
						instructions				
						(clearance,				
						bend radii)				To prevent OBC over-
										heating failure the
										development team shall ensure manufacturer
										recommended
										installation instructions
										(clearance, bend radii)
Item: EMC					-			1		
	Failure	Potential		Potential		Prevention				Functional
Function	Туре	Impact	S	Cause	0	Mode	Detection Mode	D	RPN	Requirement
Controls supply	Failure to	Unintended	10	Wiring failure	7	Ensure wiring	Vehicle technical	8	560	To prevent EMC wiring
of current to EM	control	acceleration		(not proper		is securely	inspection will			failure the development
	current			gauge,		installed using	identify wiring			team shall ensure the
Convert DC to	supply to EM	Unintended		installation or		manufacturer	fatigue or failure			wiring is securely
AC		longitudinal		manufacturing		installation				installed using
	Failure to	motion		failure)		specifications	Operator aware			manufacturer
Control direction	control						during operation			installation
	1	L _	1	1	1	- · ·	1	1	1	

	Failure to	motion	failure)	specifications	Operator aware		manufacturer	
Control direction	control				during operation		installation	
of current	current	Loss or		Ensure wiring	by identifying		specifications	
	direction	degradation		gauge is	eventual failure		-	
Control EM		of propulsion		sufficient to	of HV		To prevent EMC wiring	
temperature	Failure to	system		carry max	components		failure the development	
-	control EM			operational			team shall ensure	
	temperature			_			wiring gauge is	

Operator and/or passenger injury Damage to or loss of property			current with factor of safety Ensure wire bend radii are adhered to				sufficient to carry max operational current with factor of safety To prevent EMC wiring failure the development team shall ensure wire bend radii are adhered to
Damage to environment Potential for overheating Unintended exposure to high voltage	Unintended access or physical damage (liquid, puncture)	5	Ensure manufacturing is sufficient to prevent unintended access and physical damage Ensure use of covering at wire-EMC interface prevent unintended access Avoid adverse road condition which may produce NVH and damage EMC	Vehicle technical inspection will identify the EMC is free of unintended access Operator aware during operation by identifying eventual failure of HV components	9	450	To prevent EMC failure the development team shall ensure manufacturing is sufficient to prevent unintended access and physical damage To prevent EMC unintended access failure the development team shall ensure the use of covering at wire- EMC interface prevent unintended access failure the operator shall avoid adverse road condition which may produce NVH and damage EMC
	Installation failure (wire, mounting)	7	Ensure EMC and mounting hardware are sufficient for max operational G-force with factor of safety	Vehicle technical inspection will identify if EMC is free of manufacturing or installation fatigue or failure	8	560	To prevent EMC installation failure the development team shall ensure the EMC and mounting hardware are sufficient for max

		Ensure EMC and mounting hardware is secure and free from unintended movement	Operator aware during operation by identifying eventual failure of HV components			operational G-force with factor of safety To prevent EMC installation failure the development team shall ensure the EMC and mounting hardware is secure and free from unintended movement
Over-current	7	Ensure software limits current rates and ranges Ensure relays and fuses are in place and functional to prevent over drawing of current	Operator aware during operation by error signal and identifying eventual failure of HV components	7	490	To prevent EMC over- current failure the development team shall ensure software limits current rates and ranges To prevent EMC over- current failure the development team shall ensure relays and fuses are in place and functional to prevent over drawing of current
Operation outside of max/min temperature range (environmental or coolant failure)	8	Ensure operation within specified EMC temp range Actuate cooling fans when EMC reaches specified temperature Use manufacturer recommended installation instructions	EMC monitors and sends temperature data in real time Operator aware during operation by identifying a thermal event, error message of overheating, or failure of HV components	8	640	To prevent EMC over- heating failure the development team shall ensure software limits operation within specified EMC temp range To prevent EMC over- heating failure the development team shall ensure actuation of thermal control system (fans) when EMC reaches specified temperature

		(clearance,	To prevent EMC over-
		bend radii)	heating failure the
			development team shall
			ensure using
			manufacturer
			recommended
			installation instructions
			(clearance, bend radii)

Appendix 3.07 HARA PSI HV HazOP

				PSI I	IV Process	Paramet	er and Gu	ide Wor	d Combinatio	on Chart				
								Guide V	Vord					
HV Proc Paramete	•55	As as	s well	Part of	Reverse	Other	Early	Late	Before	After	Faster	Slower	More	Less
NVI	H										Х		Х	
Temper	ature												Х	Х
Curre	ent	X		Х	Х		Х	X					Х	X
Cleara	ince												Х	X
Unautho Acce													X	
]	PSI HV Ha	azOP						
FUNCTI	ON: A	pply NVH	Stimul	i to High V	Voltage Sys	tem								
Guide Word	Deviation	Conse	equenc	es	Caus	es		ł	Safeguards		Function	onal Requi	rement	
Faster	is applied hardware too quickly loosens/separates ESS components disconnect from each		Inade of sat	Adverse road conditions. Inadequate installation, factor of safety, or mounting hardware			Proper installat of safety, solde component sec mounting hard	TVP ESS shall be capable of withstanding a high road vibrational frequency						
		other												

		Potential thermal runaway - Fire			
More	NVH amplitude reaches threshold	ESS components disconnect from each other Potential thermal runaway - Fire ESS components disconnect from each other	Adverse road conditions. Inadequate installation, factor of safety, or mounting hardware	Proper installation, factor of safety, soldering, component security and mounting hardware.	TVP ESS shall be capable of withstanding a high road vibrational amplitude
FUNCT	TION: App	ly Temperature Stimuli to Hig	h Voltage System		
Guide Word	Deviation	Consequences	Causes	Safeguards	Functional Requirement
More	ESS temperature is greater than max	TVP/operator damage/injury	ESS component error, cooling system error, software controls error	Controls software validation during SIL. ESS controls validation. E-stop validation. ESS	The TVP ESS shall operate within a safe and specified temperature range
	operating temperature	Potential thermal runaway - Fire		thermal control validation. Thorough testing during SIL, zero velocity and closed course phases	
Less	ESS temperature is less than	Item damage or lost functionality	Extremely cold environmental conditions.	Do not operate during extremely cold environmental conditions.	
	minimum operating temperature	TVP/operator damage/injury			
FUNCT	TION: App	ly Current Stimuli to High Vo	ltage System		
Guide Word	Deviation	Consequences	Causes	Safeguards	Functional Requirement
No	No current applied when charging	ESS does not function	OBC failure. Controls software/hardware error.	Ensure ESS components, control software/hardware are installed properly. Thoroughly test during SIL, zero velocity, and closed course phases	The current applied to the ESS when charging shall match the current requested

	No current applied when discharging	EM/ESS does not function Torque request not met	Power supply error. Controls software/hardware error. EM malfunction. Contactors disengaged	Ensure ESS components, control software/hardware, APPS, and EM are installed properly. Thoroughly test during SIL, zero velocity, and closed course phases	The current applied by the ESS when discharging shall match the current requested
Part of	Only part of current applied when charging	ESS does not charge as fast as intended	OBC failure. Controls software/hardware error.	Ensure ESS components, control software/hardware are installed properly. Thoroughly test during SIL, zero velocity, and closed course phases	The current applied to the ESS when charging shall match the current requested
	Only part of current applied when discharging	EM/ESS does not function as intended TVP does not accelerate as intended Torque request not met	Power supply error. Controls software/hardware error. EM malfunction. Contactors disengaged	Ensure ESS components, control software/hardware, APPS, and EM are installed properly. Thoroughly test during SIL, zero velocity, and closed course phases	The current applied by the ESS when discharging shall match the current requested
Reverse	Current applied is reverse of intended	TVP accelerates in direction other than intended TVP collides with object TVP/operator damage/injury	Power supply error. Controls software/hardware error. EM malfunction. APPS error	Ensure ESS components, control software/hardware, APPS, and EM are installed and functioning properly. Thoroughly test during SIL, zero velocity, and closed course phases	The current applied shall match the direction of the current requested
Early	Current applied earlier than intended	TVP accelerates earlier than intended TVP collides with object TVP/operator damage/injury	Power supply error. Controls software/hardware error. EM malfunction. APPS error	Ensure ESS components, control software/hardware, APPS, and EM are installed and functioning properly. Thoroughly test during SIL, zero velocity, and closed course phases	The current applied shall be delivered at the time intended

Late	Current applied later than intended	TVP accelerates later than intended	Power supply error. Controls software/hardware error. EM malfunction. APPS error	Ensure ESS components, control software/hardware, APPS, and EM are installed and functioning properly. Thoroughly test during SIL, zero velocity, and closed course phases	
More	Current applied is greater than intended	TVP accelerates faster than intended TVP collides with object TVP/operator damage/injury Fire	Power supply error. Controls software/hardware error. EM malfunction. APPS error	Ensure ESS components, control software/hardware, APPS, and EM are installed and functioning properly. Thoroughly test during SIL, zero velocity, and closed course phases	The magnitude of the current applied shall match the magnitude of the current requested
Less	Current applied is less than intended	EM/ESS does not function as intended TVP does not accelerate as intended Torque request not met	Power supply error. Controls software/hardware error. EM malfunction. APPS error	Ensure ESS components, control software/hardware, APPS, and EM are installed and functioning properly. Thoroughly test during SIL, zero velocity, and closed course phases	

FUNCTION: Apply Clearance To High Voltage Components

Guide Word	Deviation	Consequences	Causes	Safeguards	Functional Requirement
More	Component installation clearance is more than required	Limits the space to make future modifications	Poor design. Over compensation.	Ensure manufacturer clearance and installation specifications are met.	High voltage component clearance requirements shall be minimized to ensure space is available for modifications
Less	Components installation clearance is	Thermal transfer leading to over heating TVP/operator damage/injury	Poor design. Lack understanding of clearance requirements	Ensure manufacturer clearance and installation specifications are met.	High voltage component clearance requirements shall be met to ensure safe TVP operation

	less than required	Difficulty installing and maintaining the high voltage components			
FUNCT	ION: Appl	y Unauthorized Access Stimu	III To The High Voltage System		
Guide Word	Deviation	Consequences	Causes	Safeguards	Functional Requirement
More	More/any unauthorized	Short circuit	Animals, insects, fingers, liquid, snow, dust, and debris.	Ensure ESS enclosure ventilation and ports are	The ESS enclosure and high voltage system shall prevent unauthorized
	access is applied to	Fire	Poor design of ESS enclosure	secured using mesh or other impassable filter.	access and physical damage to the high voltage components
	high voltage system	TVP/operator damage/injury			

Appendix 3.08 HARA PSI Mechanical Controls Hardware HazOP

Parameter as as as NVH Image: Constraint of the second seco								Guide Wo	ord					
NVH X X X Temperature Image: Second se	CH Process	No	As well	Part of	Reverse	Other	Early	Late	Before	After	Faster	Slower	More	Less
Temperature Image: Constraint of the state of the	Parameter		as											
Current X <t< td=""><td>NVH</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Х</td><td></td><td>Х</td><td></td></t<>	NVH										Х		Х	
Clearance X X PSI Mechanical HazOP of the Controls Hardware System	Temperature												Х	X
PSI Mechanical HazOP of the Controls Hardware System	Current	Х					Х	Х					Х	X
	Clearance												Х	X
	FUNCTION	App	y NVH Stim					Controls]	Iardware S	ystem				
	Guide													

Faster	NVH stimuli is applied too quickly	Controls hardware components loosens/separates from mounts/wiring	Adverse road conditions. Inadequate installation, factor of safety, or mounting hardware	Proper installation, factor of safety, soldering, component security and mounting hardware.	Vehicle controls hardware shall be capable of withstanding a high NVH frequency and physical damage
		Vehicle components/subsystems lose functionality			
		Vehicle/operator damage/injury			
More	NVH amplitude reaches threshold	Controls hardware components loosens/separates from mounts/wiring Vehicle components/subsystems lose functionality Vehicle/operator	Adverse road conditions. Inadequate installation, factor of safety, or mounting hardware	Proper installation, factor of safety, soldering, component security and mounting hardware.	Vehicle controls hardware shall be capable of withstanding a high NVH amplitude
		damage/injury			
FUNCT	T ION: Ap	ply Temperature Stimuli to Co	ontrols Hardware System		
FUNCT Guide Word	TON: Ap		ontrols Hardware System	Safeguards	Functional Requirement
Guide		ply Temperature Stimuli to Co		Safeguards E-stop validation. Controls hardware thermal control validation. Thorough testing during zero velocity and closed course phases	Functional Requirement The controls hardware shall operate within a safe and specified temperature range

Guide					
Word	Deviation	Consequences	Causes	Safeguards	Functional Requirement
No	No current applied when intended	Vehicle components/subsystems lose functionality	ESS, power supply, or controls software/hardware error.	Ensure control software/hardware are installed properly. Thoroughly test during SIL, zero velocity, and closed course phases	The current applied to the controls hardware shall match the current requested
Early	Current applied earlier than intended	Vehicle actuates earlier than intended Vehicle collides with object Vehicle/operator damage/injury	Power supply, ESS, or controls software/hardware error. APPS error	Ensure ESS components, control software/hardware, and APPS are installed and functioning properly. Thoroughly test during SIL, zero velocity, and closed course phases	The current applied to the controls hardware shall be delivered at the time intended
Late	Current applied later than intended	Vehicle actuates later than intended	Power supply, ESS, or controls software/hardware error. APPS error	Ensure ESS components, control software/hardware, APPS, and EM are installed and functioning properly. Thoroughly test during SIL, zero velocity, and closed course phases	
More	Current applied is greater than intended	Controls hardware/vehicle components lose functionality Controls hardware actuates vehicle components in manner other than intended Vehicle collides with object Vehicle/operator damage/injury Fire	Power supply, controls software/hardware, or ESS malfunction	Ensure ESS components, control software/hardware, and power supply are installed and functioning properly. Thoroughly test during SIL, zero velocity, and closed course phases	The magnitude of the current applied to controls hardware shall match the magnitude of the current requested

Less	Current	Controls hardware/vehicle	Power supply, controls	Ensure ESS components,	
	applied is	components lose	software/hardware, or ESS	control	
	less than	functionality	malfunction	software/hardware, and	
	intended	Controls hardware actuates		power supply are installed	
		vehicle components in		and functioning properly.	
		manner other than intended		Thoroughly test during	
		Vehicle does not accelerate		SIL, zero velocity, and	
		as intended		closed course phases	
		Torque request not met			

FUNCTION:

Apply Clearance To Controls Hardware Components

Guide Word	Deviation	Consequences	Causes	Safeguards	Functional Requirement
More	Component installation clearance is more than required	Limits the space to make future modifications	Poor design. Over compensation.	Ensure manufacturer clearance and installation specifications are met.	Controls hardware component clearance requirements shall be minimized to ensure space is available for modifications
Less	Components installation clearance is less than required	Thermal transfer leading to over heating Vehicle/operator damage/injury Difficulty installing and maintaining the controls hardware components	Poor design. Lack understanding of clearance requirements	Ensure manufacturer clearance and installation specifications are met.	Controls hardware component clearance requirements shall be met to ensure safe vehicle operation

Appendix 3.09 HARA PSI Mechanical DFMEA

PSI Mechanical DFMEA
Item: Modified Driveshaft

		Potential		Potential		Prevention	Detection			Functional
Function	Failure Type	Impact	S	Cause	0	Mode	Mode	D	RPN	Requirement
Function Transmit torque from engine/EM to rear of vehicle	Failure Type Loss of torque transmission		S 10		O 8			D 9	RPN 720	
		regenerative braking				potential unintended access or physical damage				
				Driveshaft-EM interface angle too great	2	Ensure proper manufacturing and design for minimal interface angle	Vehicle technical inspection will identify interface angle	5	100	Development team shall ensure proper manufacturing and design for minimal driveshaft-EM interface angle
				Adverse road conditions	3	Avoid adverse road condition which may	Operator aware prior to or	3	90	Operator shall avoid adverse road condition which may produce

			produce NVH and damage driveshaft	during operation. Increased NVH			NVH and damage driveshaft
	Driveshaft-rear differential interface failure (disconnection, slipping)	8	Ensure proper mounting, installation, and manufacturing of modified driveshaft and its components Ensure bolts and mounting hardware is securely fastened and free from potential loosening or unintended movement Ensure driveshaft- differential interface location is covered and free from potential unintended access or physical damage	Vehicle technical inspection will identify interface is free of manufacturing or installation fatigue or failure Operator aware during operation by identifying total functionality failure	9	720	Development team shall ensure proper mounting, installation, and manufacturing of modified driveshaft and its components Development team shall ensure driveshaft bolts and mounting hardware is securely fastened and free from potential loosening or movement Development team shall ensure driveshaft-EM interface location is covered and free from potential unintended access or physical damage
	Unintended access and	3	Ensure driveshaft	Vehicle technical	9	270	Development team shall ensure driveshaft
	physical		manufacturing	inspection will			manufacturing and use

						sufficient to prevent unintended access and physical damage	free of physical damage			unintended access and physical damage
Item: Differen	ntial									
Function	Failure Type	Potential Impact	s	Potential Cause	0	Prevention Mode	Detection Mode	D	RPN	Functional Requirement
Provides power from driveshaft to wheels and allows wheels to rotate at different speeds	Loss of power to rear wheels	Unintended Vehicle deceleration Unintended longitudinal motion Operator and/or passenger injury Damage to or loss of property Damage to environment Partial torque transmission	9	Differential- Driveshaft interface failure (disconnection, slipping)	8	Ensure proper mounting, installation, and manufacturing of modified driveshaft and its components Ensure bolts and mounting hardware is securely fastened and free from potential loosening or movement Ensure differential- driveshaft interface location is free from potential unintended access or physical damage	Vehicle technical inspection will identify if the interface is free of manufacturing or installation fatigue or failure Operator aware during operation by identifying partial or total functionality failure	9	648	Development team shall ensure proper mounting, installation, and manufacturing of modified driveshaft, differential and their components Development team shall ensure driveshaft bolts and mounting hardware is securely fastened and free from potential loosening or movement Development team shall ensure differential-driveshaft interface location is covered and free from potential unintended access or physical damage

Adverse road conditions	3	Avoid adverse road condition which may produce NVH and damage differential	Operator aware prior to or during operation. Increased NVH	3	81	Operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH
Half shaft interface failure (disconnection, slipping)	2	Ensure proper mounting, installation, and manufacturing of modified differential and its components Ensure bolts and mounting hardware is securely fastened and free from potential loosening or movement Ensure differential-half shaft interface location is free from potential unintended access or physical damage	Vehicle technical inspection will identify if the interface is free of manufacturing or installation fatigue or failure Operator aware during operation by identifying partial or total functionality failure	9	162	Development team shall ensure proper mounting, installation, and manufacturing of modified differential and its components Development team shall ensure bolts and mounting hardware is securely fastened and free from potential loosening or movement Development team shall ensure differential-half shaft interface location is free from potential unintended access or physical damage
Gear fatigue failure - slip	1	N/A	Operator aware during operation by identifying partial or total	8	72	

							functionality failure			
Item: Suspens	ion									
Function	Failure Type	Potential Impact	S	Potential Cause	0	Prevention Mode	Detection Mode	D	RPN	Functional Requirement
Support vehicle weight and absorb/reduce excess energy form road shock	Suspension fails to support vehicle weight and absorb/reduce excess energy form road shock	Unintended lateral movement Pulling to one side Difficult to steer Vehicle corner sits low Operator and/or passenger injury Damage to or loss of property Damage to environment	7	Uneven tire pressure and tire wear	5	Ensure proper tire pressure prior to operation Ensure proper tire alignment Ensure tire quality Ensure balanced, bent, or broken wheels Avoid poor drive behavior Ensure to rotate tires regularly	Error message will occur Vehicle technical inspection will identify low tire pressure and uneven tire wear	2	70	Operator shall ensure proper tire pressure prior to operation Operator shall ensure proper tire alignment Operator shall ensure tire quality Operator shall ensure wheels are balanced and suspension is free of ben tor broken wheels Operator shall avoid poor driving behaviors Operator shall ensure manufacturer recommended tire rotation
				Radius rod fatigue	2	Routine maintenance and inspection Avoid poor driving behavior	Operator aware during operation by audible clunking sound when accelerating or braking and loose steering	3	42	Development team shall ensure suspension radius rods are free from fatigue and corrosion

			Deterioration of performance. Vehicle technical inspection will identify rust or corrosion			
Poor tire alignment	4	Routine maintenance and inspection Ensure proper functioning parts (springs) Avoid poor drive behavior	Operator aware of vehicle pulling during operation and steering wheel vibration Deterioration of performance. Vehicle technical inspection will identify poor tire alignment	6	168	Operator shall ensure proper tire alignment Operator shall avoid poor driving behaviors
Adverse ro conditions		Avoid adverse road condition which may produce NVH and damage suspension	Operator aware prior to or during operation. Increased NVH	3	63	Operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH
Poorly calibrated spring compression	on 1	Routine maintenance and inspection for rust Avoid adverse road conditions	Operator aware during operation from vehicle sagging and unsettling noise Deterioration of performance.	6	42	Development team shall ensure suspension spring compression is calibrated and that springs are free of fatigue and corrosion

					Vehicle technical inspection will identify spring fatigue			
		Mounting hardware failures	3	Ensure proper mounting, installation, and routine maintenance and inspection of hardware Ensure bolts and mounting hardware is securely fastened and free from potential loosening or unintended movement	Operator aware during operation. Deterioration of performance. Vehicle technical inspection will identify rust, corrosion, and failure	3	63	Development team shall ensure the suspensions system and components have proper mounting, installation, and routine maintenance and inspection of hardware Development team shall ensure the suspensions system bolts and mounting hardware is securely fastened and free from potential loosening or unintended movement
		Wheel bearing fatigue	1	Ensure proper mounting, installation, and routine maintenance and inspection of bearing	Operator aware during operation. Deterioration of performance.	6	42	Development team shall ensure proper mounting, installation, and routine maintenance and inspection of wheel bearing
Unintended longitudinal movement Momentum makes the vehicle unstable (nose dive during braking, or lean	6	Spring fatigue	1	Routine maintenance and inspection for rust and corrosion Avoid adverse road conditions	Operator aware during operation from vehicle sagging and unsettling noise Deterioration of performance.	6	36	Development team shall ensure suspension spring compression is calibrated and that springs are free of fatigue and corrosion

back during acceleration) Operator and/or passenger injury					Vehicle technical inspection will identify spring fatigue			
Damage to or loss of property Damage to environment		Strut fatigue	1	Routine maintenance and inspection for rust and corrosion Avoid adverse road conditions	Operator aware during operation by identifying wheel vibration and tire shaking Vehicle technical inspection will identify potential leaking from strut or shock	6	36	Development team shall ensure struts are free of fatigue and corrosion
NVH (feeling every bump) Damage to or loss of property	5	Shock absorber fluid leak	1	Routine maintenance and inspection for fluid leak Avoid adverse road conditions	Operator aware during operation by identifying vibrations, swerving and nose diving Vehicle technical inspection will identify leak.	3	15	Development team shall ensure shock absorbers are free of fatigue and leaks
		Spring fatigue	1	Routine maintenance and inspection for rust and corrosion Avoid adverse road conditions	Operator aware during operation from vehicle sagging and unsettling noise	6	30	Development team shall ensure suspension spring compression is calibrated and that springs are free of fatigue and corrosion

				Adverse road conditions	2	Avoid adverse road condition	Deterioration of performance. Vehicle technical inspection will identify spring fatigue Operator aware prior to or	4	40	Operator shall avoid excessively adverse
						which may produce NVH and damage suspension	during operation. Increased NVH			road conditions (bumpy terrain, excessive grade) which may cause a high NVH
Item: Brakes	11		1				1			0
		Potential		Potential		Prevention	Detection			Functional
Function	Failure Type	Impact	S	Cause	0	Mode	Mode	D	RPN	Requirement
Inhibits vehicle motion. Slows/stops moving vehicle Keeps stopped vehicle stationary	Brakes fail to Inhibit vehicle motion. Brakes fail to slow/stop moving vehicle Brakes fail to keep stopped vehicle stationary	Unintended loss of longitudinal motion Operator and/or passenger injury Damage to or loss of property Damage to environment Unintended vehicle motion when stationary (rollaway)	9	Brake pad fatigue or failure (overheating, corrosion)	5	Ensure proper mounting and installation of pads Ensure bolts and mounting hardware is securely fastened and free from potential loosening or movement Avoid adverse road conditions Routine maintenance and inspection	Vehicle technical inspection will identify if the pads are free from fatigue or corrosion Operator aware during operation by identifying unsettling smell, and vehicle vibration	3	135	Development team shall ensure proper mounting and installation of pads Development team shall ensure brake pad bolts and mounting hardware is securely fastened and free from potential loosening or unintended movement Operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH

Brake rotor	4	for rust and corrosion Avoid poor drive behavior Ensure proper	Vehicle	3	108	Operator shall perform routine inspection of brake system to check for rust, fatigue, and corrosion Operator shall avoid poor driving behaviors Development team
fatigue or failure (overheating, corrosion)		mounting and installation of rotors Ensure bolts and mounting hardware is securely fastened and free from potential loosening or movement Avoid adverse road conditions Routine maintenance and inspection for rust and corrosion Avoid poor drive behavior	technical inspection will identify if the rotors are free from fatigue or corrosion Operator aware during operation by identifying unsettling smell, and vehicle vibration		1/2	shall ensure proper mounting and installation of rotors Development team shall ensure rotor bolts and mounting hardware is securely fastened and free from potential loosening or unintended movement Operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH Development team shall perform routine maintenance and inspection for rotor rust and corrosion Operator shall avoid poor driving behaviors
Debris (snow, mud) build-up	3	Ensure brake system is free of build-up and	Vehicle technical inspection will	6	162	Operator shall ensure brake system is free of

on brake system		debris prior to use	identify if the brake system is free from build- up Operator aware during operation by identifying vehicle NVH			build-up and debris prior to use
Adverse road conditions (bumpy terrain, excessive grade)	2	Avoid adverse road condition which may produce NVH and damage suspension	Operator aware prior to or during operation. Increased NVH	4	72	Operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH
Calipers get stuck	2	Avoid adverse road conditions Routine maintenance and inspection for rust and corrosion Avoid poor drive behavior	Operator aware during operation by identifying unsettling smell, vehicle vibration, and partial or total loss of functionality	6	108	Operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH Development team shall perform routine maintenance and inspection for caliper rust and corrosion
Brake fluid line failure (leak, air in line)	2	Ensure proper bleeding, mounting, installation, and routine maintenance and inspection of hardware	Operator aware during operation by identification of degrading performance Vehicle technical	5	90	Development team shall ensure proper bleeding, mounting, installation, and routine maintenance and inspection of hardware and functionality

						and functionality Ensure bolts and mounting hardware is securely fastened and free from potential loosening or unintended movement	inspection will identify leaks.			Development team shall ensure bolts and mounting hardware is securely fastened and free from potential loosening or unintended movement
Item: Thermal				Parking brake failure (rollaway)	1	Ensure routine maintenance and inspection of hardware and functionality	Operator aware of runaway during operation by identification of unintended vehicle motion	8	72	Development team shall ensure routine maintenance and inspection parking brake hardware and verify functionality
		Potential	C	Potential	0	Prevention Mode	Detection Mode	D	RPN	Functional
Function Detects and controls cabin and component temperatures	Failure Type Failure to detect and control cabin and component temperatures	ImpactLoss ordegradation ofpropulsionOperator and/orpassengerinjuryDamage to orloss of propertyDamage toenvironmentFire, smoke	<u>S</u> 10	Cause Engine overheats (mechanical, electrical, and ECM failure or aggressive driving)	3	Ensure thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the engine Ensure the fans are free from potential physical damage	Sensors signal to ECM Operator aware during operation. Operator views engine temp in cabin. Error message displayed.	8	240	RequirementDevelopment teamshall ensure thermalsystem components(radiator, coolantlevel, fans) arefunctional andsufficient to cool theengineDevelopment teamshall ensure thethermal systems fansare free from potentialphysical damage

ГТ		
	Ensure	Development team
	enclosure fans	shall ensure thermal
	pull air from a	system fans pull air
	cool source	from a cool source
	Ensure engine	Development team
	ventilation is	shall ensure engine
	sufficient to	ventilation is
	provide	sufficient to provide
	appropriate air	appropriate air
	movement	movement through
	through engine	engine bay
	bay	engine ouy
		Development teams
	Ensure thermal	shall ensure thermal
	system is	system is designed
	designed such	such that there is
	that there is	sufficient air flow to
	sufficient air	cool engine
	flow to cool	components
	engine	
	components	Development team
		shall ensure proper
	Ensure proper	mounting,
	mounting,	installation, and
	installation, and	manufacturing of
	manufacturing	thermal system and its
	of thermal	components
	system and its	
	components	Development team
		shall ensure thermal
	Ensure bolts	system bolts and
	and mounting	mounting hardware
	hardware are	are securely fastened
	securely	and free from
	fastened and	potential loosening or
	free from	movement
	potential	
	loosening or	Development team
	movement	shall ensure the ECM

		Ensure the ECM controls and mitigates overheating Operator drives appropriately to ensure engine temp is stable				controls and mitigates overheating Operator shall avoid poor driving behaviors
Insufficient coolant levels	2	Ensure proper coolant levels and check for leaks prior to operation	Vehicle technical inspection will identify low fluid level and leaks Operator aware during operation by identifying displayed high temperatures	3	60	Operator shall ensure proper coolant levels and check for leaks prior to operation
Pump failure	3	Ensure proper mounting, installation, and manufacturing of water pump and its components Ensure bolts, interface components (seals, gaskets), and mounting hardware are securely	Vehicle technical inspection will identify low fluid level, leaks, and belt fatigue Operator aware during operation by identifying displayed high temperatures	5	150	Development team shall ensure proper mounting, installation, and manufacturing of water pump and its components Development team shall ensure thermal system pump bolts, interface components (seals, gaskets), and mounting hardware are securely fastened

			fastened and				and free from
			free from				potential loosening or
			potential				movement
			loosening or				movement
			movement				Development team
			movement				shall ensure the
			En avenue die a				
			Ensure the				correct type of coolant
			correct type of				is used, proper coolant
			coolant is used,				levels, and check for
			proper coolant				leaks prior to
			levels, and				operation
			check for leaks				
		1	prior to				Development team
		1	operation				shall ensure thermal
							system belt drive
			Ensure belt				components are
			drive				properly installed
			components are				(tensioning, torque
			properly				specs)
			installed				
			(tensioning,				
			torque specs)				
	Radiator failure	3	Ensure proper	Vehicle	5	150	Development team
			mounting,	technical	_		shall ensure proper
			installation, and	inspection will			mounting, installation,
			manufacturing	identify low			and manufacturing of
			of radiator,	fluid level,			radiator, clamps, hoses
			clamps, hoses	leaks, and rust			and their components
			and their	icaks, and fust			and their components
		1	components	Operator aware			Development team
			components	during			shall ensure radiator
			Ensure bolts,	operation by			bolts, interface
			Elisure Dolls,	operation by	1		,
			· · · · ·				acomponents (1-
			interface	identifying			components (seals,
			interface components	identifying displayed high			gaskets), and
			interface components (seals, gaskets),	identifying			gaskets), and mounting hardware
			interface components (seals, gaskets), and mounting	identifying displayed high			gaskets), and mounting hardware are securely fastened
			interface components (seals, gaskets), and mounting hardware are	identifying displayed high			gaskets), and mounting hardware are securely fastened and free from
			interface components (seals, gaskets), and mounting hardware are securely	identifying displayed high			gaskets), and mounting hardware are securely fastened
			interface components (seals, gaskets), and mounting hardware are	identifying displayed high			gaskets), and mounting hardware are securely fastened and free from

		potential loosening or movement Ensure the correct type of coolant is used, proper coolant levels, and check for rust and leaks prior to operation				Development team shall ensure the correct type of coolant is used, proper coolant levels, and check for rust and leaks prior to operation
Hose failure	3	Ensure proper mounting, installation, and manufacturing of hoses, clamps, and their components Ensure interface components (seals, gaskets), and mounting hardware are securely fastened and free from potential loosening or movement Ensure the correct type of coolant is used, proper coolant levels, and check for leaks	Vehicle technical inspection will identify leaks Operator aware during operation by identifying displayed high temperatures	4	120	Development team shall ensure proper mounting, installation, and manufacturing of hoses, clamps, and their components Development team shall ensure thermal system hose interface components (seals, gaskets), and mounting hardware are securely fastened and free from potential loosening or unintended movement Development team shall ensure the correct type of coolant is used, proper coolant levels, and check for leaks prior to operation

			prior to				
			operation				
	Thermostat	2	Ensure proper	Operator aware	5	100	Development team
	failure		mounting,	during			shall ensure proper
			installation, and	operation by			mounting,
			manufacturing	identifying			installation, and
			of thermostat	displayed high			manufacturing of
				temperatures in			thermostat
			Ensure	the event the			thermostat
			interface	the event the			Development team
			components	stuck shut, and			shall ensure
			and mounting	low			thermostat interface
			hardware are				
				temperature in			components and
			securely	the event the			mounting hardware
			fastened and	thermostat is			are securely fastened
			free from	stuck open			and free from
			potential				potential loosening or
			loosening or				movement
			movement				
	Fan failure	2	Ensure proper	Vehicle	5	100	Development team
	Fan failure	2	mounting,	technical	5	100	shall ensure proper
	Fan failure	2	mounting, installation, and	technical inspection will	5	100	shall ensure proper mounting,
	Fan failure	2	mounting, installation, and manufacturing	technical	5	100	shall ensure proper
	Fan failure	2	mounting, installation, and	technical inspection will	5	100	shall ensure proper mounting,
	Fan failure	2	mounting, installation, and manufacturing	technical inspection will identify fan	5	100	shall ensure proper mounting, installation, and
	Fan failure	2	mounting, installation, and manufacturing of the fan and	technical inspection will identify fan	5	100	shall ensure proper mounting, installation, and manufacturing of the
	Fan failure	2	mounting, installation, and manufacturing of the fan and	technical inspection will identify fan functionality Operator aware	5	100	shall ensure proper mounting, installation, and manufacturing of the thermal system fans
	Fan failure	2	mounting, installation, and manufacturing of the fan and its components	technical inspection will identify fan functionality Operator aware during	5	100	shall ensure proper mounting, installation, and manufacturing of the thermal system fans and its components
	Fan failure	2	mounting, installation, and manufacturing of the fan and its components Ensure bolts, interface	technical inspection will identify fan functionality Operator aware during operation by	5	100	shall ensure proper mounting, installation, and manufacturing of the thermal system fans
	Fan failure	2	mounting, installation, and manufacturing of the fan and its components Ensure bolts, interface components,	technical inspection will identify fan functionality Operator aware during operation by identifying	5	100	shall ensure proper mounting, installation, and manufacturing of the thermal system fans and its components Development team shall ensure the
	Fan failure	2	mounting, installation, and manufacturing of the fan and its components Ensure bolts, interface components, and mounting	technical inspection will identify fan functionality Operator aware during operation by identifying displayed high	5	100	shall ensure proper mounting, installation, and manufacturing of the thermal system fans and its components Development team shall ensure the thermal system fans
	Fan failure	2	mounting, installation, and manufacturing of the fan and its components Ensure bolts, interface components, and mounting hardware are	technical inspection will identify fan functionality Operator aware during operation by identifying	5	100	shall ensure proper mounting, installation, and manufacturing of the thermal system fans and its components Development team shall ensure the thermal system fans bolts, interface
	Fan failure	2	mounting, installation, and manufacturing of the fan and its components Ensure bolts, interface components, and mounting hardware are securely	technical inspection will identify fan functionality Operator aware during operation by identifying displayed high	5	100	shall ensure proper mounting, installation, and manufacturing of the thermal system fans and its components Development team shall ensure the thermal system fans bolts, interface components, and
	Fan failure	2	mounting, installation, and manufacturing of the fan and its components Ensure bolts, interface components, and mounting hardware are securely fastened and	technical inspection will identify fan functionality Operator aware during operation by identifying displayed high	5	100	shall ensure proper mounting, installation, and manufacturing of the thermal system fans and its components Development team shall ensure the thermal system fans bolts, interface components, and mounting hardware
	Fan failure	2	mounting, installation, and manufacturing of the fan and its components Ensure bolts, interface components, and mounting hardware are securely fastened and free from	technical inspection will identify fan functionality Operator aware during operation by identifying displayed high	5	100	shall ensure proper mounting, installation, and manufacturing of the thermal system fans and its components Development team shall ensure the thermal system fans bolts, interface components, and mounting hardware are securely fastened
	Fan failure	2	mounting, installation, and manufacturing of the fan and its components Ensure bolts, interface components, and mounting hardware are securely fastened and free from potential	technical inspection will identify fan functionality Operator aware during operation by identifying displayed high	5	100	shall ensure proper mounting, installation, and manufacturing of the thermal system fans and its components Development team shall ensure the thermal system fans bolts, interface components, and mounting hardware are securely fastened and free from
	Fan failure	2	mounting, installation, and manufacturing of the fan and its components Ensure bolts, interface components, and mounting hardware are securely fastened and free from potential loosening or	technical inspection will identify fan functionality Operator aware during operation by identifying displayed high	5	100	shall ensure proper mounting, installation, and manufacturing of the thermal system fans and its components Development team shall ensure the thermal system fans bolts, interface components, and mounting hardware are securely fastened and free from potential loosening or
	Fan failure	2	mounting, installation, and manufacturing of the fan and its components Ensure bolts, interface components, and mounting hardware are securely fastened and free from potential loosening or unintended	technical inspection will identify fan functionality Operator aware during operation by identifying displayed high	5	100	shall ensure proper mounting, installation, and manufacturing of the thermal system fans and its components Development team shall ensure the thermal system fans bolts, interface components, and mounting hardware are securely fastened and free from
	Fan failure	2	mounting, installation, and manufacturing of the fan and its components Ensure bolts, interface components, and mounting hardware are securely fastened and free from potential loosening or	technical inspection will identify fan functionality Operator aware during operation by identifying displayed high	5	100	shall ensure proper mounting, installation, and manufacturing of the thermal system fans and its components Development team shall ensure the thermal system fans bolts, interface components, and mounting hardware are securely fastened and free from potential loosening or

Item: Steering	5	Potential		Potential		Ensure that the thermostat, fuse, fan wires, coolant level and fan clutch are functional	Detection			Development team shall ensure that the thermostat, fuse, fan wires, coolant level and fan clutch are functional
Function	Failure Type	Impact	S	Cause	0	Mode	Mode	D	RPN	Requirement
Controls lateral movement of the vehicle	Failure to control lateral movement	Unintended lateral motion Travel in wrong direction Operator and/or passenger injury Damage to or loss of property Damage to environment	10	Contamination of power steering fluid (old, air)	1	Ensure proper mounting, installation, and manufacturing of hoses, clamps, and their components Ensure interface components (seals, gaskets), and mounting hardware are securely fastened and free from potential loosening or movement Ensure functionality of pump and check for hose	Operator aware during operation by identifying a loss in steering functionality Vehicle technical inspection will identify a lack of, or discolored steering fluid Increased friction and interference with hydraulic characteristics.	3	30	Development team shall ensure proper mounting, installation, and manufacturing of EPS system hoses, clamps, and their components Development team shall ensure EPS system interface components (seals, gaskets), and mounting hardware are securely fastened and free from potential loosening or unintended movement Development team shall ensure EPS system functionality of pump and check for hose deterioration
				Low fluid and fluid leaks	2	deterioration Ensure proper mounting, installation, and	Vehicle technical inspection will	3	60	Development team shall ensure proper mounting,

			manufacturing of hoses, clamps, and their components Ensure interface components (seals, gaskets), and mounting hardware are securely fastened and free from potential loosening or movement Ensure the correct type of fluid is used, proper fluid	identify low fluid level, and leaks Operator aware during operation by identifying a loss in steering functionality			installation, and manufacturing of EPS system hoses, clamps, and their components Development team shall ensure EPS system interface components (seals, gaskets), and mounting hardware are securely fastened and free from potential loosening or unintended movement Operator shall ensure the correct type of EPS fluid is used, proper fluid levels, and check for leaks prior to operation
			check for leaks prior to				
	Broken belt which energizes power steering pump	3	operation Ensure proper mounting, installation, and manufacturing of the belt (tension, torque specs) and its components Ensure bolts, interface components, and mounting	Vehicle technical inspection will identify belt functionality Operator aware during operation by identifying a loss in steering functionality	5	150	Development team shall ensure proper mounting, installation, and manufacturing of the power steering belt (tension, torque specs) and its components Development team shall ensure EPS belt bolts, interface components, and

				Pump failure	2	hardware are securely fastened and free from potential loosening or unintended movement Ensure proper mounting, installation, and manufacturing of pump and its components Ensure bolts, interface	Vehicle technical inspection will identify pump functionality Operator aware during operation by	5	100	mounting hardware are securely fastened and free from potential loosening or unintended movement Development team shall ensure proper mounting, installation, and manufacturing of EPS pump and its components Development team
						components (seals, gaskets), and mounting hardware are securely fastened and free from	identifying a loss in steering functionality and audible increase in pump noise			shall ensure EPS pump bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from
						potential loosening or movement				potential loosening or movement
Item: Exhaus	t	1	1	1	<u> </u>	ine venient	1	I	1	
		Potential	~	Potential		Prevention	Detection	_		Functional
Function	Failure Type	Impact	S	Cause	0	Mode	Mode	D	RPN	Requirement
Removal of toxic gases, fumes and	Failure to remove toxic gases, fumes	Unintended exposure to toxic or	9	Manifold failure (cracked)	4	Ensure proper mounting, installation, and	Vehicle technical inspection will	6	216	Development team shall ensure proper mounting,
noise	and noise	flammable chemicals				manufacturing of intake manifold and	identify fluid leaks			installation, and manufacturing of intake manifold and
		Excessive noise				its components	Operator aware			its components

Operator aware during operation by

Force engine to run rich or lean Decreased fuel efficiency NVH in driver seat, gas pedal or steering Potential for overheating			Ensure bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from leaks and potential loosening or movement	identifying displayed engine high temperatures, decrease in power, misfires, stalling, or gases venting in the engine bay			Development team shall ensure manifold bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from leaks and potential loosening or movement
	Catalytic converter failure (ceramic plate breakdown, or clogs)	4	Ensure proper mounting, installation, and manufacturing of catalytic converter and its components Ensure bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from leaks and potential loosening or movement Ensure there are no leaky fuel injectors or engine misfires Ensure engine operates at	Vehicle technical inspection will identify a burned or melted ceramic substrate, sealant fatigue, or physical damage to the catalytic converter Operator aware during operation by identifying displayed engine high temperatures, the smell of exhaust fumes, Perform compression test and or leak- down test	4	144	Development team shall ensure proper mounting, installation, and manufacturing of catalytic converter and its components Development team shall ensure catalyst bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from leaks and potential loosening or movement Development team shall ensure there are no leaky fuel injectors or engine misfires Development team shall ensure engine operates at correct A/F

	correct A/F ratio (running lean causes excess heat damaging catalyst)Ensure proper functionality of exhaust gas recirculation (EGR) valve and O2 sensorEnsure current oil changesAvoid adverse road condition which may produce NVH	Failure will produce audible noise.			ratio (running lean causes excess heat damaging catalyst) Development team shall ensure proper functionality of exhaust gas recirculation (EGR) valve and O2 sensor Operator shall ensure routine oil changes Operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH
Mounting failure (loose or broken hangers or clamps)	 produce 14411 and damage the catalytic converter 5 Ensure proper mounting, installation, and manufacturing of exhaust system and its components Ensure bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and 	Vehicle technical inspection will identify loose components or physical damage to the exhaust system Operator aware during operation by identifying audible noise, or smell of exhaust fumes	3	135	Development team shall ensure proper mounting, installation, and manufacturing of the exhaust system and its components Development team shall ensure exhaust system bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from leaks

		free from leaks				and potential
		and potential				loosening or
						movement
		loosening or				movement
Muffler failure	4	movement	Vehicle	2	=0	D 1
Muffler failure	4	Ensure proper		2	72	Development team
		mounting,	technical			shall ensure proper
		installation, and	inspection will			mounting,
		manufacturing	identify			installation, and
		of muffler and	physical			manufacturing of
		its components	damage to the			muffler and its
			muffler			components
		Ensure bolts,				
		interface				Development team
		components	Operator aware			shall ensure muffler
		(seals, gaskets),	during			bolts, interface
		and mounting	operation by			components (seals,
		hardware are	identifying			gaskets), and
		securely	audible noise			mounting hardware
		fastened and	(generally loud,			are securely fastened
		free from leaks	back-fire), or			and free from leaks
		and potential	smell of			and potential
		loosening or	exhaust fumes,			loosening or
		movement.	condensation			movement.
			inside the			
			exhaust and			
			lower mpg			
Sensor failure	3	Ensure proper	Vehicle	6	162	Development team
(O2)	5	mounting,	technical	0	104	shall ensure proper
(02)		installation, and	inspection will			mounting,
		manufacturing	identify			installation, and
		of O2 sensor				manufacturing of O2
		of 02 sensor	physical			e
		F 1 1	damage to the			sensor
		Ensure bolts,	O2 sensor			D 1
		interface				Development team
		components				shall ensure O2 sensor
		(seals, gaskets),	Operator aware			Ensure bolts, interface
		and mounting	during			components (seals,
		hardware are	operation by			gaskets), and
		securely	identifying			mounting hardware
		fastened and	check engine			are securely fastened

		4	free from leaks and potential loosening or movement	light, loss in vehicle functionality (misfire, lower mpg), or smell of exhaust fumes	2	100	and free from leaks and potential loosening or unintended movement
	Exhaust pipe failure (loose or broken connectors)	4	Ensure proper mounting, installation, and manufacturing of the exhaust pipes Ensure bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from leaks and potential loosening or movement Ensure pipes are free from corrosion and physical damage Avoid adverse road condition which may produce NVH and damage suspension	Vehicle technical inspection will identify physical damage and corrosion Operator aware during operation by identifying smell of exhaust fumes, or increased noise	3	108	Development team shall ensure proper mounting, installation, and manufacturing of the exhaust pipes Development team shall ensure exhaust pipe bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from leaks and potential loosening or unintended movement Development team shall ensure exhaust pipes are free from corrosion and physical damage Operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH

Function	Failure Type	Potential Impact	s	Potential Cause	0	Prevention Mode	Detection Mode	D	RPN	Functional Requirement
Provide torque at request of operator	Failure Type Failure to meet torque request	Unintended acceleration Unintended longitudinal motion Loss or degradation of propulsion system Operator and/or passenger injury Damage to or loss of property Damage to environment Potential for overheating	10	Cause Improper lubrication (oil filter/pump failure)	5	Ensure proper mounting, installation, and manufacturing of the oil filter and pump Ensure bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from leaks and potential loosening or movement Ensure frequent oil changes, clean oil, and that the oil filter is not	Vehicle technical inspection will identify deformation to filter and unclean oil Operator aware during operation by identifying loss of vehicle functionality, Sputtering, engine grinding, dirty exhaust, or a drop in pressure smell of exhaust fumes, or increased noise	8	400	Requirement Development team shall ensure proper mounting, installation, and manufacturing of the oil filter and pump Development team shall ensure oil filter and pump bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from leaks and potential loosening or unintended movement Operator shall ensure frequent oil changes, clean oil, and that the oil filter is not ballooned or deformed
		Unintended exposure to toxic/flammable chemicals		Improper fuel octane number	1	ballooned or deformed Verify prior to filling tank	Combustion failure will lead to loss of vehicle functionality.	4	40	Operator shall ensure proper fuel octane number prior to filling tank
				Excessive heating (radiator,	4	Ensure thermal system components	Sensors signal to ECM	8	320	Development team shall ensure thermal system components

coolant leak,	(radiator,	Operator aware	(radiator, coolant
	coolant level,	during	(radiator, coolant level, fans) are
water pump,		U	
fan, or	fans) are	operation.	functional and
thermostat	functional and		sufficient to cool the
failure)	sufficient to	Operator views	engine
	cool the engine	engine temp in	
		cabin.	Development team
	Ensure the fans		shall ensure the
	are free from	Error message	thermal systems fans
	potential	displayed.	are free from potential
	physical		physical damage
	damage		
			Development team
	Ensure		shall ensure thermal
	enclosure fans		system fans pull air
	pull air from a		from a cool source
	cool source		
	coor source		Development team
	Ensure engine		shall ensure engine
	ventilation is		ventilation is
	sufficient to		sufficient to provide
	provide		appropriate air
	appropriate air		movement through
	movement		engine bay
	through engine		
	bay		Development teams
			shall ensure thermal
	Ensure thermal		system is designed
	system is		such that there is
	designed such		sufficient air flow to
	that there is		cool engine
	sufficient air		components
	flow to cool		
	engine		Development team
	components		shall ensure proper
	1		mounting,
	Ensure proper		installation, and
	mounting,		manufacturing of
	installation, and		thermal system and its
	manufacturing		÷
	manufacturing	1	components

[I			of thermal		1		
									Davalonment teem
					system and its				Development team
					components				shall ensure thermal
									system bolts and
					Ensure bolts				mounting hardware
					and mounting				are securely fastened
					hardware are				and free from
					securely				potential loosening or
					fastened and				movement
					free from				
					potential				Development team
					loosening or				shall ensure the ECM
					movement				controls and mitigates
									overheating
					Ensure the				5
					ECM controls				Operator shall avoid
					and mitigates				poor driving behaviors
					overheating				poor any ing commons
					overneuting				
					Operator drives				
					appropriately to				
					ensure engine				
			TL . 1 1	4	temp is stable	Vehicle	6	2.40	Dealersetter
			Head gasket	4	Ensure proper		6	240	Development team
			failure		mounting,	technical			shall ensure proper
					installation, and	inspection will			mounting, installation,
					manufacturing	identify fluid			and manufacturing of
					of intake	leaks			head gasket. intake
					manifold and				manifold and its
					its components	Operator aware			components
						during			
					Ensure bolts,	operation by			Development team
					interface	identifying			shall ensure head
					components	displayed			gasket components
					(seals, gaskets),	engine high			and mounting
					and mounting	temperatures,			hardware are securely
					hardware are	decrease in			fastened and free from
					securely	power,			leaks and potential
					fastened and	misfires,			loosening or
					free from leaks	stalling, or			unintended movement
				1	nee nom leaks	stannig, Or	1	l	unnueu movement

			and potential loosening or movement Ensure thermal system is functional	gases venting in the engine bay			Development team shall ensure the thermal system is functional
	Engine misfire (ECM, sparkplug, ignition system valve/spring failure)	4	Ensure proper mounting, installation, and manufacturing of the sparkplugs, fuel injectors, and air intake system Ensure bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from leaks and potential loosening or movement Ensure proper A/F ratio and functioning O2 sensor Ensure vacuum lines and manifold gasket are free from cracks	Vehicle technical inspection will identify fluid leaks Operator aware during operation by identifying hesitated power delivery, error message, reduced mpg, and increased emissions	8	320	Development team shall ensure proper mounting, installation, and manufacturing of the sparkplugs, fuel injectors, and air intake system Development team shall ensure ECM, sparkplugs, injection system valves, springs, bolts, interface components, and mounting hardware are securely fastened and free from leaks and potential loosening or unintended movement Development team shall ensure proper A/F ratio and functioning O2 sensor Development team shall ensure vacuum lines and manifold gasket are free from cracks and physical damage

		and physical damage Ensure properly functioning timing belt Ensure properly functioning EGR valve				Development team shall ensure properly functioning timing belt Development team shall ensure properly functioning EGR valve
Excessive load and improper driving	6	Ensure proper vehicle operation (reduce engine speed/load)	Vehicle technical inspection will identify tire wear, leaks, and brake component fatigue Operator aware during operation by identifying progressive loss of engine functionality	3	180	Operator shall avoid poor driving behaviors
Exhaust gas recirculation system (A/F ratio, O2 sensor failure)	2	Ensure proper mounting, installation, and manufacturing of EGR system and its components Ensure bolts, interface components (seals, gaskets),	Operator aware during operation by identifying progressive loss of engine functionality, rough idling, smell of fuel, poor mpg, error message	3	60	Development team shall ensure proper mounting, installation, and manufacturing of EGR system and its components Development team shall ensure EGR system bolts, interface, and

Item: Motor						and mounting hardware are securely fastened and free from leaks and potential loosening or movement Ensure proper functionality of exhaust gas recirculation (EGR) valve and O2 sensor				mounting hardware are securely fastened and free from leaks and potential loosening or movement Development team shall ensure proper functionality of exhaust gas recirculation (EGR) valve and O2 sensor
		Potential		Potential		Prevention	Detection			Functional
Function	Failure Type	Impact	S	Cause	0	Mode	Mode	D	RPN	Requirement
Provide torque at request of operator	Failure to meet torque request	Unintended acceleration Unintended longitudinal motion Loss or degradation of propulsion system Operator and/or passenger	10	Over-current	7	Ensure software (HSC) limits the magnitude of current to the EM Ensure relays and fuses are in place and functional to prevent over drawing of current	Operator aware during operation by vehicle response to torque request, potential EM over-heat or failure	7	490	Development team shall ensure software (HSC) limits the magnitude of current to the EM Development team shall ensure relays and fuses are in place and functional to prevent over drawing of current
		injury Damage to or loss of property Damage to environment		Contamination (EM housing or coolant system failure)	7	Ensure proper mounting, installation, and manufacturing of the EM and housing	Vehicle technical inspection will identify leaks or physical damage	8	560	Development team shall ensure proper mounting, installation, and manufacturing of the EM and housing

Potential for overheating Unintended exposure to high voltage			Ensure bolts, interface components, and mounting hardware are securely fastened and free from leaks and potential loosening or movement Ensure cooling system and its components are functioning, proper coolant levels, and hoses running to and from the motor are leak	Operator aware during operation by identifying loss of motor functionality			Development team shall ensure EM housing and coolant system bolts, interface components, and mounting hardware are securely fastened and free from leaks and potential loosening or unintended movement Development team shall ensure EM cooling system and its components are functioning, proper coolant levels, and hoses running to and from the motor are leak free
	Overheating (coolant failure)	8	free Ensure thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the EM Ensure the fans are free from potential physical damage Ensure enclosure fans	Operator aware during operation by identifying high EM temperature and loss of motor functionality	8	640	Development team shall ensure EM thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the EM Development team shall ensure EM coolant system fans are free from potential physical damage Development team shall ensure EM coolant system fans

		pull air from a cool source Ensure proper mounting,				pull air from a cool source Development team shall ensure proper
		installation, and				mounting, installation,
		manufacturing of coolant				and manufacturing of EM coolant system
		system and its				and its components
		components				and its components
		r r				Development team
		Ensure bolts,				shall ensure EM
		hoses and				coolant system bolts,
	1	mounting				hoses and mounting
	1	hardware are				hardware are securely
		securely fastened and				fastened and free from potential loosening or
		free from				unintended movement
		potential				unintended movement
		loosening or				Development team
		movement				shall ensure the HSC
						controls and mitigates
		Ensure the				EM overheating
		HSC controls				
		and mitigates				Operator shall drive
		overheating				appropriately to ensure EM temp is
	1	Operator drives				stable
	1	appropriately to				54010
		ensure EM				
		temp is stable				
Low resistance	7	Ensure thermal	Operator aware	8	560	Development team
due to	1	system	during			shall ensure EM
insufficient		components	operation by			thermal system
isolation between		(radiator, coolant level,	identifying high motor			components (radiator, coolant level, fans) are
windings	1	fans) are	temperature			functional and
(corrosion or		functional and	and loss of			sufficient to cool the
physical		sufficient to	motor			EM
damage)		cool the EM	functionality			

			Ensure bolts, hoses and mounting hardware are securely fastened and free from potential loosening or movement Ensure the HSC controls and mitigates overheating				Development team shall ensure EM bolts, hoses and mounting hardware are securely fastened and free from potential loosening or unintended movement Development team shall ensure the HSC controls and mitigates EM overheating
	Internal component failure (stator, rotor, bearings, or shaft)	3	Avoid adverse road condition which may produce NVH and damage EM internal components Ensure thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the EM	Operator aware during operation by identifying partial or total functionality failure	8	240	Operator shall avoid adverse road condition which may produce NVH and damage EM internal components Development team shall ensure EM thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the EM
	EM-driveshaft interface failure	8	Ensure proper mounting, installation, and manufacturing of EM, driveshaft, and	Vehicle technical inspection will identify if the interface is free of manufacturing	9	720	Development team shall ensure proper mounting, installation, and manufacturing of EM, driveshaft, and its

	its interfacing	or installation	interfacing
	components	fatigue or	components
		failure	
	Ensure bolts		Development team
	and mounting	Operator aware	shall ensure EM-
	hardware is	during	driveshaft interface
	securely	operation by	bolts and mounting
	fastened and	identifying	hardware is securely
	free from	partial or total	fastened and free from
	potential	functionality	potential loosening or
	loosening or	failure	unintended movement
	unintended		
	movement		Development team
			shall ensure EM-
	Ensure EM-		driveshaft interface
	driveshaft		location is covered
	interface		and free from
	location is		potential unintended
	covered and		access or physical
	free from		damage
	potential		
	unintended		Development team
	access or		shall ensure proper EM-driveshaft
	physical		
	damage		alignment
	Ensure proper		Development team
	EM-driveshaft		shall ensure EM-
	alignment		driveshaft interface
	unginnent		angle is minimized
	Ensure EM-		
	driveshaft		Operator shall avoid
	interface angle		adverse road
	is minimized		conditions which may
			produce NVH and
	Avoid adverse		damage EM-
	road condition		driveshaft interface
	which may		
	produce NVH		
	and damage		

	1					1	r	1
				EM-driveshaft				
				interface				
		EM-	8	Ensure proper	Vehicle	9	720	Development team
		transmission		mounting,	technical			shall ensure proper
		failure		installation, and	inspection will			mounting,
				manufacturing	identify if the			installation, and
				of EM,	interface is free			manufacturing of EM,
				transmission,	of			transmission, and its
				and its	manufacturing			interfacing
				interfacing	or installation			components
				components	fatigue or			
					failure			Development team
				Ensure bolts				shall ensure EM-
				and mounting	Operator aware			transmission interface
				hardware is	during			bolts and mounting
				securely	operation by			hardware are securely
				fastened and	identifying			fastened and free from
				free from	partial or total			potential loosening or
				potential	functionality			unintended movement
				loosening or	failure			
				unintended				Development team
				movement				shall ensure EM-
								transmission interface
				Ensure EM-				location is covered
				transmission				and free from
				interface				potential unintended
				location is				access or physical
				covered and				damage
				free from				
				potential				Development team
				unintended				shall ensure proper
				access or				EM-transmission
				physical				alignment
				damage				
								Operator shall avoid
				Ensure proper				adverse road
				EM-				conditions which may
				transmission				produce NVH and
				alignment				damage EM-
				anginnent				transmission interface
				1	1	L	I	d'anonnoord interrace

Item: Fuel		Potential		Potential		Avoid adverse road conditions which may produce NVH and damage EM- transmission interface	Detection			Functional
Function	Failure Type	Impact	S	Cause	0	Mode	Mode	D	RPN	Requirement
Store and supply fuel to engine	Failure to store or supply fuel to engine	Unintended longitudinal motion Loss or degradation of propulsion system Operator and/or passenger injury Damage to or loss of property	10	Fuel filter failure (clogged, leak)	4	Ensure proper mounting, installation, and manufacturing of the fuel filter Ensure the permeable material is clean and the fuel filter is free of physical damage and leaks while under pressure	Vehicle technical inspection will identify if the filter is free of leaks or physical damage Operator aware during operation by identifying a lack of engine power, stalling, or misfire	6	240	Development team shall ensure proper mounting, installation, and manufacturing of the fuel filter Development team shall ensure the permeable material is clean and the fuel filter is free of physical damage and leaks while under pressure
		Damage to environment Potential for overheating Unintended exposure to toxic/flammable chemicals		Fuel injection failure (clogged, leak)	4	Ensure proper installation of the fuel injectors Ensure injector mounting hardware is securely fastened and free from potential	Operator aware during operation by identifying a partial or total loss of engine functionality Clogged injector will produce surges of power	6	240	Development team shall ensure proper installation of the fuel injectors Development team shall ensure fuel injector mounting hardware is securely fastened and free from potential loosening or unintended movement

				loosening or movement Ensure adequate fuel level and type Ensure use of fuel system cleaners when recommended				Operator shall ensure adequate fuel level and type Operator shall ensure use of fuel system cleaners when recommended
	Fuel failu	1 1	4	Ensure proper mounting and installation of fuel pump Ensure fuel pump mounting hardware is securely fastened and free from potential loosening or movement Ensure adequate fuel level and type	Operator aware during operation by identifying a partial or total loss of engine functionality, rising temperature, surging, and decreased mpg	6	240	Development team shall ensure proper mounting and installation of fuel pump Development team shall ensure fuel pump mounting hardware is securely fastened and free from potential loosening or unintended movement Operator shall ensure adequate fuel level and type
	Poor qual	or fuel lity	2	Verify correct fuel quality prior to filling	Operator aware during operation by identifying a partial or total loss of engine functionality, surging, and decreased mpg	6	120	Operator shall verify correct fuel quality prior to filling

		Potential		Potential		Prevention	Detection			Functional
Function	Failure Type	Impact	S	Cause	0	Mode	Mode	D	RPN	Requirement
Transfers	Failure to	Unintended	10	Transmission	3	Ensure proper	Vehicle	8	240	Development team
power from	Transfers	acceleration		fluid failure		mounting,	technical			shall ensure proper
engine to	power from			(leaking,		installation, and	inspection will			mounting,
driveshaft	engine to	Unintended		contamination,		manufacturing	identify low			installation, and
	driveshaft	longitudinal		age, low fluids)		of transmission	fluid level,			manufacturing of
Gears change		motion				and its	leaks, and belt			transmission and its
drive-wheel	Failure with					components	fatigue			components
speed and	gears to	Loss or								
torque in	change drive-	degradation of				Ensure bolts,	Operator aware			Development team
relation to	wheel speed	propulsion				interface	during			shall ensure
engine speed	and torque in	system				components	operation by			transmission bolts,
and torque	relation to					(seals, gaskets),	identifying			interface component
	engine speed	Operator and/or				and mounting	displayed high			(seals, gaskets), and
	and torque	passenger				hardware are	temperatures			mounting hardware
		injury				securely				are securely fastened
		D				fastened and free from				and free from
		Damage to or				potential				potential loosening o
		loss of property				loosening or				movement
		Damage to				movement				Operator shall ensure
		environment				movement				the correct type of
		chvironnent				Ensure the				coolant (ATF) is use
		Potential for				correct type of				proper coolant levels
		overheating				coolant is used,				and check for leaks
		overneuting				proper coolant				prior to operation
						levels, and				prior to operation
						check for leaks				Development team
						prior to				shall ensure belt driv
						operation				components are
						1				properly installed
						Ensure belt				(tensioning, torque
						drive				specs)
						components are				· /
						properly				
						installed		1		

1			(tancianing		1		1
			(tensioning, torque specs)				
	Overheating	3	Ensure thermal	Operator aware	8	240	Development team
	Overneating	5	system	during	0	240	shall ensure
			components	operation by			transmission thermal
			(radiator,	identifying high			system components
			coolant level,	transmission			(radiator, coolant
			fans) are				level, fans) are
			functional and	temperature and loss of			functional and
			sufficient to				sufficient to cool the
			cool the	functionality			transmission
			transmission				transmission
			transmission				Development to an
		1	Ensure the fans				Development team shall ensure
			are free from				transmission thermal
			potential				system fans are free
			*				2
			physical				from potential
			damage				physical damage
			Ensure fans				Development to an
			pull air from a				Development team shall ensure
			*				
			cool source				transmission thermal
			Easter and a				system fans pull air from a cool source
			Ensure proper				from a cool source
			mounting,				D. I.
			installation, and				Development team
			manufacturing of coolant				shall ensure proper
							mounting, installation,
			system and its				and manufacturing of transmission thermal
			components				
			F actor 1 - 16				system and its
			Ensure bolts,				components
		1	hoses and				De alterna de
		1	mounting				Development team
			hardware are				shall ensure
		1	securely				transmission thermal
		1	fastened and				system bolts, hoses
		1	free from				and mounting
			potential				hardware are securely
							fastened and free from

	Transmission-	0	loosening or movement Ensure the TCM controls and mitigates overheating Operator drives appropriately to ensure transmission temperature is stable	Vehicle	9	720	potential loosening or unintended movement Development team shall ensure the TCM controls and mitigates overheating Operator shall drive appropriately to ensure transmission temperature is stable
	EM failure	8	Ensure proper mounting, installation, and manufacturing of EM, transmission, and its interfacing components Ensure bolts and mounting hardware is securely fastened and free from potential loosening or unintended movement Ensure transmission- EM interface location is covered and	vencie technical inspection will identify if the interface is free of manufacturing or installation fatigue or failure Operator aware during operation by identifying partial or total functionality failure	9	720	Development team shall ensure proper mounting, installation, and manufacturing of EM, transmission, and its interfacing components Development team shall ensure transmission-EM interface bolts and mounting hardware are securely fastened and free from potential loosening or unintended movement Development team shall ensure transmission-EM interface location is covered and free from potential unintended

Item: Body						free from potential unintended access or physical damage Ensure proper transmission- EM alignment Avoid adverse road conditions which may produce NVH and damage transmission- EM interface				access or physical damage Development team shall ensure proper transmission-EM alignment Operator shall avoid adverse road conditions which may produce NVH and damage transmission- EM interface
		Potential		Potential		Prevention	Detection			Functional
Function	Failure Type	Impact	S			1 i c v c ii ti o ii				1 unctional
4.11		impaci	5	Cause	0	Mode	Mode	D	RPN	Requirement
Allows access	Failure to	Unintended	S	Cause Hood failure	0	Mode Ensure proper	Mode Vehicle	D 8	RPN 40	Requirement Development team
to and protects		Unintended longitudinal			-	Ensure proper mounting,	Vehicle technical			Development team shall ensure proper
to and protects components in	Failure to	Unintended			-	Ensure proper mounting, installation, and	Vehicle technical inspection will			Development team shall ensure proper mounting,
to and protects components in engine	Failure to allow operator to see	Unintended longitudinal motion			-	Ensure proper mounting, installation, and manufacturing	Vehicle technical inspection will identify			Development team shall ensure proper mounting, installation, and
to and protects components in	Failure to allow operator to see Failure to	Unintended longitudinal motion Operator and/or			-	Ensure proper mounting, installation, and manufacturing of the hood,	Vehicle technical inspection will identify physical			Development team shall ensure proper mounting, installation, and manufacturing of the
to and protects components in engine compartment	Failure to allow operator to see Failure to prevent debris	Unintended longitudinal motion Operator and/or passenger			-	Ensure proper mounting, installation, and manufacturing	Vehicle technical inspection will identify physical damage to the			Development team shall ensure proper mounting, installation, and
to and protects components in engine compartment Allows	Failure to allow operator to see Failure to prevent debris from entering	Unintended longitudinal motion Operator and/or			-	Ensure proper mounting, installation, and manufacturing of the hood, and latch	Vehicle technical inspection will identify physical damage to the hood and			Development team shall ensure proper mounting, installation, and manufacturing of the hood, and latch
to and protects components in engine compartment Allows operator to see	Failure to allow operator to see Failure to prevent debris	Unintended longitudinal motion Operator and/or passenger injury			-	Ensure proper mounting, installation, and manufacturing of the hood, and latch Ensure bolts,	Vehicle technical inspection will identify physical damage to the hood and loosening of			Development team shall ensure proper mounting, installation, and manufacturing of the hood, and latch Development team
to and protects components in engine compartment Allows operator to see in low light	Failure to allow operator to see Failure to prevent debris from entering	Unintended longitudinal motion Operator and/or passenger injury Damage to or			-	Ensure proper mounting, installation, and manufacturing of the hood, and latch Ensure bolts, interface	Vehicle technical inspection will identify physical damage to the hood and			Development team shall ensure proper mounting, installation, and manufacturing of the hood, and latch Development team shall ensure hood
to and protects components in engine compartment Allows operator to see	Failure to allow operator to see Failure to prevent debris from entering	Unintended longitudinal motion Operator and/or passenger injury			-	Ensure proper mounting, installation, and manufacturing of the hood, and latch Ensure bolts, interface components,	Vehicle technical inspection will identify physical damage to the hood and loosening of latch			Development team shall ensure proper mounting, installation, and manufacturing of the hood, and latch Development team shall ensure hood bolts, interface
to and protects components in engine compartment Allows operator to see in low light scenarios	Failure to allow operator to see Failure to prevent debris from entering	Unintended longitudinal motion Operator and/or passenger injury Damage to or loss of property			-	Ensure proper mounting, installation, and manufacturing of the hood, and latch Ensure bolts, interface components, and mounting	Vehicle technical inspection will identify physical damage to the hood and loosening of latch Operator aware			Development team shall ensure proper mounting, installation, and manufacturing of the hood, and latch Development team shall ensure hood bolts, interface components, and
to and protects components in engine compartment Allows operator to see in low light	Failure to allow operator to see Failure to prevent debris from entering	Unintended longitudinal motion Operator and/or passenger injury Damage to or			-	Ensure proper mounting, installation, and manufacturing of the hood, and latch Ensure bolts, interface components,	Vehicle technical inspection will identify physical damage to the hood and loosening of latch Operator aware during			Development team shall ensure proper mounting, installation, and manufacturing of the hood, and latch Development team shall ensure hood bolts, interface components, and mounting hardware
to and protects components in engine compartment Allows operator to see in low light scenarios Prevent debris	Failure to allow operator to see Failure to prevent debris from entering	Unintended longitudinal motion Operator and/or passenger injury Damage to or loss of property Damage to			-	Ensure proper mounting, installation, and manufacturing of the hood, and latch Ensure bolts, interface components, and mounting hardware are	Vehicle technical inspection will identify physical damage to the hood and loosening of latch Operator aware			Development team shall ensure proper mounting, installation, and manufacturing of the hood, and latch Development team shall ensure hood bolts, interface components, and
to and protects components in engine compartment Allows operator to see in low light scenarios Prevent debris from being	Failure to allow operator to see Failure to prevent debris from entering	Unintended longitudinal motion Operator and/or passenger injury Damage to or loss of property Damage to			-	Ensure proper mounting, installation, and manufacturing of the hood, and latch Ensure bolts, interface components, and mounting hardware are securely	Vehicle technical inspection will identify physical damage to the hood and loosening of latch Operator aware during operation by			Development team shall ensure proper mounting, installation, and manufacturing of the hood, and latch Development team shall ensure hood bolts, interface components, and mounting hardware are securely fastened
to and protects components in engine compartment Allows operator to see in low light scenarios Prevent debris from being thrown into air	Failure to allow operator to see Failure to prevent debris from entering	Unintended longitudinal motion Operator and/or passenger injury Damage to or loss of property Damage to environment			-	Ensure proper mounting, installation, and manufacturing of the hood, and latch Ensure bolts, interface components, and mounting hardware are securely fastened and	Vehicle technical inspection will identify physical damage to the hood and loosening of latch Operator aware during operation by identifying			Development team shall ensure proper mounting, installation, and manufacturing of the hood, and latch Development team shall ensure hood bolts, interface components, and mounting hardware are securely fastened and free from
to and protects components in engine compartment Allows operator to see in low light scenarios Prevent debris from being thrown into air	Failure to allow operator to see Failure to prevent debris from entering	Unintended longitudinal motion Operator and/or passenger injury Damage to or loss of property Damage to environment Potential for			-	Ensure proper mounting, installation, and manufacturing of the hood, and latch Ensure bolts, interface components, and mounting hardware are securely fastened and free from	Vehicle technical inspection will identify physical damage to the hood and loosening of latch Operator aware during operation by identifying hood failure			Development team shall ensure proper mounting, installation, and manufacturing of the hood, and latch Development team shall ensure hood bolts, interface components, and mounting hardware are securely fastened and free from potential loosening or

and protects operator from environment and debris Absorb impact of minor								
collision		Grill failure prevents airflow to	1	Ensure proper mounting, installation, and	Vehicle technical inspection will	2	10	Development team shall ensure proper mounting, installation,
Signals turning and braking		radiator		manufacturing of the grill	identify physical			and manufacturing of the grill
Allows for operator to have surrounding view				Ensure bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from leaks and potential loosening or movement Ensure grill is free of clogging debris	damage or clogging or the grill Operator aware during operation by identifying signs of over heating			Development team shall ensure grill bolts, interface components, and mounting hardware are securely fastened and free from leaks and potential loosening or movement Operator shall ensure grill is free of clogging debris
		Headlight and/or taillight failure	3	Ensure functionality of lights prior to use	Vehicle technical inspection will identify light functionality	8	120	Development team shall ensure proper mounting, installation, and manufacturing of head and tail lights
					Operator aware during operation by identifying loss of light functionality			Operator shall ensure functionality of lights prior to use

Body panels,	3	Ensure proper	Vehicle	2	30	Development team
doors, or		mounting,	technical			shall ensure proper
window failure		installation, and	inspection will			mounting, installation,
		manufacturing	identify			and manufacturing of
		of the body	physical			the body panels,
		panels,	damage, loss of			windows, and doors
		windows, and	functionality,			
		doors	or loosening of			Development team
			body panels,			shall ensure body
		Ensure bolts,	windows, and			panels, doors, and
		interface	doors			window bolts,
		components				interface components,
		(seals, gaskets),				and mounting
		and mounting				hardware are securely
		hardware are				fastened and free from
		securely				leaks and potential
		fastened and				loosening or
		free from leaks				movement
		and potential				
		loosening or				Operator shall ensure
		movement				body panels, windows,
						and doors are free of
		Ensure body				physical damage prior
		panels,				to use
		windows, and				
		doors are free				Operator shall ensure
		of physical				window and door
		damage				functionality prior to
						use
		Ensure window				
		and door				
		functionality				

			PSI Mecha	anical Pro	cess Para	meter and G	auide Wo	ord Combin	ation Cha	rt			
Mechani	ical					G	uide Wo	rd					
Process	No	As well	Part of	Reverse	Other	Early	Late	Before	After	Faster	Slower	More	Less
Paramet	ter	as				2							
NV	ΥH									Х	Х	Х	
Tore	que		Х	Х		X	Х					Х	Х
Tempe	rature											Х	X
Curr	rent	X	Х	Х		X	Х					Х	X
Clear	ance											Х	Х
Ang	gle											Х	
FUNCT	ION: At	oply NVH Stimu	i to EM		PSI I	Mechanical	HazOP						
Guide Word	Deviation	Consequer		Cause	es		Safe	guards		Functio	nal Require	ement	
Faster	NVH stimu is applied to quickly	0	arates nects from nects from	Inade	ety, or mo	allation, facto	or special bolts	er installatic s, factor of s s, interfaces, nting hardwa	afety on and		chanical sys of withstand cy		
Slower	NVH stimu applied too slowly	frequency of mounting/in	nterface and increased <u>mplitude</u> nects from n	Inade of safe	ety, or mo	allation, facto	or special bolts	er installations, factor of s s, factor of s s, interfaces, nting hardwa	afety on and		chanical system of withstand le		

Appendix 3.10 HARA PSI Mechanical HazOP

More	NVH amplitude reaches threshold	Mounting/interfacing hardware loosens/separates EM disconnects from transmission EM disconnects from driveshaft	Adverse road conditions. Inadequate installation, factor of safety, or mounting hardware	Proper installation, torque specs, factor of safety on bolts, interfaces, and mounting hardware	
FUNCTI	ON: Apply	Torque Stimuli to EM			
Guide Word	Deviation	Consequences	Causes	Safeguards	Functional Requirement
Part of	Only part of intended torque applied	TVP acceleration is less than expected	Control software error. APPS error. Power supply error. EM/engine malfunction. Transmission controller error.	Torque request magnitude/direction testing, APPS validation, and gear selection control testing during zero velocity and closed course phases	The applied torque magnitude shall match the torque request intended magnitude
Reverse	Torque applied is reverse of intended	TVP accelerates in direction other than intend TVP collides with	Control software error. APPS error. Power supply error. EM/engine malfunction. Transmission controller error.	Controls software validation during SIL. Torque request magnitude/direction	The applied torque direction shall match the torque request intended direction
		object.		testing, APPS validation, and gear selection control testing during zero velocity	
		TVP/operator damage/injury		and closed course phases	
Early	Torque applied earlier than intended	TVP accelerates sooner than intended	Control software error. APPS error. Power supply error. EM/engine malfunction. Transmission controller error.	Controls software validation during SIL. Torque request magnitude/direction	The applied torque shall actuate at the time intended
		TVP collides with object	Transmission controller error.	testing, APPS validation, and gear selection control	
		TVP/operator damage/injury		testing during zero velocity and closed course phases	
Late	Torque applied later than intended	TVP accelerates later than intended	Control software error. APPS error. Power supply error. EM/engine malfunction. Transmission controller error.	Controls software validation during SIL. Torque request magnitude/direction testing, APPS validation,	

More	Torque applied is greater than intended	TVP accelerates faster than intended TVP collides with object TVP/operator damage/injury	Control software error. APPS error. Power supply error. EM/engine malfunction. Transmission controller error.	and gear selection control testing during zero velocity and closed course phases Controls software validation during SIL. Torque request magnitude/direction testing, APPS validation, and gear selection control testing during zero velocity and closed course phases	The applied torque magnitude shall match the torque request intended magnitude
Less	Torque applied is less than intended	TVP accelerates slower than intended	Control software error. APPS error. Power supply error. EM/engine malfunction. Transmission controller error.	Controls software validation during SIL. Torque request magnitude/direction testing, APPS validation, and gear selection control testing during zero velocity	
				and closed course phases	
FUNCT	TION: Apply	Temperature Stimuli to EM	1	and closed course phases	
Guide Word	Deviation	Temperature Stimuli to EM	Causes	Safeguards	Functional Requirement
Guide		-			Functional Requirement The EM shall operate with in a safe and specified temperature range

Guide Word	Deviation	Consequences	Causes	Safeguards	Functional Requirement
No	No current applied when current requested	EM does not function	Power supply error. Controls software/hardware error. APPS error. EM malfunction.	Ensure ESS, control software, APPS, and EM are installed properly. Thoroughly test during SIL zero velocity, and closed course testing	The current applied shall match the current necessary to meet EM torque request
Part of	Only part of current applied when	EM does not function as intended	Power supply error. Controls software/hardware error. APPS error. EM malfunction.	Ensure ESS, control software, APPS, and EM are installed	
	current requested	TVP does not accelerate as intended		properly. Thoroughly test during SIL zero velocity, and closed course testing	
Reverse	Current applied is reverse of intended	TVP accelerates in direction other than intend TVP collides with object. TVP/operator damage/injury	Control software error. APPS error. Power supply error. EM malfunction.	Ensure ESS, control software, APPS, and EM are installed properly. Thoroughly test during SIL zero velocity, and closed course testing	The applied current direction shall match the direction necessary to meet the EM torque request
Early	Current applied earlier than intended	TVP accelerates sooner than intended TVP collides with object TVP/operator damage/injury	Power supply error. Controls software/hardware error. APPS error. EM malfunction.	Ensure ESS, control software, APPS, and EM are installed properly. Thoroughly test during SIL zero velocity, and closed course testing	The applied current shall actuate at the time intended
Late	Current applied later than intended	TVP accelerates later than intended	Power supply error. Controls software/hardware error. APPS error. EM malfunction.	Ensure ESS, control software, APPS, and EM are installed	

				properly. Thoroughly test during SIL zero velocity, and closed course testing	
More	Current applied is greater than max operating parameter	Fire Item damage or lost functionality TVP/operator damage/injury	ESS/power supply error. Controls software/hardware error. EM malfunction.	Ensure ESS, control software, APPS, and EM are installed properly. Thoroughly test during SIL zero velocity, and closed course testing	The current applied shall not exceed max operating parameter
Less	Current applied is less than intended	EM does not function as intended TVP does not accelerate as intended	Power supply error. Controls software/hardware error. APPS error. EM malfunction.	Ensure ESS, control software, APPS, and EM are installed properly. Thoroughly test during SIL zero velocity, and closed course testing	The current applied shall match the current necessary to meet EM torque request
FUNCT	TION: Cleara	ance Applied To Mechanical	Components		
Guide Word	Deviation	Consequences	Causes	Safeguards	Functional Requirement
More	More component installation clearance is applied than required	Limits the space to make future additions	Excess clearance between components reduces availability for future additions	Ensure manufacturers clearance and installation specifications are adhered to	Mechanical component clearance requirements shall be met and minimized to ensure space is available for modifications
Less	Less component installation clearance is applied than required	Thermal transfer leading to overheating NVH causing destructive component contact	Lack of clearance between components leads to heat transfer. NVH with a lack of clearance causes destructive component contact. May restrict adequate bend radii	Ensure manufacturers clearance and installation specifications are adhered to	Mechanical component clearance requirements shall be met to ensure safe TVP operation

TVP/operator damage/injury

FUNCT	ION: Interfz	Difficulty installing and maintaining the mechanical components ace Angle Applied to Drives	haft/EM		
		te migie ripplied to Drives		Γ	
Guide Word	Deviation	Consequences	Causes	Safeguards	Functional Requirement
More	More driveshaft/EM interface angle is	NVH to powertrain system Mounting/interfacing hardware	Minimization of driveshaft/EM interface angle was not performed during development and installation	Ensure driveshaft/EM interface angle is minimized	The driveshaft shall be properly modified to minimize EM interface angle
	applied than required	loosens/separates TVP/operator damage/injury			

Appendix 3.11 HARA PSI SEFA

	SEFA Part 1 of 2																
Team	eam: PSI																
	Multiple Range			1	1	1	Ite	m O	per	atin	ig St	tates	-				
Item No.	Operating Scenario (P,R,N,D)	Item Functions	1	2	3	4	5	6	7	8	9	10	11	12	13	Impact of Item Fault	Immediate Resulting State
1	Driveshaft	Longitudinal shaft which transmits torque from engine/transmission to rear of vehicle	0	1	0	1	0	1	0	1	1	1	1	1	1	No torque transfer from engine/motor to differential	Vehicle motion slowed or stopped Zero propulsive capability
2	Motor	Provides torque at user request by converting	1	0	1	1	0	1	1	0	1	1	1	1	1	No torque generated from	Vehicle motion slowed or stopped

		onboard stored electrical energy into rotational motion. Allows for energy regeneration and transfer to the battery during negative events														electrical energy transfer from ESS No regen capability	Possible propulsive capability based on engine functionality
3	Engine	Provides torque at the request of operator	1	1	0	1	1	1	0	1	1	1	1	0	0	No engine torque generation	Vehicle motion slowed or stopped Possible propulsive capability based on EM functionality
4	Suspension	Provides dynamic energy absorption of vertical force exerted on wheels by the change in road conditions	1	1	1	0	1	1	1	1	1	1	1	1	1	No energy absorption from road conditions Non stable ride height causing damage to other components	Vehicle motion slowed or stopped possibly in an uncontrolled fashion Possible damage to other components Propulsive capability remains
5	Differential	Provides power from driveshaft to wheels	1	1	1	1	0	1	1	1	1	1	1	1	1	No torque transfer to wheels from engine/EM	Vehicle motion slowed or stopped possibly in an uncontrolled fashion Zero propulsive capability
6	Brakes	Inhibits vehicle motion Slows/stops moving vehicle Keeps stopped vehicle stationary	1	1	1	1	1	0	1	1	1	1	1	1	1	No ability to inhibit vehicle motion If the vehicle is in motion, it will uncontrollably remain in motion	Propulsive capability remains Unintended vehicle motion

																Stationary vehicle	
7	Transmission	Transfers power from engine to driveshaft Gears change drive-wheel speed and torque in relation to engine speed and torque	0	1	1	1	1	1	0	1	1	1	1	1	1	rollaway No torque transfer from engine to differential Wrong amount of torque transferred from engine to differential	Unintended vehicle propulsive behavior Lack of speed control could make driving conditions unstable and dangerous
8	Battery Pack	Stores energy in the form of electric potential for the purpose of powering the electric motor and storing energy regenerated from the motor	1	0	1	1	1	1	1	0	1	1	0	1	0	No Storage or discharge of electric energy	Vehicle motion slowed or stopped Possible propulsive capability Unintended longitudinal motion
9	BMS	Ensure safe ESS operating conditions Monitor ESS state (voltage, temperature, SOC, and current) Reporting data Controls/balances ESS environment	1	0	1	1	1	1	1	0	0	0	0	1	1	Loss of battery pack conditions Triggers fault on HSC, EMC	Vehicle motion slowed or stopped Possible propulsive capability Unpredictable control behavior
10	HSC	Acquires operator and various sensor inputs (APPS, gear, vehicle speed) Controls all hybrid driving functions Controls torque via engine/EM torque split using	0	0	0	1	0	1	0	0	0	0	0	0	0	Failure of all operational functions	Vehicle motion slowed or stopped Zero propulsive capability Unpredictable control behavior

		rules-based or PAE control strategy Maintains SOC at appropriate level Determines gear shifting Modifies stock signals															If the vehicle is not in operation, it will not function
11	EMC	Regulates supply of current to EM Convert DC to AC Controls direction of current Monitor and regulates EM temperature	1	0	1	1	1	1	1	1	1	1	0	1	1	Lack of ability to control EM behavior	Vehicle motion slowed or stopped Possible propulsive capability Unpredictable control behavior
12	ТСМ	Receives inputs from HSC, ECM, and various sensors (vehicle speed, wheel speed, throttle position) Controls gear shifting Monitors and regulates transmission thermal control system	1	1	1	1	1	1	1	1	1	1	1	0	1	Lack of ability to control transmission behavior No torque transfer from engine to differential Wrong amount of torque transferred from engine to differential	Vehicle motion slowed or stopped Possible propulsive capability Unpredictable control behavior
13	ECM	Controls engine torque output Controls engine temperature Controls A/F ratio Controls idle speed	1	1	0	1	1	1	1	1	1	1	1	1	0	Probable loss of engine functionality	Vehicle motion slowed or stopped Possible propulsive capability Unpredictable control behavior

	Controls electron	ic valve			
			SEFA Part 2 of 2		
Item No.	Potential Safety Hazard	Diagnostic Method	Mitigation Method	System State After Mitigation	Functional Requirement
1 Driveshaft	Unintended Vehicle deceleration Unintended longitudinal motion Operator and/or passenger injury Damage to or loss of property Damage to environment Unintended lateral motion Partial torque transmission Loss of regenerative braking	Vehicle technical inspection will identify if the interface is free of manufacturing or installation fatigue or failure Operator aware during operation by identifying partial or total functionality failure	Ensure proper mounting, installation, and manufacturing of modified driveshaft and its components Ensure bolts and mounting hardware is securely fastened and free from potential loosening or movement Ensure driveshaft-EM interface location is covered and free from potential unintended access or physical damage Ensure proper manufacturing and design for minimal interface angle	Stopped Zero propulsive capability	Development team shall ensure proper mounting, installation, and manufacturing of modified driveshaft and its components Development team shall ensure driveshaft bolts and mounting hardware is securely fastened and free from potential loosening or movement Development team shall ensure driveshaft- EM interface location is covered and free from potential unintended access or physical damage Development team shall ensure proper manufacturing and design for minimal driveshaft-EM interface angle
Item No.	Potential Safety Hazard	Diagnostic Method	Mitigation Method	System State After Mitigation	Functional Requirement
2 EM	Unintended acceleration Unintended longitudinal motion Loss or degradation of	Operator aware during operation by vehicle response to torque request, potential EM over-heat or	Provide real time feedback to operator of motor state (current, torque, temp, speed) Actuate motor thermal	Vehicle would be capable of normal functionality	To prevent motor failure due to overheating the EMC shall actuate thermal controls to maintain motor temperature within a specified limit To prevent motor failure due to over-
	propulsion system	failure	controls when motor temperature range exceeds specified limits	If emergency motor shut	torque or over-speed, the HSC shall impose a governor to regulate to motor torque and speed to specified limits

		Vehicle technical		off occurs	
	or and/or passenger				The second se
injury		inspection will	Actuate motor speed and	the vehicle	To prevent motor failure due to over-
	. 1 6	identify leaks or	torque governor when motor	will be	current the EMC shall impose a governor
-	e to or loss of	physical damage	speed and torque exceed	capable of	to regulate the flow of current within
property	у	to the EM	specified limits	normal	specified limits of the motor and battery
				operations	pack
Damage	e to environment	Operator aware	Actuate EMC current	(P,R,N,D)	
		during operation	governor via HSC when	with partial	To prevent motor failure the operator shall
Potentia	al for overheating	by identifying loss	motor, battery pack, or	functionality	be provided real-time diagnostics and have
		of motor	EMC exceeds specified		the capability to discontinue motor
Uninter high vo	ided exposure to	functionality	current limits		operations
ingii vo	nage	Operator aware	Allow operator override to		Development team shall ensure software
		during operation	discontinue motor operation		(HSC) limits the magnitude of current to
		by identifying	discontinue motor operation		the EM
		high EM	Ensure software (HSC)		
		temperature and	limits the magnitude of		Development team shall ensure relays and
		loss of motor	current to the EM		fuses are in place and functional to prevent
		functionality			over drawing of current
		j	Ensure relays and fuses are		
		Vehicle technical	in place and functional to		Development team shall ensure proper
		inspection will	prevent over drawing of		mounting, installation, and manufacturing
		identify if the	current		of the EM and housing
		interface is free of			
		manufacturing or	Ensure proper mounting,		Development team shall ensure EM
		installation fatigue			housing and coolant system bolts, interface
		or failure	installation, and		components, and mounting hardware are
		or randic	manufacturing of the EM		securely fastened and free from leaks and
			and housing		potential loosening or unintended
					movement
			Ensure bolts, interface		movement
			components, and mounting		Development teem shell on sure EM
			hardware are securely		Development team shall ensure EM
			fastened and free from leaks		cooling system and its components are
			and potential loosening or		functioning, proper coolant levels, and
			movement		hoses running to and from the motor are
					leak free
			Ensure cooling system and		
			its components are		Development team shall ensure EM
			functioning, proper coolant		thermal system components (radiator,
			levels, and hoses running to		

			and from the motor are leak free Ensure thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the EM Ensure the fans are free from potential physical damage		 coolant level, fans) are functional and sufficient to cool the EM Development team shall ensure EM coolant system fans are free from potential physical damage Development team shall ensure EM coolant system fans pull air from a cool source Development team shall ensure proper
			Ensure enclosure fans pull air from a cool source		mounting, installation, and manufacturing of EM coolant system and its components Development team shall ensure EM
			Ensure proper mounting, installation, and manufacturing of coolant system and its components		coolant system bolts, hoses and mounting hardware are securely fastened and free from potential loosening or unintended movement
			Ensure bolts, hoses and mounting hardware are securely fastened and free from potential loosening or		Development team shall ensure the HSC controls and mitigates EM overheating Operator shall drive appropriately to
			movement Ensure the HSC controls and mitigates overheating		ensure EM temp is stable
			Operator drives appropriately to ensure EM temp is stable		
Item No.	Potential Safety Hazard	Diagnostic Method	Mitigation Method	System State After Mitigation	Functional Requirement
3 Engine	unintended deceleration/acceleration	Vehicle technical inspection will identify deformation to	Ensure proper mounting, installation, and manufacturing of the oil filter and pump	Stopped Zero/ possibility	Development team shall ensure proper mounting, installation, and manufacturing of the oil filter and pump

DescriptionDevelopment team shall ensure thermal system frag and pump bits, interface components (cals, gaskets), and mounting hardware are accurely fastened and free from leaks and potential lossening or unintended movementDevelopment team shall ensure thermal system frag cale and unificient to cool the engine0Derator aware during operation by identifying on grinding, dirty exhaust, or a drop in pressureEnsure frequent oil changes, clean oil, and that the oil filter is notDevelopment team shall ensure thermal system frequent oil changes, clean oil, and that the oil filter is not0Sensors signal to ECMEnsure thermal system conponents (radiator, cool the engineDevelopment team shall ensure thermal system frequent oil changes, clean oil, and that the oil filter is not0Derator aware during operation. Operator views engine temp in cabin.Ensure thermal system conjonents (radiator, cool the engineDevelopment team shall ensure thermal system frage damage1Derator aware during operation.Ensure enclosure fans are free from ocol sourceDevelopment team shall ensure thermal system fans pull air from a cool source1Ensure enclosure fans pull air from a cool sourceEnsure enclosure fans pull air from a cool sourceDevelopment team shall ensure thermal system is designed such that three is sufficient to provide appropriate air movement through engine bay2Development team shall ensure thermal system is designed such that three is sufficient to provide appropriate air movementsDevelopment team shall ensure thermal system foots and mounting hardware are system	damage and/or injury to	filter and unclean		of	Development team shall ensure oil filter
Operator aware during operation by identifying loss in pressure during operation by identifying loss in pressure during operation by identifying loss in pressure during operation in pressure during operation in pressure during operation in pressure during operationcapability is capability (salastend and free from leaks and potential lossening or unintended movementOperator shall ensure frequent oil changes, clean oil, and that the oil filter is notCoperator shall ensure frequent oil changes, clean oil, and that the oil filter is notSensors signal to ECMEnsure frequent oil changes, clean oil, and that the oil filter is notOperator aware during operation.Ensure thermal system coolant level, fans) are functional and sufficient to cool the engineOperator sware during operationEnsure the fans are free from potential physical damageDevelopment team shall ensure thermal system fans audificient to cool the engineError message displayedEnsure engine ventilation is sufficient to provide appropriate aim movement through engine bayEnsure thermal system is designed such that there is sufficient if how to cool engine componentsEnsure thermal system is designed componentsEnsur			Ensure bolts interface		
Operator aware during operator during operator by identifying loss of vehicle functionality, Sputtering, engine grinding, dirty exhaust, or a drop in pressureand mounting hardware are securely fastened and free from leaks and potential lossening or movementare securely fastened and free from leaks and potential movementOperator shall ensure frequent oil changes, clean oil, and that the oil filter is not Ensure frequent oil changes, clean oil, and that the oil filter is not ECMThe securely fastened and free from leaks and potential hosening or unintended movementOperator sware during operator cool nt level, fans) are functional and sufficient to cool the engineDevelopment team shall ensure thermal system fans are free from potential physical damageDevelopment team shall ensure thermal system fans are free from potential physical damageError message displayedEnsure enclosure fans pull air from a cool sourceDevelopment team shall ensure thermal system fans are free from potential physical damageError message displayedEnsure enclosure fans pull air from a cool sourceDevelopment team shall ensure thermal system fans pull air from a cool sourceError message displayedEnsure engine ventilation is sufficient if pow to cool engine componentsDevelopment team shall ensure thermal system fans pull air from a cool sourceError message displayedEnsure nermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure thermal system and its componentsEnsure engine componentsEnsure form optime air from a cool source </td <td>pussenger/personner</td> <td>011</td> <td>· · · · · · · · · · · · · · · · · · ·</td> <td></td> <td></td>	pussenger/personner	011	· · · · · · · · · · · · · · · · · · ·		
during operation by identifying loss of vehicle functionality, grinding, dirry exhaust, or a drop in pressuresecurely fast-med and free from leaks and potential losening or movement losening or movementand potential losening or unintended movementOperator shall ensure frequent oil changes, clean oil, and that the oil filter is not in pressureEnsure frequent oil changes, clean oil, and that the oil filter is not components (radiator, coolant level, fans) are from toexial and sufficient to cool the engineDevelopment team shall ensure thermal system components (radiator, coolant level, fans) are free from potential physical damageOperator views engine temp in cabin.Coperator views engine temp in cabin.Ensure enclosure fans pull air from a cool sourceDevelopment team shall ensure thermal system fans are free from potential physical damageError message displayedEnsure engine ventilation is sufficient to provide appropriate air movement through engine bayDevelopment team shall ensure thermal system fans pull air from a cool sourceEnsure thermal system is sufficient to rovide appropriate air movement through engine bayEvelopment team shall ensure thermal system is designed such that there is sufficient to provide appropriate air movement through engine bayDevelopment team shall ensure thermal system is designed such that there is sufficient to rovide appropriate air movement through engine bayError message displayedEnsure proper mounting, installation, and manufacturing of thermalDevelopment team shall ensure thermal system is designed such that there is sufficient to rovide appropriate air		Operator aware		capability	
by identifying loss of vehiclefrom leaks and potential losening or movementmovementof vehiclefrom leaks and potential losening or movementmovementfunctionality, sputtering, engine in pressureEnsure frequent oil changes, clean oil, and that the oil filter is notOperator shall ensure frequent oil changes, clean oil, and that the oil filter is notSensors signal to ECMEnsure thermal system coolant level, fans) are functional and sufficient to cool the engineDevelopment team shall ensure thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the engineDevelopment team shall ensure thermal system sins are free from potential physical damageOperator wiews engine temp in cabin.Ensure enclosure fans pull air from a cool sourceDevelopment team shall ensure thermal system fans are free from potential physical damageError message displayedEnsure engine ventilation is sufficient to provide appropriate air movement through engine bayDevelopment team shall ensure thermal system is designed such that there is sufficient ti flow to cool engine componentsEnsure proper mounting, installation, and maunfacturing of thermalEnsure proper mounting, installation, and manufacturing of thermalDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsEnsure proper mounting, installation, and maunfacturing of thermalDevelopment team shall ensure therma					
of vehicle functionality, Sputtering, engine grinding, dirty exhaust, or a drop in pressureloosening or movement functionality, Sputtering, engine grinding, dirty exhaust, or a drop in pressureloosening or movement fusure frequent oil changes, clean oil, and that the oil filter is not ballooned or deformedSensors signal to ECMEnsure thermal system components (radiator, cool ant level, fans) are functional and sufficient to cool the engineDevelopment team shall ensure thermal system components (radiator, cool ant level, fans) are functional and sufficient to cool the engineDevelopment team shall ensure the thermal systems fans are free from potential physical damageOperator views engine temp in cabin.Ensure the fans are free from potential physical damageDevelopment team shall ensure the thermal systems fans are free from potential physical damageError message displayedEnsure enclosure fans pull air from a cool sourceDevelopment team shall ensure thermal system fans pull air from a cool sourceEnsure engine ventilation is sufficient to provide appropriate air movement through engine bayDevelopment team shall ensure thermal system is designed such that there is sufficient to provide appropriate air flow to cool engine componentsEnsure thermal system is designed such that there is sufficient to provide appropriate air flow to cool engine componentsDevelopment team shall ensure thermal system is designed such that there is sufficient to roo cool engine componentsEnsure thermal system is designed such that there is sufficient to provide engine componentsEnsure thermal system is des					
functionality, Sputtering, engine grinding, dirty exhaust, or a drop in pressureEnsure frequent oil changes, clean oil, and that the oil filter is notOperator shall ensure frequent oil changes, clean oil, and that the oil filter is notSensors signal to ECMEnsure thermal system conponents (radiator, coolant level, fans) are functional and sufficient to coolant level, fans) are functional and sufficient to cool the engineDevelopment team shall ensure thermal system components (radiator, cool the engineOperator sware during operation.Ensure the fans are free from potential physical damageDevelopment team shall ensure the thermal system fans are free from potential physical damageError message displayedEnsure enclosure fans pull air from a cool sourceDevelopment team shall ensure thermal system fans are free potential physical damageError message displayedEnsure engine ventilation is sufficient to provide appropriate air movement through engine bayDevelopment team shall ensure thermal system fans pull air from a cool sourceEnsure thermal system is designed such that ther is sufficient air flow to cool engine componentsEnsure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure proper mounting, installation, and manufacturing of thermalDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure proper mounting, installation, and manufacturing of thermalDevelopment team shall ensure thermal system and its components </td <td></td> <td></td> <td></td> <td></td> <td>novement</td>					novement
Sputtering, engine grinding, dity exhaust, or a drop in pressureEnsure frequent oil changes, clean oil, and that the oil filter is notclean oil, and that the oil ballooned or deformedSensors signal to ECMEnsure thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the engineDevelopment team shall ensure thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the engineDevelopment team shall ensure thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the engineOperator aware during operation.Coperator views engine temp in cabin.Ensure the fans are free from potential physical damageDevelopment team shall ensure the thermal system fans pull air from a cool sourceError message displayedEnsure engine ventilation is sufficient to provide appropriate air movement through engine bayDevelopment team shall ensure thermal system fans pull air from a cool sourceEnsure hermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure proper mounting, installation, and manufacturing of thermal manufacturing of thermal manufacturing of thermalDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine components			loosening of movement		Operator shall ensure frequent oil changes
grinding, dirty exhaust, or a drop in pressureclean oil, and that the oil filter is notballooned or deformedSensors signal to ECMSensors signal to ECMEnsure thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the engineDevelopment team shall ensure thermal system components (radiator, cool the cool the engineOperator wiews engine temp in cabin.Operator views engine temp in cabin.Ensure thermal system fans are free from potential physical damageDevelopment team shall ensure the thermal system fans are free from potential physical damageError message displayedEnsure enclosure fans pull air from a cool sourceDevelopment team shall ensure thermal system fans pull air from a cool sourceError message displayedEnsure engine ventilation is sufficient to provide appropriate air movement through engine bayDevelopment team shall ensure thermal system fans pull air frow to cool engine componentsDevelopment team shall ensure thermal system fans pull air from a cool sourceDevelopment team shall ensure thermal system fans pull air from a cool sourceEnsure engine ventilation is sufficient to provide appropriate air movement through engine bayDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure proper mounting, installation, and manufacturing of thermal potential phystem and its componentsDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine components			Ensure frequent oil changes		
exhaust, or a drop in pressurefilter is notDevelopment team shall ensure thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the engineDevelopment team shall ensure thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the engineOperator aware during operation.Ensure the fans are free from potential physical damageDevelopment team shall ensure the thermal systems fans are free from potential physical damageDevelopment team shall ensure the thermal systems fans are free potential physical damageOperator views engine temp in cabin.Ensure enclosure fans pull air from a cool sourceDevelopment team shall ensure thermal system fans pull air from a cool sourceEnsure engine ventilation is sufficient to provide appropriate air movement through engine bayDevelopment team shall ensure thermal system fans pull air from a cool sourceEnsure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure thermal system fans pull air from a cool sourceEnsure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsEnsure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsEnsure proper mounting, installation, and manufacturing of thermalDevelopment team shall ens					
in pressureDevelopment team shall ensure thermal system components (radiator, cool ant level, fans) are functional and sufficient to cool the engineDevelopment team shall ensure thermal system components (radiator, cool ant level, fans) are functional and sufficient to cool the engineDevelopment team shall ensure thermal system components (radiator, cool the engineOperator aware during operation.Operator views engine temp in cabin.Development team shall ensure the thermal systems fans are free from potential physical damageDevelopment team shall ensure the thermal system fans are free from potential physical damageError message displayedEnsure enclosure fans pull air from a cool sourceDevelopment team shall ensure thermal system fans pull air from a cool sourceEnsure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsEnsure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure proper mounting, installation, and manufacturing of thermal system and its components					banooned of deformed
Sensors signal to ECMEnsure thermal system components (radiator, cool and level, fans) are functional and sufficient to cool the enginesystem components (radiator, cool and level, fans) are functional and sufficient to cool the engineOperator aware during operation.Development team shall ensure the thermal system from potential physical damageDevelopment team shall ensure the thermal system fans are free potential physical damageOperator views engine temp in cabin.Ensure the fans are free from potential physical damageDevelopment team shall ensure thermal system fans pull air from a cool sourceError message displayedEnsure engine ventilation is sufficient to provide appropriate air movement through engine bayDevelopment team shall ensure thermal system fans pull air from a cool sourceEnsure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsEnsure proper mounting, installation, and manufacturing of thermal manufacturing of thermalDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine components					
Sensors signal to ECMcomponents (radiator, coolant level, fans) are functional and sufficient to coolant level, fans) are functional and sufficient to cool the enginelevel, fans) are functional and sufficient to cool the engineOperator aware during operation.Operator views engine temp in cabin.Ensure the fans are free from potential physical damageDevelopment team shall ensure the thermal systems fans are free from potential physical damageError message displayedEnsure enclosure fans pull air from a cool sourceDevelopment team shall ensure thermal system fans pull air from a cool sourceEnsure engine ventilation is sufficient to provide appropriate air movement through engine bayDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsEnsure proper mounting, installation, and manufacturing of thermalDevelopment team shall ensure thermal system and its components		in pressure	Ensure thermal system		
Coll the engineCool and level, fans) are functional and sufficient to cool the engineCool the engineOperator aware during operation.cool the engineDevelopment team shall ensure the thermal systems fans are free from potential physical damageDevelopment team shall ensure the thermal system fans are free from potential physical damageOperator views engine temp in cabin.Ensure the fans are free from potential physical damageDevelopment team shall ensure thermal system fans pull air from a cool sourceError message displayedEnsure enclosure fans pull air from a cool sourceDevelopment team shall ensure engine ventilation is sufficient to provide appropriate air movement through engine bayDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsEnsure proper mounting, installation, and manufacturing of thermalDevelopment team shall ensure proper mounting, installation, and manufacturing of thermal system and its components					
InterfaceInterfaceInterfaceInterfaceOperator aware during operation.Operator aware during operation.Cool the engineDevelopment team shall ensure the thermal systems fans are free from potential physical damageDevelopment team shall ensure the thermal system fans pull air from a cool sourceOperator views engine temp in cabin.Ensure enclosure fans pull air from a cool sourceDevelopment team shall ensure thermal system fans pull air from a cool sourceError message displayedEnsure engine ventilation is sufficient to provide appropriate air movement through engine bayDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine cool engineEnsure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure thermal appropriate air movement through engine bayEnsure proper mounting, installation, and manufacturing of thermalEnsure proper mounting, installation, and manufacturing of thermalDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine cool engine components					
Operator aware during operation.cool the engineDevelopment team shall ensure the thermal systems fans are free from potential physical damageOperator views engine temp in cabin.Cool the engineDevelopment team shall ensure the thermal systems fans are free from potential physical damageDevelopment team shall ensure thermal system fans pull air from a cool sourceError message displayedError message displayedEnsure enclosure fans pull air from a cool sourceDevelopment team shall ensure engine ventilation is sufficient to provide appropriate air movement through engine bayEnsure engine componentsDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure proper mounting, installation, and manufacturing of thermalDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure proper mounting, installation, and manufacturing of thermalDevelopment team shall ensure thermal system and its components		ECM			cool the engine
during operation.Ensure the fans are free from potential physical damageDevelopment team shall ensure thermal systems fans are free from potential physical damageOperator views engine temp in cabin.Ensure the fans are free from potential physical damageDevelopment team shall ensure thermal system fans pull air from a cool sourceError message displayedEnsure enclosure fans pull air from a cool sourceDevelopment team shall ensure thermal system fans pull air from a cool sourceEnsure engine ventilation is sufficient to provide appropriate air movement through engine bayDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsEnsure proper mounting, installation, and manufacturing of thermalDevelopment team shall ensure proper mounting, installation, and manufacturing of thermal		0			D. L. M. L. H. M. M.
Ensure the fans are free from potential physical damagepotential physical damageOperator views engine temp in cabin.Ensure onclosure fans pull air from a cool sourceDevelopment team shall ensure thermal system fans pull air from a cool sourceError message displayedEnsure engine ventilation is sufficient to provide appropriate air movement through engine bayDevelopment team shall ensure thermal system fans pull air from a cool sourceDevelopment team shall ensure engine ventilation is sufficient to provide appropriate air movement through engine bayDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure proper mounting, installation, and manufacturing of thermalDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure proper mounting, installation, and manufacturing of thermalDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine components			cool the engine		
Operator views engine temp in cabin.from potential physical damageDevelopment team shall ensure thermal system fans pull air from a cool sourceError message displayedair from a cool sourceDevelopment team shall ensure engine ventilation is sufficient to provide appropriate air movement through engine bayDevelopment team shall ensure engine ventilation is sufficient to provide appropriate air movement through engine bayDevelopment teams shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure proper mounting, installation, and manufacturing of thermalDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure proper mounting, installation, and manufacturing of thermalDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine components		during operation.	Ensure the fans are free		
ending temp in cabin.damageDevelopment team shall ensure thermal system fans pull air from a cool sourceError message displayedEnsure enclosure fans pull air from a cool sourceDevelopment team shall ensure engine ventilation is sufficient to provide appropriate air movement through engine bayDevelopment team shall ensure engine ventilation is sufficient to provide appropriate air movement through engine bayEnsure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure proper mounting, installation, and manufacturing of thermalDevelopment team shall ensure proper mounting, installation, and manufacturing of thermalDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine components					potential physical damage
Cabin.Ensure enclosure fans pull air from a cool sourceDevelopment team shall ensure engine ventilation is sufficient to provide appropriate air movement through engine bayDevelopment team shall ensure engine ventilation is sufficient to provide appropriate air movement through engine bayEnsure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure proper mounting, installation, and manufacturing of thermalDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine components					D. 1
Error message displayed Error message displayed Error message displayed Error message displayed Error message displayed Ensure engine ventilation is sufficient to provide appropriate air movement through engine bay Ensure thermal system is designed such that there is sufficient air flow to cool engine components Ensure proper mounting, installation, and manufacturing of thermal Development team shall ensure proper mounting, installation, and manufacturing of thermal system and its components		U 1	uamage		
Error message displayedair from a cool sourceDevelopment team shall ensure engine ventilation is sufficient to provide appropriate air movement through engine bayDevelopment team shall ensure engine ventilation is sufficient to provide appropriate air movement through engine bayDevelopment teams shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure proper mounting, installation, and manufacturing of thermalDevelopment team shall ensure proper mounting, installation, and its components		cabin.	Ensure enclosure fans pull		system fans pull air from a cool source
displayed bit of message displayed Ensure engine ventilation is sufficient to provide appropriate air movement through engine bay Ensure thermal system is designed such that there is sufficient air flow to cool engine components Ensure proper mounting, installation, and manufacturing of thermal Development team shall ensure thermal system is designed such that there is sufficient air flow to cool engine components Development team shall ensure proper mounting, installation, and manufacturing of thermal system and its components		E			Development to makell ensure ensine
Ensure engine ventilation is sufficient to provide appropriate air movement through engine bayappropriate air movement through engine bayDevelopment teams shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment teams shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure proper mounting, installation, and manufacturing of thermalDevelopment team shall ensure proper mounting, installation, and manufacturing of thermal system and its components					Development team shall ensure engine
sufficient to provide appropriate air movement through engine bayDevelopment teams shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure thermal sufficient air flow to cool engine componentsEnsure proper mounting, installation, and manufacturing of thermalDevelopment team shall ensure proper mounting, installation, and manufacturing of thermal system and its components		displayed	Ensure engine ventilation is		
appropriate air movement through engine bayDevelopment teams shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsbesigned such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure proper mounting, installation, and manufacturing of thermalbesigned such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure proper mounting, installation, and manufacturing of thermalbesigned such that there is sufficient air flow to cool engine componentsDevelopment team shall ensure proper mounting, installation, and manufacturing of thermal system and its components					
In our proper through engine bayDevelopment teams shall ensure thermal system is designed such that there is sufficient air flow to cool engine componentsDevelopment teams shall ensure thermal system is designed such that there is componentsDevelopment team shall ensure thermal sufficient air flow to cool engine componentsDevelopment team shall ensure thermal of thermal system and its componentsDevelopment team shall ensure proper mounting, installation, and manufacturing of thermalDevelopment team shall ensure thermal bevelopment team shall ensure thermal					bay
Ensure thermal system is designed such that there is sufficient air flow to cool engine componentsSystem is designed such that there is sufficient air flow to cool engine componentsEnsure proper mounting, installation, and manufacturing of thermalDevelopment team shall ensure proper mounting, installation, and manufacturing of thermal system and its components					Davalanment teams shall answer thereas
Ensure thermal system is designed such that there is sufficient air flow to cool engine componentssufficient air flow to cool engine componentsDevelopment team shall ensure proper mounting, installation, and manufacturing of thermalDevelopment team shall ensure proper mounting, installation, and manufacturing of thermal system and its components			un ough onghie ouy		
designed such that there is sufficient air flow to cool engine componentscomponentsDevelopment team shall ensure proper mounting, installation, and manufacturing of thermalDevelopment team shall ensure proper mounting, installation, and its components			Ensure thermal system is		
sufficient air flow to cool engine components Development team shall ensure proper mounting, installation, and manufacturing of thermal system and its components Ensure proper mounting, installation, and manufacturing of thermal Development team shall ensure thermal					e
engine components Development team shall ensure proper mounting, installation, and manufacturing of thermal system and its components installation, and manufacturing of thermal Development team shall ensure proper mounting, installation, and manufacturing of thermal system and its components					components
Ensure proper mounting, installation, and manufacturing of thermal Development team shall ensure thermal					Development teem shell ensure men-r
Ensure proper mounting, installation, and manufacturing of thermalof thermal system and its componentsDevelopment team shall ensure thermal					
installation, and manufacturing of thermal Development team shall ensure thermal			Ensure proper mounting		
manufacturing of thermal Development team shall ensure thermal					or merman system and its components
					Davelonment team shall ensure thermal
system bons and mounting nardware are					
					system bons and mounting nardware are

		Ensure bolts and mounting hardware are securely fastened and free from potential loosening or movement Ensure the ECM controls and mitigates overheating Operator drives appropriately to ensure		securely fastened and free from potential loosening or movement Development team shall ensure the ECM controls and mitigates overheating Operator shall avoid poor driving behaviors
		engine temp is stable		
	Diagnostic		System State After	
Item No. Potential Safety Hazard	Method	Mitigation Method	Mitigation	Functional Requirement
4 Suspension Unintended lateral	Error message will	Ensure proper tire pressure	Stopped	Operator shall ensure proper tire pressure
movement	occur	prior to operation	D 1111	prior to operation
Pulling to one side	Vehicle technical inspection will	Ensure proper tire alignment	Possibility of no vehicle	Operator shall ensure proper tire alignment
Difficult to steer	identify low tire pressure and	Ensure tire quality	motion/ loss of wheel	Operator shall ensure tire quality
Vehicle corner sits low	uneven tire wear	Ensure balanced, bent, or broken wheels		Operator shall ensure wheels are balanced and suspension is free of ben tor broken
Operator and/or passenger injury	Operator aware during operation from vehicle	Avoid poor drive behavior		wheels Operator shall avoid poor driving
Damage to or loss of property	sagging and unsettling noise	Ensure to rotate tires regularly		behaviors
Damage to environment	Deterioration of performance.	Routine maintenance and inspection for rust		Operator shall ensure manufacturer recommended tire rotation
	Vehicle technical inspection will identify spring	Avoid adverse road conditions		Development team shall ensure suspension spring compression is calibrated and that springs are free of fatigue and corrosion
	fatigue Vehicle technical	Ensure proper mounting, installation, and routine maintenance and inspection		Development team shall ensure the suspensions system and components have proper mounting, installation, and routine maintenance and inspection of hardware
			Vehicle technical vehicle tech	Vehicle technical vehicle tech

		identify rust, corrosion, and failure	Ensure bolts and mounting hardware is securely fastened and free from potential loosening or unintended movement	System	Development team shall ensure the suspensions system bolts and mounting hardware is securely fastened and free from potential loosening or unintended movement
		Diagnostic		State After	
Item No.	Potential Safety Hazard	Method	Mitigation Method	Mitigation	Functional Requirement
5 Differential	Unintended Vehicle deceleration Unintended longitudinal motion Operator and/or passenger injury Damage to or loss of property Damage to environment Partial torque transmission	Vehicle technical inspection will identify if the interface is free of manufacturing or installation fatigue or failure Operator aware during operation by identifying partial or total functionality failure	Ensure proper mounting, installation, and manufacturing of modified driveshaft and its components Ensure bolts and mounting hardware is securely fastened and free from potential loosening or movement Ensure differential- driveshaft interface location is free from potential unintended access or physical damage	Stopped Zero propulsive capability	Development team shall ensure proper mounting, installation, and manufacturing of modified driveshaft, differential and their components Development team shall ensure driveshaft bolts and mounting hardware is securely fastened and free from potential loosening or movement Development team shall ensure differential-driveshaft interface location is covered and free from potential unintended access or physical damage
Item No.	Potential Safety Hazard	Diagnostic Method	Mitigation Method	System State After Mitigation	Functional Requirement
6 Brakes	Unintended loss of longitudinal motion Operator and/or passenger injury	Vehicle technical inspection will identify if the pads are free from fatigue or corrosion	Ensure proper mounting and installation of pads Ensure bolts and mounting hardware is securely fastened and free from	Stopped Possibility of uncontrolled	Development team shall ensure proper mounting and installation of pads Development team shall ensure brake pad bolts and mounting hardware is securely fastened and free from potential loosening
	Damage to or loss of property	Operator aware during operation	potential loosening or movement	vehicle motion	or unintended movement Operator shall avoid excessively adverse
	Damage to environment	by identifying unsettling smell,	Avoid adverse road conditions		road conditions (bumpy terrain, excessive grade) which may cause a high NVH

	Unintended vehicle motion	and vehicle			
	when stationary (rollaway)	vibration	Routine maintenance and inspection for rust and corrosion		Operator shall perform routine inspection of brake system to check for rust, fatigue, and corrosion
			Avoid poor drive behavior		Operator shall avoid poor driving behaviors
			Ensure brake system is free		
			of build-up and debris prior to use		Operator shall ensure brake system is free of build-up and debris prior to use
			Ensure proper bleeding, mounting, installation, and routine maintenance and		ensure proper bleeding, mounting, installation, and routine maintenance and inspection of hardware and functionality
			inspection of hardware and functionality		Development team shall ensure bolts and mounting hardware is securely fastened
			Ensure bolts and mounting hardware is securely fastened and free from		and free from potential loosening or unintended movement
			potential loosening or unintended movement		
		Diagnostic		System State After	
Item No.	Potential Safety Hazard	Method	Mitigation Method	Mitigation	Functional Requirement
7 Transmission	Unintended acceleration	Vehicle technical inspection will	Ensure proper mounting, installation, and	Stopped	Development team shall ensure proper mounting, installation, and manufacturing
1141151111551011	Unintended longitudinal	identify low fluid	manufacturing of	Zero	of transmission and its components
	motion	level, leaks, and belt fatigue	transmission and its components	propulsive capability	Development team shall ensure
	Loss or degradation of	8	· · · · · · · · · · · · · · · · · · ·	capaointy	transmission bolts, interface components
	propulsion system	Operator aware	Ensure bolts, interface		(seals, gaskets), and mounting hardware
		during operation	components (seals, gaskets),		are securely fastened and free from
	Operator and/or passenger	by identifying	and mounting hardware are		potential loosening or movement
	injury	displayed high temperatures	securely fastened and free from potential loosening or		Operator shall ensure the correct type of
	Damage to or loss of	lomporaturos	movement		coolant (ATF) is used, proper coolant
	property				levels, and check for leaks prior to
			Ensure the correct type of		operation
	Damage to environment		coolant is used, proper		

Potential for overheating	coolant levels, and check for leaks prior to operation Ensure belt drive components are properly installed (tensioning, torque specs)	Development team shall ensure belt drive components are properly installed (tensioning, torque specs) Development team shall ensure transmission thermal system components (radiator, coolant level, fans) are
	Ensure thermal system components (radiator, coolant level, fans) are functional and sufficient to	functional and sufficient to cool the transmission Development team shall ensure transmission thermal system fans are free
	cool the transmission Ensure the fans are free from potential physical	from potential physical damage Development team shall ensure transmission thermal system fans pull air
	damage Ensure fans pull air from a cool source	from a cool source Development team shall ensure proper mounting, installation, and manufacturing of transmission thermal system and its
	Ensure proper mounting, installation, and manufacturing of coolant system and its components	components Development team shall ensure transmission thermal system bolts, hoses and mounting hardware are securely
	Ensure bolts, hoses and mounting hardware are securely fastened and free from potential loosening or	fastened and free from potential loosening or unintended movement Development team shall ensure the TCM
	movement Ensure the TCM controls and mitigates overheating	controls and mitigates overheating Operator shall drive appropriately to ensure transmission temperature is stable
	Operator drives appropriately to ensure transmission temperature is stable	

Item No.	Potential Safety Hazard	Diagnostic Method	Mitigation Method	System State After Mitigation	Functional Requirement
8 Battery Pack	 Unintended Vehicle deceleration Unintended longitudinal motion Thermal runaway Unintended exposure to high voltage Short circuit Operator and/or passenger injury Damage to or loss of property Loss of HV power Damage to environment 	 BMS monitors and sends temperature data in real time Operator aware during operation by identifying a thermal event, error message of overheating, or failure of HV components BMS monitors and sends SOC data in real time Vehicle technical inspection will identify authorized access OBC controls and mitigates charging while vehicle is not in operation 	Operate vehicle within specified battery temp rangeActuate cooling fans when battery pack reaches specified temperatureUse manufacturer recommended installation instructions (clearance, bend radii)Limit charge and discharge current to specified rangeBMS monitors and controls SOC.Controls software will only draw current at specified minimum SOCEnsure proper mounting, installation, and manufacturing of enclosure and HV componentsEnsure bolts and mounting hardware is securely fastened and free from potential loosening or movementEnsure all vents are covered with appropriate screening to prevent access from	Stopped Zero/ possibility of propulsive capability from EM, possible for engine to continue operation as normal	To prevent the HV battery pack from operating outside of the max/min temperature range the development team shall ensure specified temperature limits are controlled by the BMS To prevent the HV battery pack from operating outside of the max/min temperature range the development team shall ensure actuation of battery pack thermal control system (fans) when the temperature reaches limit To prevent the HV battery pack from operating outside of the max/min temperature range the development team shall ensure proper installation using manufacturer recommended specifications to include component clearances and wire bend radii To prevent the HV battery pack from operating outside of the max/min temperature range the development team shall ensure proper installation using manufacturer tecommended specifications to include component clearances and wire bend radii To prevent the HV battery pack from operating outside of the max/min temperature range the development team shall ensure a limit to charging and discharging current to a specified range To prevent the HV battery pack from operating while undercharged the development team shall ensure the BMS monitors and controls the SOC in real-time To prevent the HV battery pack from operating while undercharged the development team shall ensure controls software will only draw current at specified minimum SOC

	liquid, debris, dust, or insectsEnsure fans are pulling air from dry particulate-free sourceEnsure enclosure location is covered when vehicle is not in useEnsure software (HSC, OBC, EMC) limits charging and discharging rates and rangesEnsure relays and fuses are in place and functional to prevent over drawing of current	 To prevent the HV battery pack from unintended access the development team shall ensure proper mounting, installation, and manufacturing of enclosure and HV components To prevent the HV battery pack from unintended access the development team shall ensure bolts and mounting hardware is securely fastened and free from potential loosening or movement To prevent the HV battery pack from unintended access the development team shall ensure all HV enclosure vents are covered with appropriate screening to prevent access from liquid, debris, dust, or insects To prevent the HV battery pack from unintended access the development team shall ensure all HV enclosure vents are covered with appropriate screening to prevent access from liquid, debris, dust, or insects To prevent the HV battery pack from unintended access the development team shall ensure HV thermal control system fans are pulling air from dry particulate-free source To prevent the HV battery pack from unintended access the development team shall ensure the enclosure location is covered and free from the external environment when vehicle is not in use To prevent the HV battery pack failure from excess charging or discharging of current the development team shall ensure software (HSC, OBC, EMC) limits charging and discharging rates and ranges
--	--	--

					current the development team shall ensure relays and fuses are in place and functional to prevent over drawing of current
Item No.	Potential Safety Hazard	Diagnostic Method	Mitigation Method	System State After Mitigation	Functional Requirement
9 BMS	Foreintial barrety FrankretUnintended longitudinal motionLoss or degradation of propulsion systemOperator and/or passenger injuryDamage to or loss of propertyDamage to environmentPotential for overheatingUnintended exposure to high voltageShort circuitThermal eventInaccurate ESS state readings (voltage, temperature, SOC	Vehicle technical inspection will identify wiring fatigue or failure Operator aware during operation by identifying eventual failure of HV components Vehicle technical inspection will identify the BMS is free of unintended access and physical damage Operator aware during operation by identifying eventual failure of HV components	Ensure wiring is securely installed using manufacturer installation specifications Ensure wiring gauge is sufficient to carry max operational current with factor of safety Ensure wire bend radii are adhered to Ensure manufacturing is sufficient to prevent unintended access and physical damage Ensure use of covering at wire-BMS interface prevent unintended access Avoid adverse road condition which may produce NVH and damage BMS Ensure BMS and mounting hardware are sufficient for max operational G-force with factor of safety Ensure BMS and mounting hardware is secure and free from unintended movement	Stopped Zero/ possibility of propulsive capability from motor, possible for engine to continue operation as normal	To prevent BMS wiring failure the development team shall ensure the wiring is securely installed using manufacturer installation specifications To prevent BMS wiring failure the development team shall ensure the wiring gauge is sufficient to carry max operational current with factor of safety To prevent BMS wiring failure the development team shall ensure wire bend radii are adhered to To prevent BMS failure the development team shall ensure the manufacturing is sufficient to prevent unintended access and physical damage To prevent BMS unintended access or physical damage failure the development team shall ensure use of covering at wire- BMS interface prevent unintended access or physical damage failure the operator shall avoid adverse road condition which may produce NVH and damage BMS To prevent BMS installation failure the development team shall ensure the BMS and mounting hardware are sufficient for max operational G-force with factor of safety

				System	To prevent BMS installation failure the development team shall ensure the BMS and mounting hardware is secure and free from unintended movement
Item No.	Potential Safety Hazard	Diagnostic Method	Mitigation Method	State After Mitigation	Functional Requirement
10 HSC	Unintended accelerationUnintended longitudinal motionLoss or degradation of propulsion systemOperator and/or passenger injuryDamage to or loss of propertyDamage to environmentPotential for overheatingUnintended exposure to high voltage	Vehicle technical inspection will identify wiring fatigue or failure Operator aware during operation by identifying eventual failure of vehicle components Vehicle technical inspection will identify if the HSC is free of unintended access Operator aware during operation by identifying eventual failure of vehicle components and loss of functionality Vehicle technical inspection will identify if HSC is free of manufacturing or	Ensure wiring is securely installed using manufacturer installation specifications Ensure wiring gauge is sufficient to carry max operational current with factor of safety Ensure wire bend radii are adhered to Ensure manufacturing is sufficient to prevent unintended access and physical damage Ensure use of covering at wire-HSC interface to prevent unintended access Avoid adverse road condition which may produce NVH and damage the HSC Ensure HSC and mounting hardware are sufficient for max operational G-force with factor of safety	Stopped Zero/ possibility of propulsive capability	 To avoid HSC wiring failure the development team shall ensure wiring is securely installed using manufacturer installation specifications To avoid HSC wiring failure the development team shall ensure wiring gauge is sufficient to carry max operational current with factor of safety To avoid HSC wiring failure the development team shall ensure wire bend radii are adhered to and wiring is protected from heat sources To avoid HSC unintended access or physical damage the development team shall ensure proper mounting, installation, and manufacturing of the HSC To avoid HSC unintended access or physical damage the development team shall ensure proper mounting, installation, and manufacturing of the HSC To avoid HSC unintended access or physical damage the development team shall ensure use of covering at wire-HSC interface To avoid HSC unintended access or physical damage the operator shall avoid adverse road conditions which may produce NVH To avoid HSC installation failure the development team shall ensure the

		installation fatigue or failure Operator aware during operation by identifying eventual failure of vehicle components and loss of functionality	Ensure HSC and mounting hardware are secure and free from potential lessening or unintended movement		mounting hardware are sufficient for max operational G-force with factor of safety To avoid HSC installation failure the development team shall ensure the mounting hardware is secure and free from potential lessening or unintended movement
		Diagnostic		System State After	
Item No.	Potential Safety Hazard	Method	Mitigation Method	Mitigation	Functional Requirement
11 EMC	 Unintended acceleration Unintended longitudinal motion Loss or degradation of propulsion system Operator and/or passenger injury Damage to or loss of property Damage to environment Potential for overheating Unintended exposure to high voltage 	Vehicle technical inspection will identify wiring fatigue or failure Operator aware during operation by identifying eventual failure of HV components Vehicle technical inspection will identify if EMC is free of manufacturing or installation fatigue or failure EMC monitors and sends temperature data in real time Operator aware	Ensure wiring is securely installed using manufacturer installation specifications Ensure wiring gauge is sufficient to carry max operational current with factor of safety Ensure wire bend radii are adhered to Ensure EMC and mounting hardware are sufficient for max operational G-force with factor of safety Ensure EMC and mounting hardware is secure and free from unintended movement Ensure operation within specified EMC temp range	Stopped Zero/ possibility of propulsive capability	To avoid EMC wiring failure the development team shall ensure wiring is securely installed using manufacturer installation specifications To avoid EMC wiring failure the development team shall ensure wiring gauge is sufficient to carry max operational current with factor of safety To avoid EMC wiring failure the development team shall ensure wire bend radii are adhered to and wiring is protected from heat sources To avoid EMC installation failure the development team shall ensure the mounting hardware are sufficient for max operational G-force with factor of safety To avoid EMC installation failure the development team shall ensure the mounting hardware is secure and free from potential lessening or unintended movement

		by identifying a thermal event, error message of overheating, or failure of HV components	Actuate thermal system when EMC reaches specified temperature Ensure thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the EM Ensure the fans are free from potential physical damage Ensure bolts, hoses and mounting hardware are securely fastened and free from potential loosening or movement		To avoid EMC operation outside of max/min temperature range the development team shall ensure the EMC has a thermal controls system and software forces operation within specified EMC temperature range To avoid EMC operation outside of max/min temperature range the development team shall actuate cooling fans when EMC reaches specified temperature To avoid EMC operation outside of max/min temperature range the development team shall ensure thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the EMC To avoid EMC operation outside of max/min temperature range the development team shall ensure the fans are free from potential physical damage To avoid EMC operation outside of max/min temperature range the development team shall ensure the fans are free from potential physical damage
					fastened and free from potential loosening or unintended movement
		Diagnostic		System State After	
Item No.	Potential Safety Hazard	Method	Mitigation Method	Mitigation	Functional Requirement
12 TCM	Unintended longitudinal motion Loss or degradation of propulsion system	Vehicle technical inspection will identify wiring fatigue or failure	Ensure wiring is securely installed using manufacturer installation specifications Ensure wiring gauge is	Stopped Zero/ possibility	To avoid TCM wiring failure the development team shall ensure wiring is securely installed using manufacturer installation specifications
	propulsion system		sufficient to carry max	of propulsive	

				1 .1.	
	Operator and/or passenger	Operator aware	operational current with	capability	To avoid TCM wiring failure the
	injury	during operation	factor of safety	from motor,	development team shall ensure wiring
		by identifying		possible for	gauge is sufficient to carry max
	Damage to or loss of	eventual failure of	Ensure wire bend radii are	engine to	operational current with factor of safety
	property	vehicle	adhered to	continue	
		components		operation as	To avoid TCM wiring failure the
	Damage to environment		Ensure TCM and mounting	normal	development team shall ensure wire bend
		Vehicle technical	hardware are sufficient for		radii are adhered to and wiring is protected
	Potential for overheating	inspection will	max operational G-force		from heat sources
		identify if TCM is	with factor of safety		
		free of			To avoid TCM installation failure the
		manufacturing or	Ensure TCM and mounting		development team shall ensure the
		installation fatigue	hardware are secure and free		mounting hardware are sufficient for max
		or failure	from unintended movement		operational G-force with factor of safety
		Operator aware			To avoid TCM installation failure the
		during operation			development team shall ensure the
		by identifying			mounting hardware is secure and free from
		eventual failure of			potential lessening or unintended
		vehicle			movement
		components and			
		loss of			
		functionality			
		, , , , , , , , , , , , , , , , , , ,		System	
		Diagnostic		State After	
Item No.	Potential Safety Hazard	Method	Mitigation Method	Mitigation	Functional Requirement
13 ECM	Unintended acceleration	Vehicle technical	Ensure wiring is securely	Stopped	To avoid ECM wiring failure the
		inspection will	installed using manufacturer		development team shall ensure wiring is
	Unintended longitudinal	identify wiring	installation specifications	Zero/	securely installed using manufacturer
	motion	fatigue or failure	1.	possibility	installation specifications
			Ensure wiring gauge is	of	1
	Loss or degradation of	Operator aware	sufficient to carry max	propulsive	To avoid ECM wiring failure the
	propulsion system	during operation	operational current with	capability	development team shall ensure wiring
	1 F	by identifying	factor of safety	Capability	gauge is sufficient to carry max
	Operator and/or passenger	eventual failure of			operational current with factor of safety
	injury	vehicle	Ensure wire bend radii are		1
	5 ° J	components	adhered to		To avoid ECM wiring failure the
	Damage to or loss of	· ···· I ······			development team shall ensure wire bend
	property	Vehicle technical	Ensure ECM and mounting		radii are adhered to and wiring is protected
	Property	inspection will	hardware are sufficient for		from heat sources
		mopection with	nardware are sufficient for		nom neat sources

Damage to environment	identify if ECM is	max operational G-force	
	free of	with factor of safety	To avoid ECM installation failure the
Potential for overheating	manufacturing or		development team shall ensure the
	installation fatigue	Ensure ECM and mounting	mounting hardware are sufficient for max
	or failure	hardware are secure and free	operational G-force with factor of safety
		from unintended movement	-
	Operator aware		To avoid ECM installation failure the
	during operation	Ensure ECM is mounted	development team shall ensure the
	by identifying	such that there is proper	mounting hardware is secure and free from
	eventual failure of	clearance and sufficient air	potential lessening or unintended
	vehicle	flow to cool the ECM	movement
	components and		
	loss of		To avoid ECM over-heating failure the
	functionality		development team shall ensure the ECM is
			mounted such that there is proper
			clearance and sufficient air flow to cool
			the ECM

Appendix 4 Safety Goals and Functional Requirements – Complete Documentation

Appendix 4.1	ACC Safety	Goals and Functional	Requirements
	•		1

	CAVs / CSMS ACC Safety Goals and Functional Requirements				
SG No.	Safety Goal	FSR No.	Functional Safety Requirement		
SGA01	The ACC system shall control longitudinal velocity via braking	FSRA01.01	The ACC system shall allow operator to override automated controls with minimal braking engagement		
		FSRA01.02	To avoid wiring failures the ACC system shall be wired and installed according to manufacturer specifications to include bend radii, heat shielding, EMI avoidance, sheathing, proper gauge, and interface connections		
		FSRA01.03	The ACC brake system shall engage in timely manner such that brake pad and rotor fatigue and passenger discomfort is minimized		
		FSRA01.04	The operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH		
		FSRA01.05	Operator shall avoid poor driving behaviors		
		FSRA01.06	To avoid brake rotor failures the development teams shall ensure proper mounting and installation of brake rotors		
		FSRA01.07	To avoid brake rotor failures the development teams shall ensure brake rotor bolts and mounting hardware are securely fastened and free from potential loosening or unintended movement		
		FSRA01.08	The operator shall ensure brake system is free of build-up (snow, mud) and debris prior to use		
		FSRA01.09	To avoid caliper failures the operator shall ensure routine inspection for caliper rust and corrosion		
		FSRA01.10	ACC brake system shall engage in timely manner such that brake lines are immediately able to be actuated		

		FSRA01.11	To avoid brake fluid line failure the development team shall ensure proper bleeding, mounting, installation, and routine maintenance and inspection of brake line hardware and its functionality
		FSRA01.12	To avoid brake fluid line failure the development team shall ensure lines, bolts and mounting hardware are securely fastened and free from potential loosening or unintended movement
		FSRA01.13	The ACC brake response system shall function according to operator engagement
		FSRA01.14	The ACC brake response system shall respond (feedback, longitudinal movement) more quickly in the event of less operator engagement (hands on wheel, head tilt, eye deviation)
		FSRA01.15	The ACC brake response system shall respond (feedback, lateral movement) less quickly in the event of more operator engagement (hands on wheel, head tilt, eye deviation)
		FSRA01.16	To avoid brake pad failures the development teams shall ensure proper mounting and installation of brake pads
		FSRA01.17	To avoid brake pad failures the development teams shall ensure brake pad bolts and mounting hardware are securely fastened and free from potential loosening or unintended movement
		FSRA01.18	To avoid brake pad failures the operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH
		FSRA01.19	To avoid brake pad failures the operator shall avoid poor driving behaviors
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGA02	The ACC system shall control longitudinal velocity via throttle	FSRA02.01	The ACC system shall allow operator to override automated controls with minimal AP engagement
	position or APP	FSRA02.02	The ACC system shall be wired and installed according to manufacturer specifications to include bend radii, heat shielding, EMI avoidance, sheathing, proper gauge, and interface connections
		FSRA02.03	The development team shall ensure proper mounting, installation, and manufacturing of the fuel filter, and pump
		FSRA02.04	The development team shall ensure the fuel filter permeable material is clean and the is free of physical damage and leaks while under pressure
		FSRA02.05	The operator shall ensure adequate fuel level and type
		FSRA02.06	The operator shall ensure use of fuel system cleaners when recommended
		FSRA02.07	The operator shall ensure fuel quality prior to filling
		FSRA02.08	The development teams shall ensure proper mounting, installation, and manufacturing of oil filter and pump

RA02.09 RA02.10	The operator shall ensure frequent oil changes, clean oil, and that the oil filter is not ballooned or deformed The operator shall ensure proper fuel octane number prior to filling tank
RA02.10	The operator shall ensure proper fuel octane number prior to filling tank
RA02.11	The operator shall ensure thermal system components (radiator, coolant level, fans,
	water pump, thermostat) are functional and sufficient to cool the engine
RA02.12	The development team shall ensure the fans are free from potential physical damage
RA02.13	The development team shall ensure fans pull air from a cool source
RA02.14	The development team shall ensure engine ventilation is sufficient to provide appropriate air movement through engine bay
RA02.15	The development team shall ensure thermal system is designed such that there is sufficient air flow to cool engine components
RA02.16	The development team shall ensure the ECM controls and mitigates engine overheating
RA02.17	The development team shall ensure proper mounting, installation, and manufacturing of intake manifold, thermal system, spark plugs, EGR system, fuel injectors, coolant system, EM, driveshaft, transmission, AP, APPS and their components
RA02.18	The development team shall ensure powertrain components to include bolts, interface components, seals, gaskets, injectors, fuel pump, EGR valve, coolant system, EM-driveshaft interface, transmission-EM interface and all associated mounting hardware are securely fastened and free from leaks and potential loosening or movement
RA02.19	The operator shall ensure thermal system is functional
RA02.20	The development team shall ensure proper A/F ratio and functioning O2 sensor
RA02.21	The development team shall ensure vacuum lines and manifold gasket are free from cracks and physical damage
RA02.22	The development team shall ensure properly functioning timing belt
RA02.23	The development team shall ensure properly functioning EGR valve
RA02.24	The development team shall ensure software (HSC) limits the magnitude of current to the EM
RA02.25	The development team shall ensure relays and fuses are in place and functional to prevent over drawing of current
RA02.26	The development team shall ensure proper mounting, installation, and manufacturing of the EM and housing
RA02.27	The development team shall ensure EM cooling system and its components are
	functioning, proper coolant levels, and hoses running to and from the motor are leak free
	RA02.14 RA02.15 RA02.16 RA02.16 RA02.17 RA02.17 RA02.18 RA02.19 RA02.20 RA02.21 RA02.22 RA02.23 RA02.24 RA02.26

		FSRA02.29	The development team shall ensure the fans are free from potential physical damage
		FSRA02.30	The development team shall ensure the HSC controls and mitigates EM overheating
		FSRA02.31	The operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH
		FSRA02.32	The development team shall ensure EM-driveshaft interface location is covered and free from potential unintended access or physical damage
		FSRA02.33	The development team shall ensure proper EM-driveshaft alignment
		FSRA02.34	The development team shall ensure EM-driveshaft interface angle is minimized
		FSRA02.35	The development team shall ensure EM-transmission interface location is covered and free from potential unintended access or physical damage
		FSRA02.36	The development team shall ensure proper EM-transmission alignment
		FSRA02.37	The development team shall ensure software limits APPS current range
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGA03	ACC sensors shall observe surrounding traffic/objects distance, velocity, size and position to include operator engagement	FSRA03.01	The ACC sensors shall be wired and installed according to manufacturer specifications to include bend radii, heat shielding, EMI avoidance, sheathing, proper gauge, and interface connections
		FSRA03.02	The ACC system shall alert operator prior to and when shutdown occurs
		FSRA03.03	The ACC system shall only be operational if sensor performance meets a minimum standard (communication speed, sensor availability or visibility)
		FSRA03.04	The ACC communications shall operate independently and be free from external manipulation
		FSRA03.05	The development team shall ensure sensor enclosure manufacturing and use of materials is sufficient to prevent unintended access and physical damage
		FSRA03.06	The development team shall ensure sensor and sensor enclosure bolts and mounting hardware is securely fastened and free from potential loosening or unintended movement
		FSRA03.07	The operator shall ensure ACC system sensors have clear field of view and are free of visibility obstructions
		FSRA03.08	The ACC system shall require minimum vehicle speed based on sensor requirements
		FSRA03.09	The ACC system shall function according to operator engagement
		FSRA03.10	The ACC system shall respond (feedback, acceleration, deceleration) more quickly in the event of less operator engagement (hands on wheel, head tilt, eye deviation)
		FSRA03.11	The ACC system shall respond (feedback, acceleration, deceleration) less quickly in the event of more operator engagement (hands on wheel, head tilt, eye deviation)

SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGA04	ACC system shall transmit sensor data to associated controller	FSRA04.01	The ACC sensors shall be wired and installed according to manufacturer specifications to include bend radii, heat shielding, EMI avoidance, sheathing, proper gauge, and interface connections
		FSRA04.02	The ACC system shall alert operator prior to and when shutdown occurs
		FSRA04.03	The ACC system shall only be operational if sensor performance meets a minimum standard (communication speed, sensor availability or visibility)
		FSRA04.04	The ACC communications shall operate independently and be free from external manipulation (malicious intrusion, EMI)
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGA05	Operator shall determine and set the	FSRA05.01	The ACC system shall operate within a specified velocity range
	ACC system velocity constraint	FSRA05.02	The ACC system shall provide warning to operator that velocity input constraint is required
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGA06	Operator shall determine and set the ACC system distance constraint	FSRA06.01	The ACC system shall operate within a specified distance range
		FSRA06.02	The ACC system shall provide warning to operator that distance input constraint is required
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGA07	ACC shall provide feedback to the operator (ACC status, haptic, visual, audio)	FSRA07.01	The ACC sensors shall be wired and installed according to manufacturer specifications to include bend radii, heat shielding, EMI avoidance, sheathing, proper gauge, and interface connections
		FSRA07.02	The ACC system shall alert operator prior to and when shutdown occurs
		FSRA07.03	The ACC system shall alert operator when deviation from set distance or velocity occurs
		FSRA07.04	The ACC feedback system shall function according to operator engagement
		FSRA07.05	The ACC system shall provide audio, visual, and haptic feedback
		FSRA07.06	The ACC system shall provide feedback in manner that does not startle the operator and cause greater potential for hazard (not overly loud or bright)
		FSRA07.07	The ACC system audio feedback shall adjust to ambient volume (stereo system, excessive cabin noise)

FSRA07.08	The ACC system visual feedback shall adjust to ambient light (decrease during night, increase during day)
FSRA07.09	The ACC system shall only be operational if feedback performance meets a minimum
	standard (communication speed, audio, visual, haptic functionality)
FSRA07.10	The ACC communications shall operate independently and be free from external
	manipulation (malicious intrusion, EMI)

Appendix 4.2CAVs Safety Goals and Functional Requirements

	CAVs Safety Goals and Functional Requirements			
SG No.	Safety Goal	FSR No.	Functional Safety Requirement	
SGC01.1 SGC01.2 SGC01.3	The Intel Tank Computer shall be responsible for blending various sensors (cameras,	FSRC01.01	To avoid wiring failure of the intel tank computer the development team shall ensure wiring is securely installed using manufacturer installation specifications	
SGC01.4 SGC01.5	SGC01.4radars) data to achieve reliable, high-definition imagesSGC01.5high-definition imagesThe Intel Tank Computer shall be responsible for performing sensor fusion data verification & validation using developed algorithms and NNsThe Intel Tank Computer shall be responsible for determining if control action (EPS torque, braking,	FSRC01.02	To avoid wiring failure of the intel tank computer the development team shall ensure wiring gauge is sufficient to carry max operational current with factor of safety	
		FSRC01.03	To avoid wiring failure of the intel tank computer the development team shall ensure wire bend radii are adhered to	
		FSRC01.04	The development team shall ensure computer alerts operator when corrective action decision is disabled	
		FSRC01.05	The development team shall ensure the system determines fidelity of non-blended image and decides if corrective action should be applied	
		FSRC01.06	The development team shall ensure the computer only makes corrective action decisions when fidelity of image meets minimum specified resolution	
		FSRC01.07	The development team shall ensure if computer system fails, it does not prevent vehicle from manual driving operations	
	feedback) is required	FSRC01.08	The development team shall ensure manufacturing and installation is sufficient to prevent unintended access and physical damage to the computer	

The Intel Tank Computer shall be responsible for sending control action	FSRC01.09	To prevent unintended access and physical damage to the development team shall ensure use of coverings at wire-computer interface
request to associated controller	FSRC01.10	To prevent physical damage to the computer the operator shall avoid adverse road condition which may produce NVH
The Intel Tenk Computer shell	FSRC01.11	To prevent unintended access and physical damage the development team shall ensure computer installation is inside cabin in a dry debris-proof location
The Intel Tank Computer shall be responsible for provides	FSRC01.12	To prevent unintended access and physical damage the development team shall ensure computer is inaccessible by passengers
real-time functionalities	FSRC01.13	To prevent power failure the development team shall ensure the power supplied to the computer is within manufacturer operational range
	FSRC01.14	To prevent CAVs failure the development team shall ensure the computer NN model is thoroughly defined and highly sensitive to small variations in inputs
	FSRC01.15	To prevent CAVs failure the development team shall ensure the computer NN is thoroughly tested and validate prior to implementation
	FSRC01.16	To prevent CAVs failure the development team shall ensure the computer NN imposes limits on output to not exceed boundaries
	FSRC01.17	To prevent CAVs failure the development team shall ensure the computer NNs use of hidden layers and neurons does not over-fit training data and is sufficient to fit new and unseen data
	FSRC01.18	To prevent CAVs failure the development team shall ensure the computer program code is thoroughly vetted (Auto industry standard is one defect per 1000 executable lines of code)
	FSRC01.19	To prevent CAVs failure the development team shall ensure the computer program is developed using automotive coding standards
	FSRC01.20	To prevent CAVs failure the development team shall ensure the use of multiple software scanning tools to identify vulnerability and error in computer program code (industry uses Jarvis which analyses the binary executable action and not the mistakes in the code)
	FSRC01.21	To prevent CAVs failure the development team shall ensure the control of computational overflow and compounding rounding errors
	FSRC01.22	To prevent CAVs failure the development team shall ensure the understanding of computer input and output signal quality, noise, latency, and bandwidth accounting for measurement and control action error
	FSRC01.23	To prevent CAVs failure the development team shall reduce computer signal input and output latency, ensure use of high-quality transmission medium
	FSRC01.24	To prevent computer signal input and output bandwidth fault the development team shall ensure transmission medium gauge is sufficient to handle expected throughput (load) with factor of safety

FSRC01.25	To prevent CAVs failure the development team shall ensure an understanding of time required to analyze and route computer signal data
FSRC01.26	To reduce computer signal input and output noise the development team shall ensure
	wires are as short as possible
FSRC01.27	To reduce computer signal input and output noise the development team shall ensure wires are kept away from electrical machinery
FSRC01.28	To reduce computer signal input and output noise it is recommended to use twisted together wires
FSRC01.29	To reduce internal computer signal input and output noise the development team shall ensure thermal effects on amplifiers are minimized
FSRC01.30	To reduce computer signal input and output noise, if possible, the development team
	shall ensure the amplifier bandwidth matches input signal bandwidth
FSRC01.31	To reduce computer signal input and output noise the development team shall ensure use of proper filtering techniques
FSRC01.32	To reduce computer signal input and output noise the development team shall ensure use of wire shielding and conduit
ECDC01 22	To reduce computer signal input and output noise the development team shall ensure
FSRC01.33	understanding of ground loops and impose proper grounding practices
FSRC01.34	To ensure true data measurement the development team shall test the collection with the computer operating at the same temperature that it will be operating at in real- world scenarios
FSRC01.35	To prevent CAVs failure the development team shall ensure the understanding of potential computer signal input and output storage delays
FSRC01.36	To prevent computer memory failure the development team shall ensure the computer is capable of storing and processing the expected amount of data with a factor of safety
FSRC01.37	To prevent computer memory failure ensure the program is developed
	such that information that is too large cannot be written into a memory buffer that is too small to contain it
FSRC01.38	To prevent over-heating the development team shall ensure the computer is mounted such that there is proper clearance and sufficient air flow to cool the computer
FSRC01.39	To prevent over-heating the development team shall ensure the computer fans pull air from cool and dry source
FSRC01.40	To prevent over-heating the development team shall ensure the computer imposes thermal self-regulation
FSRC01.41	To prevent over-heating the development team shall ensure the
	computer operates within specified temperature range

FSRC01.42	To prevent operating system crash the development team shall ensure the system does not over heat
FSRC01.43	To prevent operating system crash the development team shall ensure the computer is mounted such that there is proper clearance and sufficient air flow to cool the
	computer
FSRC01.44	To prevent operating system crash the development team shall ensure the computer
	fans pull air from cool and dry source
FSRC01.45	To prevent operating system crash the development team shall ensure the computer imposes thermal self-regulation
FSRC01.46	To prevent operating system crash the development team shall ensure the computer
FSKC01.40	operates within specified temperature range
FSRC01.47	To prevent operating system crash the development team shall ensure the program is
	developed such that it does not attempt to access an incorrect memory address leading
	to general protection fault
FSRC01.48	To prevent operating system crash the development team shall ensure the program is developed such that the OS does not enter an infinite loop
FSRC01.49	To prevent operating system crash the development team shall ensure the program is
	developed such that information that is too large cannot be written into a memory
	buffer that is too small to contain it
FSRC01.50	To prevent operating system crash the development team shall ensure the program is developed such that deadlock is prevented (multiple programs having control some
ECD C01 51	resource another program needs)
FSRC01.51	To prevent operating system crash the development team shall ensure
	the program performs shutdown operations
FSRC01.52	To prevent control action decision failure the development team shall ensure the
EGD C01 52	computer operates according to a specified minimum for sensor data quality To prevent control action decision failure the development team shall ensure the
FSRC01.53	computer disables the associated corrective action decisions when minimum standard
	for lane-line, object, and traffic sign recognition is not met
FSRC01.54	To prevent control action decision failure the development team shall ensure the
1 511001.01	computer operates according to a specified minimum for lane-line recognition (lane
	dots, poorly painted lines, no lines)
FSRC01.55	To prevent control action decision failure the development team shall ensure the
-	computer operates according to a specified minimum for traffic sign recognition
FSRC01.56	To prevent control action decision failure the development team shall ensure the
	computer operates according to a specified minimum for low-light operations
FSRC01.57	To prevent control action decision failure the development team shall
	ensure the computer has control of headlights

		FSRC01.58	The development team shall ensure the computer allows the operator to increase or decrease feedback timing
		FSRC01.59	The development team shall ensure the computer allows the operator to increase or decrease feedback volume
		FSRC01.60	The development team shall ensure the computer allows the operator to increase or decrease feedback visual stimulation
		FSRC01.61	The development team shall ensure the computer allows the operator to increase or decrease haptic feedback stimulation
		FSRC01.62	To prevent CAVs failure the development team shall ensure the use of software safety and that the system is free from external unintended malicious control
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGC02.1 SGC02.2	The Intel Mobileye 6 camera shall perform multi-feature	FSRC02.01	The development team shall ensure the Intel Mobileye 6 camera wiring is securely installed using manufacturer installation specifications
SGC02.3	tracking	FSRC02.02	The development team shall ensure the Intel Mobileye 6 camera wiring gauge is sufficient to carry max operational current with factor of safety
SGC02.4 SGC02.5	The Intel Mobileye 6 camera	FSRC02.03	The development team shall ensure the Intel Mobileye 6 camera wire bend radii are adhered to
SGC02.6 SGC02.7	1 5	FSRC02.04	The development team shall ensure the Intel Mobileye 6 camera alerts the computer when failure has occurred
SGC02.8	The Intel Mobileye 6 camera	FSRC02.05	The development team shall ensure the Intel Mobileye 6 camera manufacturing and installation is sufficient to prevent unintended access and physical damage
	shall perform forward collision	FSRC02.06	The development team shall ensure the Intel Mobileye 6 camera is placed inside cabin and top-center of wind shield within operational area of windshield wipers
	warning	FSRC02.07	The development team shall ensure the use of covering at wire- Intel Mobileye 6 camera interface to prevent unintended access
	The Intel Mobileye 6 camera shall perform pedestrian	FSRC02.08	The development team shall ensure the Intel Mobileye 6 camera installation is inside cabin in a dry debris-proof location
	collision warning	FSRC02.09	The operator shall avoid adverse road conditions which may produce NVH and damage or loosen the Intel Mobileye 6 camera
	The Intel Mobileye 6 camera shall perform headway warning	FSRC02.10	The development team shall ensure the power supplied to the Intel Mobileye 6 camera is within manufacturer recommended operational range
		FSRC02.11	The development team shall ensure an understanding of Intel Mobileye 6 camera signal quality, noise, latency, and bandwidth accounting for measurement and control
	The Intel Mobileye 6 camera shall perform traffic sign recognition	FSRC02.12	action error To reduce Intel Mobileye 6 camera signal latency the development team shall ensure the use of a high-quality transmission medium

SG No.	Safety Goal	FSR No.	Functional Safety Requirement
		F3KC02.29	computer and operator when the system is unavailable
		FSRC02.29	maintain operations during low-light, poorly painted lane lines, and adverse weather conditions The development team shall ensure the Intel Mobileye 6 camera indicates to
		FSRC02.28	6 camera has control of wind shield wipers (debris may impede camera view while operator is unaware)The development team shall ensure the Intel Mobileye 6 camera is of high-quality to
		FSRC02.27	6 camera is mounted in the operational area of the wind shield wipersTo prevent field of view failure the development team shall ensure the Intel Mobileye
		FSRC02.26	software updates are performed over land-line and not through the air To prevent field of view failure the development team shall ensure the Intel Mobileye
		FSRC02.25	The development team shall ensure Intel Mobileye 6 camera system
		FSRC02.24	The development team shall ensure the use of software safety and that the Intel Mobileye 6 camera signal is free from external unintended malicious control
			camera signal storage delays
		FSRC02.23	the understanding of ground loops and impose proper grounding practices The development team shall ensure understanding of potential Intel Mobileye 6
		FSRC02.22	To reduce Intel Mobileye 6 camera signal noise the development team shall ensure
		FSRC02.21	To reduce Intel Mobileye 6 camera signal noise the development team shall ensure the use of wire shielding and conduit
			the use of proper filtering techniques
		FSRC02.20	shall ensure the amplifier bandwidth matches input signal bandwidthTo reduce Intel Mobileye 6 camera signal noise the development team shall ensure
		FSRC02.19	To reduce Intel Mobileye 6 camera signal noise, if possible, the development team
		FSRC02.18	To reduce internal Intel Mobileye 6 camera signal noise the development team shall ensure the thermal effects on amplifiers are minimized
	shan provide rear time display	FSRC02.17	To reduce Intel Mobileye 6 camera signal noise it is recommended to use twisted together wires
	The Intel Mobileye 6 camera shall provide real-time display	FSRC02.16	To reduce Intel Mobileye 6 camera signal noise the development team shall ensure the wires are kept away from electrical machinery
	controller	FSRC02.15	To reduce Intel Mobileye 6 camera signal noise the development team shall ensure the wires are as short as possible
	The Intel Mobileye 6 camera shall transmit data to associated	FSRC02.14	The development team shall ensure an understanding of time required to analyze and route Intel Mobileye 6 camera signal data
		FSRC02.13	shall ensure the transmission medium gauge is sufficient to handle expected throughput (load) with factor of safety

SGC03.1	The Bosch Front, Rear, and Corner MRR Radars shall perform early front room and compared detection	FSRC03.01	The development team shall ensure the radar wiring is securely
SGC03.2			installed using manufacturer installation specifications
	front, rear, and corner speed detection	FSRC03.02	The development team shall ensure the radar wiring gauge is sufficient
	The Deceb Front Dece and		to carry max operational current with factor of safety
	The Bosch Front, Rear, and Corner MRR Radars shall send	FSRC03.03	The development team shall ensure the radar wire bend radii are adhered to
	data to associated controller	FSRC03.04	The development team shall ensure the radar alters computer that
			system failure has occurred
		FSRC03.05	The development team shall ensure the radar manufacturing and
			installation is sufficient to prevent unintended access and physical
			damage
		FSRC03.06	The development team shall ensure the use of covering at wire- radar
			interface to prevent unintended access
		FSRC03.07	The operator shall avoid adverse road condition which may produce
			NVH and damage or loosen the radar
		FSRC03.08	The development team shall ensure the power supplied to the radar is within manufacturer operational range
		FSRC03.09	The development team shall ensure the understanding of radar signal quality, noise, latency, and bandwidth accounting for measurement and control action error
		FSRC03.10	To reduce radar signal latency, the development team shall ensure the use of high- quality transmission medium
		FSRC03.11	To prevent radar signal bandwidth faults, the development team shall ensure the transmission medium gauge is sufficient to handle expected throughput (load) with factor of safety
		FSRC03.12	The development team shall ensure the understanding of time required to analyze and route camera signal data
		FSRC03.13	To reduce radar signal noise the development team shall ensure the wires are as short as possible
		FSRC03.14	To reduce radar signal noise the development team shall ensure the wires are kept away from electrical machinery
		FSRC03.15	To reduce radar signal noise it is the development team shall ensure the to use twisted together wires
		FSRC03.16	To reduce internal radar signal noise the development team shall ensure the thermal effects on amplifiers are minimized
		FSRC03.17	To reduce radar signal noise, if possible, the development team shall ensure the amplifier bandwidth matches input signal bandwidth

			· · · · · · · · · · · · · · · · · · ·
		FSRC03.18	To reduce radar signal noise the development team shall ensure the use of proper filtering techniques
		FSRC03.19	To reduce radar signal noise the development team shall ensure the use of wire
		156005.19	shielding and conduit
		FSRC03.20	To reduce radar signal noise the development team shall ensure the understanding of
		15KC05.20	ground loops and impose proper grounding practices
		FSRC03.21	The development team shall ensure the understanding of potential radar signal storage
		151(05.21	delays
		FSRC03.22	The development team shall ensure the use of software safety and that the radar signal
		151(000)22	is free from external unintended malicious control
		FSRC03.23	The development team shall ensure the system software updates are
			performed over land-line and not through the air
		FSRC03.24	To prevent field of view failure The development team shall ensure the radar is
		1,5110,0012.1	mounted such that the signal projects unimpeded
		FSRC03.25	The development team shall ensure the radar is of high-quality to maintain operations
			during low-light, poorly painted lane lines, and adverse weather conditions2
		FSRC03.26	The development team shall ensure the radar indicates to 20mputer and operator
			when the system is unavailable
		FSRC03.27	The development team shall ensure the integrated program accounts for radar
			horizontal field of view and elevation ($\pm 6^{\circ}$ (160m), $\pm 6^{\circ}$ (100m), $\pm 10^{\circ}$ (60m),
			$\pm 25^{\circ}(36\text{m}), \pm 42^{\circ}(12\text{m}))$
		FSRC03.28	The development team shall ensure the integrated program accounts for radars speed, distance and angle measurement accuracy $(0.11 \text{ m/s} - 0.12 \text{ m} + 0.2^{\circ})$
			distance, and angle measurement accuracy $(0.11 \text{ m/s}, 0.12 \text{ m}, \pm 0.3^{\circ})$ The development team shall ensure the integrated program accounts for radars speed,
		FSRC03.29	distance, and angle object separation capability (0.72 m/s, 0.66 0m, \pm 7°)
		FSRC03.30	The development team shall ensure the integrated program accounts for radars cycle
		FSKC05.50	time (60 ms)
		FSRC03.31	The development team shall ensure the integrated program accounts for radars
			frequency modulation
		FSRC03.32	The development team shall ensure the integrated program accounts for radars
			maximum number of detectable objects (32)
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
50 110.	Salety Guai	1'SK 1\U.	
SGC04.1	The Intel Movidius Neural	FSRC04.01	The development team shall ensure the compute stick is securely input to the
SGC04.2	Compute Stick shall perform		computer
SGC04.3	vision processing tasks in	FSRC04.02	The development team shall ensure the compute stick NN model thoroughly defined
SGC04.4	assistance to Intel Tank		and highly sensitive to small variations in inputs
50004.4		FSRC04.03	The development team shall ensure the compute stick NN is thoroughly tested and
	computational capabilities		validate prior to implementation

		FSRC04.04	The development team shall ensure the compute stick NN imposes limits on output to not exceed boundaries
	The Intel Movidius Neural	FSRC04.05	The development team shall ensure the compute stick NNs use of hidden layers and neurons does not over-fit training data and is sufficient to fit new and unseen data
	Compute Stick shall assist in blending various sensors	FSRC04.06	The development team shall ensure the compute stick program code is thoroughly vetted (Auto industry standard is one defect per 1000 executable lines of code)
	(cameras, radars) data to achieve reliable, high-definition	FSRC04.07	The development team shall ensure the compute stick program is developed using automotive coding standards
	images	FSRC04.08	The development team shall ensure the use of multiple software scanning tools to identify vulnerability and error in compute stick program code (industry uses Jarvis which analyses the binary executable action and not the mistakes in the code)
	The Intel Movidius Neural	FSRC04.09	The development team shall ensure the control of computational overflow and compounding rounding errors
	Compute Stick shall assist in performing sensor fusion data verification & validation	FSRC04.10	The development team shall ensure the understanding of compute stick input and output signal quality, noise, latency, and bandwidth accounting for measurement and control action error
		FSRC04.11	The development team shall ensure the understanding of time required to analyze and route computer signal data
	The Intel Movidius Neural Compute Stick shall assist in	FSRC04.12	To reduce compute stick signal input and output noise the development team shall ensure the use of proper filtering techniques
	determining if control action (EPS torque, braking, feedback)	FSRC04.13	The development team shall ensure the understanding of potential compute stick signal input and output storage delays
	is required	FSRC04.14	The development team shall ensure the use of software safety and that the system is free from external unintended malicious control
		FSRC04.15	The development team shall ensure the compute stick is capable of storing and processing the expected amount of data with a factor of safety
		FSRC04.16	To prevent memory failure the development team shall ensure the program is developed such that information that is too large cannot be written into a memory buffer that is too small to contain it
		FSRC04.17	The development team shall ensure the compute stick and computer interface is compatible
		FSRC04.18	The development team shall ensure the computer free storage space is available to allow compute stick to operate
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGC05.1	The KVaser shall interface and transfer CAN signals to USB	FSRC05.01	The development team shall ensure KVaser manufacturing and installation is sufficient to prevent unintended access and physical damage to the computer

		FSRC05.02	To prevent unintended access and physical damage the development team shall ensure use of coverings at KVaser interfaces
		FSRC05.03	To prevent physical damage to the KVaser the operator shall avoid adverse road condition which may produce NVH
		FSRC05.04	To prevent unintended access and physical damage the development team shall ensure KVaser installation is inside cabin in a dry debris-proof location
		FSRC05.05	To prevent unintended access and physical damage the development team shall ensure KVaser is inaccessible by passengers
		FSRC05.06	The development team shall ensure KVaser functionality prior to open- road operation
		FSRC05.07	The development team shall ensure the KVaser is capable of processing the expected amount pf data with a factor of safety
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGC06.1 SGC06.2	The Niles camera shall perform real-time monitoring of	FSRC06.01	The development team shall ensure the Niles camera wiring is securely installed using manufacturer installation specifications
56600.2	operator	FSRC06.02	The development team shall ensure the Niles camera wiring gauge is sufficient to carry max operational current with factor of safety
	The Niles operator monitoring	FSRC06.03	The development team shall ensure the Niles camera wire bend radii are adhered to
	camera shall send data to associated controller	FSRC06.04	The development team shall ensure the Niles camera manufacturing and installation is sufficient to prevent unintended access and physical damage
		FSRC06.05	The development team shall ensure the Niles camera is placed inside the cabin within unobstructed operational view of the operator
		FSRC06.06	The development team shall ensure the use of covering at wire- Niles camera interface to prevent unintended access
		FSRC06.07	The development team shall ensure the Niles camera installation is inside cabin in a dry debris-proof location
		FSRC06.08	The operator shall avoid adverse road conditions which may produce NVH and damage the camera
		FSRC06.09	The development team shall ensure the power supplied to the Niles camera is within manufacturer recommended operational range
		FSRC06.10	The development team shall ensure an understanding of Niles camera signal quality, noise, latency, and bandwidth accounting for measurement and control action error
		FSRC06.11	To reduce Niles camera signal latency the development team shall ensure the use of a high-quality transmission medium

		FSRC06.12	To prevent Niles camera signal bandwidth faults the development team shall ensure the transmission medium gauge is sufficient to handle expected throughput (load)
			with factor of safety
		FSRC06.13	The development team shall ensure an understanding of time required to analyze and
			route Niles camera signal data
		FSRC06.14	To reduce Niles camera signal noise the development team shall ensure the wires are
			as short as possible
		FSRC06.15	To reduce Niles camera signal noise the development team shall ensure the wires are
			kept away from electrical machinery To reduce Niles camera signal noise it is recommended to use twisted together wires
		FSRC06.16	
		FSRC06.17	To reduce internal Niles camera signal noise the development team shall ensure the
			thermal effects on amplifiers are minimized
		FSRC06.18	To reduce Niles camera signal noise, if possible, the development team shall ensure
			the amplifier bandwidth matches input signal bandwidth
		FSRC06.19	To reduce Niles camera signal noise the development team shall ensure the use of proper filtering techniques
		FSRC06.20	To reduce Niles camera signal noise the development team shall ensure the use of
		1'SKC00.20	wire shielding and conduit
		FSRC06.21	To reduce Niles camera signal noise the development team shall ensure the
		151(000.21	understanding of ground loops and impose proper grounding practices
		FSRC06.22	The development team shall ensure understanding of potential Niles camera signal
			storage delays
		FSRC06.23	The development team shall ensure the use of software safety and that the Niles
			camera signal is free from external unintended malicious control
		FSRC06.24	The development team shall ensure system software updates are
			performed over land-line and not through the air
		FSRC06.25	To prevent field of view failure the development team shall ensure the camera is
		FOR COL 21	mounted in a location free of obstruction
		FSRC06.26	The development team shall ensure the camera is of high-quality to maintain operations during low-light
		FSRC06.27	The development team shall ensure the Niles camera indicates to computer and
			operator when the system is unavailable
SC No	Sofety Cool	ECD No	Eurotional Safety Dequirement
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGC07.1	The real-time display shall	FSRC07.01	The development team shall ensure the display wiring is securely installed using
SGC07.2	acquire sensor fusion data from		manufacturer installation specifications
SUC07.2			
SUC07.2	associated controller	FSRC07.02	The development team shall ensure the display wiring gauge is sufficient to carry max operational current with factor of safety

	FSRC07.03	The development team shall ensure the display wire bend radii are
		adhered to
The real-time display shall display sensors fusion images	FSRC07.04	The development team shall ensure the camera manufacturing and installation is sufficient to prevent unintended access and physical damage
in real-time	FSRC07.05	The development team shall ensure the display is placed inside cabin within view of the operator
	FSRC07.06	The development team shall ensure the use of covering at wire- display interface to prevent unintended access
	FSRC07.07	The development team shall ensure the display installation is inside cabin in a dry debris-proof location
	FSRC07.08	The operator shall avoid adverse road conditions which may produce NVH and damage or loosen the display
	FSRC07.09	The development team shall ensure the power supplied to the display is within manufacturer recommended operational range
	FSRC07.10	The development team shall ensure an understanding of display signal quality, noise, latency, and bandwidth accounting for measurement and control action error
	FSRC07.11	To reduce display signal latency the development team shall ensure the use of a high- quality transmission medium
	FSRC07.12	To prevent display signal bandwidth faults the development team shall ensure the transmission medium gauge is sufficient to handle expected throughput (load) with factor of safety
	FSRC07.13	The development team shall ensure an understanding of time required to analyze and route display signal data
	FSRC07.14	To reduce display signal noise the development team shall ensure the wires are as short as possible
	FSRC07.15	To reduce display signal noise the development team shall ensure the wires are kept away from electrical machinery
	FSRC07.16	To reduce display signal noise it is recommended to use twisted together wires
	FSRC07.17	To reduce internal display signal noise the development team shall ensure the thermal effects on amplifiers are minimized
	FSRC07.18	To reduce display signal noise, if possible, the development team shall ensure the amplifier bandwidth matches input signal bandwidth
	FSRC07.19	To reduce display signal noise the development team shall ensure the use of proper filtering techniques
	FSRC07.20	To reduce display signal noise the development team shall ensure the use of wire shielding and conduit
	FSRC07.21	To reduce display signal noise the development team shall ensure the understanding of ground loops and impose proper grounding practices

		FSRC07.22	The development team shall ensure the use of software safety and that the display signal is free from external unintended malicious control
		FSRC07.23	The development team shall ensure display system software updates are performed over land-line and not through the air
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGC08.1 SGC08.2	The Zed camera shall perform high-resolution depth	FSRC08.01	The development team shall ensure the ZED camera wiring is securely installed using manufacturer installation specifications
SGC08.2 SGC08.3	perception	FSRC08.02	The development team shall ensure the ZED camera wiring gauge is sufficient to carry max operational current with factor of safety
	The Zed camera shall perform	FSRC08.03	The development team shall ensure the ZED camera wire bend radii are adhered to
	6-axis positional tracking to sense space and motion	FSRC08.04	The development team shall ensure the power supplied to the ZED camera is within manufacturer recommended operational range
	The Zed camera shall perform large-scale 3D mapping	FSRC08.05	The development team shall ensure an understanding of ZED camera signal quality, noise, latency, and bandwidth accounting for measurement and control action error
		FSRC08.06	To reduce ZED camera signal latency the development team shall ensure the use of a high-quality transmission medium
		FSRC08.07	To prevent ZED camera signal bandwidth faults the development team shall ensure the transmission medium gauge is sufficient to handle expected throughput (load) with factor of safety
		FSRC08.08	The development team shall ensure an understanding of time required to analyze and route ZED camera signal data
		FSRC08.09	To reduce ZED camera signal noise the development team shall ensure the wires are as short as possible
		FSRC08.10	To reduce ZED camera signal noise the development team shall ensure the wires are kept away from electrical machinery
		FSRC08.11	To reduce ZED camera signal noise it is recommended to use twisted together wires
		FSRC08.12	To reduce internal ZED camera signal noise the development team shall ensure the thermal effects on amplifiers are minimized
		FSRC08.13	To reduce ZED camera signal noise, if possible, the development team shall ensure the amplifier bandwidth matches input signal bandwidth
		FSRC08.14	To reduce ZED camera signal noise the development team shall ensure the use of proper filtering techniques
		FSRC08.15	To reduce ZED camera signal noise the development team shall ensure the use of wire shielding and conduit

		FSRC08.16	To reduce ZED camera signal noise the development team shall ensure the
		ECD C00 17	understanding of ground loops and impose proper grounding practices
		FSRC08.17	The development team shall ensure understanding of potential ZED camera signal
		ECD C00 10	storage delays
		FSRC08.18	The development team shall ensure the use of software safety and that the ZED camera signal is free from external unintended malicious control
		FSRC08.19	The development team shall ensure system software updates are
			performed over land-line and not through the air
		FSRC08.20	To prevent field of view failure the development team shall ensure the ZED camera is mounted in the operational area of the wind shield wipers
		FSRC08.21	To prevent field of view failure the development team shall ensure the ZED camera
			has control of wind shield wipers (debris may impede camera view while operator is unaware)
		FSRC08.22	The development team shall ensure the ZED camera is of high-quality to maintain operations during low-light, poorly painted lane lines, and adverse weather conditions
		FSRC08.23	The development team shall ensure the camera indicates to computer and operator when the system is unavailable
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGC09.1 SGC09.2	The GPS shall receive global positioning data	FSRC09.01	The development team shall ensure the GPS wiring is securely installed using manufacturer installation specifications
50009.2		FSRC09.02	The development team shall ensure the GPS wiring gauge is sufficient to carry max operational current with factor of safety
	The GPS shall provide data to associated controller	FSRC09.03	The development team shall ensure the GPS wire bend radii are adhered to
		FSRC09.04	The development team shall ensure the GPS manufacturing and installation is sufficient to prevent unintended access, loosening, and physical damage
		FSRC09.05	The development team shall ensure the use of covering at wire-GPS interface to prevent unintended access
		FSRC09.06	The operator shall avoid adverse road conditions which may produce NVH and damage or loosen the GPS
		FSRC09.07	The development team shall ensure the power supplied to the GPS is
			within manufacturer recommended operational range
		FSRC09.08	The development team shall ensure an understanding of GPS signal quality, noise, latency, and bandwidth accounting for measurement and control action error
		FSRC09.08 FSRC09.09	

FSRC09.10	To prevent GPS signal bandwidth faults the development team shall ensure the transmission medium gauge is sufficient to handle expected throughput (load) with
	factor of safety
FSRC09.11	The development team shall ensure an understanding of time required to analyze and route GPS signal data
FSRC09.12	To reduce GPS signal noise the development team shall ensure the wires are as short as possible
FSRC09.13	To reduce GPS signal noise the development team shall ensure the wires are kept away from electrical machinery
FSRC09.14	To reduce GPS signal noise it is recommended to use twisted together wires
FSRC09.15	To reduce internal GPS signal noise the development team shall ensure the thermal effects on amplifiers are minimized
FSRC09.16	To reduce GPS signal noise, if possible, the development team shall ensure the amplifier bandwidth matches input signal bandwidth
FSRC09.17	To reduce GPS signal noise the development team shall ensure the use of proper filtering techniques
FSRC09.18	To reduce GPS signal noise the development team shall ensure the use of wire shielding and conduit
FSRC09.19	To reduce GPS signal noise the development team shall ensure the understanding of ground loops and impose proper grounding practices
FSRC09.20	The development team shall ensure understanding of potential GPS signal storage delays
FSRC09.21	The development team shall ensure the use of software safety and that the GPS signal is free from external unintended malicious control
FSRC09.22	The development team shall ensure the GPS is of high-quality to maintain operations during low-light, poorly painted lane lines, and adverse weather conditions
FSRC09.23	The development team shall ensure the GPS indicates to computer and operator when the system is unavailable

	CSMS Safety Goals and Functional Requirements			
SG No.	Safety Goal	FSR No.	Functional Safety Requirement	
SGS01.1 SGS01.2	The HSC shall control all hybrid functions	FSRS01.01	To avoid HSC wiring failure the development team shall ensure wiring is securely installed using manufacturer installation specifications	
SGS01.3 SGS01.4	The HSC shall control	FSRS01.02	To avoid HSC wiring failure the development team shall ensure wiring gauge is sufficient to carry max operational current with factor of safety	
SGS01.5	engine/EM torque split	FSRS01.03	To avoid HSC wiring failure the development team shall ensure wire bend radii are adhered to and wiring is protected from heat sources	
	The HSC shall maintain SOC at appropriate level	FSRS01.04	To avoid HSC unintended access or physical damage the development team shall ensure proper mounting, installation, and manufacturing of the HSC	
	The HSC shall control gear shifting The HSC shall modify stock signals	FSRS01.05	To avoid HSC unintended access or physical damage the development team shall ensure use of covering at wire-HSC interface	
		FSRS01.06	To avoid HSC unintended access or physical damage the operator shall avoid adverse road conditions which may produce NVH	
		FSRS01.07	To avoid HSC installation failure the development team shall ensure the mounting hardware are sufficient for max operational G-force with factor of safety	
		FSRS01.08	To avoid HSC installation failure the development team shall ensure the mounting hardware is secure and free from potential lessening or unintended movement	
		FSRS01.09	To avoid HSC over-current failure the development team shall ensure software limits current ranges	
		FSRS01.10	To avoid HSC over-current failure the development team shall ensure relays and fuses are in place and functional	
		FSRS01.11	To avoid HSC over-heating failure the development team shall ensure the HSC is mounted such that there is proper clearance and sufficient air flow to cool the HSC	
		FSRS01.12	The HSC shall perform a shutdown procedure	

Appendix 4.3CSMS Safety Goals and Functional Requirements

SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGS02.1	The ECM shall control engine	FSRS02.01	To avoid ECM wiring failure the development team shall ensure wiring
SGS02.2	torque output		is securely installed using manufacturer installation specification
SGS02.3		FSRS02.02	To avoid ECM wiring failure the development team shall ensure wiring
SGS02.4	The ECM shall control engine		gauge is sufficient to carry max operational current with factor of safety
SGS02.5	temperature	FSRS02.03	To avoid ECM wiring failure the development team shall ensure wire bend radii are adhered to and wiring is protected from heat sources
	The ECM shall control A/F	FSRS02.04	To avoid ECM unintended access or physical damage the development
	ratio		team shall ensure proper mounting, installation, and manufacturing of the ECM
	The ECM shall control idle	FSRS02.05	To avoid ECM unintended access or physical damage the development
	speed		team shall ensure use of covering at wire-ECM interface
	speed	FSRS02.06	To avoid ECM unintended access or physical damage the operator shall avoid adverse
	The ECM shall control		road conditions which may produce NVH
	electronic valve	FSRS02.07	To avoid ECM installation failure the development team shall ensure the
			mounting hardware are sufficient for max operational G-force with factor
			of safety
		FSRS02.08	To avoid ECM installation failure the development team shall ensure the mounting
		FSRS02.09	hardware is secure and free from potential lessening or unintended movement
		F5K502.09	To avoid ECM over-current failure the development team shall ensure
		ECDC02 10	software limits current rangesTo avoid ECM over-current failure the development team shall ensure relays and fuses
		FSRS02.10	are in place and functional
		FSRS02.11	The ECM shall perform a shutdown procedure
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGS03.1	The TCM shall control gear	FSRS03.01	To avoid TCM wiring failure the development team shall ensure wiring
SGS03.2	shifting		is securely installed using manufacturer installation specifications
		FSRS03.02	To avoid TCM wiring failure the development team shall ensure wiring
	The TCM shall control		gauge is sufficient to carry max operational current with factor of safety
	transmission temperature	FSRS03.03	To avoid TCM wiring failure the development team shall ensure wire bend radii are
	1		adhered to and wiring is protected from heat sources

	1		
		FSRS03.04	To avoid TCM unintended access or physical damage the development
			team shall ensure proper mounting, installation, and manufacturing of the
			TMC
		FSRS03.05	To avoid TCM unintended access or physical damage the development
			team shall ensure use of covering at wire-TMC interface
		FSRS03.06	To avoid TCM unintended access or physical damage the operator shall
			avoid adverse road conditions which may produce NVH
		FSRS03.07	To avoid TCM installation failure the development team shall ensure the
			mounting hardware are sufficient for max operational G-force with factor
			of safety
		FSRS03.08	To avoid TCM installation failure the development team shall ensure the mounting
		1511502100	hardware is secure and free from potential lessening or unintended movement
		FSRS03.09	To avoid TCM over-current failure the development team shall ensure
			software limits current ranges
		FSRS03.10	To avoid TCM over-current failure the development team shall ensure relays and fuses
			are in place and functional
		FSRS03.11	To avoid TCM over-heating failure the development team shall ensure
			the TCM is mounted such that there is proper clearance and sufficient air
			flow to cool the TCM
		FSRS03.12	The TCM shall perform a shutdown procedure
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGS04.1	The EMC shall control current	FSRS04.01	To avoid EMC wiring failure the development team shall ensure wiring
SGS04.2	supply to EM		is securely installed using manufacturer installation specifications
SGS04.3		FSRS04.02	To avoid EMC wiring failure the development team shall ensure wiring
	The EMC shall control current		gauge is sufficient to carry max operational current with factor of safety
	direction	FSRS04.03	To avoid EMC wiring failure the development team shall ensure wire bend radii are
			adhered to and wiring is protected from heat sources
	The EMC shall control EM	FSRS04.04	To avoid EMC unintended access or physical damage the development
	temperature		team shall ensure proper mounting, installation, and manufacturing of the
			EMC
		FSRS04.05	To avoid EMC unintended access or physical damage the development team shall ensure use of covering at wire- EMC interface

		FSRS04.06	To avoid EMC unintended access or physical damage the operator shall avoid adverse road conditions which may produce NVH
		FSRS04.07	To avoid EMC installation failure the development team shall ensure the
			mounting hardware are sufficient for max operational G-force with factor
			of safety
		FSRS04.08	To avoid EMC installation failure the development team shall ensure the mounting hardware is secure and free from potential lessening or unintended movement
		FSRS04.09	To avoid EMC over-current failure the development team shall ensure
			software limits current ranges
		FSRS04.10	To avoid EMC over-current failure the development team shall ensure relays and fuses are in place and functional
		FSRS04.11	To avoid EMC operation outside of max/min temperature range the
			development team shall ensure the EMC has a thermal controls system
			and software forces operation within specified EMC temperature range
		FSRS04.12	To avoid EMC operation outside of max/min temperature range the
		1510501.12	development team shall actuate cooling fans when EMC reaches
			specified temperature
		FSRS04.13	To avoid EMC operation outside of max/min temperature range the
		151504.15	development team shall ensure thermal system components (radiator,
			coolant level, fans) are functional and sufficient to cool the EMC
		FSRS04.14	
		F5K504.14	To avoid EMC operation outside of max/min temperature range the
			development team shall ensure the fans are free from potential physical
			damage
		FSRS04.15	To avoid EMC operation outside of max/min temperature range the development team shall ensure bolts, hoses and mounting hardware are securely fastened and free from
			potential loosening or unintended movement
		FSRS04.16	The EMC shall perform a shutdown procedure
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGS05.1	The BMS shall ensure safe	FSRS05.01	To avoid BMS wiring failure the development team shall ensure wiring
SGS05.2	ESS operating conditions		is securely installed using manufacturer installation specifications
SGS05.3		FSRS05.02	To avoid BMS wiring failure the development team shall ensure wiring
SGS05.4		131303.02	
2000011			gauge is sufficient to carry max operational current with factor of safety

SGS05.5	The BMS shall monitor ESS	FSRS05.03	To avoid BMS wiring failure the development team shall ensure wire bend radii are adhered to and wiring is protected from heat sources
	state (voltage, temperature, SOC, and current) The BMS shall protect against over-current, over-voltage, under-voltage, and over- temperature	FSRS05.04	To avoid BMS unintended access or physical damage the development
			team shall ensure proper mounting, installation, and manufacturing of the BMS
		FSRS05.05	To avoid BMS unintended access or physical damage the development
		1 51(505.05	team shall ensure use of covering at wire- BMS interface
		FSRS05.06	To avoid BMS unintended access or physical damage the operator shall avoid adverse road conditions which may produce NVH
	The BMS shall report data	FSRS05.07	To avoid BMS installation failure the development team shall ensure the mounting hardware are sufficient for max operational G-force with factor
	The BMS shall control and		of safety
	balance ESS environment	FSRS05.08	To avoid BMS installation failure the development team shall ensure the mounting hardware is secure and free from potential lessening or
			unintended movement
		FSRS05.09	To avoid BMS over-current failure the development team shall ensure
		FSRS05.10	software limits current ranges
		F5K505.10	To avoid BMS over-current failure the development team shall ensure relays and fuses are in place and functional
		FSRS05.11	To avoid BMS over-heating failure the development team shall ensure
		1510502.11	the BMS is mounted such that there is proper clearance and sufficient air
			flow to cool the BMS
		FSRS05.12	The BMS shall perform a shutdown procedure
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGS06.1	The OBC shall control	FSRS06.01	To avoid OBC wiring failure the development team shall ensure
	charging to the HV battery		charging port cover is sufficient to provide freedom from unintended
	pack		access or physical damage
		FSRS06.02	To avoid OBC wiring failure the development team shall ensure wiring
			is securely installed using manufacturer installation specifications
		FSRS06.03	To avoid OBC wiring failure the development team shall ensure wiring gauge is sufficient to carry max operational current with factor of safety

FSRS06.04	To avoid OBC wiring failure the development team shall ensure wire bend radii are
F5K500.04	adhered to and wiring is protected from heat sources
FSRS06.05	To avoid OBC unintended access or physical damage the development
	team shall ensure proper mounting, installation, and manufacturing of the
	OBC
FSRS06.06	To avoid OBC unintended access or physical damage the development
	team shall ensure use of covering at wire- OBC interface
FSRS06.07	To avoid OBC unintended access or physical damage the operator shall avoid adverse
	road conditions which may produce NVH
FSRS06.08	To avoid OBC installation failure the development team shall ensure the
	mounting hardware are sufficient for max operational G-force with factor
	of safety
FSRS06.09	To avoid OBC installation failure the development team shall ensure the
	mounting hardware is secure and free from potential lessening or
	unintended movement
FSRS06.10	To avoid OBC over-current failure the development team shall ensure
	software limits current ranges
FSRS06.11	To avoid OBC over-current failure the development team shall ensure relays and fuses
	are in place and functional
FSRS06.12	To avoid OBC operation outside of max/min temperature range the
	development team shall ensure the OBC has a thermal controls system
	and software forces operation within specified OBC temperature range
FSRS06.13	To avoid OBC operation outside of max/min temperature range the
	development team shall actuate cooling fans when OBC reaches
	specified temperature
FSRS06.14	To avoid OBC operation outside of max/min temperature range the
	development team shall ensure thermal system components (radiator,
	coolant level, fans) are functional and sufficient to cool the OBC
FSRS06.15	To avoid OBC operation outside of max/min temperature range the
	development team shall ensure the fans are free from potential physical
	damage
FSRS06.16	To avoid OBC operation outside of max/min temperature range the development team
	shall ensure bolts, hoses and mounting hardware are securely fastened and free from
	potential loosening or unintended movement

		FSRS06.17	The OBC shall perform a shutdown procedure
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGS07.1	The OBD II shall provide	FSRS07.01	To avoid OBD II wiring failure the development team shall ensure
	requested vehicle parameters to		wiring is securely installed using manufacturer installation specifications
	monitor	FSRS07.02	To avoid OBD II wiring failure the development team shall ensure
			wiring gauge is sufficient to carry max operational current with factor of safety
		FSRS07.03	To avoid OBD II wiring failure the development team shall ensure wire
		FSRS07.04	bend radii are adhered to and wiring is protected from heat sources To avoid OBD II unintended access or physical damage the development
		1/31/307.04	team shall ensure proper mounting, installation, and manufacturing of the
			OBD II
		FSRS07.05	To avoid OBD II installation failure the development team shall ensure the mounting hardware is secure, free from unintended movement, and sufficient for open road
		ECD COT OC	conditions with a factor of safety
		FSRS07.06	To avoid OBD II over-current failure the development team shall ensure
		FSRS07.07	software limits current ranges To avoid OBD II over-current failure the development team shall ensure relays and
		F3K307.07	fuses are in place and functional
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGS08.1	The CAN Bus shall transfer	FSRS08.01	To avoid CAN bus wiring failure the development team shall ensure
	necessary signals such as EM		wiring is securely installed using manufacturer installation specifications
	speed, EM torque, EM	FSRS08.02	To avoid CAN bus wiring failure the development team shall ensure
	temperature, EMC		wiring gauge is sufficient to carry max operational current with factor of
	temperature, SOC, current,		safety
	voltage, battery temperature,	FSRS08.03	To avoid CAN bus wiring failure the development team shall ensure wire
	and OBC temperature		bend radii are adhered to and wiring is protected from heat sources
		FSRS08.04	To avoid CAN bus unintended access or physical damage the
			development team shall ensure proper mounting, installation, and
			manufacturing of the CAN bus

	FSRS08.05	To avoid CAN bus unintended access or physical damage the development team shall ensure use of covering at wire- CAN bus interface
	EGD GOO OC	
	FSRS08.06	To avoid CAN bus unintended access or physical damage the operator shall avoid
	EGD 000.07	adverse road conditions which may produce NVH
	FSRS08.07	To avoid CAN bus installation failure the development team shall ensure
		the mounting hardware are sufficient for max operational G-force with
		factor of safety
	FSRS08.08	To avoid CAN bus installation failure the development team shall ensure the mounting hardware is secure and free from potential lessening or unintended movement
	FSRS08.09	To avoid CAN bus over-current failure the development team shall
		ensure software limits current ranges
	FSRS08.10	To avoid CAN bus over-current failure the development team shall ensure relays and
		fuses are in place and functional
	FSRS08.11	To avoid CAN bus over-heating failure the development team shall ensure the CAN bus
		is mounted such that there is proper clearance and sufficient air flow to cool the CAN
		bus
Safety Goal	FSR No.	Functional Safety Requirement
The APPS shall monitor the	FSRS09.01	To avoid AP/APPS wiring failure the development team shall ensure
position of the accelerator		wiring is securely installed using manufacturer installation specifications
pedal and transmit a torque	FSRS09.02	To avoid AP/APPS wiring failure the development team shall ensure
request		wiring gauge is sufficient to carry max operational current with factor of
1		safety
	FSRS09.03	To avoid AP/APPS wiring failure the development team shall ensure
	1 511507105	wire bend radii are adhered to and wiring is protected from heat sources
	ESRS09.04	To avoid AP/APPS unintended access or physical damage the
	1 51(50).04	development team shall ensure proper mounting, installation, and
		manufacturing of the AP/APPS
	ECDC00.05	· · · · · · · · · · · · · · · · · · ·
	L2K20A02	To avoid AP/APPS unintended access or physical damage the
		development team shall ensure use of covering at wire-AP/APPS
		interface
	FSRS09.06	To avoid AP/APPS unintended access or physical damage the operator
	position of the accelerator	FSRS08.09 FSRS08.10 FSRS08.10 FSRS08.11 Safety Goal FSR No. The APPS shall monitor the position of the accelerator pedal and transmit a torque FSRS09.01 FSRS09.02

		FSRS09.07 FSRS09.08 FSRS09.09 FSRS09.10 FSRS09.11	To avoid AP/APPS installation failure the development team shall ensure the mounting hardware are sufficient for max operational G-force with factor of safety To avoid AP/APPS installation failure the development team shall ensure the mounting hardware is secure and free from potential lessening or unintended movement To avoid AP/APPS over-current failure the development team shall ensure software limits current ranges To avoid AP/APPS over-current failure the development team shall ensure relays and fuses are in place and functional To avoid AP/APPS over-heating failure the development team shall ensure the
SG No.	Safety Goal	FSR No.	AP/APPS is mounted such that there is proper clearance and sufficient air flow to cool the AP/APPS Functional Safety Requirement
SGS10.1 SGS10.2 SGS10.3	The low voltage system shall control of all auxiliary functions to include air bags,	FSRS10.01	To avoid low voltage component wiring failure the development team shall ensure wiring is securely installed using manufacturer installation specifications
	windshield wipers, instrument cluster, lights, entertainment system, turn signals, haptic	FSRS10.02	To avoid low voltage component wiring failure the development team shall ensure wiring gauge is sufficient to carry max operational current with factor of safety
	feedback, security system, pumps, fans, controller and DAQ	FSRS10.03	To avoid low voltage component wiring failure the development team shall ensure wire bend radii are adhered to and wiring is protected from heat sources
	The low voltage system shall control thermal components	FSRS10.04	To avoid low voltage component unintended access or physical damage the development team shall ensure proper mounting, installation, and manufacturing of the low voltage systems
	The low voltage system shall	FSRS10.05	To avoid low voltage component unintended access or physical damage the development team shall ensure use of covering at wire-low voltage component interface
	control data acquisition	FSRS10.06	To avoid low voltage component unintended access or physical damage the operator shall avoid adverse road conditions which may produce NVH
		FSRS10.07	To avoid low voltage component installation failure the development team shall ensure the mounting hardware are sufficient for max operational G-force with factor of safety

FSRS10.08	To avoid low voltage component installation failure the development team shall ensure the mounting hardware is secure and free from potential lessening or unintended
	movement
FSRS10.09	To avoid low voltage component over-current failure the development
	team shall ensure software limits current ranges
FSRS10.10	To avoid low voltage component over-current failure the development team shall
	ensure relays and fuses are in place and functional
FSRS10.11	To avoid low voltage over-heating failure the development team shall ensure the low
	voltage component is mounted such that there is proper clearance and sufficient air flow
	to cool the low voltage
FSRS10.12	To avoid low voltage over-heating failure the development team shall ensure the low
	voltage component is mounted such that there is proper clearance and sufficient air flow
	to cool the low voltage

Appendix 4.4LKA Safety Goals and Functional Requirements

	CAVs / CSMS LKA Safety Goals and Functional Requirements			
SG No.	Safety Goal	FSR No.	Functional Safety Requirement	
SGL01	The LKA system shall safely control lateral movement via	FSRL01.01	The LKA system shall allow operator to override automated controls with minimal braking engagement	
	the braking system (EBCM)	FSRL01.02	LKA system shall brake the front wheel opposite to the side of deviation	
		FSRL01.03	The LKA brake response system shall function according to operator engagement	
		FSRL01.04	The LKA brake response system shall respond (feedback, lateral movement) more quickly in the event of less operator engagement (hands on wheel, head tilt, eye deviation)	
		FSRL01.05	The LKA brake response system shall respond (feedback, lateral movement) less quickly in the event of more operator engagement (hands on wheel, head tilt, eye deviation)	

	FSRL01.06	To avoid wiring failures the LKA system shall be wired and installed
		according to manufacturer specifications to include bend radii, heat
		shielding, EMI avoidance, sheathing, proper gauge, and interface
		connections
I	FSRL01.07	The LKA brake system shall engage in timely manner such that brake
		pad fatigue and passenger discomfort is minimized
I	FSRL01.08	To avoid brake pad failures the development teams shall ensure proper
		mounting and installation of brake pads
I	FSRL01.09	To avoid brake pad failures the development teams shall ensure brake
		pad bolts and mounting hardware are securely fastened and free from
		potential loosening or unintended movement
	FSRL01.10	To avoid brake pad failures the development shall avoid excessively
		adverse road conditions (bumpy terrain, excessive grade) which may
		cause a high NVH
I	FSRL01.11	To avoid brake pad failures the operator shall avoid poor driving
		behaviors
I	FSRL01.12	To avoid brake rotor failures the development teams shall ensure proper
		mounting and installation of brake rotors
I	FSRL01.13	The LKA brake system shall engage in timely manner such that brake
		rotor fatigue and passenger discomfort is minimized
I	FSRL01.14	To avoid brake rotor failures the development teams shall ensure brake
		rotor bolts and mounting hardware are securely fastened and free from
		potential loosening or unintended movement
I	FSRL01.15	To avoid brake rotor failures the operator shall avoid excessively adverse
		road conditions (bumpy terrain, excessive grade) which may cause a high
		NVH
I	FSRL01.16	The operator shall ensure brake system is free of build-up (snow, mud)
		and debris prior to use
	FSRL01.17	To avoid caliper failures the operator shall ensure routine inspection for
		caliper rust and corrosion
	FSRL01.18	LKA brake system shall engage in timely manner such that brake lines
		are immediately able to be actuated

		FSRL01.19 FSRL01.20	To avoid brake fluid line failure the development team shall ensure proper bleeding, mounting, installation, and routine maintenance and inspection of brake line hardware and its functionality To avoid brake fluid line failure the development team shall ensure lines, bolts and mounting hardware are securely fastened and free from potential loosening or unintended movement
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGL02	The LKA shall control lateral movement via the EPS system	FSRL02.01	The LKA EPS response system shall function according to operator engagement
		FSRL02.02	The LKA EPS response system shall respond (feedback, lateral movement) more quickly in the event of less operator engagement (hands on wheel, head tilt, eye deviation)
		FSRL02.03	The LKA EPS response system shall respond (feedback, lateral movement) less quickly in the event of more operator engagement (hands on wheel, head tilt, eye deviation)
		FSRL02.04	The LKA EPS response system shall allow operator to override automated controls with minimal steering engagement
		FSRL02.05	To avoid contamination of EPS fluid the development team shall ensure proper mounting, installation, and manufacturing of EPS hoses, clamps, and their components
		FSRL02.06	To avoid contamination of EPS fluid the development team shall ensure interface components, and mounting hardware are securely fastened and free from potential loosening or unintended movement
		FSRL02.07	To avoid contamination of EPS fluid the development team shall ensure functionality of EPS pump and check for hose deterioration
		FSRL02.08	To avoid EPS fluid leaks the development team shall ensure proper mounting, installation, and manufacturing of EPS hoses, clamps, and their components
		FSRL02.09	To avoid EPS fluid leaks the development team shall ensure interface components (seals, gaskets), and mounting hardware are securely fastened and free from potential loosening or unintended movement

		FSRL02.10	To avoid EPS fluid leaks the development team shall ensure the correct type of fluid is used, proper fluid levels, and check for leaks prior to operation
		FSRL02.11	To avoid EPS belt failure the development team shall ensure proper mounting, installation, and manufacturing of the belt (tension, torque specs) and its components
		FSRL02.12	To avoid EPS belt failure the development teams hall ensure bolts, interface components, and mounting hardware are securely fastened and free from potential loosening or unintended movement
		FSRL02.13	To avoid EPS pump failure the development team shall ensure proper mounting, installation, and manufacturing of pump and its components
		FSRL02.14	To avoid EPS pump failure the development team shall ensure bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from potential loosening or unintended movement
		FSRL02.15	To avoid EPS failure the operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH
		FSRL02.16	The development team shall ensure power steering motor is functional
		FSRL02.17	To avoid EPS response system wiring failures the LKA system shall be wired and installed according to manufacturer specifications to include bend radii, heat shielding, EMI avoidance, sheathing, proper gauge, and interface connections
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGL03	The LKA shall perform lane- line, object detection and	FSRL03.01	The development team shall impose criteria for deviation and corrective action
	multi-feature tracking	FSRL03.02	The LKA system shall monitor the operators engagement to include head tilt, hands on wheel, and eye deviation
		FSRL03.03	The LKA system shall function according to operator engagement

FSRL03.04	The LKA system shall respond (feedback, acceleration, deceleration) more quickly in the event of less operator engagement (hands on wheel,
	head tilt, eye deviation)
FSRL03.05	The LKA system shall respond (feedback, acceleration, deceleration) less
	quickly in the event of more operator engagement (hands on wheel, head tilt, eye deviation)
FSRL03.06	The LKA system shall require minimum vehicle speed based on sensor
I SILLOS.00	requirements and lane-line visibility
FSRL03.07	To avoid sensor visibility obstruction the LKA system shall have control
I SILLOUID /	of front lights
FSRL03.08	To avoid sensor visibility obstruction the LKA system shall have control
	wind shield wipers
FSRL03.09	The LKA system shall only be operational if sensor performance meets a
	minimum standard (communication speed, sensor availability or
	visibility)
FSRL03.10	To avoid sensor visibility obstruction the operator shall ensure LKA
	system sensors have clear field of view and are free of visibility
	obstructions
FSRL03.11	To avoid sensor failure the development team shall ensure sensor and
	sensor enclosure bolts and mounting hardware are securely fastened and
	free from potential loosening or unintended movement
FSRL03.12	To avoid sensor failure the development team shall ensure sensor
	enclosure manufacturing and use of materials is sufficient to prevent
	unintended access and physical damage
FSRL03.13	To avoid sensor failure the LKA sensors shall be wired and installed
	according to manufacturer specifications to include bend radii, heat
	shielding, EMI avoidance, sheathing, proper gauge, and interface
	connections
FSRL03.14	The LKA system shall alert operator prior to and when shutdown occurs
FSRL03.15	The LKA communications shall operate independently and be free from
	external manipulation
FSRL03.16	The development team shall ensure the LKA system sensors are placed
	in a location which minimizes potential visibility failures

		1	
		FSRL03.17	The development team shall ensure LKA system radars and cameras are of the quality which can produce true data during reasonably poor
			operational conditions (rain, fog, snow, dirt, poor lane-line quality)
		FSRL03.18	If LKA operating system fails, the LKA system shall alert the operator
			via audio and visual feedback
		FSRL03.19	The computer shall be aware of signal latency and the LKA program will actuate a control action accordingly
		FSRL03.20	If sensor signal stops in during a corrective control action the LKA system shall immediately disable and alert operator via visual, audio, and haptic feedback
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGL04	The LKA sensors shall transmit data to the associated controller	FSRL04.01	The LKA sensors shall be wired and installed according to manufacturer specifications to include bend radii, heat shielding, EMI avoidance, sheathing, proper gauge, and interface connections
		FSRL04.02	The LKA system shall alert operator prior to and when shutdown occurs
		FSRL04.03	The LKA system shall only be operational if sensor performance meets a minimum standard (communication speed, sensor availability or visibility)
		FSRL04.04	The LKA communications shall operate independently and be free from external manipulation
		FSRL04.05	The LKA system shall have constant enabled/disabled form of feedback (light) indicated to the operator
		FSRL04.06	The development team shall ensure the LKA system signal transfers through appropriate medium (type, gauge of wiring) and adheres to automotive wiring standards
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGL05	The operator shall initiate the LKA system	FSRL05.01	When the speed and operational environment allow, the LKA system shall alert the operator that the LKA system requires operator initiation
		FSRL05.02	When the speed and operational environment allow, the LKA initiation procedure shall be clearly defined to the operator via audio and visual

			alert with minimal required actions by the operator (single button
			initiation)
		FSRL05.03	If LKA operating system fails, the LKA system shall alert the operator
		I'SKL05.05	via audio and visual feedback
		FSRL05.04	
		FSKL05.04	To prevent accidental disabling of the LKA system, the LKA system
			shall have individual on/off buttons
		FSRL05.05	The development team shall ensure the LKA system signal transfers
			through an appropriate medium (type, gauge of wiring) and adheres to
			automotive wiring standards (twisted wires, EMI avoidance, shielding)
		FSRL05.06	The development team shall ensure the LKA system limits time of
			actuation once the operator initiates LKA system (ex. close loop after
			500ms)
		FSRL05.07	The development team shall ensure the LKA system alerts the operator
			once the LKA system has been enabled
		FSRL05.08	The LKA system shall operate within a specified vehicle velocity range
		FSRL05.09	Turn-indicator actuation shall be required for free movement out of lane,
			otherwise feedback will warn operator
		FSRL05.10	The operator shall be allowed to choose when LKA system will be
			enabled
		FSRL05.11	The development team shall ensure that if the LKA system "on" button is
			actuated, the LKA system enables, regardless of pressed time duration
		FSRL05.12	The development team shall ensure the LKA system "on" button is of the
			a reasonable quality to reduce bounce error
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGL06	The LKA system shall	FSRL06.01	The LKA feedback system shall be wired and installed according to
	provide feedback to the		manufacturer specifications to include bend radii, heat shielding, EMI
	operator (LKA status, haptic,		avoidance, sheathing, proper gauge, and interface connections
	visual, audio)	FSRL06.02	The LKA feedback system shall alert operator prior to and when
			shutdown occurs
		FSRL06.03	The LKA feedback system shall alert operator when deviation occurs

SG No.	Safety Goal	FSR No.	Functional Safety Requirement
		FSRL06.17	If LKA feedback system is disabled by the operator then the entire LKA system shall disengage until the operator initiates it again
			The operator shall be capable of disenabling the LKA feedback system
		FSRL06.16	operational conditions (rain, fog, snow, dirt, poor lane-line quality)
			of the quality which can produce true data during reasonably poor
		FSRL06.15	The development team shall ensure LKA system radars and cameras are
		FSRL06.14	The LKA system shall check for sensor obstructions (validate wheel speed with sensor data)
		FSRL06.13	The LKA system shall have constant enabled/disabled form of feedback (light) indicated to the operator
		FSRL06.12	The operator shall have control of the level of LKA system feedback stimuli
		FSRL06.11	The LKA feedback system shall alert the operator using at least two forms of feedback
		FSRL06.10	The LKA communications shall operate independently and be free from external manipulation (malicious intrusion, EMI)
			meets a minimum standard (communication speed, audio, visual, haptic functionality)
		FSRL06.09	The LKA system shall only be operational if feedback performance
		LOO.U8	during night, increase during day)
		FSRL06.08	system, excessive cabin noise) The LKA system visual feedback shall adjust to ambient light (decrease
		FSRL06.07	The LKA system audio feedback shall adjust to ambient volume (stereo
			the operator and cause greater potential for hazard (not overly loud or bright)
		FSRL06.06	The LKA system shall provide feedback in manner that does not startle
		FSRL06.05	The LKA system shall provide audio, visual, and haptic feedback
			engagement
		FSRL06.04	The LKA feedback system shall function according to operator

SGL07	The LKA computer shall safely	FSRL07.01	To avoid wiring failure of the intel tank computer the development team
	perform sensor fusion data		shall ensure wiring is securely installed using manufacturer installation
	verification & validation using		specifications
	developed algorithms and NNs	FSRL07.02	To avoid wiring failure of the intel tank computer the development team
			shall ensure wiring gauge is sufficient to carry max operational current
			with factor of safety
		FSRL07.03	To avoid wiring failure of the intel tank computer the development team shall ensure wire bend radii are adhered to
		FSRL07.04	The development team shall ensure the computer alerts operator that corrective action decision is disabled
		FSRL07.05	The development team shall ensure the computer determines fidelity of non-blended image and decide if corrective action should be applied
		FSRL07.06	The development team shall ensure the computer only makes corrective action decisions when fidelity of image meets minimum specified resolution
		FSRL07.07	The development team shall ensure if computer system fails, it does not
			prevent vehicle from manual driving operations
		FSRL07.08	The development team shall ensure manufacturing and installation is
			sufficient to prevent unintended access and physical damage to the
			computer
		FSRL07.09	To prevent unintended access and physical damage to the development team shall ensure use of coverings at wire-computer interface to prevent unintended access
		FSRL07.10	To prevent physical damage to the computer the operator shall avoid adverse road conditions which may produce NVH
		FSRL07.11	To prevent unintended access and physical damage the development team shall ensure computer installation is inside cabin in a dry debris-proof location
		FSRL07.12	To prevent unintended access and physical damage the development
			team shall ensure computer is inaccessible by passengers
		FSRL07.13	To prevent power failure the development team shall ensure the power
			supplied to the computer is within manufacturer operational range
		FSRL07.14	The development team shall ensure the computer NN model is thoroughly defined and highly sensitive to small variations in inputs
		FSRL07.15	The development team shall ensure the computer NN is thoroughly tested and validate prior to implementation
		FSRL07.16	The development team shall ensure the computer NN imposes limits on output to not exceed boundaries

FSRL07.1	
	does not over-fit training data and is sufficient to fit new and unseen data
FSRL07.1	
	(Auto industry standard is one defect per 1000 executable lines of code)
FSRL07.1	9 The development team shall ensure the computer program is developed using
	automotive coding standards
FSRL07.2) The development team shall ensure the use of multiple software scanning tools to
	identify vulnerability and error in computer program code (industry uses Jarvis which
	analyses the binary executable action and not the mistakes in the code)
FSRL07.2	
	compounding rounding errors
FSRL07.2	2 The development team shall ensure the understanding of computer input and output
	signal quality, noise, latency, and bandwidth accounting for measurement and control
	action error
FSRL07.2	3 The development team shall reduce computer signal input and output latency, ensure
	use of high-quality transmission medium
FSRL07.2	4 To prevent computer signal input and output bandwidth fault the development team
	shall ensure transmission medium gauge is sufficient to handle expected throughput
	(load) with factor of safety
FSRL07.2	5 The development team shall ensure an understanding of time required to analyze and
	route computer signal data
FSRL07.2	6 To reduce computer signal input and output noise the development team shall ensure
	wires are as short as possible
FSRL07.2	7 To reduce computer signal input and output noise the development team shall ensure
	wires are kept away from electrical machinery
FSRL07.2	
	together wires
FSRL07.2	
	ensure thermal effects on amplifiers are minimized
FSRL07.3	
	shall ensure the amplifier bandwidth matches input signal bandwidth
FSRL07.3	1 To reduce computer signal input and output noise the development team shall ensure
	use of proper filtering techniques
FSRL07.3	2 To reduce computer signal input and output noise the development team shall ensure
	use of wire shielding and conduit
FSRL07.3	3 To reduce computer signal input and output noise the development team shall ensure
	understanding of ground loops and impose proper grounding practices

		m · · · · · · · · · · · · · · · · · · ·
	FSRL07.34	To ensure true data measurement the development team shall test the collection with the computer operating at the same temperature that it will be operating at in real-world scenarios
F	FSRL07.35	The development team shall ensure the understanding of potential computer signal input and output storage delays
F	FSRL07.36	The development team shall ensure the use of software safety and that the system is free from external unintended malicious control
F	FSRL07.37	To prevent computer memory failure the development team shall ensure the computer is capable of storing and processing the expected amount of data with a factor of safety
F	FSRL07.38	To prevent computer memory failure ensure the program is developed such that information that is too large cannot be written into a memory
		buffer that is too small to contain it
F	FSRL07.39	To prevent over-heating the development team shall ensure the computer is mounted such that there is proper clearance and sufficient air flow to cool the computer
F	FSRL07.40	To prevent over-heating the development team shall ensure the computer imposes thermal self-regulation
F	FSRL07.41	To prevent over-heating the development team shall ensure the computer
		operates within specified temperature range
F	FSRL07.42	To prevent operating system crash the development team shall ensure the system does not over heat
F	FSRL07.43	To prevent operating system crash the development team shall ensure the computer is mounted such that there is proper clearance and sufficient air flow to cool the computer
F	FSRL07.44	To prevent operating system crash the development team shall ensure the computer fans pull air from cool and dry source
F	FSRL07.45	To prevent operating system crash the development team shall ensure the computer imposes thermal self-regulation
F	FSRL07.46	To prevent operating system crash the development team shall ensure the computer operates within specified temperature range
F	FSRL07.47	To prevent operating system crash the development team shall ensure the program is developed such that it does not attempt to access an incorrect memory address leading to general protection fault
F	FSRL07.48	To prevent operating system crash the development team shall ensure the program is developed such that the OS does not enter an infinite loop
F	FSRL07.49	To prevent operating system crash the development team shall ensure the program is developed such that information that is too large cannot be written into a memory buffer that is too small to contain it

		FSRL07.50	To prevent operating system crash the development team shall ensure the program is developed such that deadlock is prevented (multiple programs having control some resource another program needs)
		FSRL07.51	To prevent operating system crash the development team shall ensure the program performs shutdown operations
		FSRL07.52	To prevent over-heating the development team shall ensure the computer fans pull air from cool and dry source
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGL08	The LKA computer shall send control action decisions to the	FSRL08.01	The LKA system shall have constant enabled/disabled form of feedback (light) indicated to the operator
	associated controller	FSRL08.02	To avoid wiring failure of the intel tank computer the development team shall ensure wiring is securely installed using manufacturer installation specifications
		FSRL08.03	To avoid wiring failure of the intel tank computer the development team shall ensure wiring gauge is sufficient to carry max operational current with factor of safety
		FSRL08.04	To avoid wiring failure of the intel tank computer the development team shall ensure wire bend radii are adhered to
		FSRL08.05	The development team shall ensure the computer alerts operator that corrective action decision is disabled
		FSRL08.06	The development team shall ensure the computer only makes corrective action decisions when fidelity of image meets minimum specified resolution
		FSRL08.07	The development team shall ensure if computer system fails, it does not prevent vehicle from manual driving operations
		FSRL08.08	The development team shall ensure manufacturing and installation is sufficient to prevent unintended access and physical damage to the computer
		FSRL08.09	To prevent unintended access and physical damage to the development team shall ensure use of coverings at wire-computer interface to prevent unintended access
		FSRL08.10	To prevent physical damage to the computer the operator shall avoid adverse road conditions which may produce NVH
		FSRL08.11	To prevent unintended access and physical damage the development team shall ensure computer installation is inside cabin in a dry debris-proof location

FSI	RL08.12	To prevent unintended access and physical damage the development
		team shall ensure computer is inaccessible by passengers
FSI	RL08.13	To prevent power failure the development team shall ensure the power
		supplied to the computer is within manufacturer operational range
FSI	RL08.14	The development team shall ensure the understanding of computer input and output signal quality, noise, latency, and bandwidth accounting for measurement and control action error
FSI	RL08.15	The development team shall reduce computer signal input and output latency, ensure use of high-quality transmission medium
FSI	RL08.16	To prevent computer signal input and output bandwidth fault the development team shall ensure transmission medium gauge is sufficient to handle expected throughput (load) with factor of safety
FSI	RL08.17	The development team shall ensure an understanding of time required to analyze and route computer signal data
FSI	RL08.18	To reduce computer signal input and output noise the development team shall ensure wires are as short as possible
FSI	RL08.19	To reduce computer signal input and output noise the development team shall ensure wires are kept away from electrical machinery
FSI	RL08.20	To reduce computer signal input and output noise it is recommended to use twisted together wires
FSI	RL08.21	To reduce internal computer signal input and output noise the development team shall ensure thermal effects on amplifiers are minimized
FSI	RL08.22	To reduce computer signal input and output noise, if possible, the development team shall ensure the amplifier bandwidth matches input signal bandwidth
FSI	RL08.23	To reduce computer signal input and output noise the development team shall ensure use of proper filtering techniques
FSI	RL08.24	To reduce computer signal input and output noise the development team shall ensure use of wire shielding and conduit
FSI	RL08.25	To reduce computer signal input and output noise the development team shall ensure understanding of ground loops and impose proper grounding practices
FSI	RL08.26	To ensure true data measurement the development team shall test the collection with the computer operating at the same temperature that it will be operating at in real-world scenarios
FSI	RL08.27	The development team shall ensure the understanding of potential computer signal input and output storage delays
FSI	RL08.28	To prevent computer memory failure the development team shall ensure the computer is capable of storing and processing the expected amount of data with a factor of safety

· · · · · · · · · · · · · · · · · · ·	
FSRL08.29	
	such that information that is too large cannot be written into a memory
	buffer that is too small to contain it
FSRL08.30	
	such that there is proper clearance and sufficient air flow to cool the computer
FSRL08.31	To prevent over-heating the development team shall ensure the computer fans pull air from cool and dry source
FSRL08.32	To prevent over-heating the development team shall ensure the computer imposes thermal self-regulation
FSRL08.33	v.
	operates within specified temperature range
FSRL08.34	To prevent operating system crash the development team shall ensure the system does not over heat
FSRL08.35	To prevent operating system crash the development team shall ensure the computer is
	mounted such that there is proper clearance and sufficient air flow to cool the computer
FSRL08.36	pull air from cool and dry source
FSRL08.37	
	imposes thermal self-regulation
FSRL08.38	operates within specified temperature range
FSRL08.39	To prevent operating system crash the development team shall ensure the program is
	developed such that it does not attempt to access an incorrect memory address leading to general protection fault
	To prevent operating system crash the development team shall ensure the program is
FSRL08.40	developed such that the OS does not enter an infinite loop To prevent operating system crash the development team shall ensure the program is
FSKL08.40	developed such that information that is too large cannot be written into a memory buffer that is too small to contain it
FSRL08.41	
FSKL08.41	developed such that deadlock is prevented (multiple programs having control some resource another program needs)
FSRL08.42	
	program performs shutdown operations
FSRL08.43	
	control action via actuation of steering, braking or accelerating

FSRL08.44	The LKA system shall temporarily disengage when the operator actuates
	turn signal
FSRL08.45	The development team shall ensure the use of software safety and that
	the system is free from external unintended malicious control

Appendix 4.5PSI HV Safety Goals and Functional Requirements

	PSI HV Safety Goals and Functional Requirements			
SG No.	Safety Goal	FSR No.	Functional Safety Requirement	
SGH01	The HV battery pack shall safely store and supply energy to the EM	FSRH01.01	To prevent the HV battery pack from operating outside of the max/min temperature range the development team shall ensure specified temperature limits are controlled by the BMS	
		FSRH01.02	To prevent the HV battery pack from operating outside of the max/min temperature range the development team shall ensure actuation of battery pack thermal control system (fans) when the temperature reaches limit	
		FSRH01.03	To prevent the HV battery pack from operating outside of the max/min temperature range the development team shall ensure proper installation using manufacturer recommended specifications to include component clearances and wire bend radii	
		FSRH01.04	To prevent the HV battery pack from operating outside of the max/min temperature range the development team shall ensure a limit to charging and discharging current to a specified range	
		FSRH01.05	To prevent the HV battery pack from operating while undercharged the development team shall ensure the BMS monitors and controls the SOC in real-time	
		FSRH01.06	To prevent the HV battery pack from operating while undercharged the development team shall ensure controls software will only draw current at specified minimum SOC	

		1	
		FSRH01.07	To prevent the HV battery pack from unintended access the development
			team shall ensure proper mounting, installation, and manufacturing of
			enclosure and HV components
		FSRH01.08	To prevent the HV battery pack from unintended access the development
			team shall ensure bolts and mounting hardware is securely fastened and
			free from potential loosening or movement
		FSRH01.09	To prevent the HV battery pack from unintended access the development
			team shall ensure all HV enclosure vents are covered with appropriate
			screening to prevent access from liquid, debris, dust, or insects
		FSRH01.10	To prevent the HV battery pack from unintended access the development
			team shall ensure HV thermal control system fans are pulling air from
			dry particulate-free source
		FSRH01.11	To prevent the HV battery pack from unintended access the development
			team shall ensure the enclosure location is covered and free from the
			external environment when vehicle is not in use
		FSRH01.12	To ensure the HV battery pack is properly installed the development
			team shall ensure manufacturer recommended installation instructions
			(clearance, bend radii, and soldering)
		FSRH01.13	To ensure the HV battery pack is properly installed the development
			team shall ensure the wires, bus bars, and all interfacing components are
			securely mounted and adequate clearance used
		FSRH01.14	To prevent the HV battery pack failure from excess charging or
			discharging of current the development team shall ensure software
			(HSC, OBC, EMC) limits charging and discharging rates and ranges
		FSRH01.15	To prevent the HV battery pack failure from excess charging or
			discharging of current the development team shall ensure relays and
			fuses are in place and functional to prevent over drawing of current
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGH02	The HV enclosure shall safely	FSRH02.01	To prevent the HV enclosure failure from unintended access the
	contain enclosed components		development team shall ensure proper mounting, installation, and
	through the prevention of		manufacturing of enclosure (sealing, welds, bolt holes)
	through the prevention of		manufacturing of enclosure (searing, welds, bolt holes)

unintended horizontal or	FSRH02.02	To prevent the HV enclosure failure from unintended access the
vertical movement and		development team shall ensure bolts and mounting hardware is securely
unauthorized access		fastened and free from potential loosening or movement
	FSRH02.03	To prevent the HV enclosure failure from unintended access the
		development team shall ensure the enclosure location is covered and free
		from the external environment when vehicle is not in use
	FSRH02.04	To prevent the HV enclosure failure from improper mounting to the
		vehicle frame the development team shall ensure the use of existing
		mount locations on vehicle frame
	FSRH02.05	
		vehicle frame the development team shall ensure mounting hardware is
		sufficient for max operational G-force with factor of safety
	FSRH02.06	
		vehicle frame the development team shall ensure proper enclosure
		manufacturing (welds, thread engagement)
	FSRH02.07	1 1
		mounting of components the development team shall ensure
	FSRH02.08	1 1
		mounting of components the development team shall ensure component
		mounting hardware is fire retardant
	FSRH02.09	To prevent the HV enclosure failure from improper installation and
		mounting of components the development team shall ensure component
		mounting hardware is secure and free from unintended movement
	FSRH02.10	To prevent a HV enclosure cooling failure the development team shall
		ensure the enclosure fans are operational and sufficient to cool that
	E001100 11	battery pack
	FSRH02.11	To prevent a HV enclosure cooling failure the development team shall
	E001102.12	ensure the enclosure fans are free from potential physical damage
	FSRH02.12	To prevent a HV enclosure cooling failure the development team shall
	E001102 12	ensure the enclosure fans pull air from a dry and particulate free source
	FSRH02.13	To prevent a HV enclosure cooling failure the development team shall
		ensure the enclosure ventilation is sufficient to cool HV components

		FSRH02.14	To prevent a HV enclosure cooling failure the development team shall ensure the enclosure is designed such that there is sufficient air flow to cool HV components and that the flow is free from interference
		FSRH02.15	To prevent a HV enclosure failure the operator shall not operate vehicle during adverse environmental conditions (excessively rough roads, NVH)
		FSRH02.16	
		FSRH02.17	To prevent a HV enclosure manufacturing failure the development team shall ensure proper enclosure manufacturing (welds, thread engagement)
		FSRH02.18	To prevent a HV enclosure failure the development team shall ensure materials used in manufacturing of enclosure are fire retardant
		FSRH02.19	To prevent the HV enclosure from unintended access the development team shall ensure all vents are covered with appropriate screening
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SG No. SGH03	Safety GoalThe HV junction box shallsafely contain and consolidateHV wire connections and	FSR No. FSRH03.01	Functional Safety Requirement To prevent junction box wiring failure the development team shall ensure wiring is securely installed using manufacturer installation specifications
	The HV junction box shall safely contain and consolidate		To prevent junction box wiring failure the development team shall ensure wiring is securely installed using manufacturer installation
	The HV junction box shall safely contain and consolidate HV wire connections and relays and provide a	FSRH03.01	To prevent junction box wiring failure the development team shall ensure wiring is securely installed using manufacturer installation specifications To prevent junction box wiring failure the development team shall ensure wiring gauge is sufficient to carry max operational current with
	The HV junction box shall safely contain and consolidate HV wire connections and relays and provide a	FSRH03.01 FSRH03.02	To prevent junction box wiring failure the development team shall ensure wiring is securely installed using manufacturer installation specifications To prevent junction box wiring failure the development team shall ensure wiring gauge is sufficient to carry max operational current with factor of safety To prevent junction box wiring failure the development team shall

r		1	
		FSRH03.06	To prevent junction box failure the development team shall ensure the
			junction box and mounting hardware is sufficient for max operational G-
			force with factor of safety
		FSRH03.07	To prevent junction box failure the development team shall ensure the
			junction box and mounting hardware is fire retardant
		FSRH03.08	To prevent junction box failure the development team shall ensure the
			junction box and mounting hardware is secure and free from unintended
			movement
		FSRH03.09	To prevent junction box over-current failure the development team shall ensure software (HSC, OBC, EMC) limits current magnitude
		FSRH03.10	To prevent junction box over-current failure the development team shall
		131103.10	ensure relays and fuses are in place and functional to prevent over
			drawing of current
		FSRH03.11	To prevent junction box failure the development team shall ensure box
		13K1105.11	minimum rating of IP67
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGH04	The HV wiring harness shall	FSRH04.01	To prevent HV wiring harness failure the development team shall ensure
	safely transfer energy		wiring is securely installed using manufacturer installation specifications
		FSRH04.02	To prevent HV wiring harness failure the development team shall ensure
		1 01110 1102	
		1 51110 1102	wiring gauge is sufficient to carry max operational current with factor of
		FSRH04.03	wiring gauge is sufficient to carry max operational current with factor of
			 wiring gauge is sufficient to carry max operational current with factor of safety To prevent HV wiring harness failure the development team shall ensure wire bend radii are adhered to
			wiring gauge is sufficient to carry max operational current with factor of safety To prevent HV wiring harness failure the development team shall ensure
		FSRH04.03	 wiring gauge is sufficient to carry max operational current with factor of safety To prevent HV wiring harness failure the development team shall ensure wire bend radii are adhered to
		FSRH04.03 FSRH04.04	 wiring gauge is sufficient to carry max operational current with factor of safety To prevent HV wiring harness failure the development team shall ensure wire bend radii are adhered to To prevent HV wiring harness failure the development team shall ensure the harness manufacturing is sufficient to prevent unintended access and physical damage
		FSRH04.03	 wiring gauge is sufficient to carry max operational current with factor of safety To prevent HV wiring harness failure the development team shall ensure wire bend radii are adhered to To prevent HV wiring harness failure the development team shall ensure the harness manufacturing is sufficient to prevent unintended access and physical damage To prevent HV wiring harness failure the development team shall ensure
		FSRH04.03 FSRH04.04	 wiring gauge is sufficient to carry max operational current with factor of safety To prevent HV wiring harness failure the development team shall ensure wire bend radii are adhered to To prevent HV wiring harness failure the development team shall ensure the harness manufacturing is sufficient to prevent unintended access and physical damage
		FSRH04.03 FSRH04.04 FSRH04.05	 wiring gauge is sufficient to carry max operational current with factor of safety To prevent HV wiring harness failure the development team shall ensure wire bend radii are adhered to To prevent HV wiring harness failure the development team shall ensure the harness manufacturing is sufficient to prevent unintended access and physical damage To prevent HV wiring harness failure the development team shall ensure the use of covers and shielding to prevent unintended access and physical damage
		FSRH04.03 FSRH04.04	 wiring gauge is sufficient to carry max operational current with factor of safety To prevent HV wiring harness failure the development team shall ensure wire bend radii are adhered to To prevent HV wiring harness failure the development team shall ensure the harness manufacturing is sufficient to prevent unintended access and physical damage To prevent HV wiring harness failure the development team shall ensure the use of covers and shielding to prevent unintended access and
		FSRH04.03 FSRH04.04 FSRH04.05	 wiring gauge is sufficient to carry max operational current with factor of safety To prevent HV wiring harness failure the development team shall ensure wire bend radii are adhered to To prevent HV wiring harness failure the development team shall ensure the harness manufacturing is sufficient to prevent unintended access and physical damage To prevent HV wiring harness failure the development team shall ensure the use of covers and shielding to prevent unintended access and physical damage

		1	
		FSRH04.07	To prevent HV wiring harness installation failure the development team shall ensure the harness and mounting hardware is secure and free from
			unintended movement
		FSRH04.08	To prevent HV wiring harness over-current failure the development team
			shall ensure software (HSC, OBC, EMC) limits current rates and ranges
		FSRH04.09	To prevent HV wiring harness over-current failure the development team
			shall ensure relays and fuses are in place and functional to prevent over
			drawing of current
		FSRH04.10	To prevent HV wiring harness installation failure the development team
			shall ensure the harness and mounting hardware is sufficient for max
			operational G-force with factor of safety
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGH05.1	The BMS shall safely ensure	FSRH05.01	To prevent BMS wiring failure the development team shall ensure the
SGH05.2	the HV ESS operating		wiring is securely installed using manufacturer installation specifications
SGH05.3	conditions	FSRH05.02	To prevent BMS wiring failure the development team shall ensure the
SGH05.4			wiring gauge is sufficient to carry max operational current with factor of
	The BMS shall safely monitor		safety
	and report the data of the HV	FSRH05.03	To prevent BMS wiring failure the development team shall ensure wire
	ESS voltage, temperature,		bend radii are adhered to
	SOC, and current	FSRH05.04	To prevent BMS failure the development team shall ensure the
			manufacturing is sufficient to prevent unintended access and physical
	The BMS shall protect against		damage
	over-current, over-voltage,	FSRH05.05	To prevent BMS unintended access or physical damage failure the
	under-voltage, and over-		development team shall ensure use of covering at wire-BMS interface
	temperature		prevent unintended access
		FSRH05.06	To prevent BMS unintended access or physical damage failure the
	The BMS shall safely control and balance the HV ESS		operator shall avoid adverse road condition which may produce NVH
			and damage BMS
	environment	FSRH05.07	To prevent BMS installation failure the development team shall ensure
			the BMS and mounting hardware are sufficient for max operational G-
			force with factor of safety

[
		FSRH05.08	To prevent BMS installation failure the development team shall ensure the BMS and mounting hardware is secure and free from unintended
			movement
		FSRH05.09	To prevent BMS over-current failure the development team shall ensure
			software limits current rates and ranges
		FSRH05.10	e e e e e e e e e e e e e e e e e e e
			relays and fuses are in place and functional to prevent over drawing of
			current
		FSRH05.11	To prevent BMS over-heating failure the development team shall ensure
			the BMS is mounted such that there is proper clearance and sufficient
			air flow to cool the BMS
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGH06	The OBC shall safely control	FSRH06.01	To prevent OBC charging port failure the development team shall ensure
	charging to the HV battery		the charging port cover is sufficient to provide freedom from unintended
	pack		access or physical damage
		FSRH06.02	To prevent OBC charging port failure the development team shall ensure
			the charging port is securely installed using manufacturer installation specifications
		FSRH06.03	*
		131100.03	wiring gauge is sufficient to carry max operational current with factor of
			safety
		FSRH06.04	
			wire bend radii are adhered to
		FSRH06.05	To prevent OBC wiring failure the development team shall ensure the
			wiring is securely installed using manufacturer installation specifications
		FSRH06.06	
		EGDIIO(07	gauge is sufficient to carry max operational current with factor of safety
		FSRH06.07	To prevent OBC wiring failure the development team shall ensure wire
		FSRH06.08	bend radii are adhered to To prevent OBC failure the development team shall ensure
		L2VU0.09	manufacturing is sufficient to prevent unintended access and physical
			damage
		1	winneby

	FSRH06.09	To prevent OBC unintended access or physical damage failure the
		development team shall ensure the use of covering at wire-OBC
		interface
	FSRH06.10	To prevent OBC unintended access or physical damage failure the
		development team shall ensure charging port cover is sufficient to
		provide freedom from unintended access or physical damage
	FSRH06.11	To prevent OBC unintended access or physical damage failure the
		operator shall avoid adverse road condition which may produce NVH
		and damage OBC
	FSRH06.12	To prevent OBC installation failure the development team shall ensure
		the OBC and mounting hardware are sufficient for max operational G-
		force with factor of safety
	FSRH06.13	To prevent OBC installation failure the development team shall ensure
		the OBC, charging port, and mounting hardware are secure and free
		from unintended movement
	FSRH06.14	To prevent OBC over-current failure the development team shall ensure
		software limits current rates and ranges
	FSRH06.15	To prevent OBC over-current failure the development team shall ensure
		relays and fuses are in place and functional to prevent over drawing of
		current
	FSRH06.16	To prevent OBC over-heating failure the development team shall ensure
		software limits operation within specified OBC temperature range
	FSRH06.17	To prevent OBC over-heating failure the development team shall ensure
		actuation of thermal control system (fans) when OBC reaches specified
		temperature
	FSRH06.18	To prevent OBC over-heating failure the development team shall ensure
		manufacturer recommended installation instructions (clearance, bend
		radii)
Safaty Caal	ESD No	Functional Safety Dequirement
Salety Goal	FSK INO.	Functional Safety Requirement
	FSRH07.01	To prevent EMC wiring failure the development team shall ensure the
		wiring is securely installed using manufacturer installation specifications
	Safety Goal	FSRH06.12 FSRH06.13 FSRH06.14 FSRH06.14 FSRH06.15 FSRH06.16 FSRH06.17 FSRH06.18 Safety Goal

SGH07.3	The EMC shall safely control	FSRH07.02	To prevent EMC wiring failure the development team shall ensure
SGH07.4	the supply of current to the	1 51(107.02	wiring gauge is sufficient to carry max operational current with factor of
561107.1	EM		safety
		FSRH07.03	
	The EMC shall safely convert	1 51(107.05	bend radii are adhered to
	the DC to AC	FSRH07.04	
	the DC to AC	F3KH07.04	1 1
	The EMC shall sefely control		manufacturing is sufficient to prevent unintended access and physical
	The EMC shall safely control		damage
	the direction of current	FSRH07.05	To prevent EMC unintended access failure the development team shall
			ensure the use of covering at wire-EMC interface prevent unintended
	The EMC shall safely control		access
	the EM temperature	FSRH07.06	To prevent EMC unintended access failure the operator shall avoid
			adverse road condition which may produce NVH and damage EMC
		FSRH07.07	To prevent EMC installation failure the development team shall ensure
			the EMC and mounting hardware are sufficient for max operational G-
			force with factor of safety
		FSRH07.08	To prevent EMC installation failure the development team shall ensure
			the EMC and mounting hardware is secure and free from unintended
			movement
		FSRH07.09	To prevent EMC over-current failure the development team shall ensure
			software limits current rates and ranges
		FSRH07.10	To prevent EMC over-current failure the development team shall ensure
			relays and fuses are in place and functional to prevent over drawing of
			current
		FSRH07.11	To prevent EMC over-heating failure the development team shall ensure
		1 51(107.11	software limits operation within specified EMC temp range
		FSRH07.12	To prevent EMC over-heating failure the development team shall ensure
		1.51(107.12	actuation of thermal control system (fans) when EMC reaches specified
			temperature
		FSRH07.13	1
		ГЗКНU/.13	
			using manufacturer recommended installation instructions (clearance,
			bend radii)

SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGH08	The HV component clearance requirements shall be met to ensure safe vehicle operation	FSRH08.01	The HV ESS components shall ensure proper clearance, based on analysis, in order to prevent overheating, heat transfer, and thermal runaway
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGH09	The HV ESS shall operate	FSRH09.01	The HV ESS shall avoid, detect, mitigate, and contain overheating
	within a safe and specified	FSRH09.02	The HV ESS shall ensure accurate temperature sensing
	temperature range	FSRH09.03	The HV ESS shall ensure accurate voltage sensing
		FSRH09.04	The HV ESS shall utilize EPO system
		FSRH09.05	The BMS shall control the battery pack temperature and actuate EPO when unsafe state is detected
		FSRH09.06	The ESS enclosure shall have a cooling system to ensure temperature control and thermal ventilation
		FSRH09.07	The HV ESS shall be installed in the vehicle bed to allow for air movement and ventilation
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGH10	The magnitude of the current applied to the HV ESS when	FSRH10.01	The OBC shall control the current to the battery pack while in a stationary charging state
	charging shall match the current requested	FSRH10.02	The HSC shall control the current to the battery pack while in a mobile charging state to meet the SOC requirements
		FSRH10.03	The OBC shall determine when max SOC has been met and ensure a stop to charging operations
		FSRH10.04	
		FSRH10.05	The HV ESS shall ensure accurate current/voltage sensing system by use of EMC, BMS, and OBC
SG No.	Safety Goal	FSR No.	Functional Safety Requirement

SGH11	The magnitude of the current applied by the HV ESS when	FSRH11.01	The current supplied by the HV ESS shall be determined by the EM/engine torque split
	discharging shall match the	FSRH11.02	The HSC shall determine the torque split and ultimately the current
	current requested	FSRH11.03	8 3
		FSRH11.04	requirements The HSC and EMC shall determine and control the max current discharge
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGH12	The current applied shall match the direction of the current requested	FSRH12.01	The state of the vehicle (stationary/mobile), SOC requirements, and torque request shall determine the direction of current flow
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGH13	The current applied shall be delivered at the time intended	FSRH13.01	In a mobile state, the time of a torque request shall determine the time of current delivered

Appendix 4.6PSI Mechanical Safety Goals and Functional Requirements

	PSI Mechanical Safety Goals and Functional Requirements			
SG No.	Safety Goal	FSR No.	Functional Safety Requirement	
SGM01	The driveshaft shall transmit torque from the engine and/or EM to the	FSRM01.01	To avoid driveshaft-EM interface failure the development team shall ensure proper mounting, installation, and manufacturing of modified driveshaft and its components	
	rear of the vehicle	FSRM01.02	To avoid driveshaft-EM interface failure the development team shall ensure driveshaft bolts and mounting hardware is securely fastened and free from potential loosening or unintended movement	

		FSRM02.07	To avoid differential-half shaft interface failure the development team shall ensure differential-half shaft interface location is free from potential unintended access or physical damage
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGM03	The suspension system shall safely support the vehicle weight and	FSRM03.01	To avoid uneven tire pressure and tire wear the operator shall ensure proper tire pressure prior to operation
	absorb/reduce excess energy from road shock	FSRM03.02	To avoid uneven tire pressure and tire wear the operator shall ensure proper tire alignment
		FSRM03.03	To avoid uneven tire pressure and tire wear the operator shall ensure wheels are balanced and suspension is free of bent or broken wheels
		FSRM03.04	To avoid uneven tire pressure and tire wear the operator shall avoid poor driving behaviors which may degrade suspension performance
		FSRM03.05	To avoid uneven tire pressure and tire wear the operator shall ensure manufacturer recommended tire rotations
		FSRM03.06	To avoid radius rod failure the development team shall ensure suspension radius rods are free from fatigue and corrosion
		FSRM03.07	The operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH leading to a degradation of the suspension system
		FSRM03.08	To avoid suspension spring failure the development team shall ensure suspension spring compression is calibrated and that springs are free of fatigue and corrosion
		FSRM03.09	To avoid suspension hardware mounting failures the development team shall ensure the suspensions system and components have proper mounting, installation, and routine maintenance and inspection
		FSRM03.10	To avoid suspension hardware mounting failures the development team shall ensure the suspensions system bolts and mounting hardware is securely fastened and free from potential loosening or unintended movement
		FSRM03.11	To avoid suspension wheel bearing failures the development team shall ensure proper mounting, installation, and routine maintenance and inspection of wheel bearings
		FSRM03.12	To avoid suspension strut failure the development team shall ensure struts are installed properly and free of fatigue and corrosion
		FSRM03.13	To avoid shock absorber failure the development team shall ensure shock absorbers are installed properly and free of fatigue and leaks
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGM04	The braking system shall inhibit vehicle motion, slow or stop a	FSRM04.01	To avoid brake pad failure the development team shall ensure proper mounting and installation of pads

	vehicle in motion, and keep stationary vehicles stopped	FSRM04.02	To avoid brake pad failure the development team shall ensure brake pad bolts and mounting hardware are securely fastened and free from potential loosening or
			unintended movement
		FSRM04.03	To avoid brake pad failure the operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH
		FSRM04.04	To avoid brake pad failure the operator shall perform routine inspection of brake system to check for rust, fatigue, and corrosion
		FSRM04.05	To avoid brake pad failure the operator shall avoid poor driving behaviors
		FSRM04.06	To avoid brake rotor failure the development team shall ensure proper mounting and installation of rotors
		FSRM04.07	To avoid brake rotor failure the development team shall ensure rotor bolts and mounting hardware is securely fastened and free from potential loosening or unintended movement
		FSRM04.08	To avoid brake rotor failure the operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH
		FSRM04.09	To avoid brake rotor failure the development team shall perform routine maintenance and inspection for rotor fatigue, rust, and corrosion
		FSRM04.10	The operator shall ensure brake system is free of build-up and debris prior to use
		FSRM04.11	To avoid caliper failure the operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH leading to a degradation of the suspension system
		FSRM04.12	To avoid caliper failure the development team shall perform routine maintenance and inspection for caliper fatigue, rust, and corrosion
		FSRM04.13	To avoid brake fluid line failure the development team shall ensure proper bleeding, mounting, installation, and routine maintenance and inspection of hardware and functionality
		FSRM04.14	To avoid brake fluid line failure the development team shall ensure brake lines, bolts, and mounting hardware are securely fastened and free from potential loosening or unintended movement
		FSRM04.15	To avoid parking brake failure the development team shall ensure routine maintenance and inspection parking brake hardware and verify functionality
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGM05	The thermal system shall detect and control cabin and component temperatures	FSRM05.01	To avoid engine overheating the development team shall ensure thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the engine
		FSRM05.02	To avoid engine overheating the development team shall ensure the thermal systems fans are free from potential physical damage

FSRM		To avoid engine overheating the development team shall ensure thermal system fans pull air from a cool source
FSRM		
FSRM		To avoid engine overheating the development team shall ensure engine ventilation is
		sufficient to provide appropriate air movement through engine bay
FSRM		To avoid engine overheating the development teams shall ensure thermal system is designed such that there is sufficient air flow to cool engine components
FSRM		To avoid engine overheating the development team shall ensure proper mounting,
		installation, and manufacturing of thermal system and its components
FSRM		To avoid engine overheating the development team shall ensure thermal system bolts
1 biuti		and mounting hardware are securely fastened and free from potential loosening or
		unintended movement
FSRM		To avoid engine overheating the development team shall ensure the ECM controls and
FSKIN		mitigates engine overheating
FSRM		
FSKM	05.09	To avoid engine overheating the operator shall avoid poor driving behaviors
FSRM	05.10	To avoid engine overheating the engine temperature shall be displayed for operator to
		view in real-time
FSRM	05.11	To avoid engine overheating the vehicle shall provide feedback warning to operator
		when engine temperature exceed specified range
FSRM		The vehicle shall have fire extinguisher in event of thermal incident
FSRM	05.13	To avoid insufficient coolant levels the operator shall ensure proper coolant levels and
		check for leaks prior to operation
FSRM		To avoid thermal system pump failure the development team shall ensure proper
		mounting, installation, and manufacturing of water pump and its components
FSRM		To avoid thermal system pump failure the team shall ensure thermal system pump bolts,
FSKW		
		interface components (seals, gaskets), and mounting hardware are securely fastened and
		free from potential loosening or unintended movement
FSRM		To avoid thermal system pump failure the development team shall ensure the correct
		type of coolant is used, proper coolant levels, and check for leaks prior to operation
FSRM		To avoid thermal system pump failure the development team shall ensure thermal
		system belt drive components are properly installed (tensioning, torque specs
FSRM		To avoid radiator failure the development team shall ensure proper mounting,
		installation, and manufacturing of radiator, clamps, hoses and their components
FSRM	05.19	To avoid radiator failure the development team shall ensure radiator bolts, interface
		components (seals, gaskets), and mounting hardware are securely fastened and free
		from potential loosening or unintended movement
FSRM		To avoid radiator failure the development team shall ensure the correct type of coolant
		is used, proper coolant levels, and check for rust and leaks prior to operation
		· · · · · · · · · · · · · · · · · · ·

		FSRM05.21	To avoid hose failure the development team shall ensure proper mounting, installation,
			and manufacturing of hoses, clamps, and their components
		FSRM05.22	To avoid hose failure the development team shall ensure thermal system hose interface,
			and mounting hardware are securely fastened and free from potential loosening or
			unintended movement
		FSRM05.23	To avoid hose failure the development team shall ensure the correct type of coolant is
			used, proper coolant levels, and check for leaks prior to operation
		FSRM05.24	To avoid thermostat failure the development team shall ensure proper mounting,
			installation, and manufacturing of thermostat
		FSRM05.25	To avoid thermostat failure the development team shall ensure thermostat interface
			components and mounting hardware are securely fastened and free from potential
			loosening or unintended movement
		FSRM05.26	To avoid fan failure the development team shall ensure proper mounting, installation,
			and manufacturing of the thermal system fans and its components
		FSRM05.27	To avoid fan failure the development team shall ensure the thermal system fans bolts,
			interface components, and mounting hardware are securely fastened and free from
			potential loosening or unintended movement
		FSRM05.28	To avoid fan failure the development team shall ensure that the thermostat, fuse, fan
			wires, coolant level and fan clutch are functional
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGM06	The electric power steering system	FSRM06.01	To avoid contamination of the power steering fluid the development team shall ensure
	shall control lateral movement of the vehicle		proper mounting, installation, and manufacturing of EPS system hoses, clamps, and
			their components
		FSRM06.02	To avoid contamination of the power steering fluid the development team shall ensure
			EPS system interface components, and mounting hardware are securely fastened and
			free from potential loosening or unintended movement
		FSRM06.03	To avoid contamination of the power steering fluid the development team shall ensure
			EPS system functionality of pump and check for hose deterioration
		FSRM06.04	To avoid EPS system fluid leaks the development team shall ensure proper mounting,
			installation, and manufacturing of EPS system hoses, clamps, and their components
		FSRM06.05	installation, and manufacturing of EPS system hoses, clamps, and their components To avoid EPS system fluid leaks the development team shall ensure EPS system
		FSRM06.05	To avoid EPS system fluid leaks the development team shall ensure EPS system
		FSRM06.05	To avoid EPS system fluid leaks the development team shall ensure EPS system interface components (seals, gaskets), and mounting hardware are securely fastened and
			To avoid EPS system fluid leaks the development team shall ensure EPS system interface components (seals, gaskets), and mounting hardware are securely fastened and free from potential loosening or unintended movement
		FSRM06.05 FSRM06.06	To avoid EPS system fluid leaks the development team shall ensure EPS system interface components (seals, gaskets), and mounting hardware are securely fastened and free from potential loosening or unintended movement To avoid EPS system fluid leaks the operator shall ensure the correct type of EPS fluid
		FSRM06.06	To avoid EPS system fluid leaks the development team shall ensure EPS system interface components (seals, gaskets), and mounting hardware are securely fastened and free from potential loosening or unintended movement To avoid EPS system fluid leaks the operator shall ensure the correct type of EPS fluid is used, proper fluid levels, and check for leaks prior to operation
			To avoid EPS system fluid leaks the development team shall ensure EPS system interface components (seals, gaskets), and mounting hardware are securely fastened and free from potential loosening or unintended movement To avoid EPS system fluid leaks the operator shall ensure the correct type of EPS fluid is used, proper fluid levels, and check for leaks prior to operation To avoid EPS belt failure the development team shall ensure proper mounting,
		FSRM06.06	To avoid EPS system fluid leaks the development team shall ensure EPS system interface components (seals, gaskets), and mounting hardware are securely fastened and free from potential loosening or unintended movement To avoid EPS system fluid leaks the operator shall ensure the correct type of EPS fluid is used, proper fluid levels, and check for leaks prior to operation

		FSRM06.08	To avoid EPS belt failure the development team shall ensure EPS belt bolts, interface components, and mounting hardware are securely fastened and free from potential loosening or unintended movement
		FSRM06.09	To avoid EPS pump failure the development team shall ensure proper mounting, installation, and manufacturing of EPS pump and its components
		FSRM06.10	To avoid EPS pump failure the development team shall ensure EPS pump bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from potential loosening or movement
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGM07	The exhaust system shall safely assist in the removal of toxic gases, fumes	FSRM07.01	To avoid manifold failure the development team shall ensure proper mounting, installation, and manufacturing of intake manifold and its components
	and noise reduction	FSRM07.02	To avoid manifold failure the development team shall ensure manifold bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from leaks and potential loosening or unintended movement
		FSRM07.03	To avoid catalytic converter failure the development team shall ensure proper mounting, installation, and manufacturing of catalytic converter and its components
		FSRM07.04	To avoid catalytic converter failure the development team shall ensure catalysts bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from leaks and potential loosening or movement
		FSRM07.05	To avoid catalytic converter failure the development team shall ensure there are no leaky fuel injectors or engine misfires
		FSRM07.06	To avoid catalytic converter failure the development team shall ensure engine operates at correct A/F ratio (running lean causes excess heat damaging catalyst)
		FSRM07.07	To avoid catalytic converter failure the development team shall ensure proper functionality of exhaust gas recirculation (EGR) valve and O2 sensor
		FSRM07.08	To avoid catalytic converter failure the operator shall ensure manufacturer recommended oil changes
		FSRM07.09	To avoid catalytic converter failure the operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH
		FSRM07.10	To avoid exhaust system mounting failures the development team shall ensure proper mounting, installation, and manufacturing of the exhaust system and its components
		FSRM07.11	To avoid exhaust system mounting failures the development team shall ensure exhaust system bolts, interface components, and mounting hardware are securely fastened and free from leaks and potential loosening or unintended movement
		FSRM07.12	To avoid muffler failures the development team shall ensure proper mounting, installation, and manufacturing of muffler and its components

	1		
		FSRM07.13	To avoid muffler failures the development team shall ensure muffler bolts, interface
			components (seals, gaskets), and mounting hardware are securely fastened and free
			from leaks and potential loosening or unintended movement.
		FSRM07.14	To avoid exhaust system sensor failures the development team shall ensure proper
			mounting, installation, and manufacturing of O2 sensor
		FSRM07.15	To avoid exhaust system sensor failures the development team shall ensure O2 sensor
			bolts, interface components, and mounting hardware are securely fastened and free
			from leaks and potential loosening or unintended movement
		FSRM07.16	To avoid exhaust pipe failure the development team shall ensure proper mounting,
			installation, and manufacturing of the exhaust pip
		FSRM07.17	To avoid exhaust pipe failure the development team shall ensure exhaust pipe bolts,
			interface components (seals, gaskets), and mounting hardware are securely fastened and
			free from leaks and potential loosening or unintended movement
		FSRM07.18	To avoid exhaust pipe failure the development team shall ensure exhaust pipes are free
			from corrosion and physical damage
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGM08	The engine shall provide torque at the	FSRM08.01	To avoid improper engine lubrication the development team shall ensure proper
	request of the operator		mounting, installation, and manufacturing of the oil filter and pump
	I I I I I I I I I I I I I I I I I I I	FSRM08.02	To avoid improper engine lubrication the development team shall ensure oil filter and
			pump bolts, interface components (seals, gaskets), and mounting hardware are securely
			fastened and free from leaks and potential loosening or unintended movement
		FSRM08.03	To avoid improper engine lubrication the operator shall ensure frequent oil changes,
		1 514/100.05	clean oil, and that the oil filter is not ballooned or deformed
		FSRM08.04	To avoid improper fuel octane number the operator shall ensure proper fuel octane
			number prior to filling tank
		FSRM08.05	To avoid excessive engine heating the development team shall ensure thermal system
		1 510100.02	components (radiator, coolant level, fans) are functional and sufficient to cool the
			engine
		FSRM08.06	To avoid excessive engine heating the development team shall ensure the thermal
		1 511,100,00	system fans are free from potential physical damage
		FSRM08.07	To avoid excessive engine heating the development team shall ensure thermal system
		1 510100.07	fans pull air from a cool source
		FSRM08.08	To avoid excessive engine heating the development team shall ensure engine ventilation
		1 51(1100.00	is sufficient to provide appropriate air movement through engine bay
		FSRM08.09	To avoid excessive engine heating the development team shall ensure the thermal
		1.91/100.09	system is designed such that there is sufficient air flow to cool engine components
		FSRM08.10	To avoid excessive engine heating the development team shall ensure proper mounting,
		1.31/100.10	installation, and manufacturing of thermal system and its components
			I instantion, and manufacturing of thermal system and its components

SGM09		FSRM09.01	The engine and EM shall split the torque magnitude requested based on associated map
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
		1 51(100.25	exhaust gas recirculation (EGR) valve and O2 sensor
		FSRM08.25	To avoid EGR system failure the development team shall ensure proper functionality of
			potential loosening or unintended movement
		FSRM08.24	To avoid EGR system failure the development team shall ensure EGR system bolts, interface, and mounting hardware are securely fastened and free from leaks and
		ECDM09.24	installation, and manufacturing of EGR system and its components
		FSRM08.23	To avoid EGR system failure the development team shall ensure proper mounting,
			shall ensure proper vehicle operation (reduce engine speed/load)
		FSRM08.22	To avoid excessive load and improper driving leading to engine failure the operator
			EGR valve
		FSRM08.21	To avoid head gasket failure the development team shall ensure properly functioning
			timing belt
		FSRM08.20	To avoid head gasket failure the development team shall ensure properly functioning
			manifold gasket are free from cracks and physical damage
		FSRM08.19	To avoid head gasket failure the development team shall ensure vacuum lines and
		1.51(100.10	functioning O2 sensor
		FSRM08.18	To avoid head gasket failure the development team shall ensure proper A/F ratio and
			are securely fastened and free from leaks and potential loosening or unintended movement
			injection system valves, springs, bolts, interface components, and mounting hardware
		FSRM08.17	To avoid head gasket failure the development team shall ensure ECM, sparkplugs,
			installation, and manufacturing of the sparkplugs, fuel injectors, and air intake system
		FSRM08.16	To avoid head gasket failure the development team shall ensure proper mounting,
			functional
		FSRM08.15	To avoid head gasket failure the development team shall ensure the thermal system is
			potential loosening or unintended movement
			components and mounting hardware are securely fastened and free from leaks and
		FSRM08.14	To avoid head gasket failure the development team shall ensure head gasket
		1 510100.15	installation, and manufacturing of head gasket. intake manifold and its components
		FSRM08.13	To avoid head gasket failure the development team shall ensure proper mounting,
		F3KW00.12	and mitigates engine overheating
		FSRM08.12	To avoid excessive engine heating the development team shall ensure the ECM controls
			bolts and mounting hardware are securely fastened and free from potential loosening or unintended movement
		FSRM08.11	To avoid excessive engine heating the development team shall ensure thermal system

	The applied torque magnitude shall	FSRM09.02	The operator and HSC shall be responsible for torque request magnitude
	match the torque magnitude requested	FSRM09.03	The control algorithm shall be validated in SIL to match torque applied to torque requested
		FSRM09.04	The APPS shall be validated during zero velocity testing to match APPS applied to APPS requested
		FSRM09.05	The final torque output shall be validated in SIL, zero velocity, and under load during closed course testing
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGM10	The applied torque direction shall match the torque request intended	FSRM10.01	The EM/engine actuated torque direction shall be controlled by the HSC and PRNDL controls
	direction	FSRM10.02	The control algorithm shall validate torque direction during SIL
		FSRM10.03	Torque direction shall be validated during zero velocity testing
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGM11	The applied torque shall actuate at the time intended	FSRM11.01	The operator and HSC shall determine the timing of torque requested
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGM12	The motor shall provide torque at the request of the operator	FSRM12.01	The EM shall be hard mounted to the transmission
		FSRM12.02	The EM/transmission drivetrain system shall remain soft mounted
		FSRM12.03	The EM shall be properly modified to interface with the motor shaft exiting the transmission
		FSRM12.04	The EM shall monitor the temperature within that component
		FSRM12.05	The EM shall have a thermal control system
		FSRM12.06	To avoid over-current the development team shall ensure software (HSC) limits the magnitude of current to the EM
		FSRM12.07	To avoid over-current the development team shall ensure relays and fuses are in place
			and functional to prevent over drawing of current
		FSRM12.08	and functional to prevent over drawing of currentTo avoid contamination of the EM housing or EM coolant system the developmentteam shall ensure proper mounting, installation, and manufacturing of the EM andhousing

	mounting hardware are securely fastened and free from leaks and potential loosening or
	unintended movement
FSRM12	
	team shall ensure EM cooling system and its components are functioning, proper
	coolant levels, and hoses running to and from the motor are leak free
FSRM12	
	components (radiator, coolant level, fans) are functional and sufficient to cool the EM
FSRM12	
	are free from potential physical damage
FSRM12	
	pull air from a cool source
FSRM12	
	installation, and manufacturing of EM coolant system and its components
FSRM12	
	hoses and mounting hardware are securely fastened and free from potential loosening or
	unintended movement
FSRM12	.16 To avoid EM overheating the development team shall ensure the HSC controls and
	mitigates EM overheating
FSRM12	
	temperature display is visible by the operator
FSRM12	
	engine speed/load)
FSRM12	e
	development team shall ensure EM thermal system components (radiator, coolant level,
	fans) are functional and sufficient to cool the EM
FSRM12	0
	development team shall ensure EM bolts, hoses and mounting hardware are securely
	fastened and free from potential loosening or unintended movement
FSRM12	e
	development team shall ensure the HSC controls and mitigates EM overheating
FSRM12	.22 To avoid EM internal component failure the operator shall avoid adverse road
	conditions which may produce NVH
FSRM12	.23 To avoid EM internal component failure the development team shall ensure EM
	thermal system components (radiator, coolant level, fans) are functional and sufficient
	to cool the EM
FSRM12	.24 To avoid EM-driveshaft interface failure the development team shall ensure proper
	mounting, installation, and manufacturing of EM, driveshaft, and its interfacing
	components

		FSRM12.25	To avoid EM-driveshaft interface failure the development team shall ensure EM- driveshaft interface bolts and mounting hardware is securely fastened and free from potential loosening or unintended movement
		FSRM12.26	To avoid EM-driveshaft interface failure the development team shall ensure EM- driveshaft interface location is covered and free from potential unintended access or physical damage
		FSRM12.27	To avoid EM-driveshaft interface failure the development team shall ensure proper EM- driveshaft alignment
		FSRM12.28	To avoid EM-driveshaft interface failure the development team shall ensure EM- driveshaft interface angle is minimized
		FSRM12.29	To avoid EM-driveshaft interface failure the operator shall avoid adverse road conditions which may produce NVH
		FSRM12.30	To avoid EM-transmission failure the development team shall ensure proper mounting, installation, and manufacturing of EM, transmission, and its interfacing components
		FSRM12.31	To avoid EM-transmission failure the development team shall ensure EM-transmission interface bolts and mounting hardware are securely fastened and free from potential loosening or unintended movement
		FSRM12.32	To avoid EM-transmission failure the development team shall ensure EM-transmission interface location is covered and free from potential unintended access or physical damage
		FSRM12.33	To avoid EM-transmission failure the development team shall ensure proper EM- transmission alignment
		FSRM12.34	To avoid EM-transmission failure the operator shall avoid adverse road conditions which may produce NVH
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGM13	The current applied shall match the	FSRM13.01	The HSC shall request current from the ESS based on operator intent
	current necessary to meet EM torque request	FSRM13.02	EM current applied shall be validated during SIL
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGM14	The applied current direction shall match the direction necessary to meet the EM torque request and SOC	FSRM14.01	The operator, OBC, HSC, and SOC management strategy shall be responsible for charging and discharging
		FSRM14.02	SOC shall determine direction of current based on SOC management strategy
	requirement	FSRM14.03	The current direction shall be validated during SIL and zero velocity testing

SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGM15	The EM applied current shall actuate	FSRM15.01	The HSC shall request current from ESS at the time of the operators request
	at the time intended	FSRM15.02	The ESS shall deliver current at time Requested
		FSRM15.03	HSC shall validate current request timing during SIL and zero velocity testing
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGM16	The current applied shall not exceed	FSRM16.01	The ESS shall impose charging and discharging operating parameters
	max operating parameter	FSRM16.02	Charging and discharging operating parameters shall be validated during SIL and zero velocity testing
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGM17	The fuel system shall store and supply fuel to the engine	FSRM17.01	To avoid a fuel filter failure the development team shall ensure proper mounting, installation, and manufacturing of the fuel filter
		FSRM17.02	To avoid a fuel filter failure the development team shall ensure the permeable material is clean and the fuel filter is free of physical damage and leaks while under pressure
		FSRM17.03	To avoid fuel injection failure the development team shall ensure proper installation of the fuel injectors
		FSRM17.04	To avoid fuel injection failure the development team shall ensure fuel injector mounting hardware is securely fastened and free from potential loosening or unintended movement
		FSRM17.05	To avoid fuel injection failure the operator shall ensure adequate fuel level and type
		FSRM17.06	To avoid fuel injection failure the operator shall ensure use of fuel system cleaners when recommended
		FSRM17.07	To avoid fuel pump failure the development team shall ensure proper mounting and installation of fuel pump
		FSRM17.08	To avoid fuel pump failure the development team shall ensure fuel pump mounting hardware is securely fastened and free from potential loosening or unintended movement
		FSRM17.09	To avoid fuel pump failure the operator shall ensure adequate fuel level and type
		FSRM17.10	To avoid poor fuel quality the operator shall verify fuel quality prior to filling

SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGM18	The transmission shall transfer power	FSRM18.01	To avoid transmission fluid failure the development team shall ensure proper mounting,
	from the engine to the driveshaft		installation, and manufacturing of transmission and its components
		FSRM18.02	To avoid transmission fluid failure the development team shall ensure transmission
			bolts, interface components (seals, gaskets), and mounting hardware are securely
			fastened and free from potential loosening or unintended movement
		FSRM18.03	To avoid transmission fluid failure the operator shall ensure the correct type of coolant
			(ATF) is used, proper coolant levels, and check for leaks prior to operation
		FSRM18.04	To avoid transmission fluid failure the development team shall ensure belt drive
			components are properly installed (tensioning, torque specs)
		FSRM18.05	To avoid transmission overheating the development team shall ensure transmission
			thermal system components (radiator, coolant level, fans) are functional and sufficient
			to cool the transmission
		FSRM18.06	To avoid transmission overheating the development team shall ensure transmission
			thermal system fans are free from potential physical damage
		FSRM18.07	To avoid transmission overheating the development team shall ensure transmission
			thermal system fans pull air from a cool source
		FSRM18.08	To avoid transmission overheating the development team shall ensure proper mounting,
			installation, and manufacturing of transmission thermal system and its components
		FSRM18.09	To avoid transmission overheating the development team shall ensure transmission
			thermal system bolts, hoses and mounting hardware are securely fastened and free from
			potential loosening or unintended movement
		FSRM18.10	To avoid transmission overheating the development team shall ensure the TCM controls
			and mitigates transmission temperature
		FSRM18.11	To avoid transmission overheating the operator shall ensure proper vehicle operation
			(reduce engine speed/load)
		FSRM18.12	To avoid transmission-EM interface failure the development team shall ensure proper
			mounting, installation, and manufacturing of EM, transmission, and its interfacing
			components
		FSRM18.13	To avoid transmission-EM interface failure the development team shall ensure
			transmission-EM interface bolts and mounting hardware are securely fastened and free
			from potential loosening or unintended movement
		FSRM18.14	To avoid transmission-EM interface failure the development team shall ensure
			transmission-EM interface location is covered and free from potential unintended
			access or physical damage
		FSRM18.15	To avoid transmission-EM interface failure the development team shall ensure proper
			transmission-EM alignment

		FSRM18.16	To avoid transmission-EM interface failure the operator shall avoid adverse road conditions which may produce NVH
SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGM19	The vehicle body shall allow operator access to the vehicle, protect	FSRM19.01	To avoid a hood failure the development team shall ensure proper mounting, installation, and manufacturing of the hood, and latch
	components contained within the vehicle, prevent debris from being thrown by rotating tires, allow	FSRM19.02	To avoid a hood failure the development team shall ensure hood bolts, interface components, and mounting hardware are securely fastened and free from potential loosening or unintended movement
	operator to see in low light scenarios, protect operator from environmental	FSRM19.03	To avoid grill failure and restricted airflow to the radiator the development team shall ensure proper mounting, installation, and manufacturing of the grill
	debris, absorb impact of minor collisions, signal request to turn or brake, and allow the operator to have surrounding views	FSRM19.04	To avoid grill failure and restricted airflow to the radiator the development team shall ensure grill bolts, interface components, and mounting hardware are securely fastened and free from leaks and potential loosening or movement
		FSRM19.05	To avoid grill failure and restricted airflow to the radiator the operator shall ensure grill is free of clogging debris
		FSRM19.06	To avoid headlight or tail light failure the development team shall ensure proper mounting, installation, and manufacturing of head and tail lights
		FSRM19.07	To avoid headlight or tail light failure the operator shall ensure functionality of lights prior to use
		FSRM19.08	To avoid body panel, door, or window failure the development team shall ensure proper mounting, installation, and manufacturing of the body panels, windows, and doors
		FSRM19.09	To avoid body panel, door, or window failure the development team shall ensure body panels, doors, and window bolts, interface components, and mounting hardware are securely fastened and free from leaks and potential loosening or movement
		FSRM19.10	To avoid body panel, door, or window failure the operator shall ensure body panels, windows, and doors are free of physical damage prior to use
		FSRM19.11	To avoid body panel, door, or window failure the operator shall ensure window and door functionality prior to use

LIST OF ABBREVIATIONS

ACC	Adaptive Cruise Control
ADAS	Advanced Driver Assistance Systems
ADF	Automated Driving Function
APP	Accelerator Pedal Position
APPS	Accelerator Pedal Position Sensor
ASIL	Automotive Safety Integrity Level
AVTC	Advanced Vehicle Technology Competition
BMS	Battery Management System
CAVs	Connected and Automated Vehicles
CAE	Computer Aided Engineering
CAN	Controller Area Network
CSMS	Control Systems Modeling and Simulation
CSU	Colorado State University
D	Detectability
DAQ	Data Acquisition
DFMEA	Design Failure Mode and Effects Analysis
E/E	Electrical and or Electronic
EBCM	Electric Brake control Module
ECM	
ECM	Engine Control Module Electric Motor
EMC	Electric Motor Controller
EMC	
	Electromagnetic Interference
EPS	Electric Power Steering
ESS	Energy Storage System
FEA	Finite Element Analysis
FMEA	Failure Mode and Effects Analysis
FSR	Functional Safety Requirement
GM	General Motors
GPS	Global Positioning System
HARA	Hazard Analysis and Risk Assessment
HazOP	Hazard and Operability Study
HEV	Hybrid Electric Vehicle
HIL	Hardware in the Loop
HSC	Hybrid Supervisory Controller
HV	High-voltage
ISA	Integrated Safety Analysis
ISO	International Organization for Standardization
KDP	Key Decision Points
LKA	Lane Keeping Assist
MC	Mobility Challenge
MRR	Medium Range Radar
NASA	National Aeronautic and Space Administration

NN	Neural Network
NVH	Noise, Vibration, and Harshness
0	Occurrence
OBC	On-board Charger
OBD II	On-board Diagnostic
OEM	Original Equipment Manufacturer
PAE	Predictive Acceleration Event
PHA	Preliminary Hazard Analysis
PM	Project Manager
PRNDL	Park, Reverse, Neutral, Drive, Low
PSI	Propulsion Systems Integration
QM	Quality Managed
RISC	Risk Informed Safety Case
RPN	Risk Priority Number
S	Severity
SAE	Society of Automotive Engineers
SEFA	System Element Fault Analysis
SG	Safety Goal
SIL	Software in the Loop
SLFTA	System-level Fault Tree Analysis
SOC	State of Charge
SSM	System Safety Manager
STPA	System-Theoretic Process Analysis
TCM	Transmission Control Module
TVP	Test Vehicle Platform
UCA	Unsafe Control Action
V&V	Verification and Validation
V2X	Vehicle-to-X
VIT	vehicle Innovation Team
VTI	Vehicle Technical Inspection