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

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.

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

LIST OF TABLES

LIST OF FIGURES

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 ADFs 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.

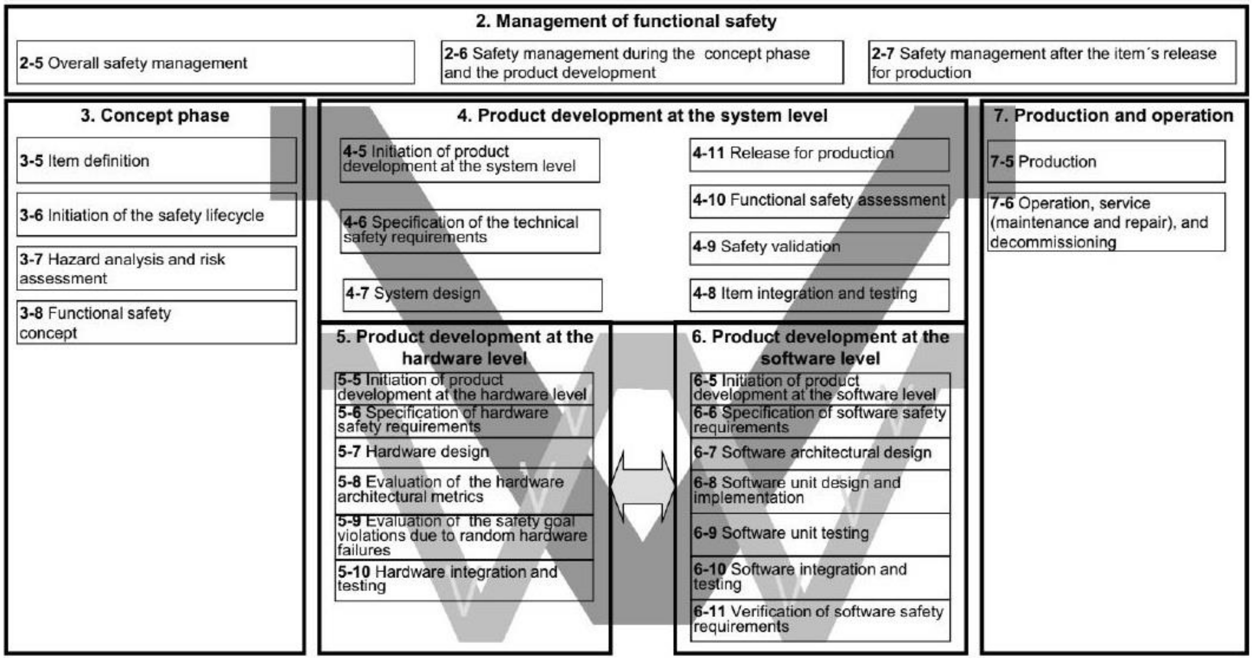


Figure 1. The management of functional safety throughout the product lifecycle [ISO 26262]

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 evaluation[2].

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].

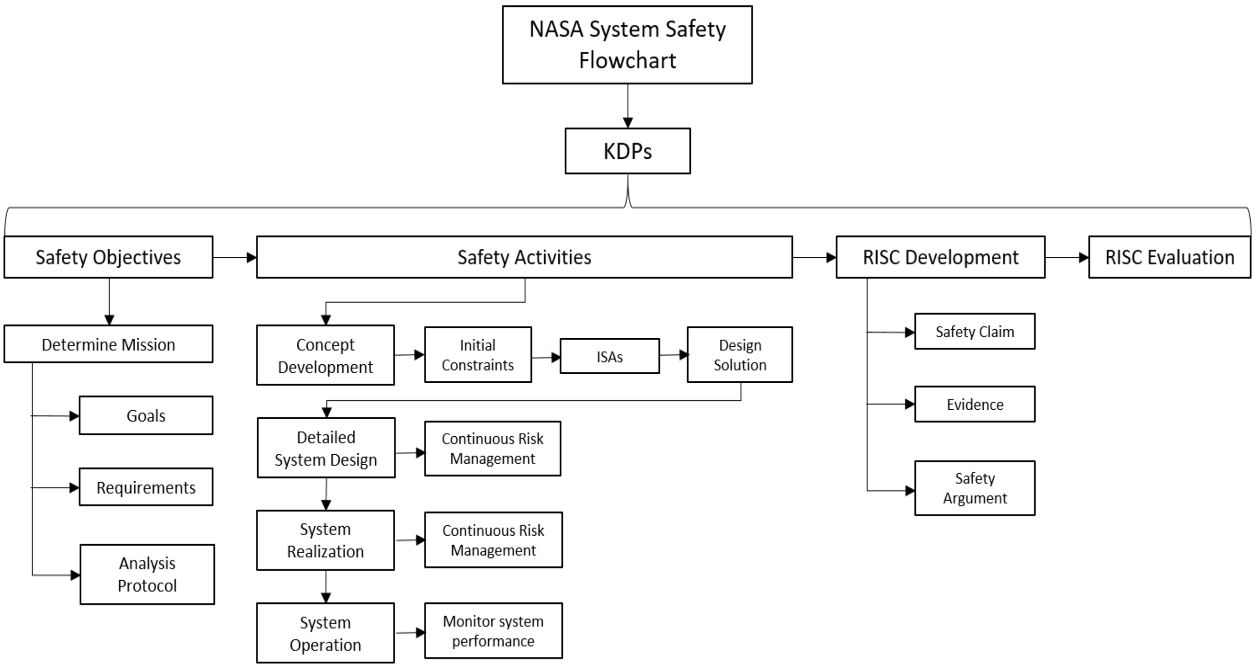


Figure 2. Overview of NASA system safety processes in flowchart format [NASA]

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.

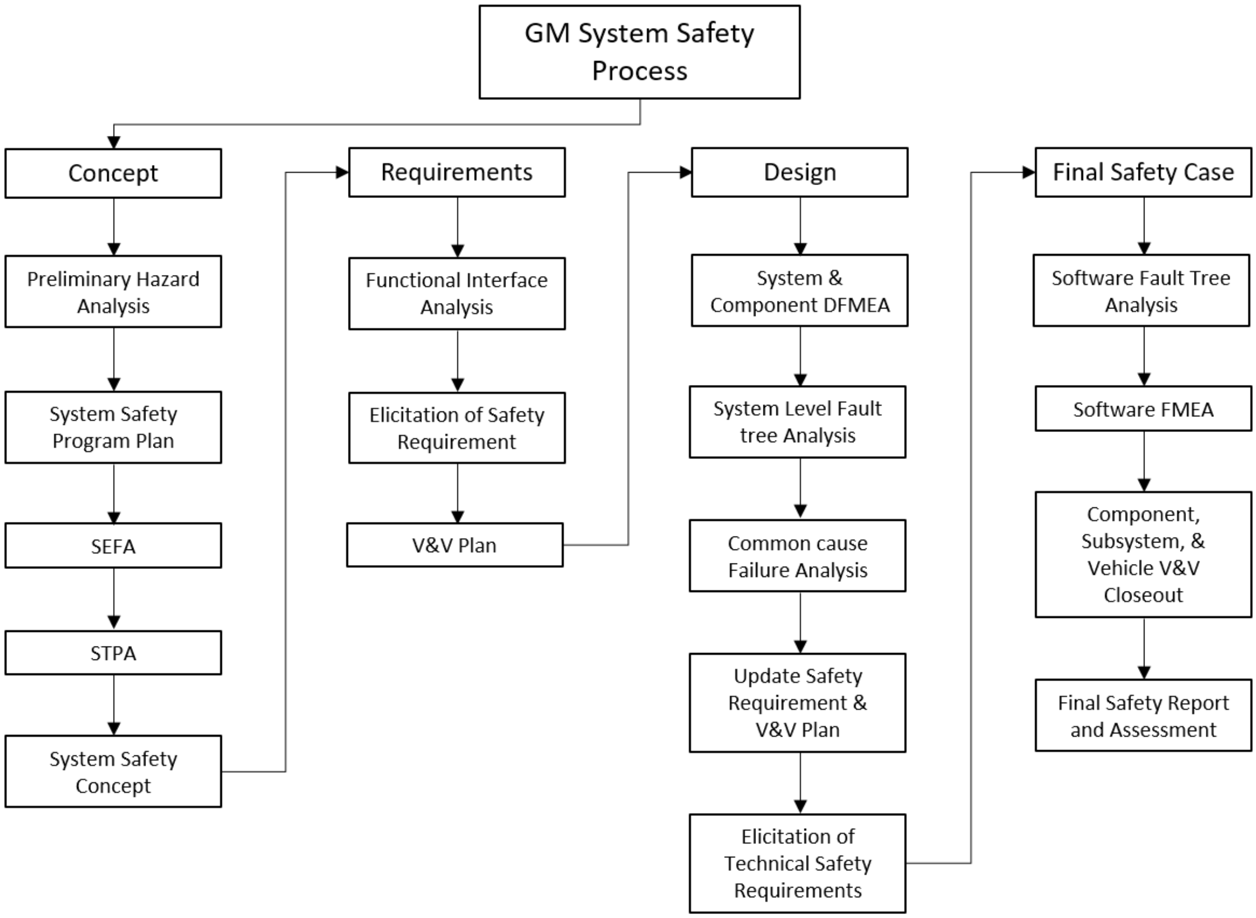


Figure 3. General Motors' System Safety Process [GM]

Key phases of the GM system safety process are:

1. 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.
2. 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.
4. 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.

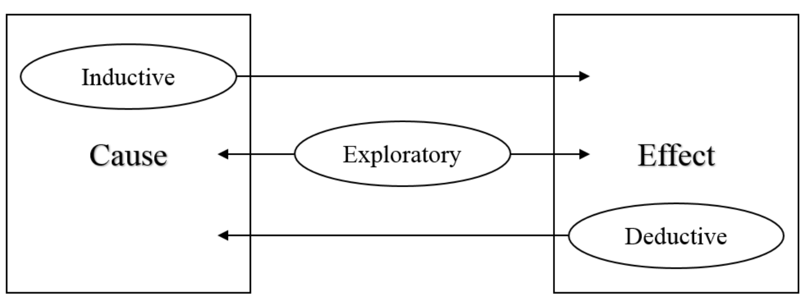


Figure 4. Relationship among cause and effect for various HARA techniques

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 controls-centric [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 high-voltage. 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.

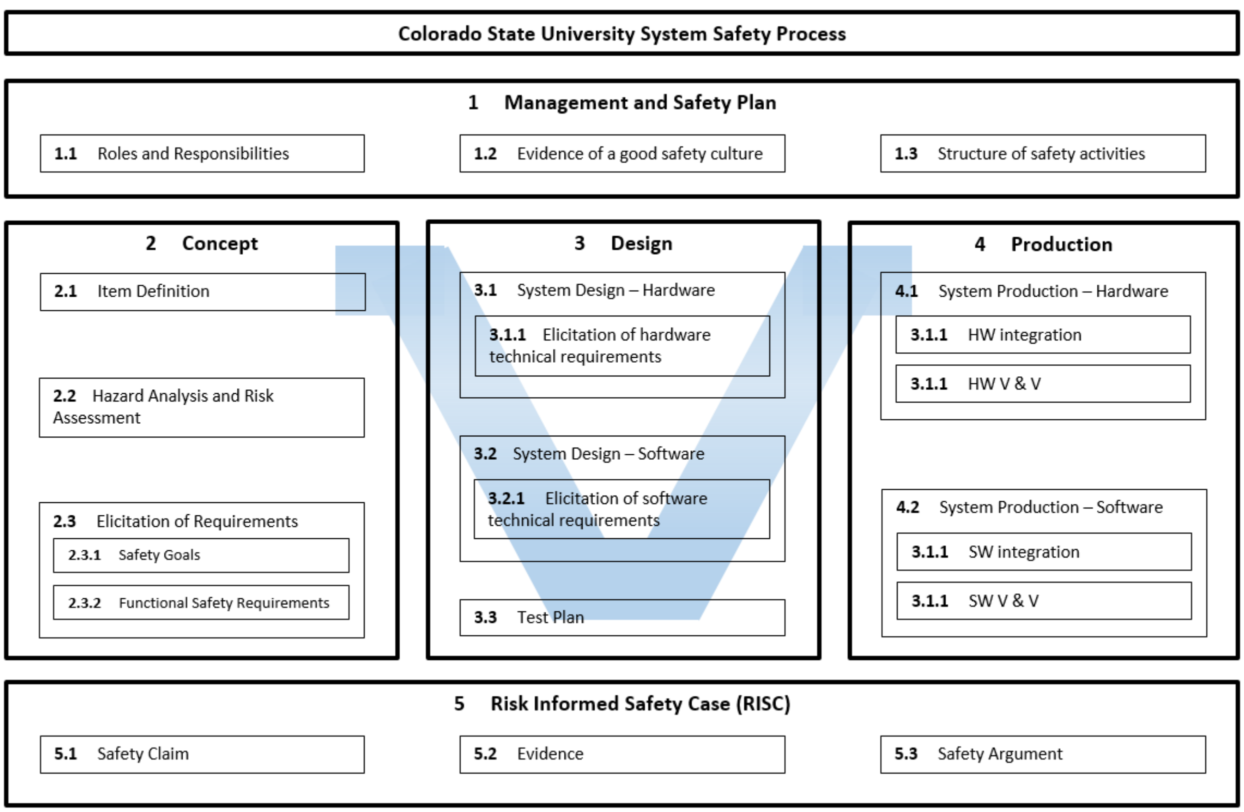


Figure 5. Colorado State University System Safety Process

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 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 sub-teams 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 cross-functional 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

Table 1. Example of "Roles and responsibilities"

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.

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 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 at 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.

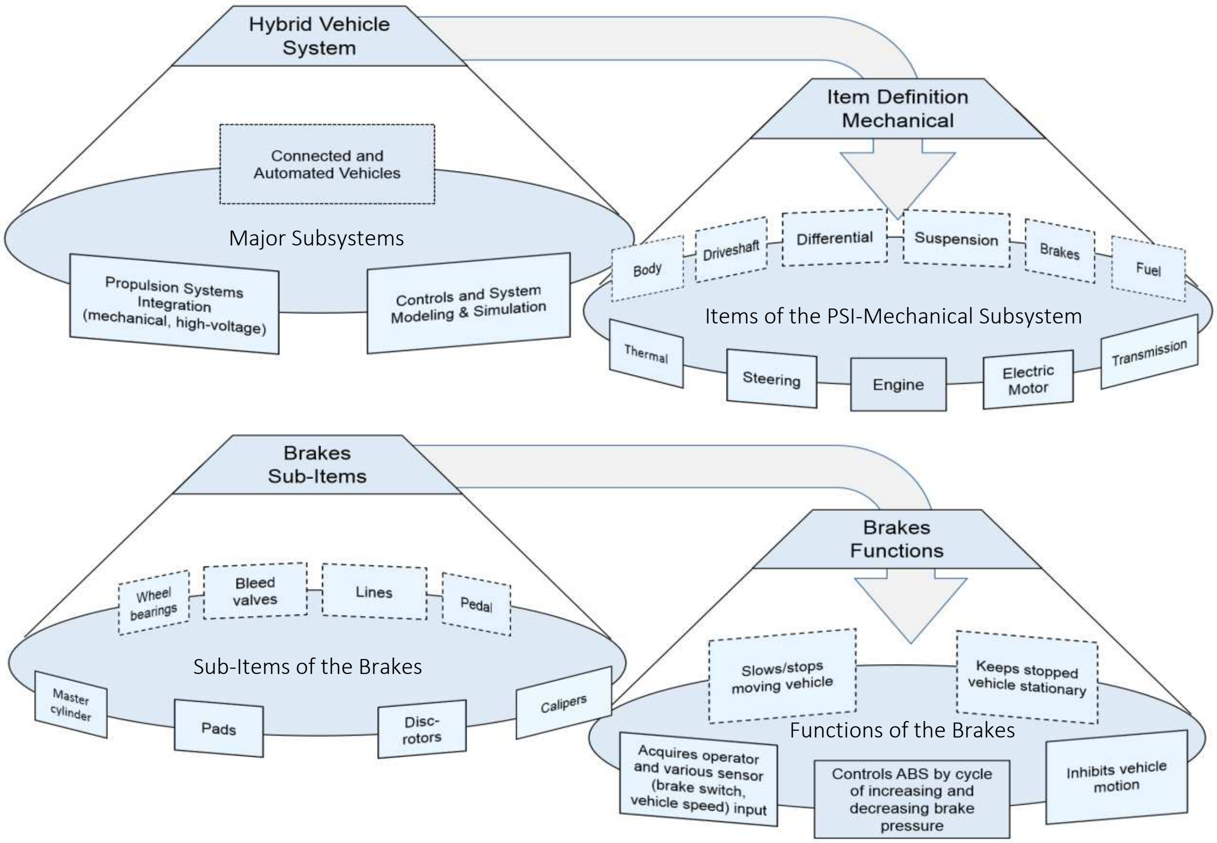


Figure 6. Flow chart describing a method for completing the Item Definition

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.

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

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

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 Mounts Wire 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

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 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 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

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**	**O**	**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]

Severity Rating Scale		
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.

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.

Table 10. Occurrence rating scale with descriptions and associated criteria [30]

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]

Detection Rating Scale		
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.

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.

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

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

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							
System:							
	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							

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

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

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

SEFA Applied to PSI Subsystem							
System: PSI Subsystem							
Item No.	**Multiple Range Operating Scenario (P,R,N,D)**	**Item Functions**	**Item No. Operating States** 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

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 include:

- Unintended longitudinal or lateral motion,
- Loss or degradation of propulsion,
- Operator and/or passenger injury,

- 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 mitigation method using correct verbiage. Table 16 describes an example of part 2 of the SEFA template as a continuation from Table 15 above.

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

SEFA Applied to the PSI Subsystem					
Item No.	**Potential Safety Hazard**	**Diagnostic Method**	**Mitigation Method**	**System State After Mitigation**	**Safety Requirement**
2 Motor	Unintended longitudinal motion (deceleration) Unintended exposure to high-voltage Damage and/or injury to passenger/ personnel	OBD II & CAN diagnostics will provide motor temperature, current to and from, torque, and speed Vehicle technical inspection will identify leaks and physical damage to motor Operator would become aware during operation (sound, throttle response, smell, visual indicators such as smoke)	Provide real time feedback to operator of motor state (current, torque, temp, speed) Actuate motor thermal controls when motor temperature range exceeds specified limits Actuate motor speed and torque governor when motor speed and torque exceed specified limits Actuate EMC current governor via HSC when motor, battery pack, or EMC exceeds specified current limits Allow operator override to discontinue motor operation	Vehicle would be capable of normal functionality If emergency motor shut off occurs the vehicle will be capable of normal operations (P,R,N,D) with partial 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-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 To prevent motor failure the operator shall be provided real-time diagnostics and have the capability to discontinue motor operations

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.

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

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

Table 18. Template used to perform the HazOP

HazOP Template					
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.

Table 19. Key process parameters and their associated systems

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 (maintenance, overheat, EMI)	Clearance (maintenance, overheat, EMI)	Signal Bandwidth	Signal Latency
Deceleration			Signal Latency	Logic faults
Current	Unauthorized Access		Logic faults	Storage
Clearance (maintenance, overheat, EMI)	Voltage		Storage	Algorithm faults
			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.

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

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

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.

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

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

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					
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.
4. The LKA computer performs sensor fusion data verification & validation using developed algorithms and NNs.
5. 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.

Table 23. Example of a STPA on the LKA system

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)

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 requirement-specific 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.

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

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

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 on-board 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.

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

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 DFMEA & STPA	**ACC analysis** 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.

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

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, visual, audio)	FSRA07.03	The ACC system shall alert operator when deviation from set distance or velocity occurs
		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)

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.

Table 31. Example of the CAVs safety goals and 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 algorithms and NNs	FSRC01.06	The development team shall ensure the Intel Tank computer only makes corrective action decisions when fidelity of image meets minimum specified resolution
		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	The Bosch Front, Rear, and Corner MRR Radars shall safely perform early front, rear, and corner speed detection	FSRC03.19	To reduce radar signal noise the development team shall ensure the use of wire shielding and conduit
		FSRC03.27	The development team shall ensure the integrated program accounts for radar horizontal field of view and elevation (±6° (160m), ±6°(100m), ±10°(60m), ±25°(36m), ±42°(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

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.

Table 32. Example of the CSMS safety goals

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 associated 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) - 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 can be found in Appendix 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.

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

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

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.

Table 36. Example of the PSI-Mechanical safety goals

PSI Mechanical Safety Goals	
SG No.	**Safety Goal**
SGM03	The suspension system shall safely support the vehicle weight and absorb/reduce excess energy from road shock
SGM04	The braking system shall inhibit vehicle motion, slow or stop a vehicle in motion, and keep stationary vehicles stopped
SGM05	The thermal system shall detect and control cabin and component temperatures
SGM07	The exhaust system shall safely assist in the removal of toxic gases, fumes and noise reduction
SGM09	The applied torque magnitude shall match the torque magnitude requested
SGM16	The current applied to the EM shall not exceed maximum operating parameter

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.

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

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 cross-functional 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.

1. 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

[1] 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.

[3] 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/ai-adoption-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.

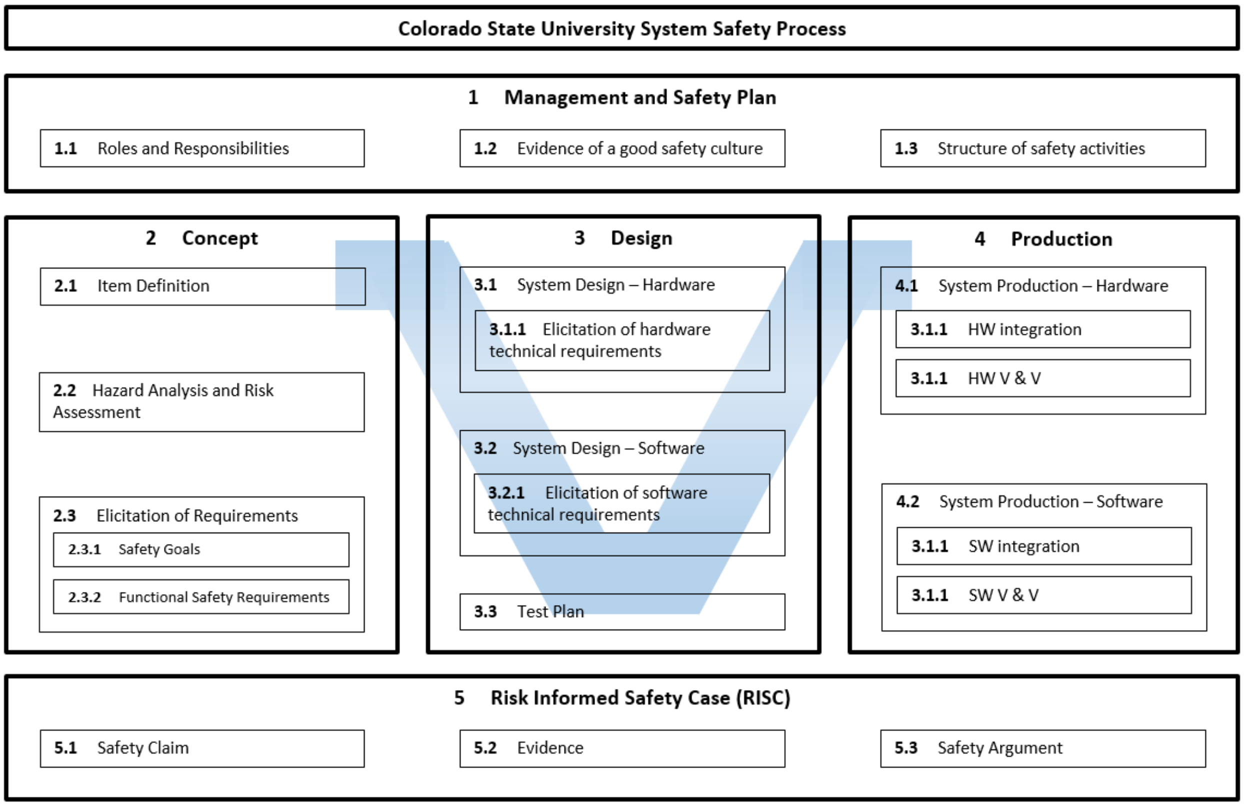
[28] Z. Asher, J. Tunnell, D. Baker, R. Fitzgerald, D. Banaei-Kashani, S. Pasricha and T. Bradley, "Enabling Prediction for Optimal Fuel Economy Vehicle Control," in *SAE World Congress Experience*, Pontiac, 2018.

[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 1 Management of Functional Safety – Complete Documentation

Appendix 1.1 Safety Activities throughout the System Safety Lifecycle



Appendix 1.2 Cross-Functional Safety Procedure

Cross-Functional Safety Procedure

Specific to the EcoCAR Mobility Challenge

Colorado State University

System Safety Manager Matthew D Knopf

CSMS Primary Safety Representative, Grant Moore

CSMS Secondary Safety Representative, Nikki Machado

CAVS Primary Safety Representative, Hein Thant

CAVS Secondary Safety Representative, Haoying Wang

PSI Primary Safety Representative, Wesley Martin

PSI Secondary Safety Representative, Benjamin McKenney

Table of Contents

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:		
Role	**Member**	**Responsibilities**

Table 2.2 Example of Roles and Responsibilities

Team: Management		
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.

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

Table 3.1 Example of Item Definition of the Mechanical System

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

Item and sub-item can be tricky when thinking about CAVS and CSMS systems. Is the item an actual controller, a piece of software, a control strategy? Think through this and do what makes most sense. Be able to defend your response if asked about it

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". That will help fill this out accurately

4

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

Item:					
Potential Hazard	**Cause**	**Major Effect**	**Severity**	**Corrective/Preventative Measures**	**Requirement**

Table 4.1 PHA example

Item: Brakes					
Potential Hazard	**Cause**	**Major Effect**	**Severity**	**Corrective/Preventative Measures**	**Requirement**
Brakes fail to Inhibit vehicle motion. Brakes fail to slow/stop moving vehicle Brakes fail to keep stopped vehicle stationary	Brake pad fatigue or failure (overheating, corrosion)	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)		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 for rust and corrosion Avoid poor drive behavior	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 Operator shall perform routine inspection of brake system to check for rust, fatigue, and corrosion Operator shall avoid poor driving behaviors

This is the failure of the function from the item definition

Don't do this part

Use similar verbiage and make it sound professional. This will nearly copy and paste into requirements

This is sort of the end goal of the analysis. Use similar verbiage and make it sound professional.

6

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

Table 4.2 SEFA template part 1

Team: CAVS												
			Item Operating States									
Item No.	**Operating Scenario (P,R,N,D)**	**Item Functions**	ECM	HSC							**Impact of Item Fault**	**Immediate Resulting State**
CAVS01	ECM											
CAVS02	HSC											

Taken from functions in item definition

Table 4.3 SEFA template part 2

Item No.	Potential Safety Hazard	Diagnostic Method	Mitigation Method	System State After Mitigation	Safety Requirement
CAVS01					
CAVS02					

Same description as effects from PHA. Verbiage includes things like unintended acceleration… loss of… damage to…

How is the fault identified?

What can be done to prevent the fault? Do this part well and it will copy and paste into requirements.

This is the end goal. Use correct verbiage. This will be very similar to the mitigation method.

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

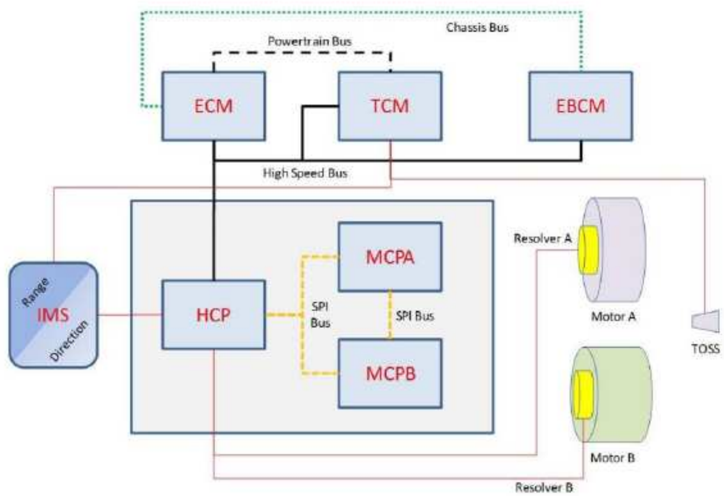


Figure 1. Hybrid Propulsion System Architecture [2]

9

Step 2. Fill out SEFA template

			PRIMARY Fault					RESULTING Fault							
Item Number	**Multiple Ranges (P,R,N,D)**	**Function(s)** **(Responsibilities)**	ECM	HCP	MCP1	MCP2	TCM	EBCM	Direction IMS	Range IMS	TOSS	MotorA Resolver	MotorB Resolver	**Impact of Element Fault** (Impact prior to any remedial or mitigation actions)	**Immediate Resulting State** (State of the system prior to any remedial or mitigation actions)
	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	0	1	1	1	1	1	0	1	1	1	1	Engine not available or shuts <OFF>	Park - Park Reverse - Reverse Neutral - Neutral Drive - Possible Acceleration
2	HCP	* 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 - Reverse Neutral - Neutral 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 - Possible Decel Neutral - No Issue 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 - Possible Accel Neutral - No Issue Drive - Possible Deceleration

10

Item 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	HCP	**Unintended Propulsion <OR> Unintended Direction**	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**	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 transition 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**	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 transition 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

Item: STPA for Lane Keeping Assist					
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

STPA example of Lane Keeping Assist (LKA) System

Step 1. Create Block Diagram

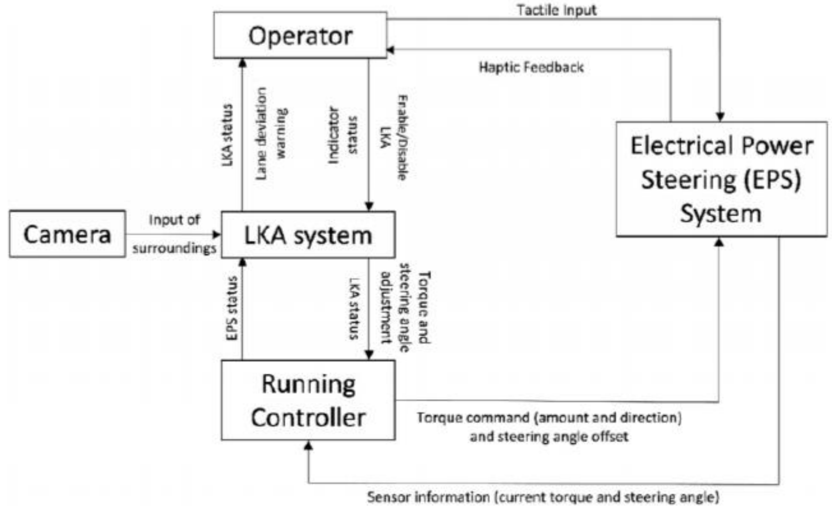


Figure 1. Block diagram of LKA system [3]

Step 2. Fill out STPA template

Table 4.5 STPA example of LKA system [3]

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

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

Table 4.7 HazOP Template

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

Table 4.8 Mechanical Process Parameter and Guide Word Combination Chart Example

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

Table 4.9 HazOP of the Mechanical System Example

FUNCTION: Apply Torque Stimuli to EM					
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

Item: Brakes											
No.	**Function**	**Failure Type**	**Potential Impact**	**S**	**Potential causes**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Requirement**

Table 4.11 FMEA of the Mechanical System Example

Item: Brakes											
No.	**Function**	**Failure Type**	**Potential Impact**	**S**	**Potential causes**	**O**	**Prevention Mode**	**Detection 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 for rust and corrosion Avoid poor drive behavior	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 Operator shall perform routine inspection of brake system to check for rust, fatigue, and corrosion Operator shall avoid poor driving behaviors

18

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

Table 5.1 Example of Mechanical Safety Goals and Functional Safety Requirements

Mechanical			
SG No.	**Safety Goal**	**FSR No.**	**Functional Safety Requirement**
SGM01	The driveshaft shall transmit torque from the engine and/or EM to the rear of the vehicle	FSRM01.01	To avoid driveshaft-EM interface failure the development team shall ensure proper mounting, installation, and manufacturing of modified driveshaft and its components
		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 team shall ensure driveshaft manufacturing and use of materials is sufficient to prevent unintended access and physical damage

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

Appendix 1.3 Roles and Responsibilities

Management of Functional Safety Roles and Responsibilities		
Team: Management		
Role	**Member**	**Responsibilities**
Faculty Advisors	Dr. Thomas Bradley Dr. Brett Windom Dr. Jason Quinn	Oversee high-level mission activities and operate in a supervisory capacity. Define project scope, and manage requirements, planning, schedule, 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		
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		
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 Grady Egan Jesus Rodriguez Michael Gaffney	Provide technical support for mechanical team functions

Appendix 1.4 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 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 1.6 Evidence 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 2 Item 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 - Fuses - Mount - Sensor fusion algorithms and NNs - Computers	- Blends various sensors (cameras, radars) data to achieve reliable, high-definition images - Performs sensor fusion data verification & validation using developed algorithms and NNs - Determines if control action (EPS torque, braking, feedback) is required - Sends control action request to associated controller - Provides real-time functionalities
Intel Mobileye 6	- Mount - - Wires - Eye-Watch Display - Sensor	- Performs multi-feature tracking - Performs object and lane detection - Performs forward collision warning - Performs pedestrian collision warning - Performs headway warning - Performs traffic sign recognition - Sends data to associated controller - Provides a real-time display
Bosch Front and Rear Radar	- CAN bus - Mount - Radar	- Performs early front and rear speed detection - Performs early front and rear position detection - Sends data to associated controller
Bosch MRR Corner Radar x2	- CAN bus - Mount - Radar	- Performs early corner speed detection - Performs early corner position detection - Sends data to associated controller
12 V CAVs Power Supply	- Wires - Fuse - Battery	- Powers all CAVs components
Intel Movidius Neural Compute Stick	- USB plug - Sensor fusion algorithms - NNs	- Performs vision processing tasks in assistance to Intel Tank computational capabilities - 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 - Mount - Camera	- Performs real-time monitoring of operator - Sends data to associated controller
CAVs real-time display	- Wires - Mount - Display	- Acquires sensor fusion images from associated controller - Displays sensors fusion images in real-time
ZED Camera	- USB cable - Mount - Camera	- Performs high-resolution depth perception - Performs 6-axis positional tracking to sense space and motion - Performs large-scale 3D mapping
GPS module	- Wires - Mount	- Receives GPS data - 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 - Mounts - Line - Controller	- Controls engine torque output - Controls engine temperature - Controls A/F ratio - Controls idle speed - Controls electronic valve
TCM	- Connectors - Mounts - Line - Controller	- Receives inputs from HSC, ECM, and various sensors (vehicle speed, wheel speed, throttle position) - Controls gear shifting - Monitors and regulates transmission thermal control system
EMC	- Connectors - Mounts - Line - Controller	- Regulates supply of current to EM - Convert DC to AC - Controls direction of current - Monitor and regulates EM temperature
BCM	- Connectors - Mounts - Line - Controller	- Powers auxiliary low-voltage systems to include power windows, power mirrors, and air conditioning
EBCM	- Connectors - -Mounts - Line - Controller	- Acquires operator and various sensor (wheel speed, brake switch) inputs - Actuates and controls the automatic braking system by a cycle of increasing and decreasing brake pressure
BMS	- Connectors - Mounts - Line - Controller	- Ensure safe ESS operating conditions - Monitor ESS state (voltage, temperature, SOC, and current) - 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 - Mount	- 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
Low Voltage	- Air bag - Windshield wipers - Instrument cluster - Lights - Entertainment system - Turn signals - Security system - Keyless entry - Power windows - Power mirrors - Power locks - Pumps - Fans - DAQ	- 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
OBC	- Connectors - Mounts - Line - Controller	- Controls charging to the HV battery pack

OBD II	- Connectors - Mounts - Line - Controller	- Provides list of vehicle parameters to monitor
CAN bus	- Wiring harness - Controllers	- 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	- Module - Lines - Mounts	- 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 - U joint - Shaft - Bearings - Clamps - Rings - Axle beam - Steering knuckle - Rods - Brake drum	- Longitudinal shaft which transmits torque from engine/transmission to rear of vehicle

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

Steering	- Wheel - Gearbox - Arms/rods - Column - Pump - Fluid reservoir - Lines	- Controls lateral movement of the vehicle
Exhaust	- Catalysts - Muffler - Tubing - Manifold - Sensors - Hanger/clamps	- Removal of toxic gases/fumes and noise
Engine	- -Cylinder head cover - 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	- Provide torque at request of operator

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

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

Appendix 3 HARA – Complete Documentation

Appendix 3.01 HARA CAVs / CSMS ACC DFMEA

CAVs / CSMS ACC DFMEA

Function	Failure Type	Potential Impact	S	Potential Cause	O	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 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 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
				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	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**	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 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 Operator aware during operation by identifying vehicle NVH	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 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,	Operator aware during operation by	5	**100**	ACC brake system shall engage in timely manner such that brake

						installation, and routine maintenance and inspection of hardware and its functionality Ensure bolts and mounting hardware is securely fastened and free from potential loosening or unintended movement	identification of degrading performance Vehicle technical inspection will identify leaks			lines are immediately able to be actuated Development team shall ensure proper bleeding, mounting, installation, and routine maintenance and inspection of 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						ACC system shall allow operator to override automated controls with minimal braking engagement
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional 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 recommended	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	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

				Engine failure - Poor fuel quality	2	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
				Engine failure - 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 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
				Engine failure - Improper fuel octane number	1	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

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

						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				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

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

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

						produce NVH and damage EM-driveshaft interface				
				EM-transmission 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 EM-transmission interface location is covered and free from potential unintended access or physical damage Ensure proper EM-	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	**720**	Development team shall ensure proper mounting, installation, and manufacturing of EM, transmission, and its interfacing components Development team shall ensure EM-transmission bolts and mounting hardware is securely fastened and free from potential loosening or unintended movement Development team shall ensure EM-transmission interface location is covered and free from potential unintended access or physical damage Development team shall ensure proper EM-transmission alignment Operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH

						transmission alignment Avoid adverse road conditions which may produce NVH and damage EM-transmission interface				
				Accelerator Pedal (AP) and/or Accelerator Pedal Position Sensor (APPS) failure	3	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
				Other						ACC system shall allow operator to override automated controls with minimal AP engagement

Function	Failure Type	Potential Impact	S	Potential Cause	O	Prevention Mode	Detection Mode	D	RPN	Functional Requirement
Sensors observe surrounding traffic/object distance, velocity, size and position to include operator engagement	Failure of sensors to observe surrounding traffic/object distance, velocity, size and position to include operator engagement	Unintended longitudinal motion ACC system shutdown	5	Wiring and/or signal failure (not proper gauge, installation or manufacturing failure) Power failure Communication 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	Vehicle technical inspection will identify wiring fatigue or failure Operator aware during operation by identifying eventual failure of vehicle components	4	**100**	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 ACC system shall alert operator prior to and when shutdown occurs ACC system shall only be operational if sensor performance meets a minimum standard (communication speed, sensor availability or visibility) ACC communications shall operate independently and be free from external manipulation
				Unintended access and physical damage (debris, puncture)	7	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 Operator aware during	4	**140**	Development team shall ensure sensor enclosure manufacturing and use of materials is sufficient to prevent unintended access and physical damage

						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

Function	Failure Type	Potential Impact	S	Potential Cause	O	Prevention Mode	Detection Mode	D	RPN	Functional Requirement
										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)
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional Requirement**
Sensor data transmits to controller	Failure of sensor data transmission to controller	Unintended longitudinal motion ACC system shutdown	3	Wiring and/or signal failure (not proper gauge, installation or manufacturing failure) Power failure Communication failure	3	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	3	**27**	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 ACC system shall alert operator prior to and when shutdown occurs ACC system shall only be operational if sensor performance meets a minimum standard (communication speed, sensor availability or visibility)

										ACC communications shall operate independently and be free from external manipulation (malicious intrusion, EMI)
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional 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
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional Requirement**
Operator sets separation distance constraint	Failure of operator to set separation distance constraint	ACC system shutdown	1	Operator unaware of responsibility to set distance constraint	10	Ensure system provides warning to operator that distance input constraint is required	N/A	1	**10**	ACC system shall provide warning to operator that distance input constraint is required The ACC system shall operate within a specified distance range
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional Requirement**
ACC provides feedback to the operator (ACC status, haptic, visual, audio)	Failure for ACC to provide feedback to the operator (ACC status,	Unintended longitudinal motion ACC system shutdown	9	Wiring and/or signal failure (not proper gauge, installation or	6	Ensure wiring is securely installed using manufacturer installation specifications	Vehicle technical inspection will identify wiring, audio, or visual	1	**54**	The ACC sensors shall be wired and installed according to manufacturer specifications to include bend radii, heat

	haptic, visual, audio)	Operator unaware of potential hazard		manufacturing failure) Power failure Communication failure Audio or visual system failure		Ensure wiring gauge is sufficient to carry max operational current with factor of safety Ensure wire bend radii are adhered to Ensure ACC alters operator when deviation from set distance or velocity occurs Ensure ACC system alerts operator prior to and when shutdown occurs Ensure ACC system provides audio, visual, and haptic feedback Ensure ACC system provides feedback in manner that does not startle the operator and cause greater	fatigue or failure Operator aware during operation by identifying eventual failure of vehicle functions			shielding, EMI avoidance, sheathing, proper gauge, and interface connections ACC system shall alert operator prior to and when shutdown occurs ACC system shall alert operator when deviation from set distance or velocity occurs ACC feedback system shall function according to operator engagement ACC system shall provide audio, visual, and haptic feedback ACC system shall provide feedback in manner that does not startle the operator and cause greater potential for hazard (not overly loud or bright) ACC system audio feedback shall adjust to ambient volume (stereo system, excessive cabin noise) ACC system visual 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										
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional Requirement**
Controls lateral movement via EBCM	Failure to control lateral movement via brakes	Unintended lateral motion Operator and/or passenger injury	10	Wiring and/or signal failure (not proper gauge, installation or manufacturing failure)	7	Ensure wiring is securely installed using manufacturer installation specifications	Vehicle technical inspection will identify wiring fatigue or failure Operator aware during operation	8	**560**	The LKA system shall be wired and installed according to manufacturer specifications to include bend radii, heat shielding, EMI

		Damage to or loss of property Damage to environment				Ensure wire bend radii are adhered to	by identifying eventual failure of vehicle components			avoidance, sheathing, proper gauge, and interface connections
				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 for rust and corrosion Avoid poor driving behaviors	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 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	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 (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

							Operator aware during 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 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
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional Requirement**
Controls lateral movement via EPS	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	**30**	Development team shall ensure proper mounting, installation, and manufacturing of EPS hoses, clamps, and their components Development team shall 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 deterioration	discolored steering fluid Increased friction and interference with hydraulic characteristics.			(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
				Power steering low fluid and fluid leaks	2	Ensure proper mounting, installation, and manufacturing of hoses, clamps, and their components Ensure interface components (seals, gaskets), and mounting hardware are	Vehicle technical inspection will identify low fluid level, and leaks Operator aware during operation by identifying a loss in steering functionality	3	**60**	Development team shall ensure proper mounting, installation, and manufacturing of EPS hoses, clamps, and their components Development team shall ensure interface components (seals, gaskets), and mounting hardware are securely fastened

						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				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
				Broken belt which energizes power steering pump	3	Ensure proper mounting, installation, and manufacturing of the belt (tension, torque specs) and its components Ensure bolts, interface components, and mounting hardware are securely fastened and	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 belt (tension, torque specs) and its components The development teams hall ensure bolts, interface components, and mounting hardware are securely fastened and free from potential

						free from potential loosening or unintended movement				loosening or unintended movement
				Pump failure	2	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 movement	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**	Development team shall ensure proper mounting, installation, and manufacturing of pump and its components Development 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	Ensure proper mounting, installation, and manufacturing of power	Operator aware during operation by identifying a loss in	8	**160**	Development team shall ensure proper mounting, installation, and manufacturing of power steering

						steering system and its components Ensure bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from potential loosening or movement Ensure operator drives appropriately to prevent damage to steering rack Ensure power steering motor is functional	steering functionality			system and its components Development team shall ensure bolts, interface components (seals, gaskets), 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 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 inspection will identify wiring fatigue or failure	8	**560**	The LKA system shall be wired and installed according to manufacturer specifications to

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

										Development team shall impose criteria for deviation and corrective action
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional Requirement**
LKA sensors transmit data to associated controller	Failure of LKA sensors transmit data to associated controller	Unintended lateral motion LKA system shutdown	6	Wiring and/or signal failure (not proper gauge, installation or manufacturing failure) Power failure Communication 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	Vehicle technical inspection will identify wiring fatigue or failure Operator aware during operation by identifying eventual failure of vehicle components	4	**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 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 manipulation
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**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 operator
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional 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	Wiring and/or signal failure (not proper gauge, installation or manufacturing failure) Power failure Communication failure Audio 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 from set distance or velocity occurs Ensure LKA system alerts operator prior to and when shutdown occurs Ensure LKA system provides audio, visual, and haptic feedback Ensure LKA system provides feedback in manner that does not startle the operator and cause greater potential for hazard (not overly loud or bright) Ensure LKA system audio and visual feedback adjust to ambient volume and light				LKA feedback system shall function according to operator engagement LKA system shall provide audio, visual, and haptic feedback LKA system shall provide feedback in manner that does not startle the operator and cause greater potential for hazard (not overly loud or bright) LKA system audio feedback shall adjust to ambient volume (stereo system, excessive cabin noise) LKA system visual feedback shall adjust to ambient light (decrease during night, increase during day) LKA system shall 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 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 but unaware of how to initiate Wiring failure Operating system failure	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) 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	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) Wiring shall be securely installed according to manufacturer specifications to include EMI avoidance, connections, gauge, and bend radii

					If LKA operating system fails, the LKA system shall alert the operator via audio and visual feedback
	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) To prevent accidental disabling of the LKA system, the LKA system will have individual on/off buttons	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 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

					The operator shall be allowed to choose when LKA system will be 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 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

					If LKA operating system fails, the LKA system shall alert the operator via audio and visual feedback
	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	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 Function	**Unsafe Control Action**	**Potential Hazard**	**Causal Factors**	**Prevention/Mitigation**	**Functional Requirement**
Sensors send data to associated computer	Required but not provided	LKA system is disabled	Wiring failure Signal corruption Power failure	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)
	Provided but not required	LKA system enabled when operator believes it is disabled Unintended lateral movement	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

		LKA system engages in correct control actions to the operators surprise			
	Provided but incorrect timing	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) 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	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 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
Control Function	**Unsafe Control Action**	**Potential Hazard**	**Causal Factors**	**Prevention/Mitigation**	**Functional Requirement**

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

				Ensure computer installation is inside cabin in a dry debris-proof location Ensure computer is inaccessible by passengers See wiring and unintended access requirements Ensure the power supplied to the computer is within manufacturer operational range Ensure 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 Ensure computer NN imposes limits on output to not exceed boundaries Ensure computer NNs use of hidden layers and neurons does not over-fit training data and is sufficient to fit new and unseen data Ensure 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 standards Ensure use of multiple software scanning tools to identify vulnerability and error in computer	sufficient to prevent unintended access and physical damage to the computer To prevent unintended access and physical damage to the development team shall ensure use of coverings at wire-computer interface to prevent unintended access To prevent physical damage to the computer the operator shall avoid adverse road conditions 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 To prevent power failure the development team shall ensure the power supplied to the computer is within manufacturer operational range The development team shall ensure the computer NN model is thoroughly defined and highly sensitive to small variations in inputs The development team shall ensure the computer NN is thoroughly

				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 Ensure understanding of computer input and output signal quality, noise, latency, and bandwidth accounting for measurement and control action error To reduce computer signal input and output latency, ensure use of high-quality transmission medium To prevent computer signal input and output 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 computer signal data To reduce computer signal input and output noise ensure wires are as short as possible To reduce computer signal input and output noise ensure wires are kept away from electrical machinery	tested and validate prior to implementation The development team shall ensure the computer NN imposes limits on output to not exceed boundaries 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 The development team shall ensure the computer program code is thoroughly vetted (Auto industry standard is one defect per 1000 executable lines of code) The development team shall ensure the computer program is developed using automotive coding standards 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) The development team shall ensure the control of computational overflow and compounding rounding errors The development team shall ensure the understanding of computer input and output signal quality,

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

				Ensure system software updates are performed over land-line and not through the air Ensure computer is capable of storing and processing the expected amount of data 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 over-heating ensure 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 computer imposes thermal self-regulation To prevent over-heating ensure computer operates within specified temperature range To prevent operating system crash ensure 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	thermal effects on amplifiers are minimized To reduce computer signal input and output noise, if possible, the development team shall ensure the amplifier bandwidth matches input signal bandwidth To reduce computer signal input and output noise the development team shall ensure use of proper filtering techniques To reduce computer signal input and output noise the development team shall ensure use of wire shielding and conduit To reduce computer signal input and output noise the development team shall ensure understanding of ground loops and impose proper grounding practices 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 The development team shall ensure the understanding of potential computer signal input and output storage delays The development team shall ensure the use of software safety and that

				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 To prevent operating system crash ensure 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 ensure 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 ensure program is developed such that deadlock is prevented (multiple programs having control some resource another program needs) To prevent operating system crash ensure program performs shutdown operations	the system is free from external unintended malicious control 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 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 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 the development team shall ensure the computer fans pull air from cool and dry source To prevent over-heating the development team shall ensure the computer imposes thermal self-regulation To prevent over-heating the development team shall ensure the computer operates within specified temperature range

					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

					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 the program performs shutdown operations
	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
Control Function	**Unsafe Control Action**	**Potential Hazard**	**Causal Factors**	**Prevention/Mitigation**	**Functional Requirement**
Computer sends control action decision to associated controller	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 Power failure	The LKA system will have constant enabled/disabled form of feedback (light) indicated to the operator Ensure wiring is securely installed using manufacturer installation specifications	The LKA system shall have constant enabled/disabled form of feedback (light) indicated to the operator To avoid wiring failure of the intel tank computer the development

	Provided but incorrect duration Provided but incorrect timing	Operator, passenger, or property damage and injury LKA system enabled when operator believes it is disabled	Unintended access or physical damage (liquid, puncture) Wiring failure (not proper gauge, installation or manufacturing failure) Over-heating Operating system crash Sensor malfunction Operator believes the LKA system is disabled when it is enabled	Ensure wiring gauge is sufficient to carry max operational current with factor of safety Ensure wire bend radii are adhered to Ensure computer alters operator that corrective action decisions are disabled stating “LKA and ACC systems disabled” “No corrective action will be made” Ensure computer only makes corrective action decisions when fidelity of image meets minimum specified resolution Ensure if computer system fails, it does not prevent vehicle from manual driving operations Ensure manufacturing and installation is sufficient to prevent unintended access and physical damage 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	team shall ensure wiring is securely installed using manufacturer installation specifications 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 To avoid wiring failure of the intel tank computer the development team shall ensure wire bend radii are adhered to The development team shall ensure the computer alerts operator that corrective action decision is disabled 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 The development team shall ensure manufacturing and installation is sufficient to prevent unintended access and physical damage to the computer To prevent unintended access and physical damage to the development team shall ensure use of coverings

				See wiring and unintended access requirements Ensure the power supplied to the computer is within manufacturer operational range To reduce computer signal input and output latency, ensure use of high-quality transmission medium To prevent computer signal input and output 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 computer signal data To reduce computer signal input and output noise ensure wires are as short as possible To reduce computer signal input and output noise ensure wires are kept away from electrical machinery To reduce computer signal input and output noise it is recommended to use twisted together wires To reduce internal computer signal input and output noise ensure thermal effects on amplifiers are minimized To reduce computer signal input and output noise, if possible, ensure	at wire-computer interface to prevent unintended access To prevent physical damage to the computer the operator shall avoid adverse road conditions 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 To prevent power failure the development team shall ensure the power supplied to the computer is within manufacturer operational range 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 The development team shall reduce computer signal input and output latency, ensure use of high-quality transmission medium To prevent computer signal input and output bandwidth fault the development team shall ensure

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

				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 ensure 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 specified temperature range To prevent operating system crash ensure 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 ensure computer fans pull air from cool and dry source To prevent operating system crash ensure computer imposes thermal self-regulation To prevent operating system crash ensure computer operates within specified temperature range To prevent operating system crash ensure program is developed such that it does not attempt to access an	To reduce computer signal input and output noise the development team shall ensure use of wire shielding and conduit To reduce computer signal input and output noise the development team shall ensure understanding of ground loops and impose proper grounding practices 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 The development team shall ensure the understanding of potential computer signal input and output storage delays The development team shall ensure the use of software safety and that the system is free from external unintended malicious control 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 To prevent computer memory failure ensure the program is developed such that information

				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 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 ensure program is developed such that deadlock is prevented (multiple programs having control some resource another program needs) To prevent operating system crash ensure program performs shutdown operations	that is too large cannot be written into a memory buffer that is too small to contain it 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 the development team shall ensure the computer fans pull air from cool and dry source To prevent over-heating the development team shall ensure the computer imposes thermal self-regulation To prevent over-heating the development team shall ensure the computer operates within specified temperature range 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 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

					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
Control Function	**Unsafe Control 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

		False positive	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	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
	Provided but incorrect timing	Operator alerted to early or late of lane deviation Operator startled and makes spontaneous corrective action False positive or negative	Sensor malfunction or obstruction (dirt, debris stuck to sensor) Environmental conditions Operator believes the LKA system is disabled when it is enabled	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	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
	Provided but incorrect duration	Annoyance to the operator Operator may believe corrective control action needs to be taken	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

			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 lateral movement via EPS	Required but not provided Provided but incorrect timing Provided but incorrect duration	Operator anticipates corrective control action but none occurs Vehicle continues lane deviation Unintended lateral movement Operator, passenger, or property damage and injury	Contamination of power steering fluid (old, air) Power steering low fluid and fluid leaks Broken belt which energizes power steering pump Pump failure Wiring failure Signal corruption EPS controls failure	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 deterioration Ensure proper mounting, installation, and manufacturing of the belt (tension, torque specs) and its components Ensure proper mounting, installation, and manufacturing of pump and its components	Development team shall ensure proper mounting, installation, and manufacturing of EPS hoses, clamps, and their components Development team shall ensure interface components (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, installation, and manufacturing of the EPS belt (tension, torque specs) and its 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 Computer

Potential Hazard	Cause	Major Effect	Corrective/Preventative Measure	Functional Requirement
Failure to blend various sensors (cameras, radars) data to achieve reliable, high-definition images Failure to perform sensor fusion data verification & validation using developed algorithms and NNs Failure to determines if control action (EPS torque, braking, feedback) is required Failure to send control action request to associated controller Failure to provides real-time functionalities	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 which the computer can determine deviations and control actions Operator expects control action but none is taken Unintended longitudinal motion Unintended lateral motion	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 computer alters operator that corrective action decisions are disabled stating “LKA and ACC systems disabled” “No corrective action will be made” Determine fidelity of non-blended image and decide if corrective action should be applied Ensure computer only makes corrective action decisions when fidelity of image meets minimum specified resolution Ensure if computer system fails, it does not prevent vehicle from manual driving operations	To avoid wiring failure of the intel tank computer the development team shall ensure wiring is securely installed using manufacturer installation specifications 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 To avoid wiring failure of the intel tank computer the development team shall ensure wire bend radii are adhered to The development team shall ensure computer alerts operator when corrective action decision is disabled The development team shall ensure the system determines fidelity of non-blended image and decides if corrective action should be applied 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 or physical damage (liquid, puncture)	Failure of CAVs computer and CAVs systems	Ensure manufacturing and installation is sufficient to prevent unintended access and physical damage 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	The development team shall ensure manufacturing and installation is sufficient to prevent unintended access and physical damage to the computer 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		Ensure 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 computer NN model is thoroughly defined and highly sensitive to small variations in inputs To prevent CAVs failure the development team shall ensure the

			Ensure computer NN imposes limits on output to not exceed boundaries Ensure computer NNs use of hidden layers and neurons does not over-fit training data and is sufficient to fit new and unseen data Ensure 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 standards Ensure 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 errors Ensure understanding of computer input and output signal quality, noise, latency, and bandwidth accounting for measurement and control action error	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 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) To prevent CAVs failure the development team shall ensure the control of computational overflow and compounding rounding errors

			To reduce computer signal input and output latency, ensure use of high-quality transmission medium To prevent computer signal input and output 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 computer signal data To reduce computer signal input and output noise ensure wires are as short as possible To reduce computer signal input and output noise ensure wires are kept away from electrical machinery To reduce computer signal input and output noise it is recommended to use twisted together wires To reduce internal computer signal input and output noise ensure thermal effects on amplifiers are minimized To reduce computer signal input and output noise, if possible, ensure amplifier bandwidth matches input signal bandwidth	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 To prevent CAVs failure the development team shall reduce computer signal input and output latency, ensure use of high-quality transmission medium 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 To prevent CAVs failure the development team shall ensure an understanding of time required to analyze and route computer signal data To reduce computer signal input and output noise the development team shall ensure wires are as short as possible To reduce computer signal input and output noise the development team shall ensure wires are kept away from electrical machinery To reduce computer signal input and output noise it is recommended to use twisted together wires To reduce internal computer signal input 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 proper filtering techniques To reduce computer signal input and output noise ensure use of wire shielding and conduit To reduce computer signal input and output noise ensure understanding of ground loops and impose proper grounding practices To ensure true data measurement test the collection with the computer operating at the same temperature that it will be operating at in real-world scenarios Ensure understanding of potential computer signal input and output storage delays Ensure the use of software safety and that the system is free from external unintended malicious control Ensure system software updates are performed over land-line and not through the air	To reduce computer signal input and output noise, if possible, the development team shall ensure the amplifier bandwidth matches input signal bandwidth To reduce computer signal input and output noise the development team shall ensure use of proper filtering techniques To reduce computer signal input and output noise the development team shall ensure use of wire shielding and conduit To reduce computer signal input and output noise the development team shall ensure understanding of ground loops and impose proper grounding practices 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 To prevent CAVs failure the development team shall ensure the understanding of potential computer signal input and output storage delays 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
	Memory failure		Ensure computer is capable of storing and processing the expected amount of data with a factor of safety	To prevent computer memory failure the development team shall ensure the computer is capable of storing and

			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 ensure 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 specified temperature range	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 the development team shall ensure the computer fans pull air from cool and dry source To prevent over-heating the development team shall ensure the computer imposes thermal self-regulation 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 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 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

			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 To prevent operating system crash ensure 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 ensure 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 ensure program is developed such that deadlock is prevented (multiple programs having control some resource another program needs)	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 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 ensure program performs shutdown operations	To prevent operating system crash the development team shall ensure the program performs shutdown operations
	Adverse environmental conditions (poor sensor output; dark, fog, poorly painted or no lane lines)		Ensure computer operates according to a specified minimum for sensor data quality Ensure computer disables corrective action decisions when minimum standard for lane-line, object, and traffic sign recognition is not met Ensure computer operates according to a specified minimum for lane-line recognition (lane dots, poorly painted lines, no lines) Ensure computer operates according to a specified minimum for low-light operations 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 sensor data quality To prevent control action decision failure the development team shall ensure the computer disables the associated corrective action decisions when minimum standard for lane-line, object, and traffic sign recognition is not met To prevent control action decision failure the development team shall ensure the computer operates according to a specified minimum for lane-line recognition (lane dots, poorly painted lines, no lines) 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 haptic feedback stimulation
Item: Intel Mobileye 6				
Potential Hazard	**Cause**	**Major Effect**	**Corrective/Preventative Measure**	**Functional Requirement**
Failure to perform multi-feature tracking Failure to perform object and lane-line detection Failure to perform forward collision warning Failure to perform pedestrian collision warning Failure to perform headway warning Failure to perform traffic sign recognition	Wiring failure (not proper gauge, installation or manufacturing failure)	Failure of CAVs functionality Computer, if operational, operates on single point source information Operator unaware of system failure Less reliable image to which the computer can determine deviations and control actions	Ensure Intel Mobileye 6 camera wiring is securely installed using manufacturer installation specifications Ensure Intel Mobileye 6 camera wiring gauge is sufficient to carry max operational current with factor of safety Ensure Intel Mobileye 6 camera wire bend radii are adhered to Ensure Intel Mobileye 6 camera alerts computer that system failure has occurred	The development team shall ensure the Intel Mobileye 6 camera wiring is securely installed using manufacturer installation specifications The development team shall ensure the Intel Mobileye 6 camera wiring gauge is sufficient to carry max operational current with factor of safety The development team shall ensure the Intel Mobileye 6 camera wire bend radii are adhered to The development team shall ensure the Intel Mobileye 6 camera alerts the computer when failure has occurred

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

			of 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 Ensure 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 ensure 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 internal Intel Mobileye 6 camera signal noise ensure thermal effects on amplifiers are minimized To reduce Intel Mobileye 6 camera signal noise, if possible, ensure amplifier bandwidth matches input signal bandwidth	shall ensure the use of a high-quality transmission medium 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 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 the development team shall ensure the wires are as short as possible 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 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, the development team shall ensure the amplifier bandwidth matches input signal bandwidth

			To reduce Intel Mobileye 6 camera signal noise ensure use of proper filtering techniques To reduce Intel Mobileye 6 camera signal noise ensure use of wire shielding and conduit To reduce Intel Mobileye 6 camera signal noise ensure understanding of ground loops and impose proper grounding practices Ensure understanding of potential Intel Mobileye 6 camera signal storage delays Ensure the use of software safety and that the Intel Mobileye 6 camera signal is free from external unintended malicious control Ensure Intel Mobileye 6 camera system software updates are performed over land-line and not through the air	To reduce Intel Mobileye 6 camera signal noise the development team shall ensure the use of proper filtering techniques To reduce Intel Mobileye 6 camera signal noise the development team shall ensure the use of wire shielding and conduit To reduce Intel Mobileye 6 camera signal noise the development team shall ensure the understanding of ground loops and impose proper grounding practices The development team shall ensure understanding of potential Intel Mobileye 6 camera signal storage delays 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 The development team shall ensure Intel Mobileye 6 camera system software updates are performed over land-line and not through the air
	Capability limitations Failure of field of view Adverse environmental conditions (dark, fog, poorly painted or no lane lines)		To prevent field of view failure ensure Intel Mobileye 6 camera is mounted in the operational area of the wind shield wipers To prevent field of view failure ensure Intel Mobileye 6 camera has control of wind shield wipers (debris may impede camera view while operator is unaware)	To prevent field of view failure the development team shall ensure the Intel Mobileye 6 camera is mounted in the operational area of the wind shield wipers To prevent field of view failure the development team shall ensure the Intel Mobileye 6 camera has control of wind shield wipers (debris may impede 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, and 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 which the computer can determine	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)		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 actions Operator expects control action but none is taken Unintended longitudinal motion Unintended lateral motion	Ensure use of covering at wire-radar interface to prevent unintended access Avoid adverse road condition which may produce NVH and damage the radar	The development team shall ensure the use of covering at wire- radar interface to prevent unintended access The operator shall avoid adverse road condition which may produce NVH and damage or loosen the radar
	Power failure		See wiring and unintended access requirements Ensure the power supplied to the radar is within manufacturer operational range	The development team shall ensure the power supplied to the radar is within manufacturer operational range
	Signal or cyber-security failure		Ensure understanding of radar signal quality, noise, latency, and bandwidth accounting for measurement and control action error To reduce radar signal latency, ensure use of high-quality transmission medium 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	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, the development team shall ensure the use of high-quality transmission medium 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 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 as short as possible To reduce radar signal noise the development team shall ensure the wires are kept away from electrical machinery

			To reduce radar signal noise ensure wires are kept away from electrical machinery To reduce radar signal noise it is recommended to use twisted together wires To reduce internal radar signal noise ensure thermal effects on amplifiers are minimized To reduce radar signal noise, if possible, ensure amplifier bandwidth matches input signal bandwidth To reduce radar signal noise ensure use of proper filtering techniques To reduce radar signal noise ensure use of wire shielding and conduit To reduce radar signal noise ensure understanding of ground loops and impose proper grounding practices Ensure understanding of potential radar signal storage delays Ensure the use of software safety and that the radar signal is free from external unintended malicious control	To reduce radar signal noise it is the development team shall ensure the to use twisted together wires To reduce internal radar signal noise the development team shall ensure the thermal effects on amplifiers are minimized To reduce radar signal noise, if possible, the development team shall ensure the amplifier bandwidth matches input signal bandwidth To reduce radar signal noise the development team shall ensure the use of proper filtering techniques To reduce radar signal noise the development team shall ensure the use of wire shielding and conduit To reduce radar signal noise the development team shall ensure the understanding of ground loops and impose proper grounding practices The development team shall ensure the understanding of potential radar signal storage delays The development team shall ensure the use of software safety and that the radar signal is free from external unintended malicious control The development team shall ensure the system software updates are performed over land-line 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 view Adverse environmental conditions (dark, fog, poorly painted or no lane lines)		To prevent field of view failure ensure radar is mounted such that the signal projects unimpeded 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°) Ensure integrated program accounts for radars cycle time (60 ms)	To prevent field of view failure The development team shall ensure the radar is mounted such that the signal projects 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 (±6° (160m), ±6°(100m), ±10°(60m), ±25°(36m), ±42°(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, ±0,3°) 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, ±7°) The development team shall ensure the integrated program accounts for radars cycle time (60 ms)

			Ensure integrated program accounts for radars frequency modulation Ensure integrated program accounts for radars maximum number of detectable objects (32)	The development team shall ensure the integrated program accounts for radars frequency modulation The development team shall ensure the integrated program accounts for radars maximum number of detectable objects (32)
Item: Intel Movidius Neural Compute Stick				
Potential Hazard	**Cause**	**Major Effect**	**Corrective/Preventative Measure**	**Functional Requirement**
Failure to perform vision processing tasks in assistance to Intel Tank computational capabilities Failure to assist in blending various sensors (cameras, radars) data to achieve reliable, high-definition images Failure to assist in performing sensor fusion data verification & validation Failure to assist in determining if control action (EPS torque, braking, feedback) is required	Power failure		Ensure compute stick is securely input to the computer	The development team shall ensure the compute stick is securely input to the computer
	Algorithm, NN, computational, or cyber-security failure		Ensure compute stick NN model thoroughly defined and highly sensitive to small variations in inputs Ensure compute stick NN is thoroughly tested and validate prior to implementation Ensure compute stick NN imposes limits on output to not exceed boundaries Ensure compute stick NNs use of hidden layers and neurons does not over-fit training data and is sufficient to fit new and unseen data Ensure compute stick program code is thoroughly vetted (Auto	The development team shall ensure the compute stick NN model thoroughly defined and highly sensitive to small variations in inputs The development team shall ensure the compute stick NN is thoroughly tested and validate prior to implementation The development team shall ensure the compute stick NN imposes limits on output to not exceed boundaries 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 The development team shall ensure the compute stick program code is thoroughly vetted (Auto industry

			industry standard is one defect per 1000 executable lines of code) Ensure compute stick program is developed 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) Ensure 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 Ensure understanding of potential compute stick signal input and output storage delays Ensure the use of software safety and that the system is free from	standard is one defect per 1000 executable lines of code) The development team shall ensure the compute stick program is developed using automotive coding standards 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 development team shall ensure the control of computational overflow and compounding rounding errors 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 The development team shall ensure the understanding of time required to analyze and route computer signal data To reduce compute stick signal input and output noise the development team shall ensure the use of proper filtering techniques The development team shall ensure the understanding of potential compute stick signal input and output storage delays The 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 requirements not met		Ensure compute stick is capable of storing and processing the expected amount of data 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 Ensure compute stick and computer interface is compatible Ensure computer free storage space is available to allow compute stick to operate	The development team shall ensure the compute stick is capable of storing and processing the expected amount of data with a factor of safety 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 The development team shall ensure the compute stick and computer interface is compatible The development team shall ensure the computer free storage space is available to allow compute stick to operate
Item: KVaser				
Potential Hazard	**Cause**	**Major Effect**	**Corrective/Preventative Measure**	**Functional Requirement**
Failure to interface CAN signals to USB	Unintended access or physical damage (liquid, puncture)		Ensure KVaser manufacturing and installation is sufficient to prevent unintended access and physical damage Ensure use of covering at KVaser interfaces to prevent unintended access Avoid adverse road condition which may produce NVH and damage KVaser or loosen interfaces	The development team shall ensure KVaser manufacturing and installation is sufficient to prevent unintended access and physical damage to the computer To prevent unintended access and physical damage the development team shall ensure use of coverings at KVaser interfaces To prevent physical damage to the KVaser the operator shall avoid adverse road condition which may produce NVH

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

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

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

			ground loops and impose proper grounding practices Ensure understanding of potential Niles camera signal storage delays Ensure the use of software safety and that the Niles camera signal is free from external unintended malicious control Ensure system software updates are performed over land-line and not through the air	To reduce Niles camera signal noise the development team shall ensure the understanding of ground loops and impose proper grounding practices The development team shall ensure understanding of potential Niles camera signal storage delays The development team shall ensure the use of software safety and that the Niles camera signal is free from external unintended malicious control The development team shall ensure system software updates are performed over land-line and not through the air
	Capability limitations Failure of field of view Adverse environmental conditions (dark, fog, poorly painted or no lane lines)		To prevent field of view failure ensure Niles camera is mounted in the location free of obstruction Ensure camera is of high-quality to maintain operations during low-light Ensure Niles camera indicates to computer and operator when the system is unavailable	To prevent field of view failure the development team shall ensure the camera is mounted in a location free of obstruction The development team shall ensure the camera is of high-quality to maintain operations during low-light The development team shall ensure the Niles camera indicates to computer and operator when the system is unavailable
Item: Real-Time Display				
Potential Hazard	**Cause**	**Major Effect**	**Corrective/Preventative Measure**	**Functional Requirement**
Failure to acquire sensor fusion data from associated controller Failure to display sensors fusion images in real-time	Wiring failure (not proper gauge, installation or manufacturing failure)		Ensure display wiring is securely installed using manufacturer installation specifications Ensure display wiring gauge is sufficient to carry max	The development team shall ensure the display wiring is securely installed using manufacturer installation specifications The development team shall ensure the display wiring gauge is sufficient to

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

			To reduce display signal latency, ensure use of high-quality transmission medium To prevent display 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 display signal data To reduce display signal noise ensure wires are as short as possible To reduce display signal noise ensure wires are kept away from electrical machinery To reduce display signal noise it is recommended to use twisted together wires To reduce internal display signal noise ensure thermal effects on amplifiers are minimized To reduce display signal noise, if possible, ensure amplifier bandwidth matches input signal bandwidth To reduce display signal noise ensure use of proper filtering techniques	To reduce display signal latency the development team shall ensure the use of a high-quality transmission medium 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 The development team shall ensure an understanding of time required to analyze and route display signal data To reduce display signal noise the development team shall ensure the wires are as short as possible To reduce display signal noise the development team shall ensure the wires are kept away from electrical machinery To reduce display signal noise it is recommended to use twisted together wires To reduce internal display signal noise the development team shall ensure the thermal effects on amplifiers are minimized To reduce display signal noise, if possible, the development team shall ensure the amplifier bandwidth matches input signal bandwidth To reduce display signal noise the development team shall ensure the use of proper filtering techniques

			To reduce display signal noise ensure use of wire shielding and conduit To reduce display signal noise ensure 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 Ensure system software updates are performed over land-line and not through the air	To reduce display signal noise the development team shall ensure the use of wire shielding and conduit To reduce display signal noise the development team shall ensure the understanding of ground loops and impose proper grounding practices The development team shall ensure the use of software safety and that the display signal is free from external unintended malicious control The development team shall ensure display system software updates are performed over land-line and not through the air
Item: ZED Camera				
Potential Hazard	**Cause**	**Major Effect**	**Corrective/Preventative Measure**	**Functional Requirement**
Failure to perform high-resolution depth perception Failure to perform 6-axis positional tracking to sense space and motion Failure to perform large-scale 3D mapping	Wiring failure (not proper gauge, installation or manufacturing failure)	Failure of CAVs functionality Computer, if operational, operates on single point source information Operator unaware of system failure Less reliable image to which the computer can determine deviations and control actions	Ensure ZED camera wiring is securely installed using manufacturer installation specifications Ensure ZED camera wiring gauge is sufficient to carry max operational current with factor of safety Ensure ZED camera wire bend radii are adhered to Ensure ZED camera alters computer that system failure has occurred	The development team shall ensure the ZED camera wiring is securely installed using manufacturer installation specifications The development team shall ensure the ZED camera wiring gauge is sufficient to carry max operational current with factor of safety The development team shall ensure the ZED camera wire bend radii are adhered to
	Power failure		See wiring and unintended access requirements	The development team shall ensure the power supplied to the ZED camera is

		Unintended longitudinal motion Unintended lateral motion	Ensure the power supplied to the ZED camera is within manufacturer operational range	within manufacturer recommended operational range
	Signal or cyber-security failure		Ensure 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 prevent ZED camera 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 ZED camera signal data To reduce ZED camera signal noise ensure 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 it is recommended to use twisted together wires To reduce internal ZED camera signal noise ensure thermal	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 the development team shall ensure the use of a high-quality transmission medium 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 The development team shall ensure an understanding of time required to analyze and route ZED camera signal data To reduce ZED camera signal noise the development team shall ensure the wires are as short as possible 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 twisted together wires To reduce internal ZED camera signal noise the development team shall ensure

			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 ensure use of proper filtering techniques To reduce ZED camera signal noise ensure use of wire shielding and conduit To reduce ZED camera signal noise ensure understanding of ground loops and impose proper grounding practices 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 Ensure system software updates are performed over land-line and not through the air	the thermal effects on amplifiers are minimized 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 the development team shall ensure the use of proper filtering techniques To reduce ZED camera signal noise the development team shall ensure the use of wire shielding and conduit To reduce ZED camera signal noise the development team shall ensure the understanding of ground loops and impose proper grounding practices The development team shall ensure understanding of potential ZED camera signal storage delays The development team shall ensure the use of software safety and that the ZED camera signal is free from external unintended malicious control The development team shall ensure system software updates are performed over land-line and not through the air
	Capability limitations Failure of field of view		To prevent field of view failure ensure ZED camera is mounted in the operational 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 camera is mounted in the operational area of the wind shield wipers 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)		Ensure GPS wiring is securely installed using manufacturer installation specifications Ensure GPS wiring gauge is sufficient to carry max operational current with factor of safety Ensure GPS wire bend radii are adhered to Ensure GPS alters computer that system failure has occurred	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
	Unintended access or physical damage (liquid, puncture)		Ensure GPS manufacturing and installation is sufficient to prevent unintended access and physical damage	The development team shall ensure the GPS manufacturing and installation is sufficient to prevent unintended access, loosening, and physical damage

			Ensure use of covering at wire-GPS interface to prevent unintended access Avoid adverse road condition which may produce NVH and damage or loosen the GPS	The development team shall ensure the use of covering at wire-GPS interface to prevent unintended access The operator shall avoid adverse road conditions which may produce NVH and damage or loosen the GPS
	Power failure		See wiring and unintended access requirements Ensure the power supplied to the GPS is within manufacturer operational range	The development team shall ensure the power supplied to the GPS is within manufacturer recommended operational range
	Signal or cyber-security failure		Ensure understanding of GPS signal quality, noise, latency, and bandwidth accounting for measurement and control action error To reduce GPS signal latency, ensure use of high-quality transmission medium To prevent GPS 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 GPS signal data To reduce GPS signal noise ensure wires are as short as possible To reduce GPS signal noise ensure wires are kept away from electrical machinery	The development team shall ensure an understanding of GPS signal quality, noise, latency, and bandwidth accounting for measurement and control action error To reduce GPS signal latency the development team shall ensure the use of a high-quality transmission medium 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 The development team shall ensure an understanding of time required to analyze and route GPS signal data To reduce GPS signal noise the development team shall ensure the wires are as short as possible To reduce GPS signal noise the development team shall ensure the wires are kept away from electrical machinery

			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 GPS signal noise, if possible, ensure amplifier bandwidth matches input signal bandwidth To reduce GPS signal noise ensure use of proper filtering techniques To reduce GPS signal noise ensure use of wire shielding and conduit To reduce GPS signal noise ensure understanding of ground loops and impose proper grounding practices Ensure understanding of potential GPS signal storage delays Ensure the use of software safety and that the GPS signal is free from external unintended malicious control	To reduce GPS signal noise it is recommended to use twisted together wires 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, the development team shall ensure the amplifier bandwidth matches input signal bandwidth To reduce GPS signal noise the development team shall ensure the use of proper filtering techniques To reduce GPS signal noise the development team shall ensure the use of wire shielding and conduit To reduce GPS signal noise the development team shall ensure the understanding of ground loops and impose proper grounding practices The development team shall ensure understanding of potential GPS signal storage delays 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 view Adverse environmental conditions (dark, fog, poorly painted or no lane lines)		Ensure GPS indicates to computer and operator when the system is unavailable	painted lane lines, and adverse weather conditions The development team shall ensure the GPS indicates to computer and operator when the system is unavailable

Appendix 3.05 HARA CSMS DFMEA

CSMS DMFEA											
Item: HSC											
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**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 signals	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 adhered to	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 Potential for overheating Unintended exposure to high voltage								To avoid HSC 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-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

							and loss of functionality			
Item: ECM										
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional Requirement**
Control engine torque output Control engine temperature Control A/F ratio Control idle speed Control electronic valve	Failure to control engine torque output Failure to control engine temperature Failure to control A/F ratio Failure to control idle speed Failure to control electronic valve	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	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 fatigue or failure Operator aware during operation by identifying eventual failure of vehicle components	8	**560**	To avoid ECM wiring failure the development team shall ensure wiring is securely installed using manufacturer installation specifications To avoid ECM wiring failure the development team shall ensure wiring gauge is sufficient to carry max operational current with factor of safety To avoid ECM 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	Vehicle technical inspection will identify if the ECM is free of unintended access and physical damage	9	**450**	To avoid ECM unintended access or physical damage the development team shall ensure proper mounting, installation, and manufacturing of the ECM

						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

						Ensure relays and fuses are in place and functional to prevent over drawing of current	eventual failure of vehicle components and loss of functionality			To avoid ECM over-current failure the development team shall ensure relays and fuses are in place and functional
				Over-heating	2	Ensure ECM is mounted such that there is proper clearance and sufficient air flow to cool the ECM	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-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										
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional Requirement**
Control gear shifting Control transmission temperature	Failure to control gear shifting Failure to control transmission temperature	Unintended longitudinal motion Loss or degradation of propulsion system	**9**	Wiring failure (not proper gauge, installation or manufacturing failure)	7	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	8	**5004**	To avoid TCM wiring failure the development team shall ensure wiring is securely installed using manufacturer installation specifications

		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			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 movement	Vehicle technical inspection will identify if TCM 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	**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 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	**441**	To avoid TCM over-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

							natural air flow cooling Operator aware during operation by identifying eventual failure of vehicle components and loss of functionality			
Item: EMC										
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional Requirement**
Controls supply of current to EM Convert DC to AC Control direction of current Control EM temperature	Failure to control current supply to EM Failure to control current direction Failure to control EM temperature	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	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 fatigue or failure Operator aware during operation by identifying eventual failure of HV components	8	**560**	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

		Potential for overheating Unintended exposure to high voltage								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-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 avoid EMC unintended access or physical damage the development team shall ensure proper mounting, installation, and manufacturing of the EMC To avoid EMC unintended access or physical damage the development team shall ensure use of covering at wire- EMC interface To avoid EMC unintended access or physical damage the operator shall avoid adverse road conditions which may produce NVH
				Installation failure (wire, mounting)	7	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	Vehicle technical inspection will identify if EMC is free of manufacturing or installation fatigue or failure Operator aware during operation by identifying	8	**560**	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

						unintended movement	eventual failure of HV components			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 HV components	7	**490**	To avoid EMC over-current failure the development team shall ensure software limits current ranges To avoid EMC over-current failure the development team shall ensure relays and fuses are in place and functional
				Operation outside of max/min temperature range (environmental or coolant failure)	8	Ensure operation within specified EMC temp range 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	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 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

						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
Item: BMS										
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional Requirement**
Ensure safe ESS operating conditions Monitor ESS state (voltage, temperature,	Failure to ensure safe ESS operating conditions Failure to monitor ESS	Unintended longitudinal motion Loss or degradation of propulsion system	10	Wiring failure (not proper gauge, installation or manufacturing failure)	7	Ensure wiring is securely installed using manufacturer installation specifications	Vehicle technical inspection will identify wiring fatigue or failure	8	**560**	To avoid BMS wiring failure the development team shall ensure wiring is securely installed using manufacturer installation specifications

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 report data Failure to control and balance ESS environment	Operator and/or passenger injury Damage to or loss of property Damage to environment Potential for overheating Unintended exposure to high voltage Short circuit Thermal event Inaccurate ESS state readings (voltage, temperature, SOC)				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
				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 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 unintended movement	Vehicle technical inspection will identify if BMS is free of manufacturing or installation fatigue or failure Operator aware during operation by identifying eventual failure of HV components	8	**560**	To avoid BMS installation failure the development team shall ensure the mounting hardware are sufficient for max operational G-force with factor of safety To avoid BMS 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 HV components	7	**490**	To avoid BMS over-current failure the development team shall ensure software limits current ranges To avoid BMS over-current failure the development team shall ensure relays and fuses are in place and functional
					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	9	**360**	To avoid 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

							natural air flow cooling Operator aware during operation by identifying eventual failure of vehicle components and loss of functionality			
Item: OBC										
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**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 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 access or physical damage (liquid, puncture)	5	Ensure manufacturing is sufficient to prevent	Vehicle technical inspection will identify the	9	**450**	To avoid OBC unintended access or physical damage 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 damage	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	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

						Ensure OBC, charging port, and mounting hardware are secure and free from unintended movement	Operator aware during operation by identifying eventual failure of HV components			To avoid OBC 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 HV components	7	**490**	To avoid OBC over-current failure the development team shall ensure software limits current ranges To avoid OBC over-current failure the development team shall ensure relays and fuses are in place and functional
				Operation outside of max/min temperature range (environmental or coolant failure)	8	Ensure operation within specified OBC temperature range Actuate thermal control system when OBC reaches specified temperature Ensure thermal system components (radiator, coolant level, fans) are	OBC temperature signal sends 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 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 To avoid OBC operation outside of max/min temperature range the development team shall actuate cooling fans when OBC reaches specified temperature

						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 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 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**	**O**	**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 and wiring is protected from heat sources
				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	9	**90**	To avoid OBD II unintended access or physical damage the development team shall ensure proper mounting, installation, and manufacturing of the OBD II
				Installation failure (wire, mounting)	7	Ensure OBD II and mounting hardware are secure, free	Vehicle technical inspection will identify if the	8	**112**	To avoid OBD II 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										
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional Requirement**
Transfer necessary signals such as EM speed, EM torque, EM temperature, EMC temperature, SOC, current, voltage, battery temperature, and	Failure to transfer necessary signals such as EM speed, EM torque, EM temperature, EMC temperature, SOC,	Unintended longitudinal motion Loss or degradation of propulsion system Operator and/or	9	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	Vehicle technical inspection will identify wiring fatigue or failure Operator aware during operation by identifying	8	**504**	To avoid CAN bus wiring failure the development team shall ensure wiring is securely installed using manufacturer installation specifications To avoid CAN bus wiring failure the

OBC temperature	current, voltage, battery temperature, and OBC temperature	passenger injury Damage to or loss of property Damage to environment Potential for overheating Short Circuit Error messages Loss of communication between controllers and a loss of their functionality Loss of DAQ functionality				operational current with factor of safety Ensure wire bend radii are adhered to Ensure wiring bus is properly protected	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 To avoid CAN bus 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 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

						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

Function	Failure Type	Potential Impact	S	Potential Cause	O	Prevention Mode	Detection Mode	D	RPN	Functional Requirement
							Operator aware during operation by identifying eventual failure of vehicle components and loss of functionality			
Item: Accelerator Pedal (AP) and Accelerator Pedal Position Sensor (APPS)										
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional Requirement**
Monitor the position of the accelerator pedal and transmit a torque request	Failure to monitor the position of the accelerator pedal and transmit a 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	10	Wiring failure (not proper gauge, installation or manufacturing failure)	2	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 error message and eventual failure of vehicle components	8	**160**	To avoid AP/APPS 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 produce NVH
				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**	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
Item: Low Voltage System										

Function	Failure Type	Potential Impact	S	Potential Cause	O	Prevention Mode	Detection Mode	D	RPN	Functional Requirement
Control of all auxiliary functions to include air bags, windshield wipers, Instrument cluster, lights, entertainment system, turn signals, haptic feedback, security system, pumps, fans, controllers, and DAQ Controls thermal components Controls data acquisition	Failure to control of 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 Failure to control thermal components Failure to controls data acquisition	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 Reduced or loss of visibility Driver unaware of vehicle operational data (velocity, RPM, engine temperature)	10	Wiring failure (not proper gauge, installation or manufacturing failure)	3	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 error message and eventual failure of vehicle components	8	**240**	To avoid low voltage component wiring failure the development team shall ensure wiring is securely installed using manufacturer installation specifications 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 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
				Unintended access or physical damage (liquid, puncture)	2	Ensure manufacturing is sufficient to prevent unintended access and physical damage	Vehicle technical inspection will identify if the low voltage components are free of unintended access and	9	**180**	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

							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 Operator aware during operation by identifying eventual failure of vehicle components and loss of functionality			functional and replace fatigued components

Appendix 3.06 HARA PSI HV DFMEA

PSI HV DFMEA										
Item: **HV** Battery Pack										
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**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				recommended installation instructions (clearance, bend radii) Limit charge and discharge current to specified range				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
				Operation while undercharged	7	BMS monitors and controls SOC. Controls software will only draw current at	BMS monitors and sends SOC data in real time	6	**420**	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

						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 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

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

	Failure to prevent unauthorized access to HV components	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				free from potential loosening or movement Ensure all vents are covered with appropriate screening Ensure fans are pulling air from dry particulate-free source Ensure enclosure location is covered when vehicle is not in use				development team shall ensure bolts and mounting hardware is securely fastened and free from potential loosening or movement To prevent the HV enclosure from unintended access the development team shall ensure all vents are covered with appropriate screening 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
				improper mounting to vehicle frame (enclosure vibration)	7	Use existing mount locations on vehicle frame to secure enclosure Ensure mounting hardware is sufficient for max operational G-force with factor of safety Ensure proper enclosure	Vehicle technical inspection will identify frame mounting fatigue or failures Operator aware during operation by identifying a failure of HV components	8	**560**	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 To prevent the HV enclosure failure from improper mounting to the vehicle frame the development team shall ensure mounting

						manufacturing (welds, thread engagement)				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)
				Improper installation and mounting of components (components within enclosure vibration)	7	Ensure 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	Vehicle technical inspection will identify component installation fatigue or failures Operator aware during operation by identifying a failure of HV components	8	**560**	To prevent the HV 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 of components the development team shall ensure component mounting hardware is

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

						from interference				such that there is sufficient air flow to cool HV components and that the flow is free from interference
				Adverse road conditions (NVH)	3	Do not operate on roads which may produce high NVH	Operator aware during operation. Increased NVH	3	**90**	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

Item: Junction Box										
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional Requirement**
Ease use for maintenance and consolidation of HV wire connections and relays	Failure to provide current	Unintended deceleration Unintended longitudinal motion Loss or degradation of propulsion system Thermal event Operator and/or passenger injury Damage to or loss of property Damage to environment Short circuit Unintended exposure to high voltage	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 junction box wiring fatigue or failure Operator aware during operation by identifying eventual failure of HV components	8	**560**	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 ensure wire bend radii are adhered to
				Unintended access and physical damage (liquid, insect, puncture)	5	Ensure box manufacturing is sufficient to prevent unintended access and physical damage Ensure use of grommets at wire-box interface prevent	Vehicle technical inspection will identify junction box is free of unintended access Operator aware during operation by identifying eventual failure	9	**450**	To prevent junction box failure from unintended access the development team shall ensure the box manufacturing is sufficient to prevent unintended access, loosening, and physical damage To prevent junction box failure from unintended access the development team shall ensure the

						unintended access	of HV components			use of grommets at wire-box interface prevent unintended access
				Manufacturing or installation failure (wire, mounting)	7	Ensure junction box and mounting hardware is sufficient for max operational G-force with factor of safety Ensure junction box and mounting hardware is fire retardant Ensure junction box and mounting hardware is secure and free from unintended movement	Vehicle technical inspection will identify junction box is free of manufacturing or installation fatigue or failure Operator aware during operation by identifying eventual failure of HV components	8	**560**	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 To prevent junction box failure the development team shall ensure the junction box and mounting hardware is fire retardant To prevent junction box failure the development team shall ensure the junction box and mounting hardware is secure and free from unintended movement
				Over-current	7	Ensure software (HSC, OBC, EMC) limits current magnitude 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 junction box over-current failure the development team shall ensure software (HSC, OBC, EMC) limits current magnitude To prevent junction box over-current failure the development team shall ensure relays and fuses are in place and

										functional to prevent over drawing of current
				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**	To prevent junction box failure the development team shall ensure box minimum rating of IP67

Item: Wiring Harness

Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional Requirement**
Transfer energy	Failure to transfer energy	Unintended deceleration Unintended longitudinal motion Loss or degradation of propulsion system Thermal event Operator and/or passenger injury Damage to or loss of property Damage to environment	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
				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 Unintended exposure to high voltage		harness (liquid, debris)		access and physical damage Ensure use of covers and shielding to prevent unintended access and physical damage Avoid adverse road condition which may project debris and damage harness	of unintended access or physical damage Operator aware during operation by identifying eventual failure of HV components			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 To prevent HV wiring harness failure the operator shall avoid adverse road condition which may project debris and damage harness
				Installation failure (wire, mounting, bend radii)	7	Ensure harness and mounting hardware is sufficient for max operational G-force with factor of safety Ensure harness and mounting hardware are fire retardant Ensure harness and mounting hardware is secure and free from unintended movement	Vehicle technical inspection will identify if harness is free of manufacturing or installation fatigue or failure Operator aware during operation by identifying eventual failure of HV components	8	**560**	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 To prevent HV wiring harness installation failure the development team shall ensure the harness and mounting hardware is secure and free from unintended movement

				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										
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional Requirement**
Ensure safe ESS operating conditions Monitor ESS state (voltage, temperature, SOC, and current) Protects against over-current, over-voltage, under-voltage, and over-temperature Reporting data	Failure to ensure safe ESS operating conditions Failure to monitor ESS state (voltage, temperature, SOC, and current) Failure to protect against over-current, over-voltage, under-	Unintended longitudinal motion Loss or degradation of propulsion system Operator and/or passenger injury Damage to or loss of property Damage to environment	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 fatigue or failure Operator aware during operation by identifying eventual failure of HV components	8	**560**	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

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)								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-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 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 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

						unintended movement	eventual failure of HV components			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 BMS over-current failure the development team shall ensure software limits current rates and ranges 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 Operator aware during operation by identifying eventual failure of TVP components and loss of functionality	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

Item: OBC

Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**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 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	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 factor of safety To prevent OBC charging port 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	Vehicle technical inspection will identify wiring fatigue or failure Operator aware during operation by identifying eventual failure	8	**560**	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 charging port cover is	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 or physical damage

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

				temperature range (environmental or coolant failure)		OBC temperature range Actuate cooling fans when OBC reaches specified temperature Use manufacturer recommended installation instructions (clearance, bend radii)	signal sends data in real time Operator aware during operation by identifying a thermal event, error message of overheating, or failure of HV components			ensure software limits operation within specified OBC temperature range To prevent OBC over-heating failure the development team shall ensure actuation of thermal control system (fans) when OBC reaches specified temperature To prevent OBC over-heating failure the development team shall ensure manufacturer recommended installation instructions (clearance, bend radii)
Item: EMC										
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional Requirement**
Controls supply of current to EM Convert DC to AC Control direction of current Control EM temperature	Failure to control current supply to EM Failure to control current direction Failure to control EM temperature	Unintended acceleration Unintended longitudinal motion Loss or degradation of propulsion system	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	Vehicle technical inspection will identify wiring fatigue or failure Operator aware during operation by identifying eventual failure of HV components	8	**560**	To prevent EMC wiring failure the development team shall ensure the wiring is securely installed using manufacturer installation specifications To prevent EMC wiring failure the development team shall ensure wiring gauge is

		Operator and/or passenger injury Damage to or loss of property Damage to environment Potential for overheating Unintended exposure to high voltage				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
				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 To prevent EMC 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, bend radii)				To prevent EMC over-heating failure the development team shall ensure using manufacturer recommended installation instructions (clearance, bend radii)

Appendix 3.07 HARA PSI HV HazOP

PSI HV Process Parameter and Guide Word Combination Chart

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

PSI HV HazOP

FUNCTION: Apply NVH Stimuli to High Voltage System

Guide Word	**Deviation**	**Consequences**	**Causes**	**Safeguards**	**Functional Requirement**
Faster	NVH stimuli is applied too quickly	Mounting/interfacing hardware loosens/separates	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 frequency
		ESS components disconnect from each other			

		Potential thermal runaway - Fire			
More	NVH amplitude reaches threshold	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
		Potential thermal runaway - Fire			
		ESS components disconnect from each other			
FUNCTION: Apply Temperature Stimuli to High Voltage System					
Guide Word	**Deviation**	**Consequences**	**Causes**	**Safeguards**	**Functional Requirement**
More	ESS temperature is greater than max operating temperature	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 thermal control validation. Thorough testing during SIL, zero velocity and closed course phases	The TVP ESS shall operate within a safe and specified temperature range
		Potential thermal runaway - Fire			
Less	ESS temperature is less than minimum operating temperature	Item damage or lost functionality	Extremely cold environmental conditions.	Do not operate during extremely cold environmental conditions.	
		TVP/operator damage/injury			
FUNCTION: Apply Current Stimuli to High Voltage 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			
FUNCTION:	Apply Unauthorized Access Stimuli To The High Voltage System				
Guide Word	**Deviation**	**Consequences**	**Causes**	**Safeguards**	**Functional Requirement**
More	More/any unauthorized access is applied to high voltage system	Short circuit	Animals, insects, fingers, liquid, snow, dust, and debris. Poor design of ESS enclosure	Ensure ESS enclosure ventilation and ports are secured using mesh or other impassable filter.	The ESS enclosure and high voltage system shall prevent unauthorized access and physical damage to the high voltage components
		Fire			
		TVP/operator damage/injury			

Appendix 3.08 HARA PSI Mechanical Controls Hardware HazOP

PSI Mechanical Controls Hardware Process Parameter and Guide Word Combination Chart

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

PSI Mechanical HazOP of the Controls Hardware System

FUNCTION:	Apply NVH Stimuli to Controls Hardware System				
Guide Word	**Deviation**	**Consequences**	**Causes**	**Safeguards**	**Functional Requirement**

Faster	NVH stimuli is applied too quickly	Controls hardware components loosens/separates from mounts/wiring Vehicle components/subsystems lose functionality Vehicle/operator damage/injury	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
More	NVH amplitude reaches threshold	Controls hardware components loosens/separates from mounts/wiring Vehicle components/subsystems lose functionality Vehicle/operator damage/injury	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
FUNCTION:	Apply Temperature Stimuli to Controls Hardware System				
Guide Word	**Deviation**	**Consequences**	**Causes**	**Safeguards**	**Functional Requirement**
More	Controls hardware temperature is greater than max operating temperature	Vehicle components/subsystems lose functionality Vehicle/operator damage/injury	ESS component error, inadequate cooling, poor design, software controls error	E-stop validation. Controls hardware thermal control validation. Thorough testing during zero velocity and closed course phases	The controls hardware shall operate within a safe and specified temperature range
Less	Controls hardware temperature is less than minimum operating temperature	Vehicle components/subsystems lose functionality Vehicle/operator damage/injury	Extremely cold environmental conditions.	Do not operate during extremely cold environmental conditions.	
FUNCTION:	Apply Current Stimuli to Controls Hardware System				

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	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
		Vehicle collides with object			
		Vehicle/operator damage/injury			
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	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
		Controls hardware actuates vehicle components in manner other than intended			
		Vehicle collides with object			
		Vehicle/operator damage/injury			
		Fire			

Less	Current applied is less than intended	Controls hardware/vehicle components lose functionality Controls hardware actuates vehicle components in manner other than intended Vehicle does not accelerate as intended Torque request not met	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	
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

Function	Failure Type	Potential Impact	S	Potential Cause	O	Prevention Mode	Detection Mode	D	RPN	Functional Requirement
Transmit torque from engine/EM to rear of vehicle	Loss of torque transmission	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	10	Driveshaft-EM 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 driveshaft-EM interface location is covered and 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	**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
				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 physical damage (debris, puncture)	3	Ensure driveshaft manufacturing and use of materials is	Vehicle technical inspection will identify if driveshaft is	9	**270**	Development team shall ensure driveshaft manufacturing and use of materials is sufficient to prevent

						sufficient to prevent unintended access and physical damage	free of physical damage			unintended access and physical damage

Item: Differential

Function	Failure Type	Potential Impact	S	Potential Cause	O	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: Suspension										
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**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 road conditions	3	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	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 Damage to or loss of property Damage to environment					Vehicle technical inspection will identify spring fatigue			
				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

							Deterioration of performance. Vehicle technical inspection will identify spring fatigue			
				Adverse road conditions	2	Avoid adverse road condition which may produce NVH and damage suspension	Operator aware prior to or during operation. Increased NVH	4	**40**	Operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH
Item: Brakes										
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional 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

						for rust and corrosion Avoid poor drive behavior				Operator shall perform routine inspection of brake system to check for rust, fatigue, and corrosion 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 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	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	**108**	Development team 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
				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
Item: Thermal										
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional Requirement**
Detects and controls cabin and component temperatures	Failure to detect and control cabin and component temperatures	Loss or degradation of propulsion Operator and/or passenger injury Damage to or loss of property Damage to environment Fire, smoke	10	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**	Development team shall ensure thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the engine Development team shall ensure the thermal systems fans are free from potential physical damage

						Ensure enclosure fans pull air from a cool source 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 system and its components Ensure bolts and mounting hardware are securely fastened and free from potential loosening or movement				Development team shall ensure thermal system fans pull air from a cool source Development team shall ensure engine ventilation is sufficient to provide appropriate air movement through engine bay Development teams 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 Development team shall ensure thermal system bolts and mounting hardware are securely fastened and free from potential loosening or movement Development team 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 free from potential loosening or movement Ensure the correct type of coolant is used, proper coolant levels, and check for leaks prior to operation Ensure belt drive components are properly installed (tensioning, torque specs)				and free from potential loosening or movement Development team shall ensure the correct type of coolant is used, proper coolant levels, and check for leaks prior to operation Development team shall ensure thermal system belt drive components are properly installed (tensioning, torque specs)
				Radiator failure	3	Ensure proper mounting, installation, and manufacturing of radiator, clamps, hoses and their components Ensure bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from	Vehicle technical inspection will identify low fluid level, leaks, and rust Operator aware during operation by identifying displayed high temperatures	5	**150**	Development team shall ensure proper mounting, installation, and manufacturing of radiator, clamps, hoses and their components Development team shall ensure radiator bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from potential loosening or movement

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

						Ensure that the thermostat, fuse, fan wires, coolant level and fan clutch are functional				Development team shall ensure that the thermostat, fuse, fan wires, coolant level and fan clutch are functional
Item: Steering										
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional 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 deterioration	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	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 levels, and check for leaks prior to operation	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
				Broken belt which energizes power steering pump	3	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

						hardware are securely fastened and free from potential loosening or unintended movement				mounting hardware are securely fastened and free from potential loosening or unintended movement
				Pump failure	2	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 movement	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**	Development team shall ensure proper mounting, installation, and manufacturing of EPS pump and its components Development team shall ensure EPS pump bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from potential loosening or movement
Item: Exhaust										
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional Requirement**
Removal of toxic gases, fumes and noise	Failure to remove toxic gases, fumes and noise	Unintended exposure to toxic or flammable chemicals Excessive noise	9	Manifold failure (cracked)	4	Ensure proper mounting, installation, and manufacturing of intake manifold and its components	Vehicle technical inspection will identify fluid leaks Operator aware during operation by	6	**216**	Development team shall ensure proper mounting, installation, and manufacturing of intake manifold and its components

		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 sensor Ensure current oil changes Avoid adverse road condition which may produce NVH and damage the catalytic converter	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)	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 loosening or movement				and potential loosening or movement
				Muffler failure	4	Ensure proper mounting, installation, and manufacturing of muffler and its components Ensure bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from leaks and potential loosening or movement.	Vehicle technical inspection will identify physical damage to the muffler Operator aware during operation by identifying audible noise (generally loud, back-fire), or smell of exhaust fumes, condensation inside the exhaust and lower mpg	2	**72**	Development team shall ensure proper mounting, installation, and manufacturing of muffler and its components Development team shall ensure muffler bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from leaks and potential loosening or movement.
				Sensor failure (O2)	3	Ensure proper mounting, installation, and manufacturing of O2 sensor Ensure bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and	Vehicle technical inspection will identify physical damage to the O2 sensor Operator aware during operation by identifying check engine	6	**162**	Development team shall ensure proper mounting, installation, and manufacturing of O2 sensor Development team shall ensure O2 sensor Ensure bolts, interface components (seals, gaskets), and mounting hardware are securely fastened

						free from leaks and potential loosening or movement	light, loss in vehicle functionality (misfire, lower mpg), or smell of exhaust fumes			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

Item: Engine											
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional 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 injury Damage to or loss of property Damage to environment Potential for overheating Unintended exposure to toxic/flammable chemicals	10	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 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 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
				Improper fuel octane number	1	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, water pump, fan, or thermostat failure)		(radiator, coolant level, fans) are functional and sufficient to cool the engine Ensure the fans are free from potential physical damage Ensure enclosure fans pull air from a cool source 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	Operator aware during operation. Operator views engine temp in cabin. Error message displayed.			(radiator, coolant level, fans) are functional and sufficient to cool the engine Development team shall ensure the thermal systems fans are free from potential physical damage Development team shall ensure thermal system fans pull air from a cool source Development team shall ensure engine ventilation is sufficient to provide appropriate air movement through engine bay Development teams 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

						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				Development team shall ensure thermal system bolts and mounting hardware are 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
				Head gasket failure	4	Ensure proper mounting, installation, and manufacturing of intake manifold and its components Ensure bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from leaks	Vehicle technical inspection will identify fluid leaks Operator aware during operation by identifying displayed engine high temperatures, decrease in power, misfires, stalling, or	6	**240**	Development team shall ensure proper mounting, installation, and manufacturing of head gasket. intake manifold and its components Development team shall ensure head gasket components and mounting hardware are securely fastened and free from leaks and potential loosening or unintended 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

						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
Item: Motor										
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional 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 injury Damage to or loss of property Damage to environment	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
				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 free	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	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, installation, and manufacturing of coolant system and its components Ensure bolts, hoses and mounting hardware are securely fastened and free from potential loosening or movement Ensure the HSC controls and mitigates overheating Operator drives appropriately to ensure EM temp is stable				pull air from a cool source Development team shall ensure proper mounting, installation, and manufacturing of EM coolant system and its components Development team shall ensure EM coolant system 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 Operator shall drive appropriately to ensure EM temp is stable
				Low resistance due to insufficient isolation between windings (corrosion or physical damage)	7	Ensure thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the EM	Operator aware during operation by identifying high motor temperature and loss of motor functionality	8	**560**	Development team shall ensure EM thermal system components (radiator, coolant level, fans) are functional and 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				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 components Ensure bolts and mounting hardware is securely fastened and free from potential loosening or unintended movement Ensure EM-driveshaft interface location is covered and free from potential unintended access or physical damage Ensure proper EM-driveshaft alignment Ensure EM-driveshaft interface angle is minimized Avoid adverse road condition which may produce NVH and damage	or installation fatigue or failure Operator aware during operation by identifying partial or total functionality failure			interfacing components Development team shall ensure EM-driveshaft interface bolts and mounting hardware is securely fastened and free from potential loosening or unintended movement Development team shall ensure EM-driveshaft interface location is covered and free from potential unintended access or physical damage Development team shall ensure proper EM-driveshaft alignment Development team shall ensure EM-driveshaft interface angle is minimized Operator shall avoid adverse road conditions which may produce NVH and damage EM-driveshaft interface

						EM-driveshaft interface				
				EM-transmission 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 EM-transmission interface location is covered and free from potential unintended access or physical damage Ensure proper EM-transmission alignment	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	**720**	Development team shall ensure proper mounting, installation, and manufacturing of EM, transmission, and its interfacing components Development team shall ensure EM-transmission interface bolts and mounting hardware are securely fastened and free from potential loosening or unintended movement Development team shall ensure EM-transmission interface location is covered and free from potential unintended access or physical damage Development team shall ensure proper EM-transmission alignment Operator shall avoid adverse road conditions which may produce NVH and damage EM-transmission interface

						Avoid adverse road conditions which may produce NVH and damage EM-transmission interface				

Item: Fuel

Function	Failure Type	Potential Impact	S	Potential Cause	O	Prevention Mode	Detection Mode	D	RPN	Functional 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 Damage to environment Potential for overheating Unintended exposure to toxic/flammable chemicals	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
				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 pump failure	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 fuel quality	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

Item: Transmission										
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional Requirement**
Transfers power from engine to driveshaft Gears change drive-wheel speed and torque in relation to engine speed and torque	Failure to Transfers power from engine to driveshaft Failure with gears to change drive-wheel speed and torque in relation to engine speed and torque	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	Transmission fluid failure (leaking, contamination, age, low fluids)	3	Ensure proper mounting, installation, and manufacturing of transmission and its components Ensure bolts, 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 prior to operation Ensure belt drive components are properly installed	Vehicle technical inspection will identify low fluid level, leaks, and belt fatigue Operator aware during operation by identifying displayed high temperatures	8	**240**	Development team shall ensure proper mounting, installation, and manufacturing of transmission and its components Development team shall ensure transmission bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from potential loosening or movement Operator shall ensure the correct type of coolant (ATF) is used, proper coolant levels, and check for leaks prior to operation Development team shall ensure belt drive components are properly installed (tensioning, torque specs)

						(tensioning, torque specs)				
				Overheating	3	Ensure thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the transmission Ensure the fans are free from potential physical damage Ensure fans pull air from a cool source Ensure proper mounting, installation, and manufacturing of coolant system and its components Ensure bolts, hoses and mounting hardware are securely fastened and free from potential	Operator aware during operation by identifying high transmission temperature and loss of functionality	8	**240**	Development team shall ensure transmission thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the transmission Development team shall ensure transmission thermal system fans are free from potential physical damage Development team shall ensure transmission thermal system fans pull air from a cool source Development team shall ensure proper mounting, installation, and manufacturing of transmission thermal system and its components Development team shall ensure transmission thermal system bolts, hoses and mounting hardware are securely fastened and free from

						loosening or movement Ensure the TCM controls and mitigates overheating Operator drives appropriately to ensure transmission temperature is stable				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
				Transmission-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	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	**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

						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
Item: Body										
Function	**Failure Type**	**Potential Impact**	**S**	**Potential Cause**	**O**	**Prevention Mode**	**Detection Mode**	**D**	**RPN**	**Functional Requirement**
Allows access to and protects components in engine compartment Allows operator to see in low light scenarios Prevent debris from being thrown into air by rotating tire Allows access to/from cabin	Failure to allow operator to see Failure to prevent debris from entering cabin	Unintended longitudinal motion Operator and/or passenger injury Damage to or loss of property Damage to environment Potential for overheating	5	Hood failure	1	Ensure proper mounting, installation, and manufacturing of the hood, and latch Ensure bolts, interface components, and mounting hardware are securely fastened and free from potential loosening or movement	Vehicle technical inspection will identify physical damage to the hood and loosening of latch Operator aware during operation by identifying hood failure obstructing view	8	**40**	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 unintended movement.

and protects operator from environment and debris Absorb impact of minor collision Signals turning and braking Allows for operator to have surrounding view										
				Grill failure prevents airflow to radiator	1	Ensure proper mounting, installation, and manufacturing of the grill 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	Vehicle technical inspection will identify physical damage or clogging or the grill Operator aware during operation by identifying signs of over heating	2	**10**	Development team shall ensure proper mounting, installation, and manufacturing of the grill 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 Operator aware during operation by identifying loss of light functionality	8	**120**	Development team shall ensure proper mounting, installation, and manufacturing of head and tail lights Operator shall ensure functionality of lights prior to use

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

Appendix 3.10 HARA PSI Mechanical HazOP

PSI Mechanical Process Parameter and Guide Word Combination Chart

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

PSI Mechanical HazOP

FUNCTION: Apply NVH Stimuli to EM

Guide Word	**Deviation**	**Consequences**	**Causes**	**Safeguards**	**Functional Requirement**
Faster	NVH stimuli is applied too quickly	Mounting/interfacing hardware loosens/separates	Adverse road conditions. Inadequate installation, factor of safety, or mounting hardware	Proper installation, torque specs, factor of safety on bolts, interfaces, and mounting hardware	TVP mechanical systems shall be capable of withstanding a high NVH frequency
		EM disconnects from driveshaft			
		EM disconnects from transmission			
Slower	NVH stimuli applied too slowly	EM approaches natural frequency causing mounting/interface instability and increased vibratory amplitude	Adverse road conditions. Inadequate installation, factor of safety, or mounting hardware	Proper installation, torque specs, factor of safety on bolts, interfaces, and mounting hardware	TVP mechanical systems shall be capable of withstanding a high NVH amplitude
		EM disconnects from transmission			
		EM disconnects from driveshaft			

More	NVH amplitude reaches threshold	Mounting/interfacing hardware loosens/separates	Adverse road conditions. Inadequate installation, factor of safety, or mounting hardware	Proper installation, torque specs, factor of safety on bolts, interfaces, and mounting hardware	
		EM disconnects from transmission			
		EM disconnects from driveshaft			
FUNCTION: 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	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 direction shall match the torque request intended direction
		TVP collides with object.			
		TVP/operator damage/injury			
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 testing, APPS validation, and gear selection control testing during zero velocity and closed course phases	The applied torque shall actuate at the time intended
		TVP collides with object			
		TVP/operator damage/injury			
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,	

				and gear selection control testing during zero velocity and closed course phases	
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	
FUNCTION: Apply Temperature Stimuli to EM					
Guide Word	**Deviation**	**Consequences**	**Causes**	**Safeguards**	**Functional Requirement**
More	EM temperature is greater than max operating temperature	Fire Item damage or lost functionality TVP/operator damage/injury	ESS malfunction. Control software error. Thermal control system error.	Controls software validation during SIL. ESS controls validation. E-stop validation. Thorough testing during SIL, zero velocity and closed course phases	The EM shall operate with in a safe and specified temperature range
Less	EM temperature is less than minimum operating temperature	Item damage or lost functionality TVP/operator damage/injury	Extremely cold environmental conditions.	Do not operate during extremely cold environmental conditions.	

FUNCTION: Apply Current Stimuli to EM					
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 current requested	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	
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
FUNCTION:	Clearance 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 TVP/operator damage/injury	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

		Difficulty installing and maintaining the mechanical components			
FUNCTION: Interface Angle Applied to Driveshaft/EM					
Guide Word	**Deviation**	**Consequences**	**Causes**	**Safeguards**	**Functional Requirement**
More	More driveshaft/EM interface angle is applied than required	NVH to powertrain system Mounting/interfacing hardware loosens/separates TVP/operator damage/injury	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

Appendix 3.11 HARA PSI SEFA

SEFA Part 1 of 2																	
Team: PSI																	
			Item Operating States														
Item No.	**Multiple Range 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 rollaway	
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	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	TCM	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 electronic 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 propulsion system	Operator aware during operation by vehicle response to torque request, potential EM over-heat or failure	Provide real time feedback to operator of motor state (current, torque, temp, speed) Actuate motor thermal controls when motor temperature range exceeds specified limits	Vehicle would be capable of normal functionality If emergency motor shut	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

	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 leaks or physical damage to the EM Operator aware during operation by identifying loss of motor functionality Operator aware during operation by identifying high EM temperature and loss of motor functionality Vehicle technical inspection will identify if the interface is free of manufacturing or installation fatigue or failure	Actuate motor speed and torque governor when motor speed and torque exceed specified limits Actuate EMC current governor via HSC when motor, battery pack, or EMC exceeds specified current limits Allow operator override to discontinue motor operation 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 Ensure proper mounting, installation, and manufacturing of the EM and housing 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	off occurs the vehicle will be capable of normal operations (P,R,N,D) with partial functionality	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 To prevent motor failure the operator shall be provided real-time diagnostics and have the capability to discontinue motor operations 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 Development team shall ensure proper mounting, installation, and manufacturing of the EM and housing 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 Development team shall ensure EM thermal system components (radiator,

			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 Ensure enclosure fans pull air from a cool source Ensure proper mounting, installation, and manufacturing of coolant system and its components Ensure bolts, hoses and mounting hardware are securely fastened and free from potential loosening or movement Ensure the HSC controls and mitigates overheating Operator drives appropriately to ensure EM temp is stable		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 mounting, installation, and manufacturing of EM coolant system and its components Development team shall ensure EM coolant system 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 Operator shall drive 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

	damage and/or injury to passenger/ personnel	filter and unclean oil Operator aware during operation by identifying loss of vehicle functionality, Sputtering, engine grinding, dirty exhaust, or a drop in pressure Sensors signal to ECM Operator aware during operation. Operator views engine temp in cabin. Error message displayed	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 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 Ensure enclosure fans pull air from a cool source 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 system and its components	of propulsive capability	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 Development team shall ensure thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the engine Development team shall ensure the thermal systems fans are free from potential physical damage Development team shall ensure thermal system fans pull air from a cool source Development team shall ensure engine ventilation is sufficient to provide appropriate air movement through engine bay Development teams 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 Development team shall ensure thermal system bolts and mounting hardware 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 engine temp is stable		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
Item No.	**Potential Safety Hazard**	**Diagnostic Method**	**Mitigation Method**	**System State After Mitigation**	**Functional Requirement**
4 Suspension	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	Error message will occur Vehicle technical inspection will identify low tire pressure and uneven tire wear Operator aware during operation from vehicle sagging and unsettling noise Deterioration of performance. Vehicle technical inspection will identify spring fatigue Vehicle technical inspection will	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 Routine maintenance and inspection for rust Avoid adverse road conditions Ensure proper mounting, installation, and routine maintenance and inspection of hardware	Stopped Possibility of no vehicle motion/ loss of wheel	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 Development team shall ensure suspension spring compression is calibrated and that springs are free of fatigue and corrosion Development team shall ensure the suspensions system and components have proper mounting, installation, and routine maintenance and inspection of hardware

		identify rust, corrosion, and failure	Ensure bolts and mounting hardware is securely fastened and free from potential loosening or unintended movement		Development team shall ensure the suspensions system bolts and mounting hardware is securely fastened and free from potential loosening or unintended movement
Item No.	**Potential Safety Hazard**	**Diagnostic Method**	**Mitigation Method**	**System State After 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 Damage to or loss of property Damage to environment	Vehicle technical inspection will identify if the pads are free from fatigue or corrosion Operator aware during operation by identifying unsettling smell,	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	Stopped Possibility of uncontrolled vehicle motion	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

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

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

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 range Actuate cooling fans when battery pack reaches specified temperature Use manufacturer recommended installation instructions (clearance, bend radii) Limit charge and discharge current to specified range BMS monitors and controls SOC. Controls software will only draw current at specified minimum SOC 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	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 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 insects Ensure fans are pulling air from dry particulate-free source Ensure enclosure location is covered when vehicle is not in use Ensure software (HSC, OBC, EMC) limits charging and discharging rates and ranges Ensure 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 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 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
Item No.	**Potential Safety Hazard**	**Diagnostic Method**	**Mitigation Method**	**System State After Mitigation**	**Functional Requirement**
9 BMS	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 Short circuit Thermal event Inaccurate 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 To prevent BMS 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

					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**	**System State After Mitigation**	**Functional Requirement**
10 HSC	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 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 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
Item No.	**Potential Safety Hazard**	**Diagnostic Method**	**Mitigation Method**	**System State After 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 during operation	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 bolts, hoses and mounting hardware are securely fastened and free from potential loosening or unintended movement
Item No.	**Potential Safety Hazard**	**Diagnostic Method**	**Mitigation Method**	**System State After 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 sufficient to carry max	Stopped Zero/ possibility of propulsive	To avoid TCM wiring failure the development team shall ensure wiring is securely installed using manufacturer installation specifications

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

	Damage to environment Potential for overheating	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	max operational G-force with factor of safety Ensure ECM and mounting hardware are secure and free from unintended movement Ensure ECM is mounted such that there is proper clearance and sufficient air flow to cool the ECM		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 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

Appendix 4 Safety Goals and Functional Requirements – Complete Documentation

Appendix 4.1 ACC Safety Goals and Functional Requirements

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 position or APP	FSRA02.01	The ACC system shall allow operator to override automated controls with minimal AP engagement
		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

		FSRA02.09	The operator shall ensure frequent oil changes, clean oil, and that the oil filter is not ballooned or deformed
		FSRA02.10	The operator shall ensure proper fuel octane number prior to filling tank
		FSRA02.11	The operator shall ensure thermal system components (radiator, coolant level, fans, water pump, thermostat) are functional and sufficient to cool the engine
		FSRA02.12	The development team shall ensure the fans are free from potential physical damage
		FSRA02.13	The development team shall ensure fans pull air from a cool source
		FSRA02.14	The development team shall ensure engine ventilation is sufficient to provide appropriate air movement through engine bay
		FSRA02.15	The development team shall ensure thermal system is designed such that there is sufficient air flow to cool engine components
		FSRA02.16	The development team shall ensure the ECM controls and mitigates engine overheating
		FSRA02.17	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
		FSRA02.18	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
		FSRA02.19	The operator shall ensure thermal system is functional
		FSRA02.20	The development team shall ensure proper A/F ratio and functioning O2 sensor
		FSRA02.21	The development team shall ensure vacuum lines and manifold gasket are free from cracks and physical damage
		FSRA02.22	The development team shall ensure properly functioning timing belt
		FSRA02.23	The development team shall ensure properly functioning EGR valve
		FSRA02.24	The development team shall ensure software (HSC) limits the magnitude of current to the EM
		FSRA02.25	The development team shall ensure relays and fuses are in place and functional to prevent over drawing of current
		FSRA02.26	The development team shall ensure proper mounting, installation, and manufacturing of the EM and housing
		FSRA02.27	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
		FSRA02.28	The development team shall ensure thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the EM

		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 ACC system velocity constraint	FSRA05.01	The ACC system shall operate within a specified velocity range
		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 4.2 CAVs 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 SGC01.4 SGC01.5	The Intel Tank Computer shall be responsible for blending various sensors (cameras, radars) data to achieve reliable, high-definition images The Intel Tank Computer shall be responsible for performing sensor fusion data verification & validation using developed algorithms and NNs The Intel Tank Computer shall be responsible for determining if control action (EPS torque, braking, feedback) is required	FSRC01.01	To avoid wiring failure of the intel tank computer the development team shall ensure wiring is securely installed using manufacturer installation specifications
		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
		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 request to associated controller The Intel Tank Computer shall be responsible for provides real-time functionalities	FSRC01.09	To prevent unintended access and physical damage to the development team shall ensure use of coverings at wire-computer interface
		FSRC01.10	To prevent physical damage to the computer the operator shall avoid adverse road condition which may produce NVH
		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
		FSRC01.12	To prevent unintended access and physical damage the development team shall ensure computer is inaccessible by passengers
		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
		FSRC01.33	To reduce computer signal input and output noise the development team shall ensure 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 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 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 computer operates according to a specified minimum for sensor data quality
		FSRC01.53	To prevent control action decision failure the development team shall ensure the 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 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 SGC02.3 SGC02.4 SGC02.5 SGC02.6 SGC02.7 SGC02.8	The Intel Mobileye 6 camera shall perform multi-feature tracking The Intel Mobileye 6 camera shall perform object and lane-line detection The Intel Mobileye 6 camera shall perform forward collision warning The Intel Mobileye 6 camera shall perform pedestrian collision warning The Intel Mobileye 6 camera shall perform headway warning The Intel Mobileye 6 camera shall perform traffic sign recognition	FSRC02.01	The development team shall ensure the Intel Mobileye 6 camera wiring is securely installed using manufacturer installation specifications
		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
		FSRC02.03	The development team shall ensure the Intel Mobileye 6 camera wire bend radii are adhered to
		FSRC02.04	The development team shall ensure the Intel Mobileye 6 camera alerts the computer when failure has occurred
		FSRC02.05	The development team shall ensure the Intel Mobileye 6 camera manufacturing and installation is sufficient to prevent unintended access and physical damage
		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
		FSRC02.07	The development team shall ensure the use of covering at wire- Intel Mobileye 6 camera interface to prevent unintended access
		FSRC02.08	The development team shall ensure the Intel Mobileye 6 camera installation is inside cabin in a dry debris-proof location
		FSRC02.09	The operator shall avoid adverse road conditions which may produce NVH and damage or loosen the Intel Mobileye 6 camera
		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 action error
		FSRC02.12	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
	The Intel Mobileye 6 camera shall transmit data to associated controller The Intel Mobileye 6 camera shall provide real-time display	FSRC02.13	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
		FSRC02.14	The development team shall ensure an understanding of time required to analyze and route Intel Mobileye 6 camera signal data
		FSRC02.15	To reduce Intel Mobileye 6 camera signal noise the development team shall ensure the wires are as short as possible
		FSRC02.16	To reduce Intel Mobileye 6 camera signal noise the development team shall ensure the wires are kept away from electrical machinery
		FSRC02.17	To reduce Intel Mobileye 6 camera signal noise it is recommended to use twisted together wires
		FSRC02.18	To reduce internal Intel Mobileye 6 camera signal noise the development team shall ensure the thermal effects on amplifiers are minimized
		FSRC02.19	To reduce Intel Mobileye 6 camera signal noise, if possible, the development team shall ensure the amplifier bandwidth matches input signal bandwidth
		FSRC02.20	To reduce Intel Mobileye 6 camera signal noise the development team shall ensure the use of proper filtering techniques
		FSRC02.21	To reduce Intel Mobileye 6 camera signal noise the development team shall ensure the use of wire shielding and conduit
		FSRC02.22	To reduce Intel Mobileye 6 camera signal noise the development team shall ensure the understanding of ground loops and impose proper grounding practices
		FSRC02.23	The development team shall ensure understanding of potential Intel Mobileye 6 camera signal storage delays
		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
		FSRC02.25	The development team shall ensure Intel Mobileye 6 camera system software updates are performed over land-line and not through the air
		FSRC02.26	To prevent field of view failure the development team shall ensure the Intel Mobileye 6 camera is mounted in the operational area of the wind shield wipers
		FSRC02.27	To prevent field of view failure the development team shall ensure the Intel Mobileye 6 camera has control of wind shield wipers (debris may impede camera view while operator is unaware)
		FSRC02.28	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
		FSRC02.29	The development team shall ensure the Intel Mobileye 6 camera indicates to computer and operator when the system is unavailable

SGC03.1 SGC03.2	The Bosch Front, Rear, and Corner MRR Radars shall perform early front, rear, and corner speed detection The Bosch Front, Rear, and Corner MRR Radars shall send data to associated controller	FSRC03.01	The development team shall ensure the radar wiring is securely installed using manufacturer installation specifications
		FSRC03.02	The development team shall ensure the radar wiring gauge is sufficient to carry max operational current with factor of safety
		FSRC03.03	The development team shall ensure the radar wire bend radii are adhered to
		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 shielding and conduit
		FSRC03.20	To reduce radar signal noise the development team shall ensure the understanding of ground loops and impose proper grounding practices
		FSRC03.21	The development team shall ensure the understanding of potential radar signal storage delays
		FSRC03.22	The development team shall ensure the use of software safety and that the radar signal 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 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 2omputer 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 (±6° (160m), ±6°(100m), ±10°(60m), ±25°(36m), ±42°(12m))
		FSRC03.28	The development team shall ensure the integrated program accounts for radars speed, distance, and angle measurement accuracy (0.11 m/s, 0.12 m, ±0,3°)
		FSRC03.29	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, ±7°)
		FSRC03.30	The development team shall ensure the integrated program accounts for radars cycle 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**
SGC04.1 SGC04.2 SGC04.3 SGC04.4	The Intel Movidius Neural Compute Stick shall perform vision processing tasks in assistance to Intel Tank computational capabilities	FSRC04.01	The development team shall ensure the compute stick is securely input to the computer
		FSRC04.02	The development team shall ensure the compute stick NN model thoroughly defined and highly sensitive to small variations in inputs
		FSRC04.03	The development team shall ensure the compute stick NN is thoroughly tested and 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 Compute Stick shall assist in blending various sensors (cameras, radars) data to achieve reliable, high-definition images	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
		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)
		FSRC04.07	The development team shall ensure the compute stick program is developed using automotive coding standards
		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 Compute Stick shall assist in performing sensor fusion data verification & validation	FSRC04.09	The development team shall ensure the control of computational overflow and compounding rounding errors
		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 determining if control action (EPS torque, braking, feedback) is required	FSRC04.12	To reduce compute stick signal input and output noise the development team shall ensure the use of proper filtering techniques
		FSRC04.13	The development team shall ensure the understanding of potential compute stick signal input and output storage delays
		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 operator The Niles operator monitoring camera shall send data to associated controller	FSRC06.01	The development team shall ensure the Niles camera wiring is securely installed using manufacturer installation specifications
		FSRC06.02	The development team shall ensure the Niles camera wiring gauge is sufficient to carry max operational current with factor of safety
		FSRC06.03	The development team shall ensure the Niles camera wire bend radii are adhered to
		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
		FSRC06.16	To reduce Niles camera signal noise it is recommended to use twisted together wires
		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 wire shielding and conduit
		FSRC06.21	To reduce Niles camera signal noise the development team shall ensure the 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 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
SG No.	**Safety Goal**	**FSR No.**	**Functional Safety Requirement**
SGC07.1 SGC07.2	The real-time display shall acquire sensor fusion data from associated controller	FSRC07.01	The development team shall ensure the display wiring is securely installed using manufacturer installation specifications
		FSRC07.02	The development team shall ensure the display wiring gauge is sufficient to carry max operational current with factor of safety

	The real-time display shall display sensors fusion images in real-time	FSRC07.03	The development team shall ensure the display wire bend radii are adhered to
		FSRC07.04	The development team shall ensure the camera manufacturing and installation is sufficient to prevent unintended access and physical damage
		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 SGC08.3	The Zed camera shall perform high-resolution depth perception The Zed camera shall perform 6-axis positional tracking to sense space and motion The Zed camera shall perform large-scale 3D mapping	FSRC08.01	The development team shall ensure the ZED camera wiring is securely installed using manufacturer installation specifications
		FSRC08.02	The development team shall ensure the ZED camera wiring gauge is sufficient to carry max operational current with factor of safety
		FSRC08.03	The development team shall ensure the ZED camera wire bend radii are adhered to
		FSRC08.04	The development team shall ensure the power supplied to the ZED camera is within manufacturer recommended operational range
		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 understanding of ground loops and impose proper grounding practices
		FSRC08.17	The development team shall ensure understanding of potential ZED camera signal 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 The GPS shall provide data to associated controller	FSRC09.01	The development team shall ensure the GPS wiring is securely installed using manufacturer installation specifications
		FSRC09.02	The development team shall ensure the GPS wiring gauge is sufficient to carry max operational current with factor of safety
		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
		FSRC09.09	To reduce GPS signal latency the development team shall ensure the use of a high-quality transmission medium

		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

Appendix 4.3 CSMS Safety Goals and Functional Requirements

CSMS Safety Goals and Functional Requirements			
SG No.	**Safety Goal**	**FSR No.**	**Functional Safety Requirement**
SGS01.1 SGS01.2 SGS01.3 SGS01.4 SGS01.5	The HSC shall control all hybrid functions The HSC shall control engine/EM torque split The HSC shall maintain SOC at appropriate level The HSC shall control gear shifting The HSC shall modify stock signals	FSRS01.01	To avoid HSC wiring failure the development team shall ensure wiring is securely installed using manufacturer installation specifications
		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
		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
		FSRS01.04	To avoid HSC unintended access or physical damage the development team shall ensure proper mounting, installation, and manufacturing of the HSC
		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

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

		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 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 SGS04.2 SGS04.3	The EMC shall control current supply to EM The EMC shall control current direction The EMC shall control EM temperature	FSRS04.01	To avoid EMC wiring failure the development team shall ensure wiring is securely installed using manufacturer installation specifications
		FSRS04.02	To avoid EMC wiring failure the development team shall ensure wiring gauge is sufficient to carry max operational current with factor of safety
		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
		FSRS04.04	To avoid EMC unintended access or physical damage the development 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 development team shall actuate cooling fans when EMC reaches specified temperature
		FSRS04.13	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
		FSRS04.14	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 SGS05.2 SGS05.3 SGS05.4	The BMS shall ensure safe ESS operating conditions	FSRS05.01	To avoid BMS wiring failure the development team shall ensure wiring is securely installed using manufacturer installation specifications
		FSRS05.02	To avoid BMS wiring failure the development team shall ensure wiring gauge is sufficient to carry max operational current with factor of safety

SGS05.5	The BMS shall monitor ESS state (voltage, temperature, SOC, and current) The BMS shall protect against over-current, over-voltage, under-voltage, and over-temperature The BMS shall report data The BMS shall control and balance ESS environment	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
		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 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
		FSRS05.07	To avoid BMS installation failure the development team shall ensure the mounting hardware are sufficient for max operational G-force with factor of safety
		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 software limits current ranges
		FSRS05.10	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 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 charging to the HV battery pack	FSRS06.01	To avoid OBC wiring failure the development team shall ensure charging port cover is sufficient to provide freedom from unintended 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 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 requested vehicle parameters to monitor	FSRS07.01	To avoid OBD II wiring failure the development team shall ensure wiring is securely installed using manufacturer installation specifications
		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 bend radii are adhered to and wiring is protected from heat sources
		FSRS07.04	To avoid OBD II unintended access or physical damage the development 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 conditions with a factor of safety
		FSRS07.06	To avoid OBD II over-current failure the development team shall ensure software limits current ranges
		FSRS07.07	To avoid OBD II over-current failure the development team shall ensure relays and fuses are in place and functional
SG No.	**Safety Goal**	**FSR No.**	**Functional Safety Requirement**
SGS08.1	The CAN Bus shall transfer necessary signals such as EM speed, EM torque, EM temperature, EMC temperature, SOC, current, voltage, battery temperature, and OBC temperature	FSRS08.01	To avoid CAN bus wiring failure the development team shall ensure wiring is securely installed using manufacturer installation specifications
		FSRS08.02	To avoid CAN bus wiring failure the development team shall ensure wiring gauge is sufficient to carry max operational current with factor of safety
		FSRS08.03	To avoid CAN bus wiring failure the development team shall ensure wire 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
		FSRS08.06	To avoid CAN bus unintended access or physical damage the operator shall avoid 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
SG No.	**Safety Goal**	**FSR No.**	**Functional Safety Requirement**
SGS09.1	The APPS shall monitor the position of the accelerator pedal and transmit a torque request	FSRS09.01	To avoid AP/APPS wiring failure the development team shall ensure wiring is securely installed using manufacturer installation specifications
		FSRS09.02	To avoid AP/APPS wiring failure the development team shall ensure wiring gauge is sufficient to carry max operational current with factor of safety
		FSRS09.03	To avoid AP/APPS wiring failure the development team shall ensure wire bend radii are adhered to and wiring is protected from heat sources
		FSRS09.04	To avoid AP/APPS unintended access or physical damage the development team shall ensure proper mounting, installation, and manufacturing of the AP/APPS
		FSRS09.05	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 shall avoid adverse road conditions which may produce NVH

		FSRS09.07	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
		FSRS09.08	To avoid AP/APPS installation failure the development team shall ensure the mounting hardware is secure and free from potential lessening or unintended movement
		FSRS09.09	To avoid AP/APPS over-current failure the development team shall ensure software limits current ranges
		FSRS09.10	To avoid AP/APPS over-current failure the development team shall ensure relays and fuses are in place and functional
		FSRS09.11	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
SG No.	**Safety Goal**	**FSR No.**	**Functional Safety Requirement**
SGS10.1 SGS10.2 SGS10.3	The low voltage system shall control of 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 low voltage system shall control thermal components The low voltage system shall control data acquisition	FSRS10.01	To avoid low voltage component wiring failure the development team shall ensure wiring is securely installed using manufacturer installation specifications
		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
		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
		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
		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
		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 4.4 LKA 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 the braking system (EBCM)	FSRL01.01	The LKA system shall allow operator to override automated controls with minimal braking engagement
		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
		FSRL01.07	The LKA brake system shall engage in timely manner such that brake pad fatigue and passenger discomfort is minimized
		FSRL01.08	To avoid brake pad failures the development teams shall ensure proper mounting and installation of brake pads
		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
		FSRL01.11	To avoid brake pad failures the operator shall avoid poor driving behaviors
		FSRL01.12	To avoid brake rotor failures the development teams shall ensure proper mounting and installation of brake rotors
		FSRL01.13	The LKA brake system shall engage in timely manner such that brake rotor fatigue and passenger discomfort is minimized
		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
		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
		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	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
		FSRL01.20	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 multi-feature tracking	FSRL03.01	The development team shall impose criteria for deviation and corrective action
		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 requirements and lane-line visibility
		FSRL03.07	To avoid sensor visibility obstruction the LKA system shall have control 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

		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 via audio and visual feedback
		FSRL05.04	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 provide feedback to the operator (LKA status, haptic, visual, audio)	FSRL06.01	The LKA feedback system shall be wired and installed according to manufacturer specifications to include bend radii, heat shielding, EMI avoidance, sheathing, proper gauge, and interface connections
		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

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

SGL07	The LKA computer shall safely perform sensor fusion data verification & validation using developed algorithms and NNs	FSRL07.01	To avoid wiring failure of the intel tank computer the development team shall ensure wiring is securely installed using manufacturer installation specifications
		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

		FSRL07.17	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
		FSRL07.18	The development team shall ensure the computer program code is thoroughly vetted (Auto industry standard is one defect per 1000 executable lines of code)
		FSRL07.19	The development team shall ensure the computer program is developed using automotive coding standards
		FSRL07.20	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)
		FSRL07.21	The development team shall ensure the control of computational overflow and compounding rounding errors
		FSRL07.22	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
		FSRL07.23	The development team shall reduce computer signal input and output latency, ensure use of high-quality transmission medium
		FSRL07.24	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
		FSRL07.25	The development team shall ensure an understanding of time required to analyze and route computer signal data
		FSRL07.26	To reduce computer signal input and output noise the development team shall ensure wires are as short as possible
		FSRL07.27	To reduce computer signal input and output noise the development team shall ensure wires are kept away from electrical machinery
		FSRL07.28	To reduce computer signal input and output noise it is recommended to use twisted together wires
		FSRL07.29	To reduce internal computer signal input and output noise the development team shall ensure thermal effects on amplifiers are minimized
		FSRL07.30	To reduce computer signal input and output noise, if possible, the development team shall ensure the amplifier bandwidth matches input signal bandwidth
		FSRL07.31	To reduce computer signal input and output noise the development team shall ensure use of proper filtering techniques
		FSRL07.32	To reduce computer signal input and output noise the development team shall ensure use of wire shielding and conduit
		FSRL07.33	To reduce computer signal input and output noise the development team shall ensure understanding of ground loops and impose proper grounding practices

		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
		FSRL07.35	The development team shall ensure the understanding of potential computer signal input and output storage delays
		FSRL07.36	The development team shall ensure the use of software safety and that the system is free from external unintended malicious control
		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
		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
		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
		FSRL07.40	To prevent over-heating the development team shall ensure the computer imposes thermal self-regulation
		FSRL07.41	To prevent over-heating the development team shall ensure the computer operates within specified temperature range
		FSRL07.42	To prevent operating system crash the development team shall ensure the system does not over heat
		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
		FSRL07.44	To prevent operating system crash the development team shall ensure the computer fans pull air from cool and dry source
		FSRL07.45	To prevent operating system crash the development team shall ensure the computer imposes thermal self-regulation
		FSRL07.46	To prevent operating system crash the development team shall ensure the computer operates within specified temperature range
		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
		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
		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 associated controller	FSRL08.01	The LKA system shall have constant enabled/disabled form of feedback (light) indicated to the operator
		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

		FSRL08.12	To prevent unintended access and physical damage the development team shall ensure computer is inaccessible by passengers
		FSRL08.13	To prevent power failure the development team shall ensure the power supplied to the computer is within manufacturer operational range
		FSRL08.14	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
		FSRL08.15	The development team shall reduce computer signal input and output latency, ensure use of high-quality transmission medium
		FSRL08.16	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
		FSRL08.17	The development team shall ensure an understanding of time required to analyze and route computer signal data
		FSRL08.18	To reduce computer signal input and output noise the development team shall ensure wires are as short as possible
		FSRL08.19	To reduce computer signal input and output noise the development team shall ensure wires are kept away from electrical machinery
		FSRL08.20	To reduce computer signal input and output noise it is recommended to use twisted together wires
		FSRL08.21	To reduce internal computer signal input and output noise the development team shall ensure thermal effects on amplifiers are minimized
		FSRL08.22	To reduce computer signal input and output noise, if possible, the development team shall ensure the amplifier bandwidth matches input signal bandwidth
		FSRL08.23	To reduce computer signal input and output noise the development team shall ensure use of proper filtering techniques
		FSRL08.24	To reduce computer signal input and output noise the development team shall ensure use of wire shielding and conduit
		FSRL08.25	To reduce computer signal input and output noise the development team shall ensure understanding of ground loops and impose proper grounding practices
		FSRL08.26	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
		FSRL08.27	The development team shall ensure the understanding of potential computer signal input and output storage delays
		FSRL08.28	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	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
		FSRL08.30	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
		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	To prevent over-heating the development team shall ensure the computer 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	To prevent operating system crash the development team shall ensure the computer fans pull air from cool and dry source
		FSRL08.37	To prevent operating system crash the development team shall ensure the computer imposes thermal self-regulation
		FSRL08.38	To prevent operating system crash the development team shall ensure the computer 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 developed such that the OS does not enter an infinite loop
		FSRL08.40	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
		FSRL08.41	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)
		FSRL08.42	To prevent operating system crash the development team shall ensure the program performs shutdown operations
		FSRL08.43	The LKA system shall allow the operator to easily override the corrective 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 4.5 PSI 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

		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 contain enclosed components through the prevention of	FSRH02.01	To prevent the HV enclosure failure from unintended access the development team shall ensure proper mounting, installation, and manufacturing of enclosure (sealing, welds, bolt holes)

	unintended horizontal or vertical movement and unauthorized access	FSRH02.02	To prevent the HV enclosure failure from unintended access the development team shall ensure bolts and mounting hardware is securely 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	To prevent the HV enclosure failure from improper mounting to the vehicle frame the development team shall ensure mounting hardware is sufficient for max operational G-force with factor of safety
		FSRH02.06	To prevent the HV enclosure failure from improper mounting to the vehicle frame the development team shall ensure proper enclosure manufacturing (welds, thread engagement)
		FSRH02.07	To prevent the HV enclosure failure from improper installation and mounting of components the development team shall ensure
		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
		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 battery pack
		FSRH02.11	To prevent a HV enclosure cooling failure the development team shall ensure the enclosure fans are free from potential physical damage
		FSRH02.12	To prevent a HV enclosure cooling failure the development team shall 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	To prevent a HV enclosure manufacturing failure the development team shall ensure materials used in enclosure manufacturing are capable of withstanding high NVH
		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**
SGH03	The HV junction box shall safely contain and consolidate HV wire connections and relays and provide a maintenance ease of use	FSRH03.01	To prevent junction box wiring failure the development team shall ensure wiring is securely installed using manufacturer installation specifications
		FSRH03.02	To prevent junction box wiring failure the development team shall ensure wiring gauge is sufficient to carry max operational current with factor of safety
		FSRH03.03	To prevent junction box wiring failure the development team shall ensure wire bend radii are adhered to
		FSRH03.04	To prevent junction box failure from unintended access the development team shall ensure the box manufacturing is sufficient to prevent unintended access, loosening, and physical damage
		FSRH03.05	To prevent junction box failure from unintended access the development team shall ensure the use of grommets at wire-box interface prevent unintended access

		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 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 minimum rating of IP67

SG No.	Safety Goal	FSR No.	Functional Safety Requirement
SGH04	The HV wiring harness shall safely transfer energy	FSRH04.01	To prevent HV wiring harness failure the development team shall ensure wiring is securely installed using manufacturer installation specifications
		FSRH04.02	To prevent HV wiring harness failure the development team shall ensure wiring gauge is sufficient to carry max operational current with factor of safety
		FSRH04.03	To prevent HV wiring harness failure the development team shall ensure wire bend radii are adhered to
		FSRH04.04	To prevent HV wiring harness failure the development team shall ensure the harness manufacturing is sufficient to prevent unintended access and physical damage
		FSRH04.05	To prevent HV wiring harness failure the development team shall ensure the use of covers and shielding to prevent unintended access and physical damage
		FSRH04.06	To prevent HV wiring harness failure the operator shall avoid adverse road condition which may project debris and damage harness

		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 SGH05.2 SGH05.3 SGH05.4	The BMS shall safely ensure the HV ESS operating conditions The BMS shall safely monitor and report the data of the HV ESS voltage, temperature, SOC, and current The BMS shall protect against over-current, over-voltage, under-voltage, and over-temperature The BMS shall safely control and balance the HV ESS environment	FSRH05.01	To prevent BMS wiring failure the development team shall ensure the wiring is securely installed using manufacturer installation specifications
		FSRH05.02	To prevent BMS wiring failure the development team shall ensure the wiring gauge is sufficient to carry max operational current with factor of safety
		FSRH05.03	To prevent BMS wiring failure the development team shall ensure wire bend radii are adhered to
		FSRH05.04	To prevent BMS failure the development team shall ensure the manufacturing is sufficient to prevent unintended access and physical damage
		FSRH05.05	To prevent BMS unintended access or physical damage failure the development team shall ensure use of covering at wire-BMS interface prevent unintended access
		FSRH05.06	To prevent BMS unintended access or physical damage failure the operator shall avoid adverse road condition which may produce NVH and damage BMS
		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	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
		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 charging to the HV battery pack	FSRH06.01	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
		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	To prevent OBC charging port failure the development team shall ensure wiring gauge is sufficient to carry max operational current with factor of safety
		FSRH06.04	To prevent OBC charging port failure the development team shall ensure 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	To prevent OBC wiring failure the development team shall ensure wiring 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 bend radii are adhered to
		FSRH06.08	To prevent OBC failure the development team shall ensure manufacturing is sufficient to prevent unintended access and physical damage

		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)
SG No.	**Safety Goal**	**FSR No.**	**Functional Safety Requirement**
SGH07.1 SGH07.2		FSRH07.01	To prevent EMC wiring failure the development team shall ensure the wiring is securely installed using manufacturer installation specifications

SGH07.3 SGH07.4	The EMC shall safely control the supply of current to the EM The EMC shall safely convert the DC to AC The EMC shall safely control the direction of current The EMC shall safely control the EM temperature	FSRH07.02	To prevent EMC wiring failure the development team shall ensure wiring gauge is sufficient to carry max operational current with factor of safety
		FSRH07.03	To prevent EMC wiring failure the development team shall ensure wire bend radii are adhered to
		FSRH07.04	To prevent EMC failure the development team shall ensure manufacturing is sufficient to prevent unintended access and physical damage
		FSRH07.05	To prevent EMC unintended access failure the development team shall ensure the use of covering at wire-EMC interface prevent unintended access
		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 software limits operation within specified EMC temp range
		FSRH07.12	To prevent EMC over-heating failure the development team shall ensure actuation of thermal control system (fans) when EMC reaches specified temperature
		FSRH07.13	To prevent EMC over-heating failure the development team shall ensure 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 within a safe and specified temperature range	FSRH09.01	The HV ESS shall avoid, detect, mitigate, and contain overheating
		FSRH09.02	The HV ESS shall ensure accurate temperature sensing
		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 charging shall match the current requested	FSRH10.01	The OBC shall control the current to the battery pack while in a stationary charging state
		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	The HV ESS shall ensure accurate SOC sensing
		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 discharging shall match the current requested	FSRH11.01	The current supplied by the HV ESS shall be determined by the EM/engine torque split
		FSRH11.02	The HSC shall determine the torque split and ultimately the current request
		FSRH11.03	The current discharged shall also be determined by the SOC requirements
		FSRH11.04	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 4.6 PSI 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 rear of the vehicle	FSRM01.01	To avoid driveshaft-EM interface failure the development team shall ensure proper mounting, installation, and manufacturing of modified driveshaft and its components
		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 team shall ensure driveshaft manufacturing and use of materials is sufficient to prevent unintended access and physical damage
SG No.	**Safety Goal**	**FSR No.**	**Functional Safety Requirement**
SGM02	The differential shall provide power from the driveshaft to the wheels and shall allow the wheels to rotate independently	FSRM02.01	To avoid differential-driveshaft interface failure the development team shall ensure proper mounting, installation, and manufacturing of modified driveshaft, differential and their components
		FSRM02.02	To avoid differential-driveshaft interface failure the development team shall ensure the differential bolts and mounting hardware is securely fastened and free from potential loosening or unintended movement
		FSRM02.03	To avoid differential-driveshaft interface failure the development team shall ensure differential-driveshaft interface location is covered and free from potential unintended access or physical damage
		FSRM02.04	To avoid differential-driveshaft interface failure the operator shall avoid excessively adverse road conditions (bumpy terrain, excessive grade) which may cause a high NVH and damage the differential and interfacing components
		FSRM02.05	To avoid differential-half shaft interface failure the development team shall ensure proper mounting, installation, and manufacturing of half-shafts and their components
		FSRM02.06	To avoid differential-half shaft interface failure the development team shall ensure half-shaft 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 absorb/reduce excess energy from road shock	FSRM03.01	To avoid uneven tire pressure and tire wear the operator shall ensure proper tire pressure prior to operation
		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

		FSRM05.03	To avoid engine overheating the development team shall ensure thermal system fans pull air from a cool source
		FSRM05.04	To avoid engine overheating the development team shall ensure engine ventilation is sufficient to provide appropriate air movement through engine bay
		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
		FSRM05.06	To avoid engine overheating the development team shall ensure proper mounting, installation, and manufacturing of thermal system and its components
		FSRM05.07	To avoid engine overheating the development team shall ensure thermal system bolts and mounting hardware are securely fastened and free from potential loosening or unintended movement
		FSRM05.08	To avoid engine overheating the development team shall ensure the ECM controls and mitigates engine overheating
		FSRM05.09	To avoid engine overheating the operator shall avoid poor driving behaviors
		FSRM05.10	To avoid engine overheating the engine temperature shall be displayed for operator to view in real-time
		FSRM05.11	To avoid engine overheating the vehicle shall provide feedback warning to operator when engine temperature exceed specified range
		FSRM05.12	The vehicle shall have fire extinguisher in event of thermal incident
		FSRM05.13	To avoid insufficient coolant levels the operator shall ensure proper coolant levels and check for leaks prior to operation
		FSRM05.14	To avoid thermal system pump failure the development team shall ensure proper mounting, installation, and manufacturing of water pump and its components
		FSRM05.15	To avoid thermal system pump failure the team shall ensure thermal system pump bolts, interface components (seals, gaskets), and mounting hardware are securely fastened and free from potential loosening or unintended movement
		FSRM05.16	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
		FSRM05.17	To avoid thermal system pump failure the development team shall ensure thermal system belt drive components are properly installed (tensioning, torque specs
		FSRM05.18	To avoid radiator failure the development team shall ensure proper mounting, installation, and manufacturing of radiator, clamps, hoses and their components
		FSRM05.19	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
		FSRM05.20	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 shall control lateral movement of the vehicle	FSRM06.01	To avoid contamination of the power steering fluid the development team shall ensure 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	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
		FSRM06.06	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
		FSRM06.07	To avoid EPS belt failure the development team shall ensure proper mounting, installation, and manufacturing of the power steering belt (tension, torque specs) and its components

		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 and noise reduction	FSRM07.01	To avoid manifold failure the development team shall ensure proper mounting, installation, and manufacturing of intake manifold and its components
		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

		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 request of the operator	FSRM08.01	To avoid improper engine lubrication the development team shall ensure proper mounting, installation, and manufacturing of the oil filter and pump
		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, 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 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 system fans are free from potential physical damage
		FSRM08.07	To avoid excessive engine heating the development team shall ensure thermal system fans pull air from a cool source
		FSRM08.08	To avoid excessive engine heating the development team shall ensure engine ventilation is sufficient to provide appropriate air movement through engine bay
		FSRM08.09	To avoid excessive engine heating the development team shall ensure the thermal 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, installation, and manufacturing of thermal system and its components

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

	The applied torque magnitude shall match the torque magnitude requested	FSRM09.02	The operator and HSC shall be responsible for torque request magnitude
		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 direction	FSRM10.01	The EM/engine actuated torque direction shall be controlled by the HSC and PRNDL controls
		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	To avoid contamination of the EM housing or EM coolant system the development team shall ensure proper mounting, installation, and manufacturing of the EM and housing
		FSRM12.09	To avoid contamination of the EM housing or EM coolant system the 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
		FSRM12.10	To avoid contamination of the EM housing or EM coolant system 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
		FSRM12.11	To avoid EM overheating the development team shall ensure EM thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the EM
		FSRM12.12	To avoid EM overheating the development team shall ensure EM coolant system fans are free from potential physical damage
		FSRM12.13	To avoid EM overheating the development team shall ensure EM coolant system fans pull air from a cool source
		FSRM12.14	To avoid EM overheating the development team shall ensure proper mounting, installation, and manufacturing of EM coolant system and its components
		FSRM12.15	To avoid EM overheating the development team shall ensure EM coolant system bolts, 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
		FSRM12.17	To avoid EM overheating the development team shall ensure a real time EM temperature display is visible by the operator
		FSRM12.18	To avoid EM overheating the operator shall ensure proper vehicle operation (reduce engine speed/load)
		FSRM12.19	To avoid low EM resistance and insufficient insolation between windings the development team shall ensure EM thermal system components (radiator, coolant level, fans) are functional and sufficient to cool the EM
		FSRM12.20	To avoid low EM resistance and insufficient insolation between windings the development team shall ensure EM bolts, hoses and mounting hardware are securely fastened and free from potential loosening or unintended movement
		FSRM12.21	To avoid low EM resistance and insufficient insolation between windings the 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 current necessary to meet EM torque request	FSRM13.01	The HSC shall request current from the ESS based on operator intent
		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 requirement	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
		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 at the time intended	FSRM15.01	The HSC shall request current from ESS at the time of the operators request
		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 max operating parameter	FSRM16.01	The ESS shall impose charging and discharging operating parameters
		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 from the engine to the driveshaft	FSRM18.01	To avoid transmission fluid failure the development team shall ensure proper mounting, 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 components contained within the vehicle, prevent debris from being thrown by rotating tires, allow operator to see in low light scenarios, protect operator from environmental debris, absorb impact of minor collisions, signal request to turn or brake, and allow the operator to have surrounding views	FSRM19.01	To avoid a hood failure the development team shall ensure proper mounting, installation, and manufacturing of the hood, and latch
		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
		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
		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	Engine Control Module
EM	Electric Motor
EMC	Electric Motor Controller
EMI	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
O	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