System Theoretic Process Analysis of Electric Power Steering for Automotive Applications

By

Rodrigo Sotomayor Martínez

S.B. Mechanical Engineering with a minor in Industrial Engineering
Instituto Tecnológico y de Estudios Superiores de Monterrey, México, 2008

Submitted to the System Design and Management Program
In Partial Fulfillment of the Requirements for the Degree of

Master of Science in Engineering and Management

at the

Massachusetts Institute of Technology

June 2015

Signature of Author _____
System Design and Management Program
May 15, 2015

Certified by _____
John Thomas
Research Scientist, Department of Aeronautics and Astronautics
Thesis Co-Supervisor

Certified by _____
Nancy G. Leveson
Professor of Aeronautics and Astronautics and Engineering Systems
Thesis Co-Supervisor

Accepted by_____
Patrick Hale
Director
System Design and Management Program

Full Disclaimer: The opinions expressed in this thesis are those of the author and do not reflect the official policy or position of Ford Motor Company or other Automobile manufacturer.

(Page intentionally left blank)

A System Theoretic Process Analysis of Electric Power Steering for Automotive Applications

By

Rodrigo Sotomayor Martínez

Submitted to the System Design and Management Program
In Partial Fulfillment of the Requirements for the Degree of
Master of Science in Engineering and Management

Abstract

The automotive industry is constantly challenged with meeting and exceeding customer expectations while reducing time to market of new products in order to remain competitive. Providing new features and functionality into vehicles for customer satisfaction is becoming more challenging and driving design complexity to a higher level.

Although traditional methods of Product Development Failure Mode identification such as FMEA (Failure Mode and Effect Analysis) or FTA (Fault Three Analysis) have been used to analyze failures in automotive systems, there are limitations when it comes to design errors, flawed requirements, human factors implications, and component interaction accidents in which all components operated as required but the system behavior was not as expected.

In order to determine if there is room for improvement in current automotive product development process, this thesis applies Dr. Nancy Leveson's Systems-Theoretic Process Analysis (STPA) technique to compare and contrast with a Failure Modes and Effects Analysis (FMEA) approach as used in the automotive industry through a case study.

A formal method of comparing results is proposed. This study found limitations with FMEA in terms of identifying unsafe interactions between systems, anticipating human error and other behaviors dependent on human interaction, identifying engineering design flaws, and producing requirements. STPA was able to find causes that had a direct relationship with those found in FMEA while also finding a portion of causes related to a higher level of abstraction of those in FMEA. STPA also found a subset of causes that FMEA was not able to find, which relate mainly to engineering design flaws and system interaction.

Thesis Co-Supervisor: John Thomas
Title: Research Scientist, Department of Aeronautics and Astronautics

Thesis Co-Supervisor: Nancy G. Leveson
Title: Professor of Aeronautics and Astronautics and Engineering Systems

(Page intentionally left blank)

Acknowledgements

I am thankful to Professor Nancy Leveson, for changing my perception regarding safety management and accident causation. I was able to learn the value of taking system theory applied to hazard analysis and witness how these ideas are changing the way people think about safety. I would like to extend my sincere thanks to Dr. John Thomas for his guidance and encouragement throughout my thesis work. With your guidance I was able to endeavor on exploring new possibilities on a topic that is relevant to me while questioning state of the art. I must thank William Bouse, whose direction and support made this work possible.

I would also like to thank my colleagues and friends in Ford of Mexico. Mauricio Burguete, Aldo Martínez, Luis Monterrosas, and Edgar Tlapalamatl, thank you for your help and friendship. Over the past two years and a half you have provided invaluable support at the time I needed the most.

I need to thank Marcos Perez for giving me the opportunity to pursue my Master degree at MIT. I like to acknowledge the Global Chassis Office of Ford Motor Company for their encouragement and allowing me the flexibility to attend to the System Design and Management program while growing my career and contributing to my knowledge. This degree would not have been obtained without the support of many managers, including Rob Gelven, Flavio Gonzalez, Dave Rodgers, Greg Hayden and Felicia Paluzzi, as well as the rest of the team of Chassis Integration.

To my family, thank you for pushing me to aim higher and supporting me to pursue this dream come true. To my Mom, Norma, thank you for your love and tender care. To my Dad, Juan, thank you for your encouragement. To my brothers, Juan Pablo and Diego, you have been a constant source of support and friendship.

Finally, my deepest gratitude is to my wife Cristina. Thank you for your patience, resilience, and tender love during all these challenges. I would not have done any of this without you.

(Page intentionally left blank)

Table of Contents

List of Tables

List of Figures

(Page intentionally left blank)

Chapter 1: Introduction

Motivation

Corporations seek to gain competitive advantage in product development in the form of innovation, efficiency, quality and the delivering of products that provoke excitement in drivers. The increasing demand of new products that satisfy and surpass customer expectations is a constant battle among automotive incumbents. This race puts pressure on product development organizations to meet time to market of new products and increase functionality of vehicles. Complex system interactions stretch the limits of traditional failure causal models, and it is not possible to exhaustively test every possible interaction in modern vehicles. The purpose of this thesis is to apply a System Theoretic Process Analysis (STPA) to a complex system in the automotive product development process and compare it with a widely used process Failure Mode and Effects Analysis (FMEA) to understand if there is room for improvement in terms of ensuring safe functionality and reducing unanticipated behavior.

Failure Mode and Effect Analysis is a forward search technique based on an underlying chain of events model that was developed by reliability engineers to permit them to predict equipment reliability [1]. It is currently used in the automotive industry to identify potential failure modes in a design and to document actions to mitigate findings, among other things. System Theoretic Process Analysis (STPA) is a new hazard analysis technique based on systems theory to identify scenarios leading to identified hazards and thus to losses so they can be eliminated or controlled [2].

The pressure of innovation and improving time to market may have a negative effect on new product launches if the process does not evolve with new technology. Responsible innovation must ensure that the customers make use of the product in safe conditions. By adapting Product Development Processes to increasingly complex architectures, vehicle manufacturers can ensure a positive customer experience, which in turn may help to achieve goals for short and long-term success.

In recent years most automobile manufacturers have faced unwanted outcomes in terms of unwarranted cost and faults associated with vehicle controllers and sensors. Those unwanted outcomes constantly increase the safety challenges posed by integrating new functionality and implementation of complex electronic-mechanic systems [3]. Given the severity of those failures

and the industry trend to widen the use of embedded control systems to provide safety critical functions, this research questions if current product development practices remain effective and there is room for improvement to prevent accident causes, especially in complex systems.

The development of new automotive applications takes a great amount of time and resources. Organizations around the world spend years in preparation, testing and iterating designs employing methodologies such as FMEA that are used as a state of the art to deliver safe functionality to their customers. However recent studies show a trend of growing portion of automotive recalls associated with software error [3]. These accidents are not associated with the development of a specific Automotive Organization however the research points out that most of these recalls are associated with flaws in implementation of control actions. Why do these designs escape the review processes of the industry? Are the methods used in the industry effective to prevent these accidents?

Failure Mode and Effect Analysis (FMEA) is a widespread and preferred methodology to analyze hazards in many industries. In the automotive industry, it is used to analyze designs, reduce parts variability and implement manufacturing processes that are capable of meeting the design specifications. STPA is a relatively new approach that has been applied to many industries revealing promising results. STPA was developed to address limitations when it comes to design errors, flawed requirements, human factors implications, and component interaction accidents in which all components operated as required but the system behavior was not as expected. Although STPA has been applied to automotive systems showing promising results, a formal comparison between the two methods on a relevant automotive system has not been done.

As demand for functionality from automotive electronic module increases, so does the complexity in the vehicle architecture, which in turn leads to bigger challenges in intellectual manageability. Design teams find themselves spending countless hours filling in worksheets with information that might not be yet available, which drives constant iteration. The process then becomes tedious and complex to manage. Thus, facilitating the safety development through improving the way potential accidents are found and prevented in new designs is a cornerstone for automotive organizations. The constant drive for innovation and to deliver new functionality in a way that the industry requires accentuates the motivation of this thesis.

1.1 Goals

The goals of this thesis are:

1. To perform STPA on a complex automotive system to compare and contrast with the current product development process (FMEA) to find failure modes.
2. Understand strengths and limitations of the current process as compared to STPA to find and prevent accidents in the product development process.
3. Propose a timeframe for STPA introduction within the automotive Product Development Process.
4. Identify and provide opportunities of improvement for the current automotive product development process.

1.2 Research questions

This thesis proposes the following research questions:

1. Is FMEA the most effective tool for complex automotive systems?
2. Is doing a FMEA enough in early design stages to ensure safety when developing complex automotive systems?
3. What does it take in terms of resources and planning to develop a robust FMEA to capture all possible interactions and critical safety constraints?
4. What are the resources required to perform a STPA analysis and how do they compare to the ones needed with FMEA?
5. Can STPA be implemented effectively with a complex automotive system? And how the results compare to the ones obtained through FMEA?

1.3 Research methodology

In order to answer these questions a complex automotive system is selected and both methodologies are applied through a case study. To understand the effectiveness of FMEA at early stages of design, SAE J1739, a widely used automotive standard, is performed over the selected system. STPA is also applied to the same system in order to compare effectiveness and compare how accident prevention is addressed in both methodologies. Chapter 5 proposes a formal method for comparing the results.

The architecture of the modern automobile continues to evolve. The wide use of embedded control systems depends on its correct interaction to provide function. Since more functionality is being demanded from the integration of such systems, there is a need to assess if current hazard analyses are suitable to detect all of the system related hazards in early stages of the product development cycle.

Chapter 2: Literature overview

2.1 Failure avoidance in the automotive industry

Passenger vehicles produced nowadays are composed of the integration of more than 10,000 moving parts that are installed in a production line to provide function[4]. Before electronics started to be used in automobiles as often as in today's latest vehicles, the industry arguably followed a dominant design established in 1923 [5] to which significant improvements and innovation in product design are traced to when Dodge introduced the all-steel, closed body, internal combustion engine automobile [6]. After World War II, the rate at which product innovation was introduced in the automobile industry declined steadily as the industry stabilized between the number of entrants and exits. After the 1960's, the innovation in industry came face to face with quality, reliability and manufacturing processes, such as the Toyota Product Development System [7].

Although process and automotive parts design were refined, technology and preferred architecture changed occasionally in an integrated systemic way and the industry remained in a Specific Phase. Specific Phase is defined by Utterback and Abernathy [5] as the period of time after the dominant design in an industry appears and competition would shift from differentiation to product performance and cost. Probably because of this reason, the need for reliability improvement of the automotive industry gained more strength. Reliability methods such as FMEA became appealing to the industry and proved to be successful in controlling variation and failures associated with reliability of components.

2.2 FMEA in automotive industry

FMEA is a structured approach for identifying possible failures in a design, production or process [5]. It is also used for mitigation of risk by requiring appropriate actions given the known failure modes of a process or design [8]. FMEA was developed by reliability engineers working in the military in late 1940's [9], but it was the introduction into the Apollo program by NASA that expanded its popularity. NASA reports demonstrated enhanced individual items integrity and reliability when failure modes were previously known [10]. NASA included a variation of FMEA where it used a critical parameter method which was called Failure Modes, Effects and

Criticality Analysis (FMECA). It was not long after that the automotive industry adopted this methodology and included it in its process

The automotive industry included the usage of FMEA as a standard in its development process in the early 1980's. The method was first used by a car manufacturer, Ford Motor Company, which applied it to assess and solve quality issues raised by the Ford Pinto [11].

There are several standards used in a wide range of industries for FMEA, from military, as mentioned before, to semiconductor industry. Automotive industry consistently employs FMEA for Failure Mode Avoidance. Most automotive organizations have published related standards that provide detailed guidance on applying the method. Such methods are used both by car manufactures and by its supply base. SAE J1739 and the Automotive Industry Action Group (AIAG) are common processes referenced in these organizations [8][12].

SAE J1739 details the scope of FMEA and provides guidance on the identification and mitigation of risk by stipulating appropriate terms, requirements, ranking charts and worksheets [8] to recognize and evaluate potential failure of a design or process. At the beginning of the methodology, a design or process team needs to evaluate and agree on the elements to be analyzed. It often employs functional diagrams of parts that represent the primary relationships between the items covered by the analysis and its interaction with other parts. Although the structure of such analysis is left open to better suit the purpose of the evaluation team, it seeks to establish a logical order of the analysis. A system boundary is defined and the team should discuss and document interfaces with other components and systems. Interactions between the system and surroundings may or may not be analyzed, and it is left for the team to decide if an Interface FMEA should be employed to study these interactions.

In preparation for the analysis, the team should review inputs related to the standards that might contribute to the analysis such as [8]:

a. Warranty data
b. Recall data
c. Engineering Requirements
d. Drawings
e. Lessons learned
f. Preliminary design verification plan

g. Best Practices
h. Baseline/family or prior DFMEA
i. Higher level FMEA (System FMEA or Design FMEA)
j. Bill of Material
k. Manufacturing feasibility study
l. Diagrams such as a Block Diagram or Boundary Diagram

Functional FMEA is often employed for new developments and designs. The analysis begins by listing the intended functions the design is set to achieve. There are no specific rules on how these functions are determined in the SAE standard, and each organization employs different strategies to determine which functions will be analyzed. A preferred practice is to start with the highest level of abstraction of the intent of the system and decompose into tangible functions through System Engineering methods. After all functions have been properly identified, a revision and identification of potential failure modes of those functions needs to be performed. Potential failure modes are defined as:

> "[…] the manner in which a component, subsystem or system could potentially fail to meet or deliver the intended function(s) or requirements." [8]

Such failure modes must be captured independently in a worksheet and the team assigns a priority to each function in order to provide a future mitigation strategy for the process as shown in Table 1. The standard recommends treating each potential failure mode independently from each other to enable identification of unique failure modes.

After a failure mode has been recognized and recorded, potential effects of each failure mode must be assessed. Potential effects of failure are defined as:

> "[…] the consequences or results of each failure mode. […] The effects should be considered against the next level up assembly, the final product and the customer when known." [8]

Once functions are provided, failure modes are assessed, and potential effects are populated in the standardized table as shown in Table 1. A Severity Ranking Number must be provided for

each effect. Severity Ranking is contained in the SAE J1739 standard but a summary can be found in the Appendix 2 of this thesis.

The Classification column is optional in DFMEA. Classification is used to highlight failure mode or causes that are recognized as extraordinary or may have high impact if a failure occurs. Such classification can also include management concerns. Such causes can be classified into Critical Characteristics and Significant Characteristics. Critical Characteristics are those that could lead to violating a regulatory requirement or to violating the safe operation of the vehicle [8]. Significant Characteristics are those that are deemed as a concern for the team but not necessarily endangering compliance or safety of the vehicle [8]. The design team is free to choose the symbol that is assigned to each type of characteristic but the symbol must remain constant throughout the analysis and cascaded later on to other users, such as the PFMEA team.

After the Effect of Failure is included in the worksheet, the evaluation team needs to analyze how such failure could occur. The causes for each Potential Effect of Failure should be populated in the worksheet. Potential Causes of Failure is defined as:

> […] is an indication of how the failure could occur. The consequence of a cause is the failure mode.[…][8]

After Potential Causes are identified, each cause must be assessed with Occurrence criteria. Although it is beyond the scope of the methods to determine an appropriate criterion for Occurrence, Appendix 2 shows a recommended chart from the SAE J1739 standard [8]. The occurrence ranking considers the likelihood of occurrence during the design life of the product. Such value determination is a relative number and can be updated based on warranty data about useful life of the product. The ranking takes into consideration the prevention-type controls used in the design. SAE J1739 standard suggests that if a new design or new technology is being evaluated, the Occurrence ranking can be reduced from 10 (new design, no history) once test or field data is available.

The manner in which implemented Prevention Controls avoid the identified causes, failure mode or effect by design, should be indicated in a different column. Prevention design controls are

based on the application of automotive standards, specification, design rules, legal standards, etc. as means of preventing a failure from occurring on the field.

When applicable, Detection Controls should be analyzed similarly to how Prevention Controls are determined. Detection controls describe how cause or failure mode is detected either by analytical or physical methods. Such analysis is used as an input to a third rank called Detection in the worksheet. When not known or not applicable, the Standard SAE J1739 says to assign a high value according to the ranking provided in Appendix 2 (i.e., Detection 10).

The outcome of the criteria described above is used for the determination of a Risk Priority Number. The Risk Priority Number is defined by equation 1.1:

$$RPN = S \times O \times D \quad \text{.....(1.1)}$$

Where:

S refers to the Severity ranking.

O refers to the Occurrence ranking.

D refers to the Detection ranking.

According to the SAE J1739 Standard, the Risk Priority Number (RPN) is commonly used as a tool available for the evaluating team to evaluate potential risk. It is also specified that although the RPN may be used as an indication for priority, the result should not be used as an absolute criterion to address potential issues. Higher prioritization is given for higher severity ranking failure modes, causes or effects. The Standard also details a Criticality index, determined by the result of the multiplication of Severity times Occurrence, which is intended to provide a guidance to prioritize efforts.

Function/ Requirement	Potential Failure Mode	Potential Effect(s) of Failure	SEV	CLASS	Potential Causes	OCC	Current Prevention Controls	Current Detection Controls	DET	RPN	Recommended Action	Target Completion Date & Responsible	Action Results				
													Actions taken & Effective Date	SEV	OCC	DET	RPN
Wheel and tire assembly / Function: Support vehicle weight	Wheel and tire assembly does not support vehicle weight	Unable to control vehicle	8		Flat tire	8	- Wheel and tire structural robustness test	- None	10	640	- Include tire pressure monitor (TPMS)	John Doe, May-2015	TPMS included in vehicles, June-2015	8	8	4	128
		Vehicle not operable	10	YC	Tire and wheel assembly does not support GAWR	5	- CAE - Wheel and tire structural curve selection for GAWR + TBD σ	- Structural testing at component and vehicle level	2	100	- Strong correlation of CAE and durability test, none at this time	Revise data of component structural testing	None				
		Customer not satisfied	10	YC	Tires do not stand vehicle duty cycle (premature wear)	5	- CAE - GAWR + TBD σ setting	- Traction to failure test - Structural test at vehicle level	5	250	- Revise GAWR + TBD σ after results from traction to failure test correlation	John Doe, May-2015	- GAWR and CAE correlation after durability with high confidence	10	5	2	100

Table 1 - FMEA excerpt for explanatory purposes only

When the RPN is determined, the evaluation team defines which causes need to be addressed to prevent or mitigate the risk of the failure (Severity). The recommended actions are intended to reduce either the likelihood of failure (Occurrence) and/or improve the ability to detect failures (Detection).

Once Potential Failure Modes, Effects and Causes are determined, SAE J1739 details the format of how subsequent actions will be taken to mitigate, reduce or control the causes.

After Recommended Actions are determined and actions prioritized, assignment of responsible contact and target completion date should be included. Once the date set up for review is due, the team must assess each recommended action and populate the field named as *action taken* to compare results. The expectation of those actions is that the Occurrence and/or Detection mechanism will be improved such that the RPN is reduced. The outcome of the exercise is that the system behaves more reliably with respect to the intended functions analyzed and supported by a revised ranking metrics. Only a design change can bring a reduction in the severity ranking. The Design FMEA commonly provides description of how design controls are employed to detect failure modes of the system in the detection methods section. Such descriptions are used to also set targets for performance testing. Besides providing structure and completeness of analysis of identified functions, FMEA is strongly connected to the automotive process because it provides structure on how to mitigate and control design and process characteristics. Such methodology is aimed to ensure that the automotive product does not fail. Many of these principles have been applied to a wide variety of systems across the vast majority of the design and production process.

As previously described, the method assumes that the system is correctly manufactured to the design intent. The standard indicates that each function should be considered independently of another function, which prevents assessment of multiple failure scenarios that may occur in complex and integrated systems [1]. Because FMEA focuses on failures of items that occur internally, it avoids recognizing scenarios that may happen from the integration of systems in which no failure has occurred. FMEA requires a block diagram preceding the elaboration of the worksheet, however the method does not provide a clear direction on how to address identified interaction. Therefore, the analysis team often requires developer expertise on how the system may interact with other systems. Conflicts may arise when correctly functioning systems interact

with each other if their requirements do not consider combined operations or are otherwise flawed [1].

Traditional methods of hazard analysis such as FMEA, have helped increase system reliability once all the system interactions have been understood and failure modes identified. However, common criticisms about FMEA include that all the significant failure modes must be known in advance [1]. Although failures may be found after evaluation, if found late in the Product Development Process, the design team may find it difficult to completely address all design flaws due to schedule pressure, limited resources and non-anticipated changes.

2.3 Systems Theoretic Process Analysis

Leveson [2] introduced Systems Theoretic Process Analysis (STPA) to capture more types of accident causal factors, including social and organizational structures. STPA is based on Systems Theory rather than on Reliability Theory, and more specifically on the System Theoretic Accident Model and Processes (STAMP). STAMP focuses on the emergent properties of engineered systems rather than on the reliability of individual components. STAMP treats safety as a control problem. It is a new causality model that emphasizes enforcing behavioral safety constraints rather than preventing failures [2]. In STAMP, component failure accidents are still included, but the conception of causality is extended to include component interaction accidents [2].

STAMP uses system theory to represent the system as hierarchical control structures, where each level imposes constraints on the activity of the level beneath it [2]. This hierarchical structuring allows the system model to capture not only accidents due to component failures and component interactions but also extends to understanding incomplete or missing requirements from external regulatory bodies. Leveson [2] points out that viewing safety as a control problem leads to a broader examination of how control actions fail or succeed at enforcing safety rather than focusing on reliability and component failure.

While STAMP is accident causality model based on system theory, STPA is a step-by-step process based on STAMP also proposed by Leveson that was designed to analyze safety in socio-technical systems with many diverse components interacting together [13]. STPA starts by defining the system of interest and determines the accidents that the system should not

experience [14]. Subsequently, the system accidents and hazards are defined. An accident is defined in STAMP as “undesired and unplanned event that results in a loss” [2]. Hazards are “system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss)” [2]. As described before, the system is defined as a hierarchical structure with numerous levels; for each level there is a set of control constraints on the level beneath it. Figure 1 shows a generic example of a hierarchical control structure. Enforcing safety constraints in the entire sociotechnical system, is needed to ensure safety [2]. Commands or control actions are given by higher levels of control processes to lower levels throughout the hierarchy and feedback is provided from lower levels to higher levels [13].

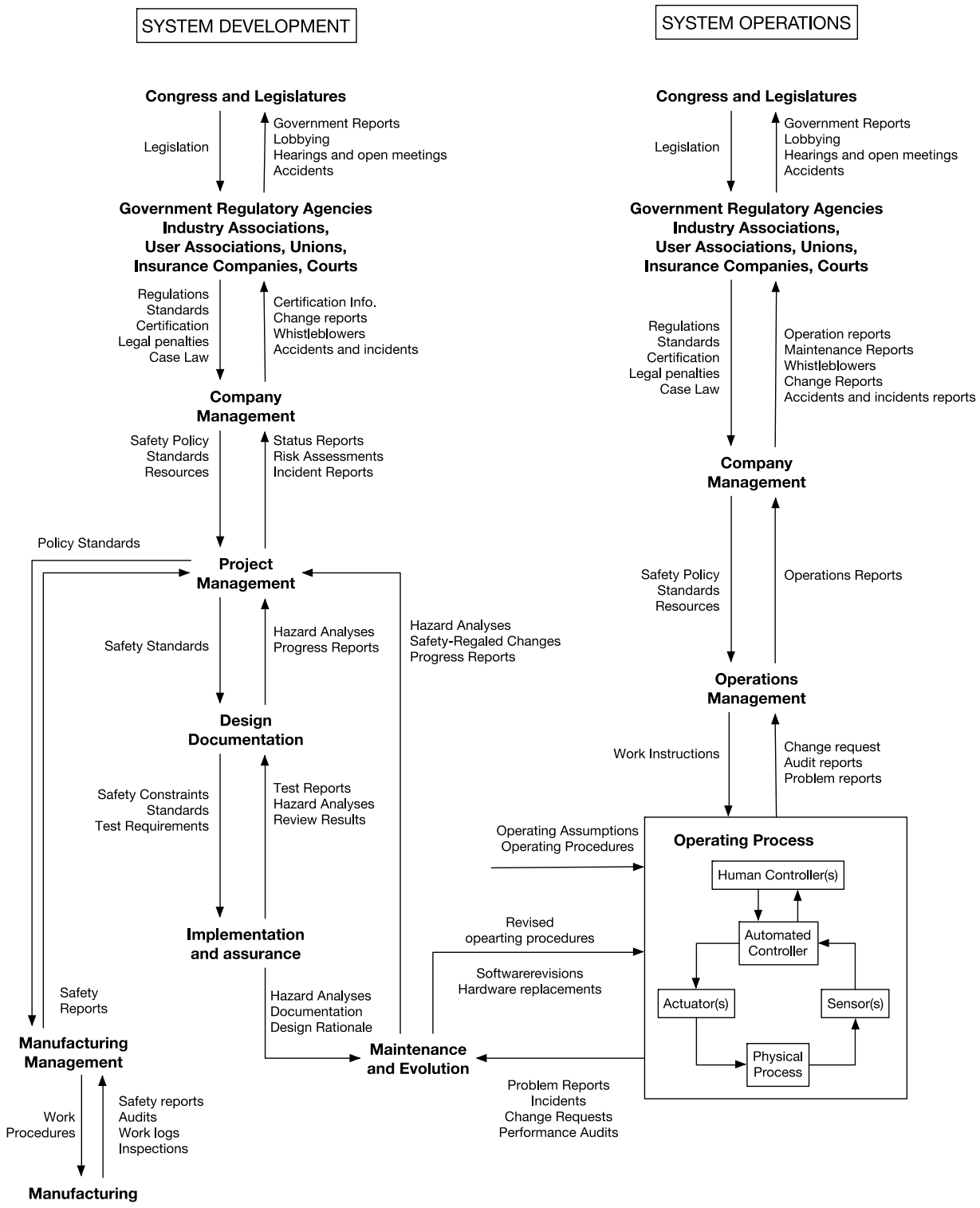

Figure 1 - Generic example of a hierarchical control structure [2]

Understanding the controller process models provides insight on interaction related accidents. Failures where individual components achieve the functions they are required to deliver but their interactions leads to unsafe system behaviors are more common than before. Consequently, it is important to understand when controllers may issue control actions, executed by actuators in a manner that is unsafe [2]. According to STAMP [2] there are four types of unsafe control actions that may lead to hazards and that must be eliminated or mitigated to prevent accidents:

1. Incorrect or unsafe control commands are given that lead to hazards.
2. Required control actions (for safety) are not provided that are required to prevent hazards.
3. Potentially correct control commands are provided at the wrong time (too early or too late).
4. Control is stopped too soon or applied too long.

Different instances of these types of Unsafe Control Actions (UCA) are often captured in a table showing the conditions under which the control actions are hazardous. Table 2 shows an example of a table of Unsafe Control Actions. After they have been identified, each UCA is re-written as a safety constraint. These safety constraints are high-level constraints on the system behavior that must be enforced to ensure that an accident does not occur. This first part of the analysis is called Step 1.

Consider an example of an electronic parking brake operation. The control action is to power on and off the actuator to lock the rear wheels. For this example, the vehicle is thought to be in motion.

Control Action	Not providing Causes Hazard	Providing Causes Hazard	Wrong timing or Oder Causes Hazard	Stopped too soon or Applied too long
Power off	Power not turned off when vehicle is in motion	Not hazardous	Controller waits too long to turn off power when vehicle starts motion.	Not applicable
Power on	Not hazardous	Power turned on while vehicle is in motion	Power turned on too early when vehicle remains in motion.	Not applicable

Table 2 – Table for identifying hazardous behavior[1]

Then STPA Step 2 focuses on finding the reasons the UCA's found in Step 1 may be issued and identifying scenarios leading to hazardous control actions that violate the component safety constraints [2].

The engineer is asked to provide a set of scenarios leading to unwanted system behavior for each UCA. The purpose of the scenarios is to aid the engineer to critically think of plausible causes that may occur in the system context. Once the causal factors that may lead to system hazards have been identified, they can be used to write requirements on the system components and their interactions. The results of the causal factors analysis are used to eliminate or reduce the presence of hazardous scenarios.

Thomas showed how STPA can be applied iteratively [15]. The first iteration of STPA is done quickly focusing on more conceptual issues and deriving an initial set of safety requirements to drive the following design decisions. The second iteration of STPA focuses on more detailed requirements and is used to provide immediate feedback regarding more detailed design decisions..

[1] Table 2 shows an example on how Unsafe Control Actions are identified. Electric parking brake was selected for explanatory purposes only.

STAMP has been used with positive results in many multidisciplinary fields that include aerospace, defense, energy, chemical, healthcare and transportation systems [16]. STAMP has proven to be particularly useful to capture behavior for complex socio-technical systems that include human and software-intensive structures where interactive effects between systems causes hazards while each component individually delivers designed function [13].

2.4 Summary of literature review

FMEA is considered as the state of the art to perform potential failure mode analysis in the automotive industry. Although its use is widespread and well accepted by both OEM's and the supplier base, accidents and recalls involving multiple car manufacturers is a growing concern. STPA on the other hand is a relatively new method developed to address the limitations of methodologies such as FMEA, but it hasn't been rigorously compared to an automotive FMEA, there are very few automotive examples demonstrating its use, and few evaluations of its effectiveness in an automotive context.

Chapter 3: FMEA analysis on automotive system

In this chapter, FMEA is applied to an automotive system. The next chapter applies STPA to the same system for comparison. The first step is to select an automotive system to study. Electric Power Steering (EPS) is chosen because it is a complex automotive system that maintains interactions with other vehicle systems, including hardware, software, and the human driver; consequently it could provide a meaningful comparison between these two methods.

3.1 Case Study Overview

One of many automotive systems that is evolving is the steering system. Electric Power Steering (EPS) has been positioned as preferred equipment in today's common vehicle architectures to assist the driver in steering efforts to direct the vehicle [17]. Once considered a luxury option, there is a trend of becoming standard in most new passenger vehicles produced around the world. The pursuit of this trend is attractive to vehicle manufactures due to several reasons that include: the simplicity of architecture, ease of installation in an assembly line, and increasing availability of integrated systems that allow additional feature development such as varying the amount of assistance under different driving conditions. The owner benefits because assistance is provided only when commanded, which leads to improved fuel economy. The EPS provides assistance through the use of an electric motor that delivers torque when the system senses that the driver is requesting steering assistance. EPS is increasingly being preferred over Hydraulic Power Steering Systems because it provides assistance upon driver request, while Hydraulic Power Steering is constantly running a hydraulic pump to provide assistance.

The FMEA analysis is performed on a generic EPS system with the objective of covering common architectures. It should also be considered that the analysis is performed in the early stages of the design process so it can be used as a baseline for design decisions that would allow mitigating potential failures. Therefore, the recommended actions section in FMEA would not be shown because they are set after initial testing has been completed. The analysis is not based on a particular architecture, because the architecture may not be known during early states of the design process. In order to provide results within the time constraints to develop this thesis, it was necessary to select a fictional EPS system. The focus of this work is to understand limitations of both methods by comparing them and not to design a new system. Although fictional, the EPS system selected is considered realistic as it is based on common

architectures of EPS Systems used in modern production automobiles. It is the intent of this thesis that the work presented could be applicable as a base for analysis of most EPS systems.

The increased availability of integrated systems favors choosing EPS as a preferred system to perform a case study because new features that involve the use of electro-mechanical components can be incorporated faster. Such new features include Active Park Assist, which enables the driver to allow the vehicle to search for a parking spot while driving and upon driver command to initiate parking maneuvers without the driver needing to control the steering wheel. The incremental interaction of different vehicle subsystems pushes the limits of traditional hazard analysis used in the industry to exhaustively investigate every potential interface interaction hazard that needs to be controlled in order to safely provide the desired function.

3.2 Overview of Electric Power Steering

Electric Power Steering (EPS) is an electro-mechanical device that assists the driver in steering by increasing the mechanical force provided by the driver to the outer tie rods that turn the front knuckle, which subsequently turns the wheels and tires. Such assistance allows the driver to provide desired direction to the vehicle during operation. The EPS attaches to the steering column at one end and to the front knuckle at the other end. The driver provides steering commands through the steering wheel into the steering column. The EPS consists of an input shaft and pinion, an electric motor, angular and torque sensors, inner and outer tie rods, a mechanical rack and housing and a controller called the Steering Control Module (SCM). Figure 2 shows the elements described above. The figure is only for explanatory purposes.

The system interacts with other vehicle modules to monitor and provide required assistance to the driver. In most architectures, it receives information about vehicle speed from the Anti-lock Braking System Control Module (ABS CM) and engine speed and wheel torque from the Engine Control Module (ECM). The Steering Control Module (SCM) sends information about the position of the steering wheel to the ABS CM and the state of the system to the Body Control Module (BCM), which passively warns the driver about the state of the system through the cluster. The cluster informs the diver if there is a failure in the system or if maintenance is required.

Figure 2 - Electric Power Steering system for explanatory purposes only [18]

Figure 3 shows a generic block diagram of the EPS system

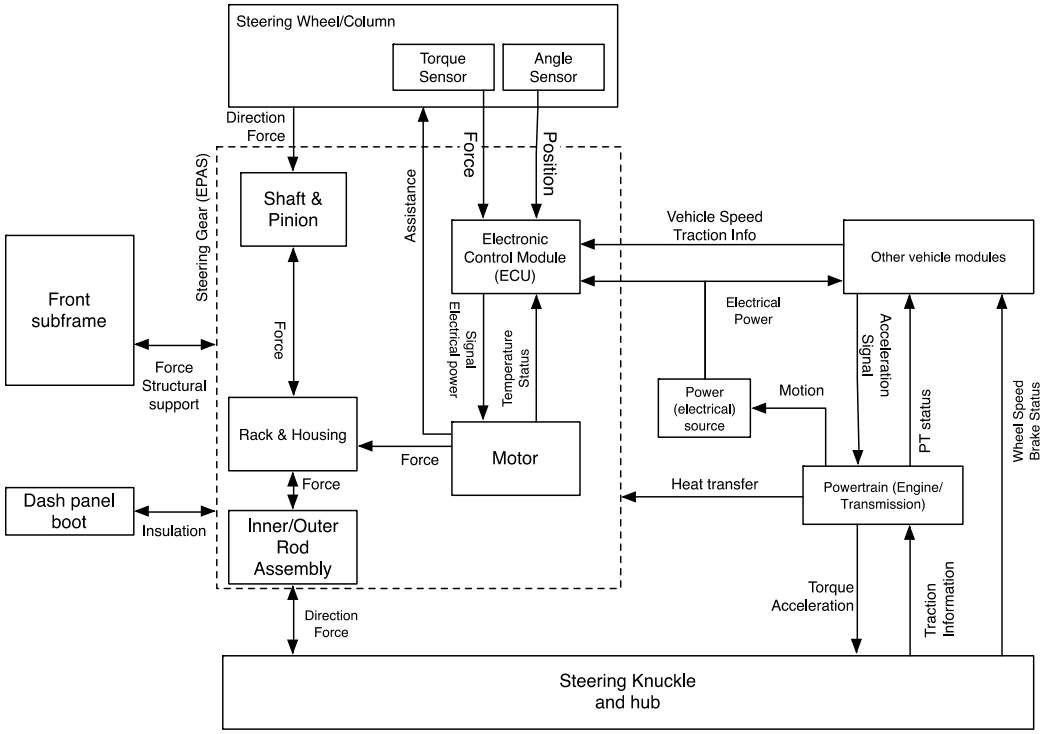

Figure 3 - Generic EPS Block diagram

3.2 Overview of main functions

FMEA is performed on the system to analyze the system's main functions in order to find, mitigate and avoid potential error states and failure modes so functions are reliably provided over the operational range of the vehicle [19]. The SAE J1739 standard does not provide guidance on how these functions should be defined. The standard, however does accentuates that the "[…] function(s) of each item being analyzed must be written […]" [8] in the worksheet and that "The more precise the function, the easier is to identify failure modes for preventive/corrective action" [8]. The following are functions that were defined for this case study for hardware, but it is up to each manufacturer and their design organizations to determine the depth of the functions to analyze:

1. Transfer diver input (torque and angular displacement) to linear displacement and force to knuckle assembly.
2. Convert linear displacement/force of the steering knuckle to angular displacement/torque of the steering column to provide feedback from road to driver and allow self-centering of the steering.
3. Provide damping to isolate the driver from road harshness and driveline input.
4. Provide assistance to reduce driver's steering efforts to levels that match the functional requirements of the vehicle.
5. Vary power assist with vehicle speed.
6. Provide function under the Noise Vibration and Harshness (NVH) targets.
7. Meet electromagnetic compatibility (EMC) requirements
8. Meet power consumption targets.
9. Position the inner and outer ball joint centers for correct suspension geometry.
10. Position EPS system properly to ensure correct column routing and steering uniformity.

The system selected for this case study has an embedded control system structure, so function is provided through both hardware and software. There is no clear direction on whether to combining software and hardware functions in the same worksheet or to treating them separately and it is usually up to the design team to decide. The SAE J1739 standard does not provide specific guidance on which approach to use. In this case study, it was decided to keep

them separate to avoid overlooking failure modes in the software. The software functions required are listed:

1. Provide assistance to reduce driver's steering efforts to levels that match the functional requirements of the vehicle.
2. Vary power assist with vehicle speed.
3. Allow service of the system.
4. Provide electrical signals to other systems.
5. Diagnose high friction conditions in the system.
6. Transfer diver input (torque and angular displacement) to linear displacement and force to knuckle assembly.
7. Convert linear displacement/force of the knuckle arms to angular displacement/torque of the steering column to provide feedback from road to driver and allow self-centering of the steering.
8. Provide function under the Noise Vibration and Harshness (NVH) targets.
9. Meet power consumption targets.

It is important to notice that some of these functions are repeated in the software and hardware list. That means that the system uses both hardware and software methods to achieve the function desired, however, following SAE J1739 recommendation, both parts are treated separately to analyze each domain failure mode independently and find its associated causal factors that could impede the delivery of the desired function.

It should also be noted that this analysis has been performed with a level of abstraction that allows applicability for most EPS architectures.

3.3 Failure Modes and Effects Analysis

The full FMEA analysis and results can be found in Appendix 2. This section explains the main parts of the analysis and reviews the types of results that were found.

Identifying Failure Modes

Table 3 shows an excerpt of the hardware FMEA worksheet for function *4,* i.e.. *Provide assistance to reduce driver's steering efforts to levels that match the functional requirements of the vehicle* and failure mode *4.1 No assistance - Full loss of power assist*. The first two causes that could lead to the potential failure mode are also shown. The occurrence of these causes is highly dependent on the manufacturer records of quality data and understanding of the system. If the design is completely new, an occurrence of 10 should be used. Most manufacturing firms expect to use legacy designs when applicable due to high confidence on the design reliability. If there is a high confidence in the data of similar designs or there is a strong correlation between simulation and testing, SAE J1739 allows using lower rankings. However proof and validation data to sustain such ranking must be available.

Potential Causes Identification

The following is a list of Potential Causes that could contribute to the driver not getting assistance upon request:

(4.1.1) Belt assembly does not transmit torque between Electric Motor and Rack.
(4.1.2) Electric motor does not provide torque to belt assembly.
(4.1.3) Torque sensor does not provide torque measurement to Electric motor ECU.
(4.1.4) Torque sensor cover assembly does not protect outboard housing assembly.
(4.1.5) Power supply harness does not supply required current to Electric motor.
(4.1.6) Damage / wear of gear system
(4.1.7) Stalled engine.
(4.1.8) Connector fittings or attachment failure.

Function	Potential Failure Mode	Potential Effect(s) of Failure	SEV	CL	Potential Cause(s) of Failure	OCC	Prevention Controls	Detection Controls	DET	RPN
(4) Provide assistance to reduce driver's steering efforts to levels that match the functional requirements of the vehicle	(4.1) No assistance - Full loss of power assist	(4.1.1) Increased steering efforts due to complete loss of power assist	8		(4.1.1) Belt assembly does not transmit torque between Electric Motor and rack	5	- Belt assembly FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	6	240
		(4.1.2) Customer dissatisfaction	8		(4.1.2) Electric motor does not provide torque to belt assembly	5	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out - Electrical hardware testing review - Vehicle steering communications message design review	6	240

Table 3 – Hardware FMEA Excerpt

Recall that the functions in the first column of Table 3 came from the hardware function list in section 3.2. A number of failure modes were identified for this function, the first of which is shown in the excerpt for Table 3: (*4.1) No assistance - Full loss of power assist*. Two effects were identified for this failure mode, *(4.1.1) Increased steering efforts due to complete loss of power assist* and *(4.1.2) Customer dissatisfaction*. These effects were both assigned severity 8 according to the severity classification explained in section 2.2 and the Severity table provided in Appendix 2. Table 3 shows also two causes that could potentially lead to the failure mode of full loss of power assist: *(4.1.1) Belt assembly does not transmit torque between Electric Motor and rack* and *(4.1.2) Electric motor does not provide torque to belt assembly*. Both causes have an assigned occurrence ranking of 5 based on the classification explained in section 2.2 and the occurrence table from the SAE standard and also provided in Appendix 2 as reference.

Prevention Controls - Hardware

The Prevention Controls column often includes component FMEA as appropriate action to prevent failures. It is common practice that the FMEA analysis may stop when the component FMEA has been conducted and agreed on by the evaluation team. Since this thesis attempts to perform a comparison at the system level, it does not include an individual component FMEA and it is assumed that component analysis addresses all component related failure modes.

Detection Controls - Hardware

The detection controls shown in Table 3 refer to how the system-level failure modes would be detected in a testing phase of product development. Although specific component related failures might be detected earlier in the component validation phase, such detection methods would be recorded in the component FMEA. The basis for selecting the ranking for this detection ranking are provided in Appendix 2 according to SAE J1739. The detection methods described in this section refer to testing and verification performed in a period between the declaration of an initial design and prior to the launch phase. Therefore design revisions can still be implemented within the appropriate windows, hence the ranking of 6 is the most appropriate value. The Risk Priority Number (RPN) for both causes shown in Table 3 results in value of 240. From SAE J1739:

$$RPN = S \times O \times D \quad \text{.....(1.1)}$$

$$RPN = 8 \text{ x } 5 \text{ x } 6 \ = \ 240$$

After all RPN's have been calculated, the evaluation team would prioritize higher Severity and Occurrence priority number (SO) above high RPN in order to prevent or mitigate risk associated with failure and increase customer satisfaction.

FMEA Software analysis

Table 4 shows an excerpt of the FMEA analysis for the software portion of the system. One of the main assumptions of the SAE J1739 specified analysis is that designs are manufactured and assembled to their intent. That assumption often leads to beliefs that the algorithm and logic in the software are complete and without faults. In essence, software is pure design; therefore, there is no manufacturing or assembly process to control. Once the code is written, it is replicable and reproducible as originally intended until a change is made. It is worth noting that software analysis in FMEA often corresponds to hardware related failures. For example, when the same function is analyzed for software: *Provide assistance to reduce driver's steering efforts to levels that match the functional requirements of the vehicle*, it is to be expected that both Potential Failure Modes and Potential Effects of Failure are identical to the hardware part, because how the failure is experienced and its consequences are identical. The causes identified are associated with incorrect parameters selected for the software or lead to hardware failures or false readings, i.e., torque and angle sensors failure.

Function	Potential Failure Mode	Potential Effect(s) of Failure	SEV	Cl	Potential Cause(s) of Failure	OCC	Prevention Controls	Detection Controls	DET	RPN
(2) Provide assistance to reduce driver's steering efforts to levels that match the functional requirements of the vehicle	(2.1) No assistance provided by software - Full loss of power assist	(2.1.1) Increased steering efforts due to complete loss of power assist (2.1.3) Customer dissatisfaction	8		(2.1.1) Incorrect thresholds values set for assistance curve	3	- Calibration testing at system level - Calibration testing at vehicle level	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	3	72
			8		(2.1.2) Torque sensor does not provide torque measurement to Electric motor SCM	3	- Torque sensor FMEA		3	72
			8		(2.1.3) Steering Wheel angle sensor does not provide angle change to SCM	3	- Steering Wheel Angle sensor FMEA		3	72

Table 4 - Software FMEA excerpt

Similar to the hardware section, the functions in the first column of Table 4 came from the software function list in section 3.2. From the many failure modes identified for this function, the first failure mode is shown in the excerpt for Table 4: (*2.1) No assistance - Full loss of power assist*. Two effects were identified for this failure mode, *(2.1.1) Increased steering efforts due to complete loss of power assist* and *(2.1.2) Customer dissatisfaction*. Note that the failure mode is the same as in the hardware section because the function is delivered to the driver by both hardware and software. Should the function fail for either software of hardware, the effect to the driver would be the same, and the same criterion is applied to each failure mode for severity. The potential causes for this failure mode are shown in Table 4: *(2.1.1) Incorrect thresholds values set for assistance curve, (2.1.2) Torque sensor does not provide torque measurement to Electric motor SCM* and *(2.1.3) Steering Wheel angle sensor does not provide angle change to SCM*.

For this case study, and for ease of FMEA development, it is assumed that that there are only isolated failures associated with almost similar designs. The reason to make this assumption is based on the selection of a design built from a generic architecture that could be already implemented in other applications. However, if a new design is analyzed a higher occurrence ranking must be used, especially when there is no data or surrogated data of occurrence. This ranking assignment is also highly dependent on the manufacturer's data and quality assurance process. Occurrence ranking of 3 is given based on the Occurrence ranking table provided in Appendix 2. Note that the ranking is highly dependable on the assumptions made on the system.

Prevention Controls - Software

The detection controls are listed in the 8th column of Table 4. Cause *(2.1.1) Incorrect thresholds values set for assistance curve* shows *calibration testing at system and vehicle level as prevention.* Similar to the hardware section, causes *(2.1.2) Torque sensor does not provide torque measurement to Electric motor SCM* and *(2.1.3) Steering Wheel angle sensor does not provide angle change to SCM,* stops at the FMEA component level. Recall that it is common practice to stop when the component FMEA has been conducted and agreed on by the evaluation team.

Detection Controls - Software

As seen before, the next column in Table 4 refers to Detection Controls that state how the failure modes for the system would be detected. For this case study, it is assumed that the FMEA for components has been completed before the design freeze of the system. The Detection ranking according to SAE standard is 3. RPN for each line was also developed following the method shown in the Detection section for Hardware, which shows a value of 72.

Appendix 2 shows the complete analysis for the generic EPS system. Only design functions were considered and listed below:

1. Transfer diver input (torque and angular displacement) to linear displacement and force to knuckle assembly
2. Convert linear displacement/force of the steering knuckle to angular displacement/torque of the steering column
3. Provide damping to isolate the driver from road harshness and driveline input
4. Provide assistance to reduce driver's steering efforts to levels that match the functional requirements of the vehicle
5. Vary power assist with vehicle speed
6. Provide function under the NVH targets
7. Meet Electromagnetic Compatibility requirements (EMC)
8. Meet power consumption targets
9. Position the inner and outer ball joint centers for correct suspension geometry
10. Position EPS system properly to ensure correct column routing and steering uniformity
11. Provide damping to isolate the driver from road harshness and driveline input
12. Diagnose high friction condition in the system
13. Provide electrical signals to other systems

Common additional functions such as allowing assembly on a production line and manufacturing related failures were not considered because the intent is to understand the causes that would cause a design to fail from conceptual development. Assembly and service requirements take place once a design solution has been selected.

Out of the 13 functions listed above, the initial FMEA analysis discovers 72 failure modes that lead to 95 independent causes. Consequently, 53 generic preventive actions are identified.

Chapter 4: STPA of Electric Power Steering

The goal of System-Theoretic Process Analysis (STPA) is to understand how hazards can occur so cause(s) can be eliminated or controlled by design. For the STPA analysis presented in this thesis, the analysis is broken down into two iterations as proposed in Thomas [15]. The first iteration of STPA is performed without any assumptions about redundancy or protective features. Instead, requirements are derived from the analysis to determine what features need to be added or included for safety. In this way, it is shown that following a top-down system engineering structured method such as STPA is aligned with current engineering practice and design solutions developed through an iterative engineering process.

4.1 Accident and Hazards definition of the system

STPA uses a top-down system engineering approach that begins with potential losses (accidents) that must be prevented. Unacceptable losses for this analysis are:

A1: Vehicle occupants are injured during operation
A1.1: Two or more vehicles collide
A1.2: Vehicle collides with a moving body
A1.3: Vehicle collides with a non-moving body
A2: Vehicle is damaged (economic loss)
A3: Loss of customer preference/ brand loyalty

First, unacceptable safety-related losses were listed. STPA is often utilized for safety-related analysis. However, the methodology is flexible enough so that other unacceptable losses by the decision makers of the system can be included. Safety should always be the main system goal, however, any vehicle manufacturer focuses its competiveness in meeting customer expectations. If customer expectations cannot be met, it would lead to loss of customer preference and such losses should be unacceptable too. When a conflict between unacceptable losses is found, a prioritization can be used so safety is never compromised.

Following accident definition, system hazards are stated. The system hazards, or, the system state or set of conditions that, together with a particular set of environment conditions, will lead to the accidents defined above [16] include:

H1: Vehicle occupants experience harmful conditions during vehicle operation.
H2: Vehicle does not maintain minimum separation from other moving bodies.
H3: Vehicle does not maintain minimum separation from static bodies.
H4: Vehicle is difficult to operate.
H5: Vehicle equipment is operated beyond limits (experience excessive wear and tear)

4.2 Hazards to Accidents relationship

Hazard	Description	Accident
H1	Vehicle occupants experience harmful conditions during vehicle operation.	A1, 2, 3
H2	Vehicle does not maintain minimum separation from other moving bodies.	A1, 2, 3
H3	Vehicle does not maintain minimum separation from static bodies.	A1, 2, 3
H4	Vehicle is difficult to operate	A1, 2, 3
H5	Vehicle equipment is operated beyond limits (experience excessive wear and tear)	A2, 3

Table 5 – Hazards to Accident relationship

Figure 4 shows the high-level control structure for the Electric Power Steering system.

The role of the driver in Figure 4 is to control the vehicle throughout the different operating environments the vehicle is exposed to. The driver controls the direction of the vehicle through the steering wheel, and controls the acceleration and braking commands through the accelerator pedal and braking pedal respectively. In this example, it is assumed that the driver controls a vehicle with automatic transmission, so the clutch pedal and gearbox selector are not involved. The interfaces that allow the driver to control the vehicle have associated electronic modules that receive information from different sensors that detect and measure observable conditions of the vehicle. The electronic modules control actuators that provide the vehicle with speed, braking, and steering capabilities so they must contain a model of the current state of the vehicle. The driver gets the model of the state of the vehicle through the different gauges that are displayed in the cluster (gauges display in the instrument panel) and in addition, the driver

gets information about the overall state of the vehicle through observable conditions (engine noise, weather, etc.). In most vehicles, the failure information to the driver is passive; that means that it only displays a warning when a change in the state of the vehicle requires the driver's attention. It is common practice to inform the driver this way to avoid distraction from the road and also to prevent obliviously ignoring warnings by not paying attention to notifications that ensures that the vehicle is functioning as expected. In this way, the driver is also able to carry a mental model about the state of the environment in which they are driving (traffic laws, surrounding objects including other vehicles, environmental conditions, etc.)

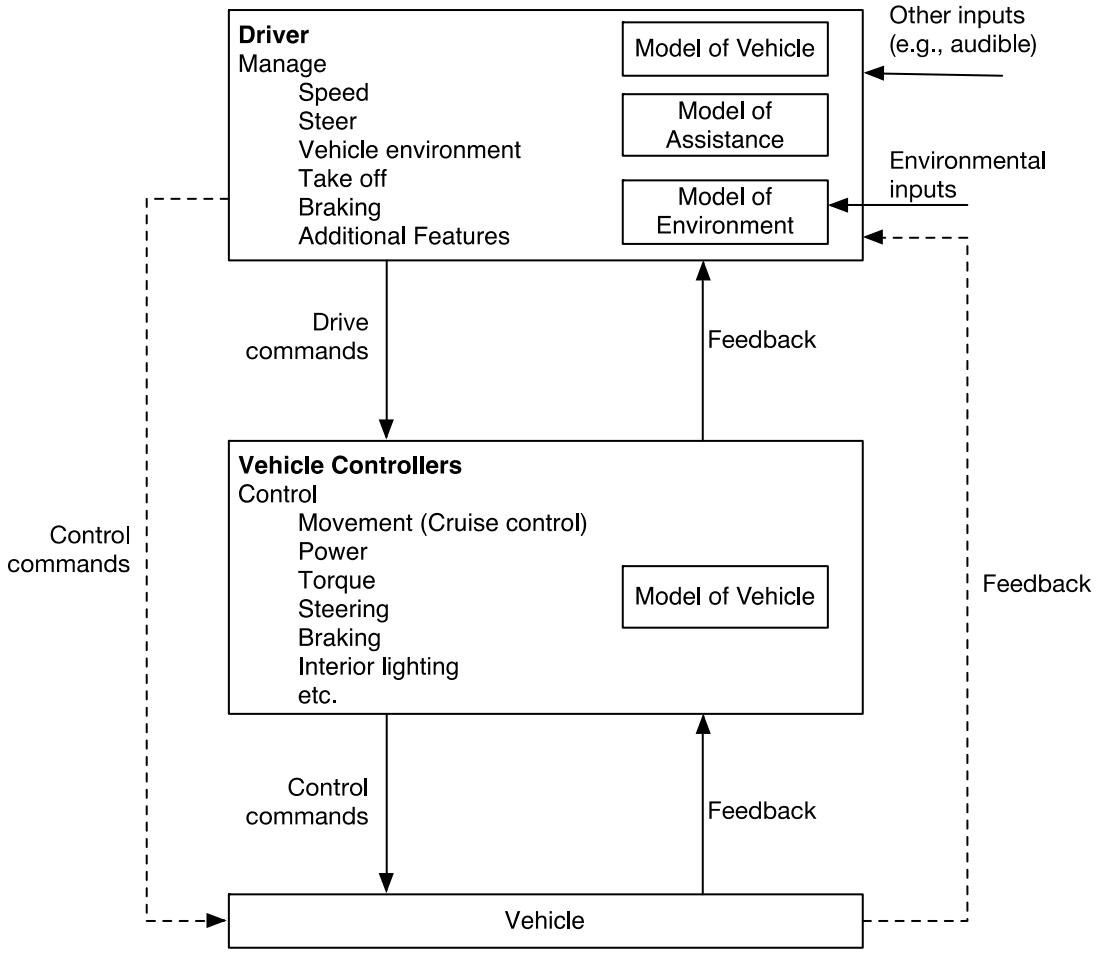

Figure 4 – High-Level control structure at Vehicle Level

Beginning with a high-level control structure allows the designers to establish a holistic view of the system within its main operational environment and also includes one of the most important controllers of engineered systems: the human controller. A holistic analysis also enables intellectual manageability by understanding the system interactions and including not only the

designed intent but also its environment, regulating bodies and entities that are directly and indirectly impacted by its operation.

Figure 5 shows a more detailed control structure focusing on EPS controls. The control structure does not show the physical implementation of the architecture of the EPS system. Instead, it depicts the functional structure. It is useful to start with the basic required functional behavior in order to understand which interactions as well as feedback are needed to enforce the safety constraints of the system.

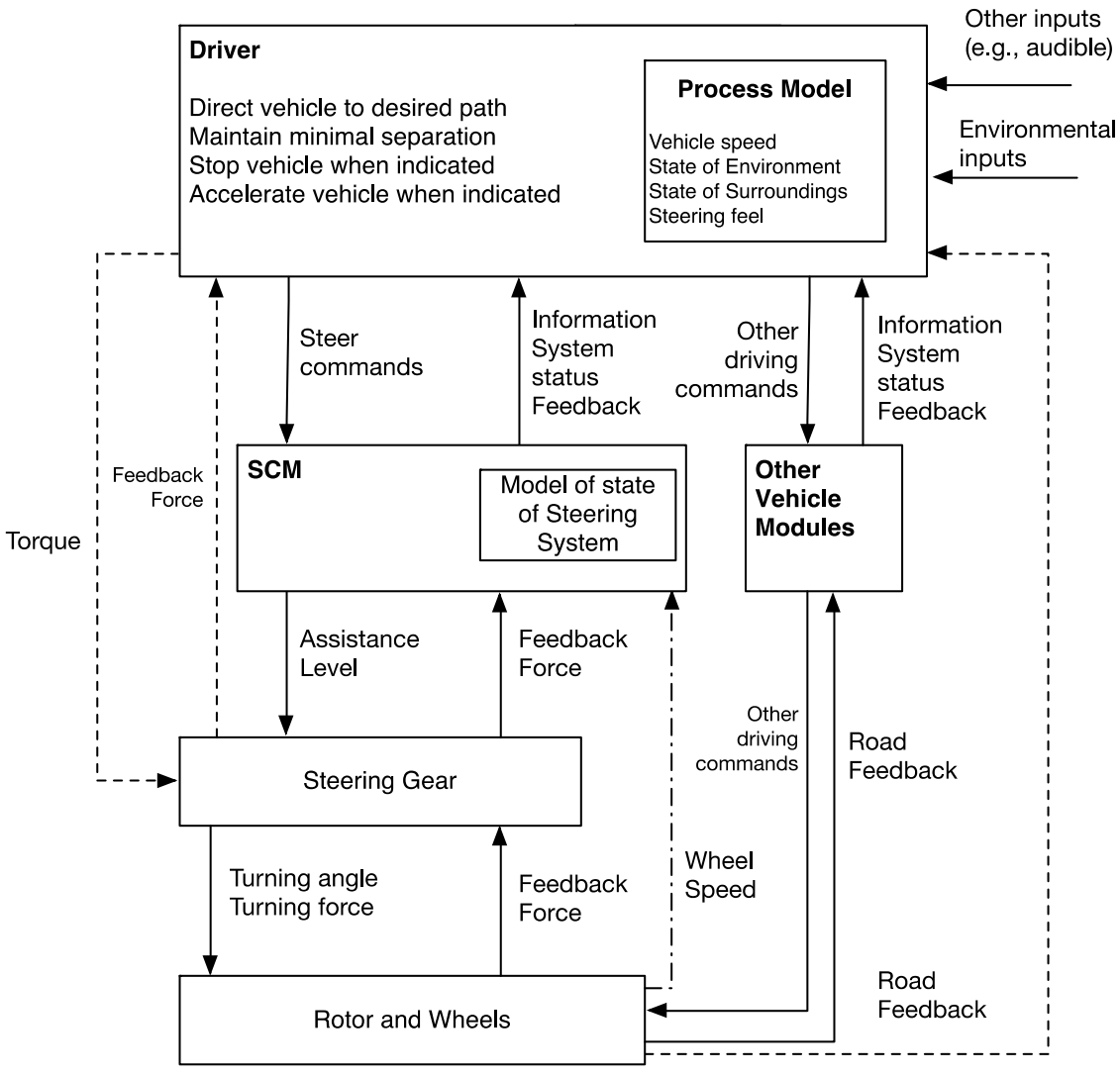

Figure 5 - Control Structure first iteration

Figure 5 also shows the interactions required for the EPS to provide function. Dashed arrows show direct properties exchanged between the different components. For example, part of the driver's effort to steer the vehicle (Torque) is directly driven to the vehicle wheels through the steering gear system due to a hard mechanical link. The force is transferred to the wheels with minimal loss due to system friction. Also in dashed lines, direct feedback is conveyed to the driver through the vehicle. Although the suspension dampens the majority of the road vibrations that the vehicle experiences, it dampens proportionally in the same amount and rate for every type of road condition, so for this example, no active dampening is assumed.

4.3 STPA- Iteration 1

4.3.1 Step 1: Identifying Unsafe Control Actions

As described in section 2.3, there are four types of unsafe control action. The analysis can be organized in a table to facilitate an organized analysis. Unsafe control actions depend on the context in which the system operates. For example not providing assistance when the vehicle is stopped at a traffic light is not hazardous, however, not providing assistance when the driver needs to conduct a parking lot maneuver may lead to a hazardous situation. Table 6 presents an excerpt of the conditions under which the control actions issued by the Steering Control Module (SCM) may be hazardous.

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing or Order	Stopped Too Soon/ Applied Too Long
SCM provides assistance level command to the motor	UCA1: SCM does not provide assistance level command when driver executes a steering maneuver (H-1,2,3,4)	UCA2: SCM provides high assistance level while traveling at high speeds (H-1,2,3,4,5)	UCA3: SCM provides assistance command too late when driver executes a steering maneuver (H-1,2,3,4,5)	UCA4: SCM stops providing assistance command while driver executes a steering maneuver (H-1,2,3,4)
		UCA5: SCM provides low assistance level while traveling at low speeds (H-1,2,3,4)	UCA6: SCM provides assistance command intermittently when driver executes a steering maneuver (H-1,2,3,4,5)	UCA7: SCM continues providing assistance command when safe angle has been reached (H-1,2,3,4,5)

Table 6 - Step 1 SCM excerpt

4.3.2 Safety constraints for SCM

Safety Constraints that can be generated from this first Step include:

SC-R1 : Minimum assistance (TBD) Nm shall always be ensured when the driver executes a steering maneuver. (UCA1)

Rationale: If the vehicle lacks assistance, it might be difficult to maneuver when assistance is required. If the driver is expecting a low assistance for the current state of the vehicle and receives high assistance or vice versa, it may limit the way he or she would react should a hazard-leading situation be present. Furthermore, refinement will lead to providing an auxiliary assistance that would enable the driver to maneuver the vehicle.

SC-R2: High assistance must not be provided when vehicle speed is high. (UCA2)

Rationale: Could lead to oversteer, understeer, roll over or incorrect direction of the vehicle, depending on vehicle speed. Also, it can lead to a dissatisfied driver if the vehicle does not operate as expected.

SC-R3: Assistance shall be provided within (TBD) ms of when the steering command is received. (UCA 3)

Rationale: Delayed assistance may lead to an accident if the driver provides more force when he or she realizes that assistance was not delivered initially. When the commanded assistance is provided, the directional resultant force to steer the vehicle is a combination of the force from the driver and the compensation force from the EPS. If the compensation force from the EPS is provided too late the vehicle might take an undesired path.

SC-R4: Assistance must not be interrupted while the steering command is being received. (UCA4)

Rationale: May lead to a difficult control of vehicle depending on vehicle speed and road conditions. If the assistance is suddenly removed when the driver is executing a steering maneuver, he or she could experience a sudden increase in the steering efforts that could lead to loss of control.

For illustrative and length purposes, this chapter addresses the first row of Unsafe Control Actions (UCA) for the SCM. STPA also analyses the driver as a controller that may enable conditions that could lead to an accident. The actions taken by the driver are studied in detailed in the complete STPA analysis in Appendix 1.

4.3.3 Requirements for the driver

Similar to how the safety constraints for the SCM were determined addressing the Unsafe Control Actions from Table 6, the requirements from the driver are determined from Table 7.

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing or Order	Stopped Too Soon/ Applied Too Long
Driver provides commands steering (force and direction) to steering wheel	UCA11: Driver does not provide steering command when there are people or objects in his/her path (H-1,2,3,4,5)	UCA12: Driver provides steering command towards a static or moving object (H-1,2,3,4)	UCA15: Driver performs a steering maneuver before or after safe path direction (H-1,2,3,4,5)	UCA13: Driver leaves safe path before steering maneuver is being completed (H-1,2,3,4,5)
		UCA14: Driver provides abrupt steering command while traveling at degraded road conditions (H-1,2,3,4,5)		

Table 7 – Step 1 Driver

Safety constraints that can be generated include:

DR-R1: The Driver must be provided with information about the state of the vehicle, such as vehicle speed, steering assistance level, and clear vision of vehicle surroundings, required to ensure safe operation. (UCA11)

Driver not providing input might be due to lack of awareness of the state of the vehicle at the time of operation, further analysis will lead to understanding the causes.

DR-R2: Driver must operate vehicle for the conditions for which it has been designed. Proper documentation and media must be available to the driver to warn about potential misuse (e.g., using passenger cars for off-road situation) (UCA13, 15, 16)

Rationale: Although it cannot be prevented that the vehicle is used under conditions for which it was not designed, making information available to the user should reinforce their mental model towards the safe operation of the vehicle.

An excerpt of the requirements generated by STPA about the driver is presented above. Using a system based analysis such a STPA allows the inclusion of the main controller of the vehicle: the driver. It also shows that a certain subset of requirements is generated that involves the environment in which the system is being operated. Controllers outside of the control structure of the SCM enforce requirements like DR-R1 as shown in Figure 1. This is an important observation for the design organization, not only because the design should comply with governmental regulations, but also because when new designs are introduced, it must be understood how the operation of the system may affect the driver's ability to operate the vehicle safely. For example, if a new feature, like autonomously performing parking maneuvers, is introduced in the next generation of EPS, proper information should be given to the driver to avoid unintentional operation

The driver contributions are included in the full analysis in Appendix 1. It is not typical that FMEA analysis would include the driver contributions to hazardous scenarios when a particular system is analyzed. Therefore the results from the driver portion are not included in the comparison section because they cannot be compared with a section in the FMEA. However, that does not mean that those requirements are not necessary.

4.3.4 Step 2: Identifying Accident Scenarios

The goal for the next section is to identify the causes that would lead to the unsafe control actions analyzed in Step 1 and the relationships with other causes that could lead to those hazards. The purpose of the selected scenarios is to demonstrate the methodology and would be further refined in next iterations.

Complete scenarios might not necessarily be limited to a single controller. We can expect that one controller UCA might cause or relate to a different controller UCA.

<u>Control action is not provided:</u>

UCA1: Assistance is not provided when the driver executes a steering maneuver (H-1,2,3,4)

Scenario1: SCM does not provide assistance because SCM incorrectly believes that assistance is not needed (incorrect process model).

SCM does not know assistance is needed because the torque sensor feedback incorrectly indicates high torque. The incorrect feedback could be due to:

- SCM electronic failure (circuit internal failure).
- Steering wheel/Torque sensor failure.
- Shorted harness, open circuit.
- Delayed signal information provided by sensor, in the BUS.
- Algorithm minimum or maximum threshold for torque is incorrect and assistance is not provided.
- Sensors degrade over time (incorrect assembly, corrosion).
- Incorrect sensors calibration for vehicle architecture and geometry.
- Internal components overheat causing degradation of the system and false readings.
- Electromagnetic disturbance interferes with signal from sensor.
- An old value or parameter is used to calculate the input torque form the driver

SCM does not know assistance is needed because SCM incorrectly believes vehicle turning angle is too large. SCM believes turning angle is too large because:

- Vehicle turning angle feedback is incorrect. Causes include:
    - Failed turning angle sensor.
    - Shorted harness, open circuit.
    - Signal delay in the BUS.
    - Sensor degrades over time.
    - Electromagnetic disturbance interferes with signal from sensor.
    - A pervious value for vehicle turning angle is used to determine real angle.
- Vehicle turning angle threshold or calibration is incorrect. Causes include:
    - Incorrect factory calibration.
    - Changes or modifications to vehicle's steering system without recalibration
    - Incorrect sensor calibration for vehicle architecture and geometry.

SCM does not know assistance is needed because SCM incorrectly believes vehicle speed is too high. SCM believes vehicle speed is too high because:

- Vehicle speed feedback is incorrect. Causes include:
    - Failed vehicle speed sensor

    - Wheel speed is used to determine vehicle speed, but wheel speed doesn't match vehicle speed
        - Acceleration in uneven or slippery surface could cause wheel speed to differ from vehicle speed
        - Anti-lock brakes affect wheel speeds
        - System is too sensitive to differential speed measurements
        - Connection or assembly improperly made.
    - Electromagnetic disturbance interferes with signal from wheel speed sensors (high signal to noise ration)
    - Measurements from several diverse independent sensors are used to estimate vehicle speed, but the sensor readings do not agree and the SCM is unable to combine the data accurately.
- Internal components overheat causing degradation of the system and false readings.
- A pervious value for vehicle speed is used to determine the vehicle speed.

Possible requirements that may come out of this scenario include:

UCA1-S1-R1: Provide additional feedback for determining vehicle speed and steering angle.

UCA1-S1-R2: System level validation shall ensure that electric sensors, actuators and modules do not radiate electromagnetic noise that could cause improper behavior of modules, actuators and sensors of the system and the vehicle.

UCA1-S1-R3: System level validation shall ensure that electric sensors, actuators and modules signal to noise ratio remains functional during vehicle operation and through common (environmental) electro-magnetic noises.

UCA1-S1-R4: Algorithm shall include logic to detect if signals from sensors are received in the time interval the system requires.

UCA1-S1-R5: System operation must be ensured within the operational range of system temperature. Means to control the operational temperature shall be in place. **Additional temperature sensor is required to monitor system temperature**.

UCA1-S1-R6: System shall start operations free of previously stored values that could influence the way required assistance is determined.

Identifying causes of Unsafe Control Actions are provided is necessary but it is not enough. The analysis should also look for causes of safe control actions that might have been provided but were not followed or not executed.

Control action is provided but not followed:

Scenario2: SCM provides assistance command but it is not effective because the current to power the motor is low. The current is too low because:

- System voltage is too low.
- Electrical system does not account for voltage drain during high assistance situations.
- The system enters into a reboot or protection mode that impedes normal functionality.
- Engine stalls while driving (unrelated to EPS) and power is insufficient to command the vehicle.
- Motor continues to provide high assistance In lock-to-lock events (once the rack has reached the travel limit).
- Circuit interruption in the electrical harness (short circuit, open circuit, etc.).

Possible requirements that may come out of this scenario include:

UCA1-S2-R1: Sufficient power shall be provided to the motor in order to provide assistance at different vehicle speeds..

UCA1-S2-R2: The SCM shall provide feedback to the Power Distribution Module about the voltage demanded from the motor to provide assistance.

UCA1-S2-R3: Current requested by the module shall drop within TBD s after rack's end of travel has been reached.

UCA1-S2-R4: The system shall not reinitiate after the vehicle has initiated operation or is below TBD speed.[2]

UCA1-S2-R5: Auxiliary power in vehicle shall be capable to maintain a minimum of TBD [Nm] assistance in the event of engine stall and vehicle speed is higher than TBD [kph]

UCA1-S2-R6: Power distribution shall contemplate providing power to actuators that are required for safe operation of the vehicle under different driving conditions that include system low voltage.

Scenario 3: SCM provides steering command but it is insufficient due to steering lock condition. The system could be locked because:

- High friction in the system due to improper geometry selected.
- Tolerances for friction components are outside allowable limits.
- Incorrect geometry selected for the type of suspension of the vehicle.
- Faults related to material and geometry for steering components.
- Suspension geometry or tuning does not correspond with the performance target of vehicle. Suspension might be too sensitive to road conditions, or response too harsh causing the steering system to react accordingly.
- Hardware failure. Includes:
    - Gear damaged
        - Wear in pinion or rack assembly
        - Ball joint degraded or making noise.
        - Belt assembly failure (rupture)
        - Electric Motor internal failure
- Corrosion protection is not adequate for usage under stringent conditions causing high friction/locking condition with internal components.
- Degrades over time. The system may degrade over time due to:

[2] Reinitialize or rebooting refers to the action the system takes when it restarts operation from a initial state. Recall that UCA1-S1-R6 requires that the system starting operation from an initial state to avoid using old stored values to deliver function. UCA1-S1-R6 allows the system to reboot, however it should not happen a particular time after the vehicle has started operation.

    - Corrosion is formed within steering gear components that prevent assistance from the motor to move the front knuckle.
    - Premature wear of components due to improper alignment.
    - Material and geometry selected does not withstand the duty cycle designed for the vehicle.
    - System does not store failure or errors for service inspection.
- Foreign components lodge in steering system.
- Steering rack travel limiters set incorrectly.
- Assembly connections improperly made or do not retain torque/ torqued out of specification or alignment.

The requirements that were generated from these scenarios include:

UCA1-S4-R1: High friction conditions shall be able to be estimated by the algorithm.

UCA1-S4-R2: Control plan and quality assurance plans shall be in place to ensure parts meet design tolerances and material specifications called in part prints.

UCA1-S4-R3: The system shall allow alignment setting (Toe) and access for update in periodic revisions (scheduled maintenance). The system shall retain the alignment setting (Toe) for the time in between scheduled inspections.

UCA1-S4-R4: The system shall be guarded against foreign components and environmental conditions that could degrade performance.

UCA1-S4-R5: The system shall provide notification to the driver when failures of motor, sensors, or SCM have been identified. The system shall store fault codes for inspection and service.

The same methodology presented is performed for each of the UCAs identified in the first iteration of STPA. With these results, the design team can address the requirements derived from the first iteration and eliminate and/or mitigate possible occurrence of hazards.

4.4 STPA- Iteration 2

Now that initial requirements have been identified, a second iteration can be performed to incorporate any additional controls and feedback that were added as well as additional design details that may not have been known initially. A revised control structure that includes findings of iteration 1 is shown in Figure 6

4.4.1 Step 1: Identifying Unsafe Control Actions

With the control structure derived from Iteration 2, each UCA found in iteration 1 is revised in order to assess if the added control actions may also contribute to an unsafe control action. In the second iteration, any new control actions are analyzed to determine if they can contribute to any hazards. Based on the requirements from the first iteration, a new control action for the SCM was added: *Command auxiliary assistance*. This new command can enable an auxiliary assistance mode when a fault is detected or high temperature is detected. Such a control action is also aligned with current industry design solutions. Should a problem occur that disables assistance, auxiliary default assistance independent of vehicle speed is provided. With auxiliary assistance, the system continues providing assistance while the vehicle is taken for service for inspection and repair. Unsafe control actions for this new command are shown in Table 8.

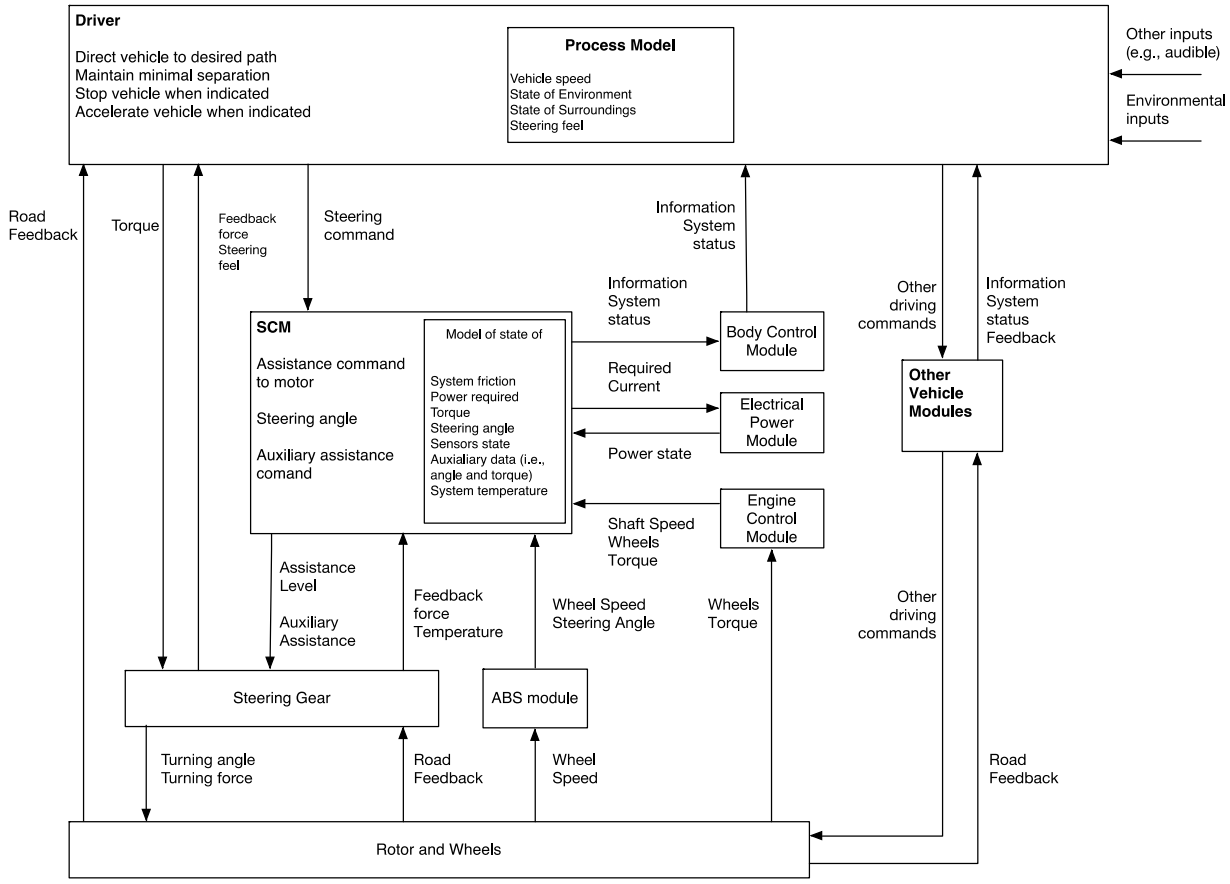

Figure 6 - Control structure second iteration

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing or Order	Stopped Too Soon/ Applied Too Long
Command auxiliary assistance mode when fault is detected or high temperature is detected	UCA18: SCM does not command limited assistance when fault is detected or there is a high temperature event (H-4,5)	UCA19: SCM sends auxiliary assistance command when there is no fault or high temperature event (H-4)	UCA20: SCM intermittently commands auxiliary assistance (H-1,2,3,4,5)	UCA21: Stops providing auxiliary assistance command while there is a fault (H-1,2,3,4,5)

Table 8 - New Control Action Step 1

Table 8 shows the UCA's from the new control action determined by the first iteration of STPA. *UCA18: SCM does not command limited assistance when fault is detected or there is a high temperature event (H-4,5)*, refers to situations where no auxiliary assistance is provided when normal assistance cannot continue to be provided because it is not safe. For example, if there is a high temperature event due to the combination of harsh environmental conditions and high efforts demanded, an auxiliary assistance could allow the motor to have less demand and decrease the operational temperature. The driver could then have limited assistance to take the vehicle in for service and inspection.

Recall *UCA19: SCM sends auxiliary assistance command when there is no fault or high temperature event (H-4)* in Table 6. There could be situations where providing auxiliary assistance might be unsafe. Vehicles traveling at low speeds require higher steering assistance than when traveling at high speeds. Higher assistance means higher loads demanded from the electric motor, and higher loads increase the operating temperature. A default speed is usually selected as value associated with the auxiliary steering assistance. If auxiliary assistance is commanded while traveling at higher speeds than the default vehicle speed for assistance, providing auxiliary steering assistance would cause higher loads on the motor and it also might disturb the driver's belief about the assistance level. If the temperature level of the system was high, providing auxiliary assistance in this situation would contribute to the system hazard.

UCA20: SCM intermittently commands auxiliary assistance (H-1,2,3,4,5) refers to situations where auxiliary assistance is provided intermittently. Providing assistance when operating temperature is close to the temperature range for auxiliary assistance could lead to this UCA.

UCA21: Stops providing auxiliary assistance command while there is a fault (H-1,2,3,4,5) refers to situations in which the auxiliary assistance stops being provided while there are still faults in the system that require auxiliary assistance. False beliefs that system has returned to a safe state where normal assistance might be provided or assistance is interrupted are a few examples of this UCA. The scenarios provided in Appendix 1 go more into detailed explanation.

4.4.2 Step 2: Revising Accident Scenarios

In the second iteration, the revised control structure can be analyzed to identify any additional accident scenarios that have been introduced. This section revises accident scenarios from the

first iteration to include additional causes that may have been introduced. The next section will identify scenarios for any new UCA's that were not analyzed in the first iteration.

UCA1: Assistance is not provided when driver executes a steering maneuver (H-1,2,3,4)

Scenario1: SCM does not provide assistance because SCM incorrectly believes that assistance is not needed (incorrect process model). The SCM may not know assistance is needed because:

- ABS and transmission output shaft does not match the actual vehicle speed. ABS vehicle speed does not match the actual vehicle speed because:
    - Failed vehicle speed sensor
    - Acceleration in uneven or slippery surface could cause wheel speed to differ from vehicle speed
    - Anti-lock brakes affect wheel speeds
    - System is too sensitive to differential speed measurements
    - Connection or assembly improperly made.
    - Electromagnetic disturbance interferes with signal from wheel speed sensors (high signal to noise ration)
    - Internal components overheat causing degradation of the system and false readings.
    - A pervious value for vehicle speed is used to determine the vehicle speed.
    - Errors in the calculation from the ABS Control Module.
- The transmission output shaft speed does not match the actual vehicle speed because:
    - Failed transmission speed sensor
    - Transmission shaft turning speed differential between Right and Left hand side causing conflict between measured speed and actual speed.
    - Connection or assembly improperly made.
    - Electromagnetic disturbance interferes with signal from transmission speed sensors (high signal to noise ration)
    - Internal components overheat causing degradation of the system and false readings.
    - Errors in the calculation from the transmission module.
    - ABS module goes to error estate and last value of vehicle speed keeps being sent.

Additional Requirements:

UCA1-S1-R7: The system shall provide a minimum assistance of TBD [Nm] to help the driver bring the vehicle to a safe state when vehicle speed does not match the calculated vehicle speed by other modules. Assistance shall be available when the SCM detects that system is in error state, or other modules are sending information that does not match with the model of SCM.

Given that an additional control action is identified, a new scenario is derived that could not be justified before because there were no interactions with other vehicle modules. New causes are identified from Scenario 4:

Scenario4: SCM does not provide assistance command because SCM incorrectly believes that it is not safe to provide assistance. SCM believes it is unsafe because:

- There is no correlation between steering wheel angle measured by sensor and provided by ABS module.
- Incorrectly reported high temperature (sensor failure).
- Incorrectly reported high friction.
- Incorrectly reported low voltage.

<u>Control action is provided but not followed</u>:

Scenario2: SCM provides assistance command but it is not effective because the current to power the motor is low. The current may be too low because:

- Electrical power module commands shutting down power to prevent battery drain.

Scenario3: SCM provides steering command but it is insufficient due to steering lock condition. The system could be locked because:

- Friction detection algorithm does not account correctly for high friction in the system. This could be because:
    - Thresholds for friction are too low.
    - Driving in low friction or split friction roads.
    - Changing vehicle conditions (process model) (i.e., GVW, tires)
    - Input signals variability (angle, torque, speed)

- High torque events that could provide false readings (i.e., High lateral acceleration, aggressive take off, aggressive maneuvers)

Additional requirements:

UCA1-S4-R1: High friction conditions shall be able to be estimated by the algorithm. If high friction conditions are detected, driver shall be informed so vehicle can be taken for inspection.

The rationale for this requirement is to avoid false readings and trigger false high friction conditions when in reality the vehicle is being driven in a context where it could be inferred as high friction, such as off-road situation or partially dampen roads.

4.4.3 Step 2: Identifying Accident Scenarios

Step 1 identified a new set of unsafe control actions. For example, consider UCA21 from Table 8: *SCM does not command auxiliary assistance when a fault is detected or when there is a high temperature event (H4, H5).* This control action could not have been analyzed in the first iteration because the control action: *Command auxiliary assistance mode when fault is detected or high temperature is detected*, had not been incorporated. However, now that it has been decided to incorporate this control action to eliminate possible hazards, STPA requires detailing possible causes that may trigger a new hazard.

<u>Control action is not given</u>

UCA18: SCM does not command auxiliary assistance when fault is detected or there is a high temperature event (H4, H5)

Scenario1: SCM believes there is high friction but the speed is low. If high friction is detected at low speed SCM should not command auxiliary assistance because the amount of assistance provided at low speed should be higher than the auxiliary assistance. Possible causes include:

- Torque sensor failure, measurement error or false signal (contributor to miscompute high friction)

- Steering wheel angle sensor failure. If steering wheel angle cannot be estimated any other way than with its sensor, it might be hazardous providing assistance because it could lead to scenarios analyzed in UCA7.
- Temperature sensor incorrect measurement, indicating high friction in system.
- Shorted harness, open circuit.
- Algorithm threshold for high friction is incorrectly specified
- Detection algorithm is not sensible enough to identify high friction conditions.
- Electromagnetic disturbance interferes with signals from sensors.
- Old values are used to calculate friction (e.g. The SCM would believe that low assistance is required when using a high value for speed previously stored, but if the actual state of vehicle speed is low, the input torque from the driver will be higher. The SCM would believe that higher torque input is required for certain level of assistance, hence interpreting that there is high friction in the system).

Scenario2: SCM does not command auxiliary assistance because SCM incorrectly believes there is high temperature and high speed. If high temperature is detected at high speed, SCM must not command auxiliary assistance because that would deliver more assistance, contributing to an increase in temperature. Possible contributors are:

- Torque sensor failure, measurement error or false signal (contributor to miscompute high friction)
- Temperature sensor calibration set incorrectly.
- SCM reads the correct temperature but incorrectly thinks that the vehicle speed is high. SCM believes vehicle speed is too high because:
    - Vehicle speed feedback is incorrect. Causes include:
        - Failed vehicle speed sensor.
        - Wheel speed is used to determine vehicle speed, but wheel speed does not match vehicle speed.
        - Acceleration in uneven or slippery surface could cause wheel speed to differ from vehicle speed.
        - Anti-lock brakes affect wheel speeds.
        - System is too sensitive to differential speed measurements.
        - Connection or assembly improperly made.

- Electromagnetic disturbance interferes with the signals from wheel speed sensors (high signal to noise ratio)
- Internal components overheat causing degradation of the system and false readings.
- A previous value for vehicle speed is used to determine the vehicle speed.

It can be observed that enforcing the new control action without any restriction may also drive the system to hazardous situations. Often designers encounter these types of contradictory solutions, that is, enforcing one safety constraint may violate another one. Thomas [13] proposed a new method for identifying unsafe control actions. Thomas observed that the UCA's derived from STPA often exhibit a common structure. Such structure may be formalized in four-part construction: A source, a type, a control action, and a context.

The *source* and *control action* are found in the relevant system control structure developed as part of the system engineering foundation. The *type* refers to whether the control action is provided or not provided, following the four types of unsafe control actions (provided, not provided, out of order or timing and applied too soon or too long). A context could be defined by a set of process model variables (PMV) – variables that describe the system state [13].

An example of PMV is exemplified using high friction in Figure 7.

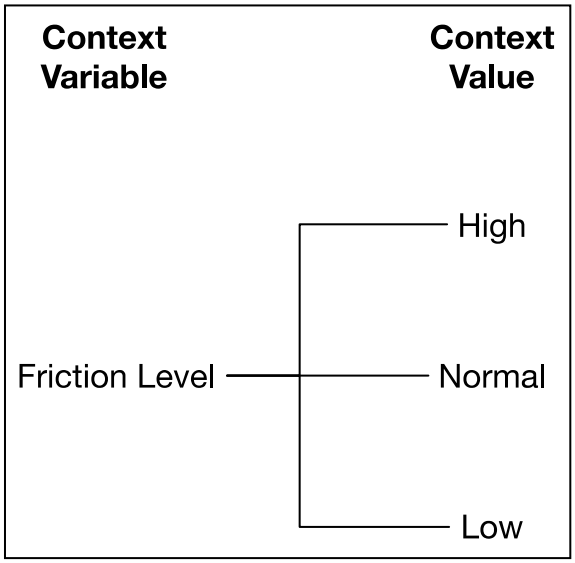

Figure 7 - PMV of Auxiliary Assistance

Context variables	State
Friction Level High: Above TBD threshold Normal: Within TBD range Low: Below TBD threshold	[High, Normal, Low]
Temperature High: Above TBD threshold Normal: Within TBD range Low: Below TBD threshold	[High, Normal, Low]
Vehicle Speed High: TBD range for high speed Low: TBD range for low speed	[High, Low]

Table 9 - Context variables for auxiliary assistance

Once PMV is formalized, a context table may be constructed to identify unsafe control actions and generate applicable requirements. The requirements specify when a control action must be commanded and when it must not be commanded to ensure safety and prevent the system hazards. Following Thomas' proposal, functional requirements for Auxiliary Assistance are provided in Table 10**.**

SC: Source controller that can issue the control action of the system
T: is the type of control action (Provided or not provided)
CA: Control Action (i.e.) command that is output by the controller.
Co: Context in which the control action is or is not provided

For Auxiliary Assistance command:
SC= SCM
T= Provided, left blank are specified as don't care or wildcards.
CA= Command Auxiliary assistance
Co= Friction condition, temperature condition, speed.

Specification Tools and Requirements Methodology Requirements Language (SpecTRM-RL)

Although it is not part of STPA, this analysis uses a formal requirements language called Specification Tools and Requirements Methodology Requirements Language (SpecTRM-RL) [20]. The author found it useful using this formal system modeling language following the method proposed by Thomas [13] to understand how apparent conflicting actions should be used to satisfy safety constraints. Therefore a brief explanation of SpecTRM-RL will be given in this section.

The requirements generated specify when control actions must be issued to satisfy safety constraints. The resulting requirements may be presented in a formal language. SpecTRM-RL is a black box formal system modeling language that uses a state-based representation of a system. In addition to mathematical constructs, SpecTRM-RL provides a graphical representation of formal requirements that can be used effectively with very little explanation [13].

Table 10 shows the SpecTRM-RL representation of Requirement for issuing an auxiliary assistance command. Each row in the table represents a state or input to the SCM controller and a value for that state or input. The columns in the right represent the AND-OR logic used to determine if auxiliary assistance command should be issued. Columns hold OR relationships while AND relationships exist between rows. The empty cells are treated as irrelevant states which means that the controller does not care if the vehicle exhibits this state when issuing the command.

The first column shows that when the vehicle is in a high-friction state while traveling at high speeds and temperature is within the normal operating range, the command for auxiliary assistance may be given. The second column specifies another situation in which the auxiliary assistance command will be provided: High temperature while traveling at high speeds. Note that this last column is independent of the friction state of the vehicle. If friction is high when temperature is high and the speed is low, auxiliary assistance should be provided to prevent the system temperature from continuing to increase due to higher loads. Although high friction condition would contribute to the driver experiencing higher efforts to turn the steering wheel, the auxiliary level of assistance is preferable than no assistance at all.

SpecTRM-RL for auxiliary assistance is presented next.

Provide auxiliary assistance command

		S-F	S-F
Friction =	High	T	
	Normal		
	Low		
Temperature =	High		T
	Normal	T	
Vehicle Speed =	High	T	
	Low		T

Table 10 - SpecTRM-RL of Auxiliary Assistance

STPA Requirements for auxiliary assistance

Following the method for determining when auxiliary assistance should be provided that was described in the previous section, STPA analysis continues to determine the applicable requirements.

UCA16-S1-R1: Auxiliary assistance of TBD [Nm] shall start when the system detects internal temperature above TBD1 [C] and below TBD2 [C]. If the system reaches or surpasses TBD2 [C], assistance shall stop being provided.

UCA4-S3-R1: If high system temperature is detected, the system shall provide minimum TBD [Nm] auxiliary assistance to ensure that the driver can take the vehicle in for inspection. Algorithm shall include logic to display MIL and laudable chimes to the driver so he can be made aware that the vehicle is in a reduced performance mode.

UCA3-S1-R3: If discrepancy is constant among correlated signals, the algorithm shall include logic to display MIL and laudable chimes to the driver so he or she can be made aware that the vehicle requires inspection. When a discrepancy occurs, the system shall provide minimum TBD [Nm] auxiliary assistance to ensure the driver can take the vehicle for inspection.

Control action provided but not followed

Scenario2: SCM provides limited assistance when a fault is detected but high assistance is provided. High assistance is provided because:

- The system is operated in a degraded high friction state that leads to overheat.
- Signal interference to command motor (Electromagnetic noise)
- Value for auxiliary assistance provided is too high.

Requirements affecting this scenario:

UCA4-S3-R1: If high system temperature is detected, the system shall provide minimum TBD [Nm] auxiliary assistance to ensure the driver can take the vehicle for inspection. Algorithm shall include logic to display MIL and sonorous chimes to the driver so he or she can be made aware that the vehicle is in a reduced performance mode.

UCA1-S1-R2: System level validation shall ensure that electric sensors, actuators and modules does not produce electromagnetic noise that could cause improper behavior of modules, actuators and sensors of the system and the vehicle.

UCA1-S1-R3: System level validation shall ensure that electric sensors, actuators and modules signal to noise ratio remain functional during vehicle operation and through common (environmental) electro-magnetic noises.

Full STPA analysis of the EPS system can be found in Appendix 1. STPA enabled finding of 22 UCA's that lead to 49 different scenarios and identified 121 causes. From causes and unsafe control actions differentiation, 47 high-level requirements and 10 Safety Constraints were derived. Such requirements and safety constraints should guide the design team through the decision-making process within system design development.

Chapter 5: Comparison between STPA and FMEA

Because the approaches are different and are based on dissimilar causality models, it is difficult to compare step-by-step results of both methodologies. However, because the objective of both processes is to derive and address causes that might lead to hazardous situations, this section aims to compare and understand the types of the results derived from each methodology. In order to do so, a classification of types of causes needs to occur.

5.1 Classification of causes

Although many other classifications may apply to these causes, the classification was selected so as not to favor a specific methodology, but rather to generate an appropriate classification such that the causes that share similar characteristics are clustered while those that do not belong are discernable among each other. Thus, five different groups are identified for hazardous causes:

- Engineering Design: inadequate design selections.
- Component Failure: parts that fail to meet their design constraints.
- Lack of correspondence between component capacity and task requirements: the environment in which the system is used does not match what was assumed during design.
- Interaction with other systems: causes involving interactions between EPS and other vehicle systems.
- Physical Degradation: desired characteristics of a design degrade over time.

Another subset of causes belonging to manufacturing process was identified. These causes are related to when design constraints are set up correctly, and somewhere in the manufacturing process the product does not meet the design requirements. These causes would be developed in more detail for FMEA in a process FMEA, and they can also be included in STPA if a manufacturing loop is analyzed. However, these two analyses were outside of the scope of this thesis.

5.1.1 Engineering Design types of causes

Engineering Design type of causes refers to inadequate design selections that would prevent the system from achieving the function for which it was designed. Such design selections can be due to a variety of different causes, from flawed requirements to incomplete analysis performed on the system (e.g., fastener joint analysis).

To illustrate how these types of problems are determined, consider cause 1.1.1.1 from FMEA excerpt in Table 11: *Incompatibility between gears*. This problem may occur because the internal gears assembly that multiplies the torque provided by the motor does not maintain a geometric relationship or such relationship is not set correctly by design (Tooth profile, Pitch circle, Addendum, etc.). The manufacturing process may also be unable to achieve the geometric tolerances set by the design. However, as Chapter 2 explains, one of the main assumptions specified in SAE J1739 is that the components are manufactured to meet the design specifications. Therefore, if the gears are not compatible, under FMEA analysis, it is because the gears interfere with each other. Consequently, an engineering design decision (geometrical relationship between gears) is the cause.

Failure 1.1.1.1 from FMEA is derived from the one of the main functions of the EPS: *to transfer the driver input to linear displacement and force to the knuckle assembly*. When the function is not achieved, the system does not convert angular displacement from the driver to the knuckle, which may cause the vehicle to be difficult to control or to provide direction.

Function	Potential Failure Mode	Potential Effect(s) of Failure	S E V	Class	Potential Cause(s) of Failure	O C C
(1) Transfer driver input (torque and angular displacement) to linear displacement and force to knuckle assembly	(1.1) EPS does not convert angular displacement/torque to linear displacement/force	(1.1.1) Unable to control direction of vehicle	10	YC	(1.1.1.1) Incompatibility between gears assembly	2

Table 11 - FMEA Excerpt for Engineering Design causes

In STPA the same problem can be identified in Scenario 3 from UCA1. The first iteration of STPA, presented in Chapter 4 details UCA Scenario 3 as: *SCM provides steering command but it is insufficient due to steering lock condition*. Several causes are identified, but cause *high friction in the system due to improper geometry selected* corresponds to cause 1.1.1.1 in the FMEA. It is important to notice that such compatibility not only applies to gears (such as the rack and pinion assembly and internal driving gears), it also applies to the travel arms and the internal bearings of the EPS that aim to reduce friction. If such geometry selection is incompatible, it will cause the EPS system to lock, consequently assistance would not be enabled. Because geometry selection for gears and bearings is a decision made by the Engineering Design group, the same criteria for allocating this cause remains.

Another example of an Engineering Design cause can be found in UCA 18 under Scenario 1.

> UCA18: SCM does not command auxiliary assistance when a fault is detected or there is a high temperature event (H4, H5)
>
> Scenario1: SCM does not command auxiliary assistance a when a fault is detected or when there is a high temperature event because there are conflicting signals that impede providing auxiliary assistance. Possible contributors include:
> […]
> - False detection of high temperature at high speed. If high temperature is detected at high speed, SCM should not command auxiliary assistance because that would deliver more assistance, contributing to an increase in temperature. Possible contributors:
>   - Temperature sensor incorrect measurements.
>   - Incorrect thresholds selected for high temperature.

The first cause is associated with a component failure, cause *Incorrect thresholds selected for high temperature* is associated with the software within the SCM. Because the engineering team develops software, such causes fall under Engineering Design. Note that FMEA finds causes associated with the temperature sensor failing (component failure causes) but does not account for incorrect thresholds selected for high temperature in the SCM logic.

5.1.2 Component Failure types of causes

Component Failure causes are causes that can be associated with components that fail to meet the design constraints. Often these types of failures are associated with parts not meeting the duty cycle the product must withstand. Although parts are manufactured to meet the design specifications for geometry, materials and installation under certain operation contexts, failures still can occur. Many duty cycle tests are designed to simulate severe duty scenarios that many drivers will not experience with the magnitude with which the system is tested. However, ensuring that all 10, 000 moving parts installed in an automobile perform exactly the same without allowable variation for every production vehicle is unrealistic. A competent design team would acknowledge that despite the best design, chances that a part fails may not be completely eliminated, but may be mitigated.

FMEA is a very good tool to find component related failure causes and provides a structured method for addressing such causes to ensure reliability of the system. Notice in Table 12 how causes associated with component failure are found in FMEA. Starting from the main function: *Transfer driver input (torque and angular displacement) to linear displacement and force to knuckle assembly,* it is expected that the same Potential Failure Modes and Failure Effects remain when the function is not delivered. This differs from the Engineering Design cause shown in Table 11 because the cause could be due to the EPS motor failing to allow the rotation of the input shaft. Thus, a component related failure prevents the function from being delivered.

To understand all the different causes of an EPS motor failure, the FMEA directs the analysis to Component FMEA of the EPS motor. When such reference is made, the design team needs to provide evidence that the Component FMEA analysis is complete and available. For complex designs with many components, this type of analysis is extensive and often not easy to manage.

Function	Potential Failure Mode	Potential Effect(s) of Failure	S E V	Class	Potential Cause(s) of Failure	O C C
(1) Transfer driver input (torque and angular displacement) to linear displacement and force to knuckle assembly	(1.1) EPS does not convert angular displacement/torque to linear displacement/force	(1.1.1) Unable to control direction of vehicle	10	YC	(1.1.1.11) Motor fails to allow rotation of input shaft under driver input	1

Table 12 - FMEA Excerpt for Component Failure causes

STPA is able to find the same cause of a mechanical failure occurring in the electric motor when analyzing UCA1 Scenario 3 in the first iteration:

> UCA1: Assistance is not provided when driver executes a steering maneuver (H-1,2,3,4)
>
> Scenario3: SCM provides steering command but it is insufficient due to steering lock condition. The system is locked because:
> […]
> - Mechanical failure with electric motor

5.1.3 Lack of Correspondence types of causes

This category is set for those causes where a design characteristic is set such that it is able to meet the design intent under conditions scoped by the designers. The usage of the system may be such that it is outside of the scope thought by the engineers. Although these types of causes may be seen as a subset of Engineering Design, it is useful to separate basic design decisions from those decisions that cannot be accurately set in the initial context assumptions of the system. For these causes, there is a lack of correspondence between the component capacity and the task requirements [1] that it is deemed to fulfill.

An example of these types of causes is certain types of corrosion. When a component of the system exhibits corrosion because it could not withstand more stringent conditions that were not

scoped, there is a lack of correspondence between the task demanded from the materials employed and the task requirements (corrosion protection). For example, ferrous materials used near the ocean corrode faster than those used in another type of environment. Therefore, a vehicle used to tow a motor boat in and out of a dock would experience constant immersion in sea water and thus risks to accelerating corrosion in underbody components if housing materials are made of unprotected ferrous materials.

An example of how FMEA finds overall corrosion causes is presented in Table 13.

Function	Potential Failure Mode	Potential Effect(s) of Failure	S E V	Class	Potential Cause(s) of Failure	O C C
(1) Transfer driver input (torque and angular displacement) to linear displacement and force to knuckle assembly	(1.1) EPS does not convert angular displacement/torque to linear displacement/force	(1.1.1) Unable to control direction of vehicle	10	YC	(1.1.1.4) Corrosion	2

Table 13 - FMEA Excerpt for Lack of Correspondence causes

STPA is able to find corrosion related causes with two causes that are separated. The corrosion associated with lack of correspondence is described in cause *Corrosion protection is not adequate for usage under stringent conditions causing high friction/locking condition with internal components* of UCA1 Scenario3.

Scenario3: SCM provides steering command but it is insufficient due to steering lock condition. The system is locked because:
[…]

- Corrosion protection is not adequate for usage under stringent conditions causing high friction/locking condition with internal components.

Although corrosion also may be present due to physical degradation of the parts (not enough corrosion protection for normal operation of the vehicle), STPA differentiates between corrosion

causes. For cause *Corrosion protection is not adequate for usage under stringent conditions causing high friction/locking condition with internal components* in UCA 1 Scenario 3, the corrosion protection does not correspond to the required performance in more stringent environment.

Another example of a lack of correspondence cause is electromagnetic disturbance. Often referred as electromagnetic compatibility (EMC), it is understood as a physical noise in which electromagnetic energy may induce unintentional generation, propagation and reception of electromagnetic signals. Such emission may affect the performance of electric components by generating unintended noise. Emission of electromagnetic signals is intrinsic to the operation of electronic components, however the interaction of such signals may interfere with those of another component or even cause interference with its own operation. Often these components include design solutions such as housings to insulate noise and emission strategy control by software to prevent noise being induced by the surroundings. When such failures are present, there is a lack of correspondence of the task demanded from the component in regards to EMC (insolating from external noise and preventing inducing frequency) and the actual properties of the components.

Table 14 shows how these causes are found in a FMEA.

Function	Potential Failure Mode	Potential Effect(s) of Failure	S E V	Class	Potential Cause(s) of Failure	O C C
(7) Meet Electromagnetic Compatibility requirements (EMC)	(7.1) Interference with other systems, loss of function	(7.1.1) Degraded vehicle performance	8		(7.1.1) Torque sensor signal interference by other vehicle systems	10
		(7.1.2) Customer dissatisfaction	8			10
	(7.2) Generates more than XX dBuV/m Function affected by XX dBuV/m	(7.2.1) Interference with other electronic equipment in vehicle. Not immune to external EMC inputs. Loss of function	10	YC	(7.2.1) Electric motor emissions exceed required levels	10
			10	YC	(7.2.2) Electric motor affected by XX dBuV/m of EMC	10

Table 14 - EMC Excerpt FMEA Lack of Correspondence

UCA1 Scenario1 shows how an EMC related cause is found in STPA:

UCA1: Assistance is not provided when driver executes a steering maneuver (H-1,2,3,4)

Scenario1: SCM does not provide assistance because SCM incorrectly believes that assistance is not needed (incorrect process model). SCM does not know assistance is needed because:

[…]

- Electromagnetic disturbance interferes with signal from wheel speed sensors (high signal to noise ratio)

5.1.4 Interaction between systems types of causes

Causes associated with interaction between systems are causes that might be originated in other vehicle systems but directly affect the behavior of the EPS system. Many of the types of causes covered so far are related to internal process of the EPS system. However, there is another subset of causes where problems result from interaction between different entities that are functioning as intended with unanticipated outcomes. These types of problems are a growing concern to many design organizations who find it difficult to intellectually manage, especially in complex systems [3].

Table 15 shows how a signal originating from the wheel speed sensor may be analyzed in the FMEA analysis. If the wheel speed sensor stops sending vehicle speed, the SCM may incorrectly believe that the vehicle speed is zero, therefore it would provide maximum assistance. Providing the maximum assistance constantly may cause the system to degrade prematurely and also may distract the driver by not providing anticipated countering force when steering commands are given.

Function	Potential Failure Mode	Potential Effects of Failure	SEV	Class	Potential Cause	OCC
(2) Provide assistance to reduce driver's steering efforts to levels that match the functional requirements of the vehicle	(2.3) System provides more assistance than required	(2.3.1) System degradation	10	YC	(2.3.1) Incorrect or no signal provided of vehicle speed	3

Table 15 - FMEA Excerpt for Interaction between Systems causes

STPA finds specifically that the feedback from the vehicle speed may be incorrect and therefore prompt the SCM to send a command of assistance that is not meant for the vehicle speed. Such causes are shown in UCA2 and UCA8:

UCA2: High assistance is provided while traveling at high speeds (H-1,2,3,4,5)

<u>Control action not provided</u>

Scenario1: SCM incorrectly provides high assistance when vehicle speed is high. SCM incorrectly believes that vehicle speed is low because:

- Inadequate external speed feedback could explain incorrect SCM process model (calibration issues, sensor failure, delays in receiving information).

UCA8: Too much turning force provided when the driver executes a steering maneuver (over assist) (H-1,2,3,4,5)

Scenario1: SCM incorrectly believes that incremental assistance is required for low speed conditions (incorrect process model). The SCM might believe that incremental assistance is required because:

- Inadequate external speed feedback could explain incorrect SCM process model (sensor calibration, sensor failure, signal delays).

Note that two UCAs and two scenarios may result from the same cause: an inadequate external speed feedback. STPA captures these in two different scenarios: high assistance provided when vehicle speed is high and also too much turning force when traveling at low speeds. Both situations may cause the driver to get distracted and experience a hazardous condition.

5.1.5 Physical Degradation types of causes

Many of the desired characteristics of a design degrade over time. The loss of such characteristics that occurs under normal operation of the system is classified as Physical Degradation. The system may meet the design characteristics specified by the engineering team initially, but as the vehicle is used and exposed to varying operating conditions such as temperature, road conditions, humidity, etc., the properties that maintain those characteristics may degrade over time. Normal wear of components may induce causes of failures in the EPS system. Friction caused by degradation of components (lack of lubrication, poor maintenance) is also a common cause associated with this classification. The difference between Physical Degradation and Lack of Correspondence is that physical degradation is to be expected in the environment of operation, whereas Lack of Correspondence is about degradation when the environment does not match with the initial assumptions of the system.

Table 12 shows how Physical Degradation causes are found in FMEA analysis:

Function	Potential Failure Mode	Potential Effect(s) of Failure	S E V	Class	Potential Cause(s) of Failure	O C C
(2) Convert linear displacement/force of the steering knuckle to angular displacement/torque of the steering column to provide feedback from road to driver and allow self-centering of the steering	(2.4) EPS does not self-return	(2.4.1) Driver requires to provide force to recover from turn	8		(2.4.1) Damage / Wear of the gear system	2
		(2.4.2) Customer dissatisfaction	8		(2.4.2) Improper use of gear to vehicle geometry	2
			8		(2.4.3) Friction above the designed ranges in the system	2

UCA1 Scenario3 shows how Physical Degradation causes are found in STPA.

UCA1: Assistance is not provided when driver executes a steering maneuver (H-1,2,3,4)

Scenario3: SCM provides steering command but it is insufficient due to a steering lock condition. The system is locked because it:

[..]

- Degrades over time:
    - Corrosion is formed within steering gear components that prevent assistance from motor to move the front knuckle.
    - Premature components wear due to improper alignment.
    - Material and geometry selected does not withstand the duty cycle designed for the vehicle.
    - High friction due to components not aligned properly or premature wear.

5.2 Analysis of results

This section analyzes the results generated from both methodologies based on the classification described above. For both methodologies, the different causes were classified and distributed amongst the proposed criteria. Many causes were associated with multiple failure effects and scenarios. Often a combination of different causes may occur in an unwanted hazardous condition.

5.2.1 Overall comparison by category

Table 16 shows a comparison of the number of causes found by each process and how it is broken down amongst the categories selected.

Type of causes / process	STPA	FMEA
Engineering Design	47	28
Component Failure	18	22
Correspondence (lack of)	14	15
Interaction	32	13
Physical Degradation	10	5
Total	**121**	**83**

Table 16 - Total causes per category

It can be seen that the majority of causes found by STPA are related to Engineering Design and system interaction. STPA was able to find all the FMEA Engineering Design related causes. Some of these causes have direct relationship to the examples shown in section 5.1 and some causes correspond to a higher level of abstraction of a cause identified in FMEA. For example, FMEA finds cause *(2.7.1) Improper or defective gear installation on vehicle* as a possible reason for the driver experiencing degraded road feedback and wheel fight. STPA finds in Scenario1 from UCA10: *Assembly connections improperly made or do not retain torque/ torqued out of specification or alignment.* Because a defective gear may not be properly placed in the FMEA analysis according to SAE J1739 (assumption of components manufactured to design specifications), the design cause would be that an improper gear assembly is causing such noise in the system. STPA acknowledges that an individual component could cause these noises, but also it acknowledges that overall assemblies in the system may contribute to such

effect. Therefore, addressing the higher level of abstraction (ensuring proper alignment of all components by design) captures individual instances of noises associated with bad alignment.

In Component failures type of causes, STPA also finds causes that correspond to a failure mode cause in FMEA. As Table 16 shows, the specific number of component failures is higher for FMEA. This is because STPA identified some failures at a higher level of abstraction than FMEA did. For example, STPA finds in Scenario1 from UCA10 the cause *Hardware failure (Includes Gear damaged, Wear in pinion or rack assembly, Ball joint degraded or making noise, Belt assembly failure (rupture), Electric Motor internal failure)*, which was counted as a single cause. FMEA finds under causes *(6.1.2) Pinion assembly makes unwanted noise and (1.1.1.12) Rack and ball nut assembly does not permit axial movement of the rack* as causes for not meeting function under the targets set for acceptable vibration and it is counted as two causes. Both methods identified similar hardware component failures in this case.

STPA also finds some specific causes associated to Component Failures that may contribute to the system entering a hazardous state. Although it is expected that these specific causes will be further analyzed in the Component FMEA, they are useful when they are included in the System analysis. As an example, Scenario1 for UCA18, finds that if a failure occurs with the temperature sensor does not detect high temperature conditions at high speeds, commanding auxiliary assistance would cause the system to provide higher assistance than would be required for that vehicle speed. Such assistance could contribute to the current high temperature condition in the system. FMEA identifies a failure to detect an error in measurement, but it is not extended to specific conditions in which providing high assistance at high speed could lead to hazardous situations. FMEA could later find this situation as product of exhausting testing, which usually takes time to complete and reduces the time to react if failure is found.

Lack of Correspondence causes are comparable between STPA and FMEA. FMEA seems to find one more cause than STPA, however this is again due to differences in level of abstraction. FMEA proposes specific targets for electrical components for EMC immunity and emission. STPA addresses EMC for example in Scenario 1 of UCA17 as *Electromagnetic noise allowed in the system providing erratic behavior of sensors.* The identification of this cause allows the design team to set appropriate levels of allowable noise for the system (either in or out of the system). Because the design assumptions at this stage are in early development, the STPA

causal analysis covers both EMC emission and immunity related causes. Therefore, this analysis finds the total causes within Lack of Correspondence comparable between the two methods.

STPA is able to find all the interaction related causes found by FMEA. STPA finds more than double the causes than FMEA for system interaction. Although identifying unsafe system interactions can be achieved without iterating STPA, the author found it valuable iterating STPA to determine those interactions. Unfortunately, FMEA was not designed to find failure causes related to required interactions. To be successful from the initial set up of the analysis, FMEA requires that all interactions are already known. This is often not the case in new developments. To be fair, FMEA could be updated to include these types of failure after initial testing of the system if unexpected interactions are discovered. However, finding those causes during design and before testing can be difficult and the FMEA process does not provide much guidance for this problem.

The Physical degradation causes are higher in STPA than in FMEA. The amount of causes might be perceived higher for STPA initially. However, STPA makes a distinction between component failure and component physical degradation, whereas it is often treated the same in FMEA. It is expected that physical degradation type of causes would be included in the component FMEA.

Figure 8 shows the distribution of individual causes found by both methodologies. FMEA found more detailed component causes, whereas STPA found significantly more interaction causes and Engineering Design related causes that were missing from FMEA.

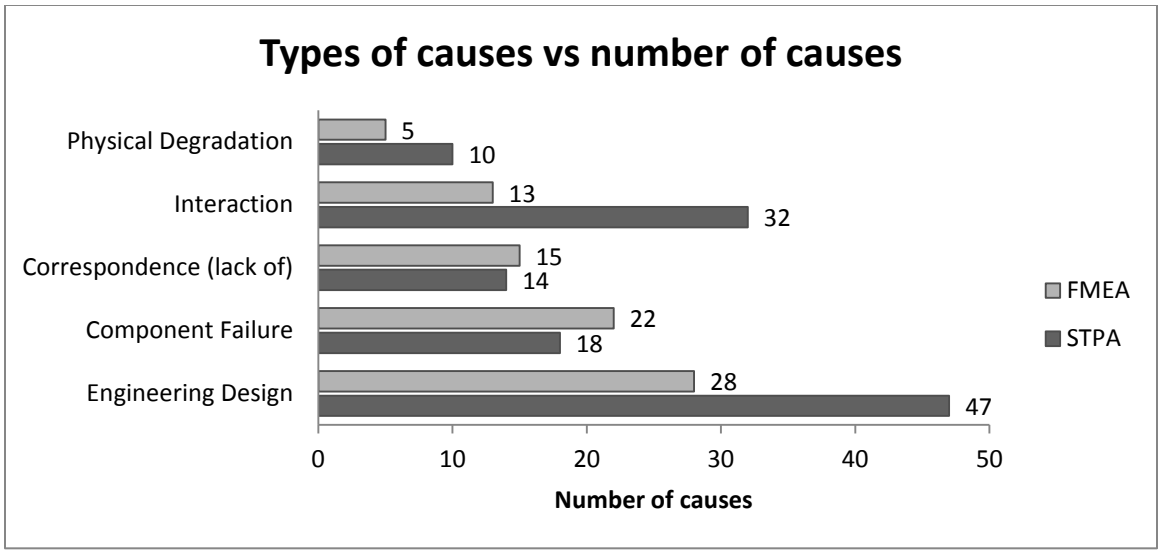

Figure 8 - Distribution of causes found by STPA and FMEA[3]

Figure 9 shows the Histogram of the Severity ranking found in FMEA. Notice that initial FMEA finds mostly high-ranking severity numbers and there is a trend for finding less severe causes later on, except for causes with severity 6. Severity 6 causes refer to causes where loss of secondary functions affects the comfort of the passengers or driver. Non-safety critical function loss or degradations were evaluated with highest severity ranking because it is not clear how a degraded secondary function may contribute to the system hazards initially. Lower numbers of severity are also hard to derive when doing initial assessments of new designs.

[3] STPA finds a subset of higher level of abstraction for component failure and lack of correspondence causes which makes the methodology able to capture all FMEA causes. STPA also finds more Engineering Design causes and Interaction related causes.

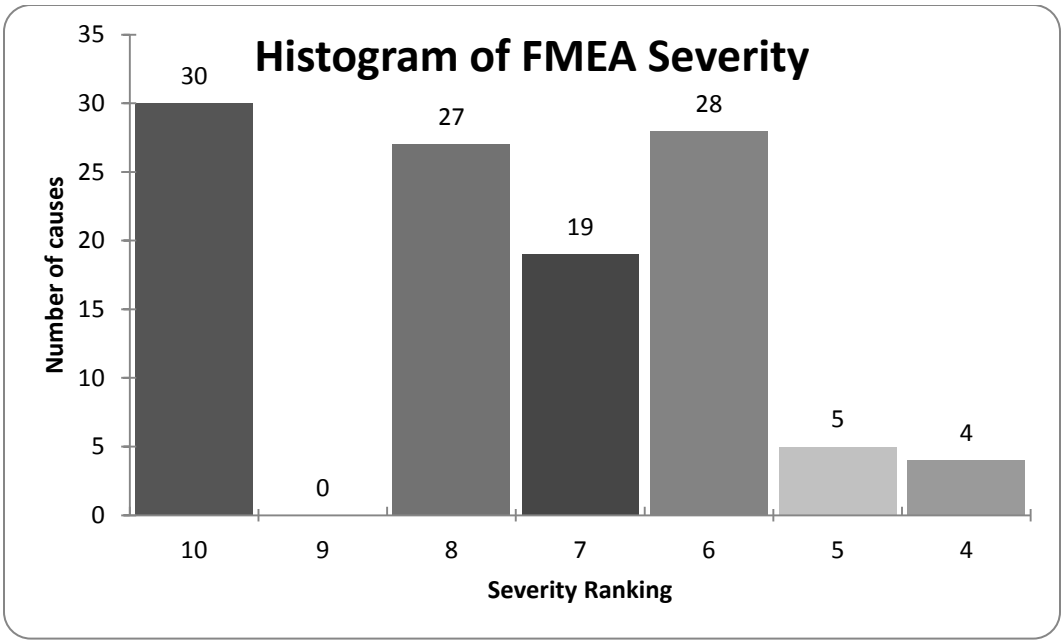

Figure 9 - Histogram of Severity ranking found in FMEA[4]

5.2.2 Causes found only by FMEA

All causes in FMEA considered for this comparison and analysis were also found in STPA. STPA was able to find some causes that had direct correlation with those found by FMEA while other FMEA causes were covered by STPA at a higher level of abstraction.

5.2.3 Causes found only by STPA

STPA is mainly focused in preventing hazards by deriving requirements to mitigate the causes identified. STPA also provides traceability of such causes all the way to the system accidents or losses that must be prevented. Recall that Table 5 presented in Chapter 4 shows the Hazards to Accident relationship from the system:

[4] FMEA Severity histogram is shown. FMEA founds high portion of Safety related causes that are ranked severely for initial developments. Highest-ranking FMEA is also applied to secondary function loss due to lack of initial data.

Hazard	Description	Accident
H1	Vehicle occupants experience harmful conditions during vehicle operation.	A1, 2, 3
H2	Vehicle does not maintain minimum separation from other moving bodies.	A1, 2, 3
H3	Vehicle does not maintain minimum separation from static bodies.	A1, 2, 3
H4	Vehicle is difficult to operate	A1, 2, 3
H5	Vehicle equipment is operated beyond limits (experience excessive wear and tear)	A2, 3

Table 5 – Hazards to Accident relationship

Hazard	A1	A2	A3	Number of causes
H1	x	x	x	99
H2	x	x	x	102
H3	x	x	x	103
H4	x	x	x	121
H5		x	x	89

Table 17 – Number of causes per system Hazard and Accident relationship

Table 17 shows the breakdown of causes found associated to the system Hazards and Accidents. Hazards 1 to 4 have a direct relationship with the three main System Accidents. The causes that are able to be found by STPA not only address safety concerns, but they also address accidents related to economic loss and customer satisfaction. It is expected that *A3: Loss of customer preference/ brand loyalty*, would contain a higher number of causes, as the loss of associated with the other system accidents have a direct relationship on customer preference and loyalty, but not all these causes are related to safe operation.

Figure 10 shows the break down by cause associated with each Hazard.

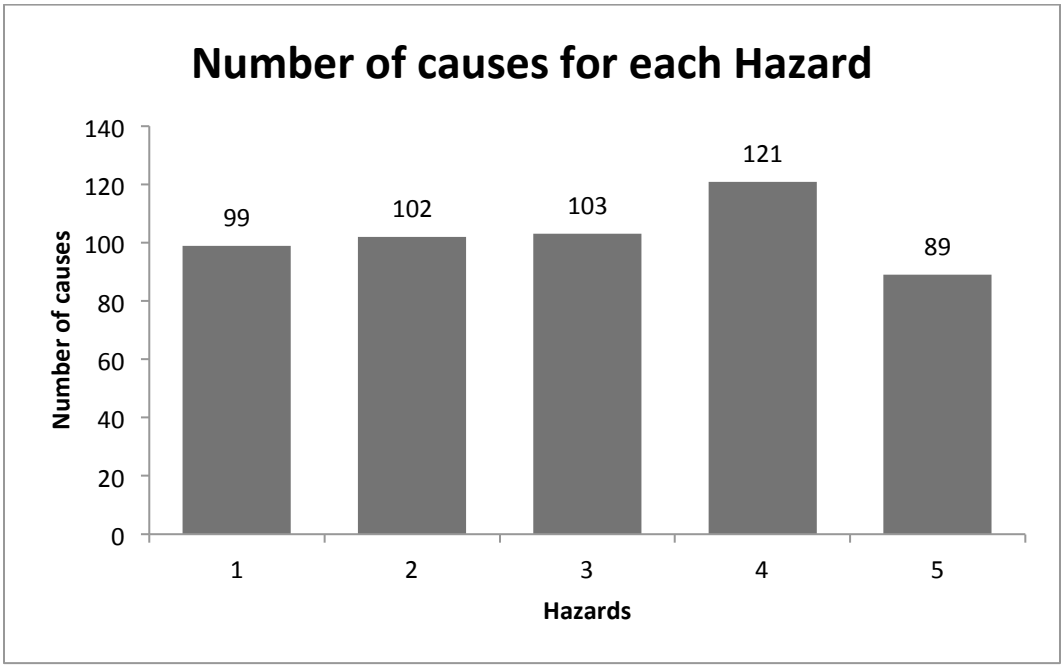

Figure 10 - Cause breakdown by Hazard[5]

The system hazards and accidents could be prioritized or ranked by severity if needed. Since every output of STPA is traceable to the system hazards, each cause can be prioritized based on the associated system hazards.

Section 5.2.1 presented the general outcome of causes identified in both methodologies. Each category was explained and examples were provided. STPA was able to find a portion of causes that had direct correlation with those found by FMEA. STPA also found another potion of causes that had governed the remaining set of causes of FMEA in a higher level of abstraction that would completely cover the cause identified by FMEA. On the other hand, there is a set of causes in STPA that were not covered by FMEA. Figure 11 shows these causes divided into the categories described earlier in this chapter. This section reviews the causes that could not be found by FMEA and provides some examples.

[5] Causes-Hazards relationship shown. STPA shows an fairly even distribution of causes associated to system Hazards. *Hazard 4: Vehicle is difficult to operate*, is related to most causes.

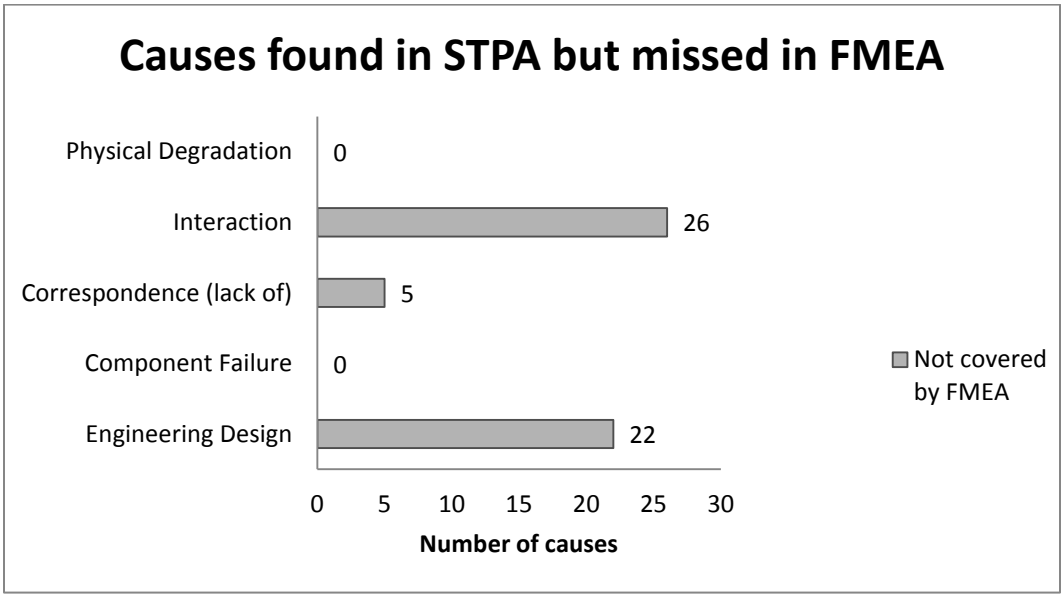

Figure 11 - Causes found by STPA but missed by FMEA[6]

5.2.3.1 Causes related to **Interactions**

STPA is able to find more Interaction related causes than FMEA. The author found it useful to follow the method proposed by Thomas [15] to provide functionality first and iterate STPA to incorporate the changes that could address initial findings in STPA. This action allowed to capture more detailed causes that related to interaction, as in UCA20 Scenario1:

> UCA20: SCM commands auxiliary assistance command but driver is not made aware of it (H1, 2, 3, 4, 5)
>
> Scenario1: There is an event of either hot temperature or high friction, which provides limited assistance behavior, but driver is not made aware of it.
> Possible causes include:
>
> - Missing communication to BCM.
> - BCM is in fault mode, not receiving information.

[6] The graphic shows the causes that FMEA was not able to find compared with STPA for each category explained. Note that Physical Degradation and Component Failure does not show a number. This is because STPA found causes that either have a close relationship to a cause in FMEA or a higher abstraction level that would capture those causes of FMEA.

- Signal delay.
- Chimes are not audible.
- Driver gets distracted or something prevents the driver to become aware of it e.g., music volume too high.

STPA proposes from the first iteration that Auxiliary assistance can be commanded when the system detects there is a reason that would degrade the performance of the system and in consequence cause an accident. While this mitigation strategy could be effective, there are other considerations that need to be taken. It is not enough to provide auxiliary assistance when a fault is detected. There are situations in which auxiliary assistance can contribute to worsening the hazardous state of the system. Should the system enter an auxiliary mode to protect itself and the driver when it is acceptable to do so, it is important that the driver gets notified in a proper manner. If this notification fails or is not effective, the driver may add to a hazardous state by demanding more assistance out of the system. In order for the notification to be effective, the SCM needs to communicate with the module that governs the displays to the driver. Such a module is called the Body Control Module (BCM). If the BCM enters an error state due to causes not related to the EPS system, a hazardous situation can be avoided by not providing auxiliary assistance.

FMEA is not able to include these types of relationships because ensuring communication with other modules is not part of the initial functions of the system analyzed. Although the initial assessment in FMEA does not capture this scenario, the analysis suggests that these types of failures are incorporated once the evaluation of the initial causes has been completed. However, it is uncertain all possible system interactions could be tested when conducting the vehicle level testing. To ensure that these types of failures are caught during the product development cycle, the testing plan would need to exhaustively test all modes of operations that the driver could experience. This action is simply not possible when analyzing embedded software systems [2].

Product Development organizations expend considerably large amounts of resources developing verification and testing procedures that would verify that the design requirements are met. These sets of tests often take a considerable amount of resources and time, which puts more pressure on achieving the design deliverables in order to launch a product. The later a

new system interaction type of cause is found, the later development efforts may be pushed outside of the timely delivery of the project and the more costly to fix.

5.2.3.2 Causes related to human behavior and human error

Another set of important interaction causes included in STPA and not included in FMEA, are the interactions of the system with the driver. The driver is the ultimate controller of the vehicle system and many of the decisions in regards to the safe operation of the vehicle follow through him or her. Although FMEA includes the driver or customer commonly in the Failure Effect of each function as the effects of a failure may have on the driver, it does not include the driver functions in regards to the system. Including the driver and his or her interaction with the system also prevents hazardous conditions to occur, as shown in STPA. STPA goes even further by understanding how the experience of such failures can change the driver's mental model. To consider the driver's mental model if a failure occurs, allows the design team to provide mitigation actions more effectively. An interesting example is shown next. Consider UCA13 Scenario2:

> UCA13: Driver leaves safe path before steering maneuver is being completed (H-1,2,3,4,5)
>
> Scenario2: Driver performs a steering maneuver in a desired direction but is unable to maintain a desired path because assistance perceived is too low. The driver may experience that the assistance is too low because:
> - Assistance is not provided (loss of assistance) and the driver is not informed or neglects a low sound warning (See UCA1)
> - Torque steer event opposite to the driver commanded direction.
> - See SCM UCA5.

This is scenario is interesting because it relates to a portion of the analysis where it observes how the SCM may not being able to provide the required assistance by the driver (UCA1) and also how it may provide low assistance when the vehicle speed is low (UCA5). However it also points that the driver may enter a torque steering situation where he or she may not be aware that the vehicle will pull to a side with heavy acceleration. Torque steer refers to the tendency of

a vehicle to pull to one side as the engine drives the vehicle. This phenomenon is specially perceived in high performance vehicles where a heavy acceleration provides a sudden increase in torque driven to the wheels and an unbalanced power delivery. Such unbalanced power would cause that the vehicle to pull to one side and it is inherent to the suspension geometry of the vehicle. The intensity of this pulling force depends on the vehicle dynamic characteristics. If the driver is not made aware of this situation, the EPS may be delivering the appropriate assistance to the vehicle according to speed and input torque, but he or she might experience a sudden increase of steering effort while performing a steering maneuver. This sudden increase may contribute to leave a safe path while performing a steering maneuver.

5.2.3.3 Causes related to Engineering Design

Just as Interactions related causes, STPA is able to find Engineering Design causes with close correlation to FMEA, as well as subset of generalization instances to cover all causes found by FMEA. However, as shown in Figure 11, STPA also finds 22 causes that cannot provide a strong relationship with a similar cause in FMEA, either at a higher or lower abstraction level. Although some of these 22 causes might be included in a component FMEA, if the system grows in complexity, it becomes difficult for the evaluation team to trace the component related failures that could contribute to impeding the system in delivering its function. Sensor calibration can be used as an example. UCA1 Scenario1 shows:

> UCA1: Assistance is not provided when driver executes a steering maneuver (H-1,2,3,4)
>
> Scenario1: SCM does not provide assistance because SCM incorrectly believes that assistance is not needed (incorrect process model). SCM does not know assistance is needed because:
> […]
>
> - Incorrect sensors calibration for vehicle architecture and geometry.

Such failure might be overlooked in the system FMEA because by following the SAE J1739 assumption that components are manufactured to meet the design specifications would indicate that the sensors should be assembled to the gear assembly calibrated as specified. Engineering Design, however, is responsible for determine the correct calibration of sensor to accommodate the requirements of the vehicle suspension geometry. FMEA may include that the right

calibration should be received from the development team in the component FMEA, but it is not visible at early stages of design. Since it cannot be assumed that such failure will be contained in each FMEA sensor analysis, this cause is not found by the FMEA analysis.

Another example of Engineering Design causes not covered by FMEA and covered by STPA, are the causes related to the software to incorporate characteristics that need to be monitored to enforce the safety constraints of the system. FMEA does not cover the logic to which the software responds or specific conditions that contribute to the system hazards. UCA 18 Scenario1 shows how selecting incorrect thresholds for high temperature can cause the Auxiliary Command to mitigate a hazardous condition that is not given.

> UCA18: SCM does not command auxiliary assistance when a fault is detected or there is a high temperature event (H4, H5)
>
> Scenario1: SCM does not command auxiliary assistance because SCM believes there is high friction but the speed is low. If high friction is detected at low speed SCM should not command auxiliary assistance because the amount of assistance provided at low speed should be higher than the auxiliary assistance. Possible causes include:
>
> - False detection of high temperature at high speed. Possible contributors:
>   - Temperature sensor incorrect measurements.
>   - Incorrect thresholds selected for high temperature.

FMEA may include causes for the temperature sensor in the component analysis to provide incorrect measurements, but it did not account for the correct thresholds for high temperature to be correctly stated in the SCM logic.

5.2.3.4 Causes related to Software

STPA finds a subset of causes that are attributable to how the software is developed and helps to derive requirements to address those causes. Although software FMEA was developed to analyze how the EPS software could find errors to deliver function, it was observed that the analysis often stopped at component related failures. Because the FMEA function analyzed in this case specifically mentions friction, the FMEA analysis did identify some errors involving incorrect thresholds for steering friction. However, it did not identify errors related to

measurements or logic conflicts when auxiliary assistance should be provided. Notice that FMEA required adding additional functions into the analysis to determine such causes.

Function	Potential Failure Mode	Potential Effects of Failure	SEV	Class	Potential Cause	OCC
(6) Diagnose high friction condition in system	(6.1) Does not detects high friction condition	(6.1.1) High efforts to steer to driver	6		(6.1.1) Thresholds set too high	2
		(6.1.2) Premature ware of components	6		(6.1.2) Road friction coefficient is too low	2
	(6.3) Detects high friction condition intermittently	(6.3.4) Increased maintenance cost of vehicle	4		(6.3.5) Vehicle speed variability larger than tolerances	4
			4		(6.3.6) Assist torque variability larger than tolerances	4

Table 18 – Software FMEA excerpt for high friction

Table 18 shows how FMEA finds that specifying friction threshold too high would contribute to not detecting high friction condition.

STPA finds in UCA 18 Scenario1 causes on how the algorithm may not command auxiliary assistance when there is high friction in the system. It finds errors related to how the SCM might believe that the system is operating under normal friction conditions and also errors associated with algorithm measurement error and logic conflicts:

UCA18: SCM does not command auxiliary assistance when fault is detected or there is a high temperature event (H4, H5)

Scenario1: SCM does not command auxiliary assistance because SCM believes there is high friction but the speed is low. If high friction is detected at low speed SCM should not command auxiliary assistance because the amount of assistance provided at low speed should be higher than the auxiliary assistance. Possible causes include:

- Torque sensor failure, measurement error or false signal (contributor to miscompute high friction)

[…]

- Temperature sensor incorrect measurement, indicating high friction in system.
- Wheel speed sensor failure or speed can't be estimated. It might be hazardous for the SCM to provide assistance when speed can't be estimated.
- Algorithm threshold for high friction is incorrectly specified
- Detection algorithm is not sensible enough to identify high friction conditions.
- Old values are used to calculate friction (e.g. The SCM would believe that low assistance is required when using a high value for speed previously stored, but if the actual state of vehicle speed is low, the input torque from the driver will be higher. The SCM would believe that higher torque input is required for certain level of assistance, hence interpreting that there is high friction in the system).

STPA goes more into detail about how the algorithm may incorrectly interpret high friction conditions that would not enable auxiliary assistance additionally to choosing incorrect friction thresholds. It also shows how the SCM may interpret that there is a high friction condition if old values for vehicle speed are used. This type of analysis allows determining requirements about how often would these values should be updated.

Another example of how software analysis is done can be seen when determining the causes of how low assistance may be provided when the vehicle speed is low. FMEA shows this analysis from function *3) Vary power assist with vehicle speed*, and Potential Failure Mode *3.1) Under assist at low speed only*. Table 19 is an excerpt of the software FMEA.

Function	Potential Failure Mode	Potential Effects of Failure	SEV	Class	Potential Cause	OCC	Prevention Controls
(3) Vary power assist with vehicle speed	(3.1) Under assist at low speed only	(3.1.1) Steering efforts high	10	YC	(3.1.1) Electric motor failure	4	- Electric motor FMEA
		(3.1.2) Customer discomfort	6		(3.1.2) Electric motor provides incorrect torque to belt assembly	4	- Electric motor FMEA
			7		(3.1.3) Incorrect module command (too high)	3	- Electric breadboard testing at system level - Calibration settings

Table 19 – FMEA excerpt of software function 3) Vary power assist with vehicle speed

UCA5 Scenario1 also addresses this hazard in STPA:

UCA5: Low assistance is provided while traveling at low speeds (H-1,2,3,4)

Scenario 1: SCM provides low assistance because incorrectly believes that the vehicle speed is high. SCM might incorrectly believe that vehicle speed is high because:

- Vehicle speed feedback is incorrect. Causes include:
    - Failed vehicle speed sensor
    - Wheel speed is used to determine vehicle speed, but wheel speed doesn't match vehicle speed
        - Acceleration in uneven or slippery surface could cause wheel speed to differ from vehicle speed
        - Anti-lock brakes affect wheel speeds
        - System is too sensitive to differential speed measurements

        - Connection or assembly improperly made.
    - Electromagnetic disturbance interferes with signal from wheel speed sensors (high signal to noise ration)
    - Internal components overheat causing degradation of the system and false readings.
    - A pervious value for vehicle speed is used to determine the vehicle speed.
- Inadequate external speed feedback could explain incorrect SCM process model (sensor calibration, sensor failure, signal delays).
- Maximum torque threshold is set up too low in algorithm.
- Traction differential between wheels causing uneven speeds measurements that provide high-speed readings.
- SCM does not update change in speed fast enough. Using an old (high) speed value to provide assistance at low speed.

SCM provides low assistance because SCM incorrectly believes vehicle turning angle is too large. SCM believes turning angle is too large because:

- Vehicle turning angle feedback is incorrect. Causes include:
    - Failed turning angle sensor.
    - Shorted harness, open circuit.
    - Signal delay in the BUS.
    - Sensor degrades over time.
    - Electromagnetic disturbance interferes with signal from sensor.
    - A pervious value for vehicle turning angle is used to determine real angle.
- Vehicle turning angle threshold or calibration is incorrect. Causes include:
    - Incorrect factory calibration.
    - Changes or modifications to vehicle's steering system without recalibration

SCM provides low assistance because the torque sensor feedback incorrectly indicates high torque. The incorrect feedback could be due to:

- SCM electronic failure (circuit internal failure).
- Steering wheel/Torque sensor failure.
- Shorted harness, open circuit.
- Delayed signal information provided by sensor, in the BUS.
- Algorithm minimum or maximum threshold for torque is incorrect and assistance is not provided.

- Sensors degrade over time (incorrect assembly, corrosion).
- Incorrect sensors calibration for vehicle architecture and geometry.
- Electromagnetic disturbance interferes with signal from sensor.
- An old value or parameter is used to calculate the input torque form the driver.

STPA covers multiple conditions in which the algorithm may be set up incorrectly like *Maximum torque threshold is set up too low in algorithm* or *Vehicle turning angle threshold or calibration is incorrect* for the steering angle sensor.

5.2.4 Producing Requirements

STPA generates a list of system safety constraints and requirements, however FMEA outcomes do not involve requirements. Although requirement generation cannot be compared between both methodologies, it is important to note this difference in the comparison. In this case STPA generated a set of 47 high-level requirements that are linked to the System Safety Constraints and can be used to evaluate system performance.

FMEA on the other hand generates 53 Preventive actions that are intended to address the potential failure causes found in the analysis. The results of the FMEA also often involve component parameters that deviate from the system requirements. Therefore, such requirements need to be known before performing FMEA

5. 3 Summary

This chapter presented a way of comparing the results achieved by both methodologies. First, categories of shared characteristics were defined and used to compare the results of both approaches. There were identified causes in each methodology that had direct correspondence to a similar cause in the other methodology. Another set of causes in the STPA analysis was found in which a more abstract STPA scenario cover several detailed causes found in FMEA. By addressing a generalization of causes, those set of causes found by STPA were able to cover all causes found by FMEA.

The analysis of STPA causes includes conflict resolution provided by Thomas method presented in Chapter 4. By identifying which control action combinations lead to conflict, STPA

can systematically identify potential design issues so engineers can decide how to mitigate or eliminate them. FMEA is not able to provide an analysis framework to identify causes, that when addressed, may result in conflicts with other control actions.

STPA found more interaction related causes than FMEA. As a top-down analysis, STPA allows the engineers to include the system interactions from the start of the control structure when analyzing the system. In its simplicity, STPA emphasizes that a certain level of abstraction is required at the beginning of the methodology so that system analysis can begin during the earliest development phases. Simplicity does not mean incomplete. On the contrary, STPA requires the initial control structure to ensure completeness of initial interactions to derive meaningful results. The method proposed by Thomas [15] to perform STPA iteratively allows for the structured derivation of specific system interactions after an initial iteration of STPA. The iterative process allows the engineers to understand not only which system interactions are required, but also what other entities might be affected during system operation.

The STPA analysis also included interactions with the driver to understand how different sets of conditions may influence his or her mental model. Considering the mental model of the driver when a hazardous condition is present allows for improved avoidance and mitigation of possible accidents, including those related to human error. FMEA does not provide an analysis framework to systematically identify and explain human error.

STPA also found Engineering Design causes that could not be covered by FMEA. STPA includes some causes that are related to a certain condition of component failure that would directly contribute to the enabling of a hazardous condition. Although FMEA may cover these causes in individual FMEA components, it is often difficult to maintain the flow of information from different sources, especially if there are different engineering groups responsible for the design of individual components. If this is the case, the interactions among those design groups need to be cohesive so proper information is included in the analysis. As design becomes more complex and design groups are scattered among diverse locations globally, it becomes increasingly difficult to be able to allocate revisions with all affected stakeholders.

Another set of causes that only STPA is able to discover is related to the different thresholds for specific situations that could lead to hazards. Those thresholds are engineering values of properties that need to be closely monitored to enforce the safety constraints of the system. The

embedded systems include these parameters in their logic. It is not sufficient to provide accurate measurements of hazardous situations, but also to properly detail them in order to solve conflicting scenarios to ensure conflict resolution. As seen throughout this analysis, it is important to understand the context in which function is provided to ensure that safety is enforced through control actions. Such context is provided by the different interactions of the system. These interactions may be intended or unintended, but ultimately both contribute to the context in which the system operates. The engineering team often tries to eliminate unintended interactions by enforcing system constraints. Therefore, it is of extreme importance that the system constraints are as complete as possible.

Table 20 shows the summary of findings by methodology performed in this thesis.

STPA	FMEA
Analyzes 22 UCA's	Analyzes 13 System Functions
49 Scenarios	72 Failure modes
121 Causes	83 Causes
47 high-level requirements and 10 System Safety Constraints	53 Prevention Actions

Table 20 - Summary of FMEA and STPA outcome

Chapter 6: Conclusions

The work presented in this thesis demonstrates how STPA can be introduced in the early stages of product development for complex automotive system such as Electric Power Steering. This thesis validates that despite analyzing broad application of EPS systems, STPA enables insightful discovery about hazard conditions that traditional analysis techniques such as FMEA are limited in finding, especially in early stages of design conception and those that do not involve component or functional failure. FMEA and STPA were compared within the automotive industry to understand if the current practice holds room for improvement.

FMEA is a tool widely used across the industry that has helped to improve reliability of individual components once failure modes have been identified. It also appeals to industry because some of the results generated from design FMEA's are used as input for controlling the manufacturing process through Process FMEA. However, this study found limitations with FMEA in terms of identifying unsafe interactions between systems, anticipating human error and other behaviors dependent on human interaction, identifying engineering design flaws, and producing requirements.

Complex automotive systems are relying on both hardware and software to achieve designed functions more often. As in the EPS system, there has been an increased usage of embedded software in modern automobiles to ease manageability of both physical properties and information exchange and to allow functions and complexity that would be impossible or impractical to provide purely with hardware. In the case study presented, FMEA was used to identify accident causes by partitioning the analysis and duplicating the functions that are controlled by both hardware and software. Software analysis often stopped at a component failure. The top-down analysis done by STPA allows for the engineers to investigate hazardous causes regardless of whether it involves a hardware failure or unsafe software behavior. The type of causes discovered can be related to hardware, to software or a combination of both.

6.1 Recommendation for the automotive Product Development process

STPA allows safety analysis to be performed before a design is produced. Instead, the constraints and requirements for safe behavior are first identified and then used to create a safe

design. Chapter 2 presented the foundation for iterative STPA process. By incorporating such a process in the design cycle, the product development organization can leverage early discovery of required behavior for safety in order to include it in the early stages of System Engineering. This process should reduce the amount of resources involved in rework and subsequent iterations compared to current practice where a vast amount of interaction-related hazardous behavior is not discovered until later stages in the design and testing process. The later these errors are discovered, the higher the risk of delaying development completion exists.

As it has been previously shown, STPA provides a comprehensive analysis that helps to intellectually manage automotive complex systems. The strength of STPA relies on the generation of functional safety requirements. However, it can also generate functional quality requirements aligned to achieve customer satisfaction (e.g., UCA10 relates to providing functionality within acceptable ranges by the customer and causal analysis that could lead to not meeting NVH requirements, mapped to H5-> A3). Quality targets can be included to enforce both safety and functional constraints. STPA can be used for any emergent system property, including safety and security, but also many other important system properties.

6.2 Future work

This thesis focused on analyzing a generic Electric Power Steering system to include most of high-level design decisions to achieve safe functionality. These concepts can be introduced in the next generation of Electric Power Steering and compare and contrast against actual values derived from testing. Automotive Product Development Organization can incorporate STPA in the product development process and measure time and resources used for developing and implementing results from STPA.

STPA can be applied to additional automotive systems. It should be expected that STPA is able to provide similar results. Many researchers at MIT and in the automotive industry have applied STPA to automotive systems and provided valuable insights following slightly different approaches while ensuring that the method is followed as developed by Leveson [2]. The development of an across the industry standard such as the one provided by SAE for FMEA can ensure that automotive organizations recognize the value of STPA and incorporate it into their organization following an automotive standard. The standardization of STPA to the automotive

industry may ensure that different organizations deliver results similarly, which is helpful when managing a wide supply base.

Realistic recommendations can include a plan to gradually incorporate STPA. Future work can be developed to understand how Product Development organizations see the benefit of incorporating STPA in their organizations, and what it does in terms of timely delivery of targets and safety assurance.

As described before, FMEA is widely used in the automotive process because it uses certain outputs of the Design FMEA as input to the process FMEA. A comparison between the manufacturing controls was outside of the scope of this thesis, and although both analyses showed some manufacturing related causes, it was decided not to include these results in the comparison. FMEA is known for identifying important characteristics in the design that are specifically controlled in the manufacturing process. However, STPA can also be expanded to develop a manufacturing control loop that follows through enforcing safety constraints in the manufacturing process discovered in the design analysis.

References

[1] N. Leveson, *SafeWare: system safety and computers*. Addison-Wesley, Mass, 1995.

[2] N. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety*. 2011.

[3] Q. V. E. Hommes, “Applying STAMP Framework to Analyze Automotive Recalls,” 2014.

[4] D. Kiley, “The New Heat On Ford - Businessweek,” 2007. [Online]. Available: http://www.bloomberg.com/bw/stories/2007-06-03/the-new-heat-on-ford. [Accessed: 25-Apr-2015].

[5] W. J. Abernathy, *The productivity dilemma: roadblock to innovation in the automobile industry*. Baltimore: Johns Hopkins University Press, 1978.

[6] F. Utterback, J., Suarez, “Patterns of Industrial Evolution, Dominant Designs, and Firms’ Survival,” Cambridge, MA, 1992.

[7] J. P. Womack, D. T. Jones, and D. Roos, *The Machine that Changed the World: The Story of Lean Production*. 1990.

[8] SAE, “J1739,” vol. 4970. SAE International, 2009.

[9] U. S. D. of Defense, “Procedures for performing a Failure Mode, Effects and Criticality Analysis,” *MIL-P-1629*. 1949.

[10] N. A. and S. Administration, “Failure Mdes, Effects and Criticality Analysis (FMECA).” [Online]. Available: http://www.klabs.org/DEI/References/design_guidelines/analysis_series/1307.pdf. [Accessed: 02-Dec-2014].

[11] M. Mania, “FMEA (Failure Mode and Effect Analysis) - ManagementMania.com,” 2013. [Online]. Available: https://managementmania.com/en/fmea-failure-mode-and-effect-analysis. [Accessed: 02-Dec-2014].

[12] AIAG, “AIAG FMEA-4 Potential Failure Mode and Effect Analysis (FMEA).” p. 151, 2008.

[13] J. Thomas, “Extending And Automating A Systems-Theoretic Hazard Analysis For Requirements Generation And Analysis,” 2013.

[14] M. Placke, “Application Of STPA To The Integration Of Multiple Control Systems: A Case Study And New Approach.” [Online]. Available: http://sunnyday.mit.edu/papers/placke-thesis.pdf. [Accessed: 12-Nov-2014].

[15] J. Thomas, J. Sgueglia, D. Suo, and P. Leveson, Nancy Vernacchia, Mark Sundaram, “Integrated Approach to Requirements Development and Hazard Analysis,” 2015.

[16] N. Leveson, “Engineering a Safer World,” *2014 STAMP Workshop Presentations*, 2014. [Online]. Available: http://psas.scripts.mit.edu/home/wp-content/uploads/2014/03/Workshop-Tutorial-2014-final-out.pdf. [Accessed: 26-Apr-2015].

[17] J. Kerr, “The evolution of electric power steering | The Chronicle Herald,” 2012. [Online]. Available: http://thechronicleherald.ca/wheelsnews/140045-the-evolution-of-electric-power-steering. [Accessed: 15-Dec-2014].

[18] F. Mercedez.com, “36-nouvelle-classe-m-w166-direction.jpg (797×654),” 2012. [Online]. Available: http://www.forum-mercedes.com/img/members/3/36-nouvelle-classe-m-w166-direction.jpg. [Accessed: 27-Apr-2015].

[19] S. Burge, “Functional Failure Modes and Effects Analysis (FFMEA),” 2010. [Online]. Available: http://www.burgehugheswalsh.co.uk/uploaded/documents/FFMEA-Tool-Box-V1.2.pdf. [Accessed: 27-Apr-2015].

[20] N. Leveson, “Completeness in formal specification language design for process-control systems,” in *Proceedings of the third workshop on Formal methods in software practice*, 2000, pp. 75–87.

[21] Q. A. International, “Severity, Occurrence, and Detection Criteria for Process FMEA.” [Online]. Available: http://www.fmeainfocentre.com/guides/ProcessPktNewRatings.pdf. [Accessed: 12-Nov-2014].

[22] N. Leveson, C. Wilkinson, C. Fleming, J. Thomas, and I. Tracy, “A Comparison of STPA and the ARP 4761 Safety Assessment Process,” 2014.

[23] Y. Matsumoto, K., Matsumoto, T., and Goto, “Reliability Analysis of Catalytic Converter as an Automotive Emission Control System.” SAE International, 1975.

[24] U. D. of Transportation, “Transportation Systems Safety Hat Analysis Tool,” 2014. [Online]. Available: http://ntl.bts.gov/lib/51000/51500/51522/SafetyHAT_User_Guide_v1.pdf. [Accessed: 12-Nov-2014].

[25] J. M. Utterback, *Mastering the dynamics of innovationle*. Boston. MA: Harvard Business School Press, 1996.

[26] W. J. Abernathy and J. M. Utterback, “Patterns of industrial innovation,” *Technol. Rev.*, pp. 40–47, 1978.

List of Acronyms

ABS	Anti-Lock Braking System
ABS CM	ABS Control Module
AIAG	Automotive Industry Action Group
BCM	Body Control Module
BUS	Vehicle buss, refers to internal communication network in the vehicle
C	Celsius
CAE	Computer Aided Engineering
DFMECA	Design Failure Mode Effects and Criticality Analysis
ECM	Engine Control Module
EPS	Electric Power Steering
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode Effects and Criticality Analysis
FTA	Fault Three Analysis
GAWR	Gross Axle Weight Rating
GVW	Gross Vehicle Weight
kph	Kilometers per hour
lb-ft	Pound-feet
ms	milliseconds
N-m	Newton-meter
NASA	National Aeronautics and Space Administration
NHTSA	National Highway Traffic Safety Administration
NVH	Noise Vibration and Harshness
PFMECA	Process Failure Mode Effects and Criticality Analysis
PMV	Process Model Variables
RPN	Risk Priority Number
SAE	Society of Automotive Engineers
SCM	Steering Control Module
STAMP	System Theoretic Accident Model and Processes
STPA	System Theoretic Process Analysis
TPMS	Tire Pressure Monitor Sensor

Appendix 1: STPA analysis of EPS system

STPA of Electric Power Steering

Accident and Hazards definition of the system

STPA states initially unacceptable losses using a top-down system engineering approach that includes potential losses (accidents) and hazards that combined with worst case scenarios conditions will lead to those loses. Unacceptable losses for this analysis are:

A1: Vehicle occupants are injured during operation
- A1.1: Two or more vehicles collide
- A1.2: Vehicle collides with a moving body
- A1.3: Vehicle collides with a non-moving body

A2: Vehicle is damaged (economic loss)
A3: Loss of customer preference/ brand loyalty

In the same line, the system hazards must be stated. The system hazards related to those losses include:

H1: Vehicle occupants experience harmful conditions during vehicle operation.
H2: Vehicle does not maintain minimum separation against other moving bodies.
H3: Vehicle does not maintain minimum separation against static bodies.
H4: Vehicle is difficult to operate.
H5: Vehicle equipment is operated beyond limits (experience excessive wear and tear)

Hazards to Accidents relationship

Hazard	Description	Accident
H1	Vehicle occupants experience harmful conditions during vehicle operation	A1,2,3
H2	Vehicle does not maintain minimum separation against other moving bodies	A1,2,3
H3	Vehicle does not maintain minimum separation against static bodies	A1,2,3
H4	Vehicle is difficult to operate	A1,2,3
H5	Vehicle equipment is operated beyond limits (experience excessive wear and tear)	A2,3

After both accidents and hazards for the system have been defined, it is necessary to construct a control structure in which the Safety analysis can be performed. Figure 1 describes the general functional model of the Electric Power Steering system.

The role of the driver in for Figure 1 is to control the vehicle through the different operation environments the driver is exposed. The driver controls the direction of the vehicle through the steering wheel and the speed and braking events through the accelerator and braking pedal respectively. For this example it would be assumed that the driver controls a vehicle with automatic transmission, so the clutch pedal is not involved. The interfaces that allow the driver to control de vehicle have associated electronic modules that receive information from different sensors that detect and measure observable conditions of the vehicle. The electronic modules control actuators that provide the vehicle with speed, braking and steering capabilities so they must contain a model of the current state of the vehicle. The driver gets the model of the state of the vehicle through the different gages that are displayed in the cluster (gages display in the instrument panel) and in addition the driver gets information about the overall state of the vehicle. In most vehicles, the information to the driver is passive; that means that it only displays a warning when a change in the state of the vehicle requires the driver's attention. This is common practice to avoid driver distraction from the road and also to avoid that the driver unconsciously ignores important information due getting used to ignore information that ensures that the vehicle is function as expected. The driver also carries within a mental model about the state of the environment in which they are driving (traffic laws, surrounding objects including other vehicles, environmental conditions, etc.)

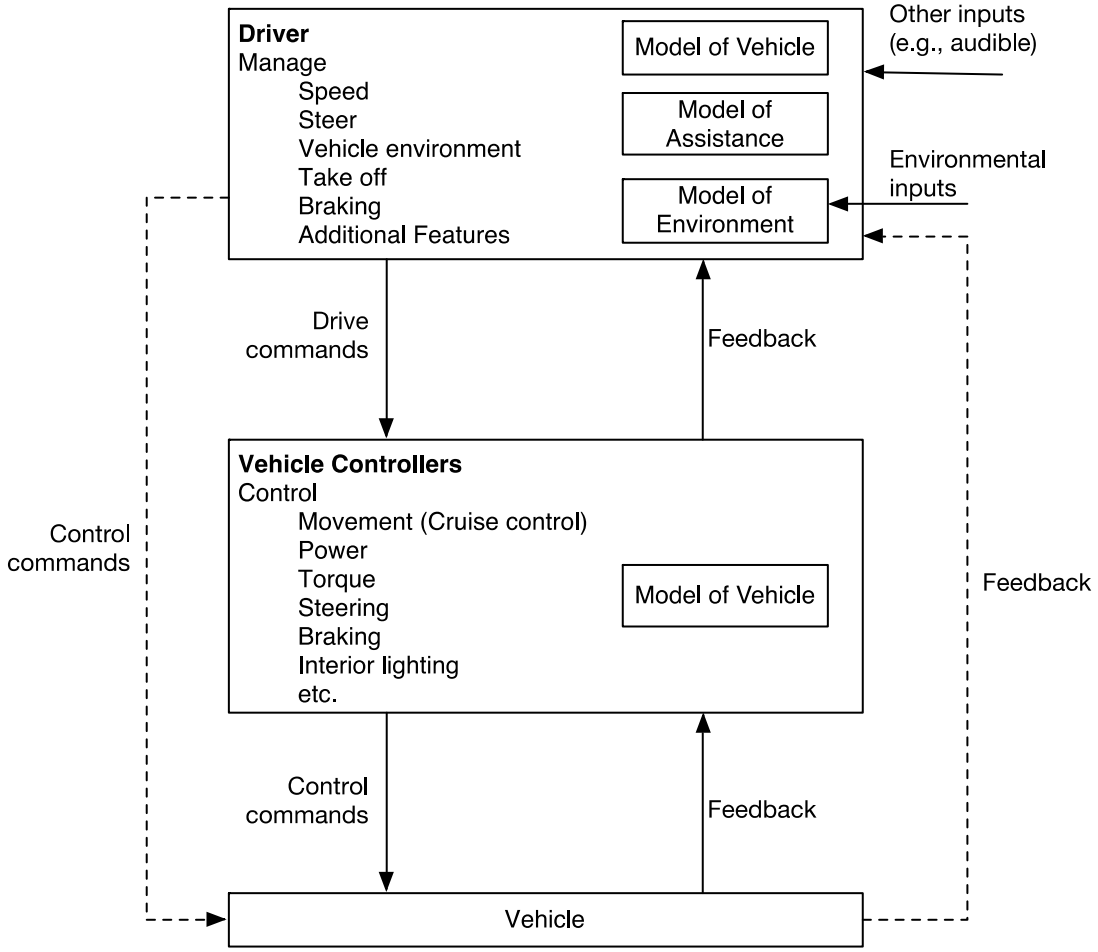

Figure 12 – High-Level control structure at Vehicle Level

For this analysis it would be useful to partition STPA into two iterations. The control structure of the first iteration does not show the physical implementation of the architecture of the EPS system, however it attempts to portrait the functional structure without any assumptions. This level of detail will suffice to analyze hazardous scenarios associated with primary control errors. It is useful to start with the basic required functional behavior so it can be understand which feedback and interaction is necessary to enforce the safe operation of the system.

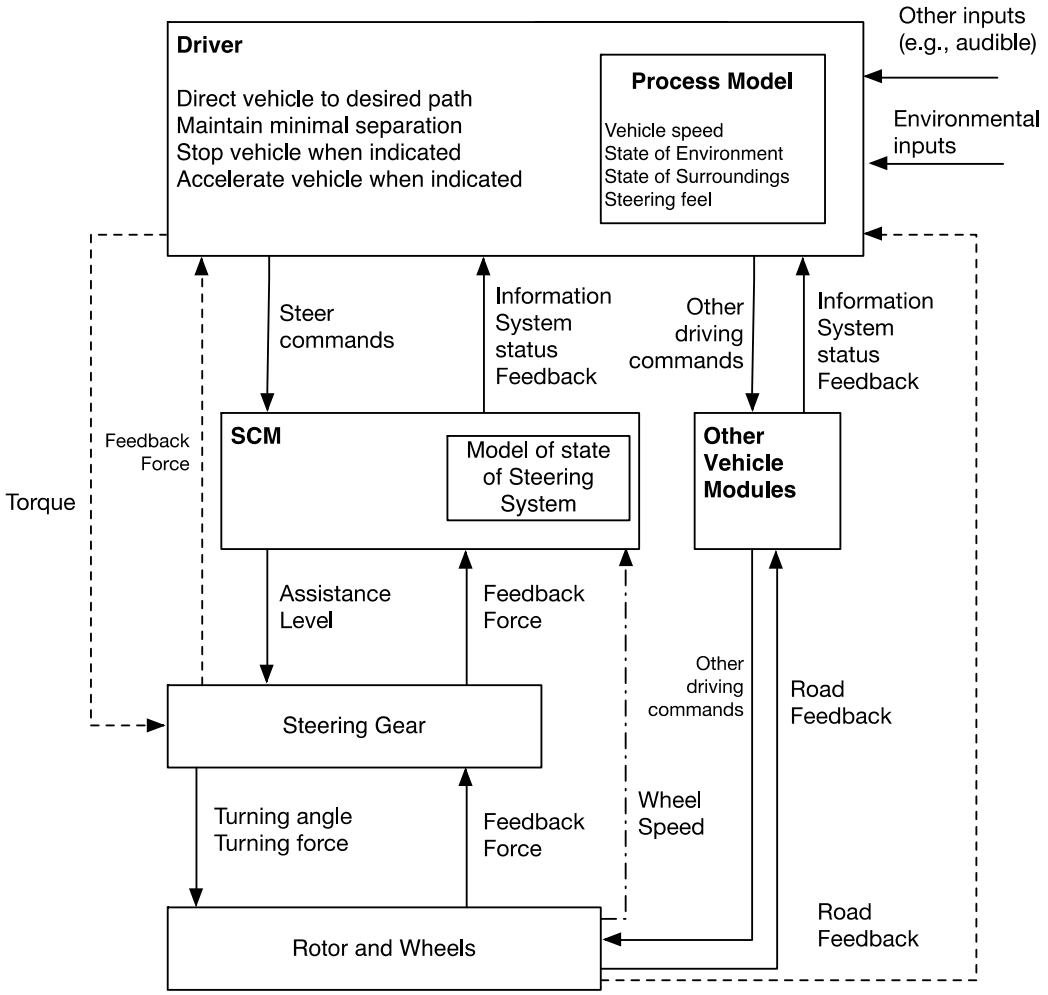

Figure 13 - Control Structure first iteration

Figure 2 shows the interaction required for the EPS to provide function. Dashed lines shows direct properties exchanged between the different components. For example, part of driver's effort to steer the vehicle (Torque) is directly driven to the vehicle wheels through the steering gear system due to a hard mechanical link, that force is transferred to the wheels with minimal loss due to system friction. Also in dashed lines, direct feedback is conveyed to the driver through the vehicle. The driver can experience road conditions through the vehicle depending on the load conditions. Although the suspension dampens the majority of the road vibrations that the vehicle experience, it dampens proportionally in the same amount and rate for every type of road condition, for this example, no active dampening is assumed.

STEP 1

Unsafe control actions depend on the operational phase. For example not providing assistance when the vehicle is stopped at a traffic light is not hazardous, however, not providing assistance when the driver needs to conduct a parking lot maneuver may lead to a hazardous situation.

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing or Order	Stopped Too Soon/ Applied Too Long
SCM provides assistance command to the motor	UCA1: Assistance is not provided when driver executes a steering maneuver (H-1,2,3,4)	UCA2: High assistance is provided while traveling at high speeds (H-1,2,3,4,5)	UCA3: Assistance is provided too late when driver executes a steering maneuver (H-1,2,3,4,5)	UCA4: Assistance is interrupted while driver executes a steering maneuver (H-1,2,3,4)
		UCA5: Low assistance is provided while traveling at low speeds (H-1,2,3,4)	UCA6: Assistance is provided intermittently when driver executes a steering maneuver (H-1,2,3,4,5)	UCA7: Assistance continues being provided when safe angle has been reached (H-1,2,3,4,5)
		UCA8: Too much turning force provided when the driver executes a steering maneuver (over assist) (H-1,2,3,4,5)		
		UCA9: Assistance is provided in a direction not commanded by the driver (H-1,2,3,4,5)		
		UCA10: Assistance is provided in a manner that discomforts the driver (H4, 5)		

Driver provides commands steering (force and direction) to steering wheel	UCA11: Driver does not provide steering command when there are people or objects in his/her path (H-1,2,3,4,5)	UCA12: Driver provides steering command towards a static or moving object (H-1,2,3,4)	UCA15: Driver performs a steering maneuver before or after safe path direction (H-1,2,3,4,5)*	UCA13: Driver leaves safe path before steering maneuver is being completed (H-1,2,3,4,5)
		UCA14: Driver provides abrupt steering command while traveling at degraded road conditions (H-1,2,3,4,5)		

Safety Constraints that can be generated from this first step include:

SC-R1 : Minimum assistance (TBD) Nm shall always be ensured when driver executes a steering maneuver. (UCA1)

Rationale: If the vehicle lacks assistance it might be difficult to maneuver when assistance is required. If the driver is expecting a low assistance for the current state of the vehicle and receives high assistance or vice versa, it may limit the way he or she would react should a hazard-leading situation be present. Further refinement will lead to providing an auxiliary assistance that would enable the driver to maneuver the vehicle.

SC-R2: High assistance shall not be provided when vehicle speed is high. (UCA2)
Rationale: Could lead to oversteer, understeer, roll over or incorrect direction to the vehicle depending on vehicle speed. Also, it can lead to a dissatisfied driver if the vehicle does not operate as expected.

SC-R3: Assistance shall be provided within (TBD) ms of steering command is received. (UCA 3)

Rationale: Delayed assistance may lead to an accident if the driver provides more force when he or she realizes that assistance was not delivered initially. When the commanded assistance is provided, the directional resultant force to steer the vehicle is a combination of the force from the driver and the compensation force from the EPS. If

the compensation force from the EPS is provided too late the vehicle might take undesired path.

SC-R4: Assistance shall not be interrupted while steering command is being received. (UCA4)

Rationale: May lead to a difficult control of vehicle depending on vehicle speed and road conditions. If the assistance is suddenly removed when the driver is executing a steering maneuver, he or she could experience a sudden increase in the steering efforts that could lead to lose of control.

SC-R5: Minimum Assistance (TBD) shall be provided when vehicle speed is below TBD [kph] (UCA5)

Rationale: Not providing minimum assistance could lead to driving difficulties and the impossibility to direct the vehicle to a desired path. It would also lead to loss of preference due to the vehicle does not meet customer expectations of providing assistance while steering the vehicle.

SC-R6: Assistance shall be delivered following a ramp proportional to vehicle speed. Such ramp function shall be estimated according to the vehicle architecture and dynamic targets. (UCA6)

Rationale: Providing abrupt changes of assistance to the driver when varying speed may cause confusion to the driver and affect the reaction capability given the mental model (believed state of the vehicle) he or she possess at the time of operation. Additionally, having punctual assistance for given speeds may lead to unwanted interactions and incorrect assistance delivery for the vehicle speed. Delivering assistance with a ramp function would make assistance to transition accordingly.

SC-R7: Assistance shall stop within TBD ms after steering command stops being requested by the driver. (UCA7)

Rationale: If assistance is kept while vehicle is taking a corner, it may lead to possible loss of directional control.

Requirements for the driver

DR-R1: The Driver must be provided with information about the state of the vehicle such as vehicle speed, steering assistance level, and clear vision of vehicle surroundings required to ensure safe operation. (UCA11)

Rationale: Driver not providing input might be due to lack of awareness of the state of the vehicle at the time of operation, further analysis will lead to understanding the causes.

DR-R2: Driver must operate vehicle for the conditions it has been designed. Proper documentation and media must be available to the driver to warn about potential miss-use (e.g., using passenger cars for off-road situation) (UCA13, 15, 16)

Rationale: Although it cannot be prevented that the vehicle is used under conditions it was not designed, making information available to the user should reinforce their mental model towards the safe operation of the vehicle.

Step 2

By identifying causes of the instance of the unsafe controllers, STPA seeks to generate the general requirements for the system-required interactions and feedback. The goal for the next section is to identify the causes that would lead to the unsafe control actions analyzed in Step 1, and the relationships that could lead to those hazards. The purpose of the selected scenarios is to demonstrate the methodology and would be further refined in next iterations.

UCA1: Assistance is not provided when driver executes a steering maneuver (H-1,2,3,4)

Scenario1: SCM does not provide assistance because SCM incorrectly believes that assistance is not needed (incorrect process model).
SCM does not know assistance is needed because the torque sensor feedback incorrectly indicates high torque. The incorrect feedback could be due to:

- SCM electronic failure (circuit internal failure).
- Steering wheel/Torque sensor failure.
- Shorted harness, open circuit.
- Delayed signal information provided by sensor, in the BUS.

- Algorithm minimum or maximum threshold for torque is incorrect and assistance is not provided.
- Sensors degrade over time (incorrect assembly, corrosion).
- Incorrect sensors calibration for vehicle architecture and geometry.
- Internal components overheat causing degradation of the system and false readings.
- Electromagnetic disturbance interferes with signal from sensor.
- An old value or parameter is used to calculate the input torque form the driver

SCM does not know assistance is needed because SCM incorrectly believes vehicle turning angle is too large. SCM believes turning angle is too large because:

- Vehicle turning angle feedback is incorrect. Causes include:
    - Failed turning angle sensor.
    - Shorted harness, open circuit.
    - Signal delay in the BUS.
    - Sensor degrades over time.
    - Electromagnetic disturbance interferes with signal from sensor.
    - A pervious value for vehicle turning angle is used to determine real angle.
- Vehicle turning angle threshold or calibration is incorrect. Causes include:
    - Incorrect factory calibration.
    - Changes or modifications to vehicle's steering system without recalibration
    - Incorrect sensor calibration for vehicle architecture and geometry.

SCM does not know assistance is needed because SCM incorrectly believes vehicle speed is too high. SCM believes vehicle speed is too high because:

- Vehicle speed feedback is incorrect. Causes include:
    - Failed vehicle speed sensor
    - Wheel speed is used to determine vehicle speed, but wheel speed doesn't match vehicle speed
        - Acceleration in uneven or slippery surface could cause wheel speed to differ from vehicle speed
        - Anti-lock brakes affect wheel speeds
        - System is too sensitive to differential speed measurements
        - Connection or assembly improperly made.
    - Electromagnetic disturbance interferes with signal from wheel speed sensors (high signal to noise ration)

- Measurements from several diverse independent sensors are used to estimate vehicle speed, but the sensor readings do not agree and the SCM is unable to combine the data accurately.
- Internal components overheat causing degradation of the system and false readings.

A pervious value for vehicle speed is used to determine the vehicle speed.

Possible requirements that may come out of this scenario include:

UCA1-S1-R1: Provide additional feedback for determining vehicle speed and steering angle.

UCA1-S1-R2: System level validation shall ensure that electric sensors, actuators and modules do not irradiate electromagnetic noise that could cause improver behavior of modules, actuators and sensors of the system and the vehicle.

UCA1-S1-R3: System level validation shall ensure that electric sensors, actuators and modules signal to noise ratio remains functional during vehicle operation and through common (environmental) electro-magnetic noises.

UCA1-S1-R4: Algorithm shall include logic to detect if signals from sensors are received in the time interval the system requires.

UCA1-S1-R5: System operation must be ensured within the operational range of system temperature. Means to control the operational temperature shall be in place. **Additional temperature sensor is required to monitor system temperature**.

UCA1-S1-R6: System shall start operations free of previously values stored that could influence the way required assistance is determined.

<u>Control action is provided but not followed</u>:

Scenario2: SCM provides assistance command but it is not effective because the current to power the motor is low. The current is too low because:

- System voltage is too low.

- Electrical system does not account for voltage drain during high assistance situations.
- The system enters into a reboot or protection mode that impedes normal functionality.
- Engine stalls while driving (unrelated to EPS) and power is insufficient to command the vehicle.
- Motor continues to provide high assistance In Lock-to-lock events (once the rack has reached the travel limit).
- Circuit interruption in the electrical harness (short circuit, open circuit, etc).

Possible requirements that may come out of this scenario include:

UCA1-S2-R1: Sufficient power shall be provided to the motor in order to provide assistance at different vehicle speeds..

UCA1-S2-R2: The SCM shall provide feedback to the Power Distribution Module about the voltage demanded from the motor to provide assistance.

UCA1-S2-R3: Current requested by the module shall drop within TBD s after rack's end of travel has been reached.

UCA1-S2-R4: The system shall not reinitiate after the vehicle has initiated operation or is below TBD speed.

UCA1-S2-R5: Auxiliary power in vehicle shall be capable to maintain a minimum of TBD [Nm] assistance in the event of engine stall and vehicle speed is higher than TBD [kph]

UCA1-S2-R6: Power distribution shall contemplate providing power to actuators that are required for safe operation of the vehicle under different driving conditions that include system low voltage.

Scenario3: SCM provides steering command but it is insufficient due to a steering lock condition. The system is locked because:

- High friction in the system due to improper geometry selected.
- Tolerances for friction components are outside allowable limits.
- Incorrect geometry selected for the type of suspension of the vehicle.

- Faults related to material and geometry for steering components.
- Suspension geometry or tuning does not correspond with the performance target of vehicle. Suspension might be too sensitive to road conditions, or response too harsh causing the steering system to react accordingly.
- Hardware failure. Includes:
    - Gear damaged
    - Wear in pinion or rack assembly
    - Ball joint degraded or making noise.
    - Belt assembly failure (rupture)
    - Electric Motor internal failure
- Corrosion protection is not adequate for usage under stringent conditions causing high friction/locking condition with internal components.
- Degrades over time. The system may degrade over time due to:
    - Corrosion is formed within steering gear components that prevent assistance from motor to move the front knuckle.
    - Premature wear of components due to improper alignment.
    - Material and geometry selected does not withstand the duty cycle designed for the vehicle.
    - High friction due to components not aligned properly or premature wear.
- Foreign components lodge in steering system.
- Steering rack travel limiters set incorrectly.
- Assembly connections improperly made or do not retain torque/ torqued out of specification or alignment.

The requirements that could be generated from this scenario include:

UCA1-S4-R1: High friction conditions shall be able to be estimated by the algorithm.

UCA1-S4-R2: Control plan and quality assurance plans shall be in place to ensure parts meet design tolerances and material specifications called in part prints.

UCA1-S4-R3: The system shall allow alignment setting (Toe) and access for update in periodic revisions (scheduled maintenance). The system shall retain the alignment setting (Toe) for the time in between scheduled inspections.

UCA1-S4-R4: System shall be guarded against foreign components and environmental conditions that could detriment performance.

UCA1-S4-R5: System shall provide notification to the driver when failures of motor, sensors, or SCM have been identified. System shall store fault codes for inspection and service.

UCA2: High assistance is provided while traveling at high speeds (H-1,2,3,4,5)

Control action not provided

Scenario1: SCM incorrectly provides high assistance when vehicle speed is high. SCM incorrectly believes that vehicle speed low because:

- Vehicle speed feedback is incorrect. Causes include:
    - Failed vehicle speed sensor
    - Wheel speed is used to determine vehicle speed, but wheel speed doesn't match vehicle speed
        - Acceleration in uneven or slippery surface could cause wheel speed to differ from vehicle speed
        - Anti-lock brakes affect wheel speeds
        - System is too sensitive to differential speed measurements
        - Connection or assembly improperly made.
    - Electromagnetic disturbance interferes with signal from wheel speed sensors (high signal to noise ration)
    - Internal components overheat causing degradation of the system and false readings.
    - A pervious value for vehicle speed is used to determine the vehicle speed.

SCM provides high assistance because the torque sensor feedback incorrectly indicates low torque. The incorrect feedback could be due to:

- SCM electronic failure (circuit internal failure).
- Steering wheel/Torque sensor failure.

- Shorted harness, open circuit.
- Delayed signal information provided by sensor, in the BUS.
- Algorithm minimum or maximum threshold for torque is incorrect and assistance is not provided.
- Sensors degrade over time (incorrect assembly, corrosion).
- Incorrect sensors calibration for vehicle architecture and geometry.
- Electromagnetic disturbance interferes with signal from sensor.
- An old value or parameter is used to calculate the input torque form the driver.

SCM provides high assistance because SCM incorrectly believes vehicle turning angle is too small. SCM believes turning angle is too small because:

- Vehicle turning angle feedback is incorrect. Causes include:
    - Failed turning angle sensor.
    - Shorted harness, open circuit.
    - Signal delay in the BUS.
    - Sensor degrades over time.
    - Electromagnetic disturbance interferes with signal from sensor.
    - A pervious value for vehicle turning angle is used to determine real angle.
- Vehicle turning angle threshold or calibration is incorrect. Causes include:
    - Incorrect factory calibration.
    - Changes or modifications to vehicle's steering system without recalibration
    - Incorrect sensor calibration for vehicle architecture and geometry.

Possible requirements from this scenario include:

UCA2-SC1-R1: Vehicle speed signal shall have higher hierarchy than other signals.

UCA2-SC1-R2: Calibration information for sensor and algorithm shall be available and traceable for the vehicle architecture.

<u>Control action provided but not followed</u>

Scenario2: The SCM provides a low assistance command but it is not effective because high assistance remains being delivered. Possible reasons for remain providing high assistance include:

- Actuation is delayed.
- SCM does not update change in speed fast enough. Using an old (low) speed value to provide assistance at high speed.

Possible requirements

UCA2-SC1-R1: Vehicle speed signal shall have higher hierarchy than other signals.

UCA5-S1-R3: Wheel speed signal shall be updated in TBD [ms] intervals to avoid signal delays.

UCA9-S1-R1: Steering wheel angle shall be received each TBD [ms] to avoid delay in signal.

UCA3-S1-R1: SCM shall have enough processing capability to process signals at the required speed.

UCA5: Low assistance is provided while traveling at low speeds (H-1,2,3,4)

Scenario 1: SCM provides low assistance because incorrectly believes that the vehicle speed is high. SCM might incorrectly believe that vehicle speed is high because:

- Vehicle speed feedback is incorrect. Causes include:
    - Failed vehicle speed sensor
    - Wheel speed is used to determine vehicle speed, but wheel speed doesn't match vehicle speed
        - Acceleration in uneven or slippery surface could cause wheel speed to differ from vehicle speed
        - Anti-lock brakes affect wheel speeds
        - System is too sensitive to differential speed measurements
        - Connection or assembly improperly made.
    - Electromagnetic disturbance interferes with signal from wheel speed sensors (high signal to noise ration)

    - Internal components overheat causing degradation of the system and false readings.
    - A pervious value for vehicle speed is used to determine the vehicle speed.
- Inadequate external speed feedback could explain incorrect SCM process model (sensor calibration, sensor failure, signal delays).
- Maximum torque threshold is set up too low in algorithm.
- Traction differential between wheels causing uneven speeds measurements that provide high-speed readings.
- SCM does not update change in speed fast enough. Using an old (high) speed value to provide assistance at low speed.

SCM provides low assistance because SCM incorrectly believes vehicle turning angle is too large. SCM believes turning angle is too large because:

- Vehicle turning angle feedback is incorrect. Causes include:
    - Failed turning angle sensor.
    - Shorted harness, open circuit.
    - Signal delay in the BUS.
    - Sensor degrades over time.
    - Electromagnetic disturbance interferes with signal from sensor.
    - A pervious value for vehicle turning angle is used to determine real angle.
- Vehicle turning angle threshold or calibration is incorrect. Causes include:
    - Incorrect factory calibration.
    - Changes or modifications to vehicle's steering system without recalibration

SCM provides low assistance because the torque sensor feedback incorrectly indicates high torque. The incorrect feedback could be due to:

- SCM electronic failure (circuit internal failure).
- Steering wheel/Torque sensor failure.
- Shorted harness, open circuit.
- Delayed signal information provided by sensor, in the BUS.
- Algorithm minimum or maximum threshold for torque is incorrect and assistance is not provided.
- Sensors degrade over time (incorrect assembly, corrosion).
- Incorrect sensors calibration for vehicle architecture and geometry.
- Electromagnetic disturbance interferes with signal from sensor.

- An old value or parameter is used to calculate the input torque form the driver.

Requirements:

UCA5-S1-R1: Torque sensor shall be calibrated to measure TBD [Nm] maximum required torque to steer the vehicle including geometrical characteristics of the vehicle.

UCA5-S1-R2: If equipped, additional information from traction control shall be used to determine if vehicle is operating in uneven traction conditions.

UCA5-S1-R3: Wheel speed signal shall be updated in TBD [ms] intervals to avoid signal delays.

UCA9-S1-R1: Steering wheel angle shall be received each TBD [ms] to avoid delay in signal.

UCA10-S2-R1: If assistance corresponding to the vehicle speed can't be provided, chime above TBD [dB] and discernable display that ensures the driver is aware of reduced assistance shall be provided.

Control action provided but not followed

Scenario2: SCM provides high assistance command correctly but assistance delivered to turn the wheels is low. Possible reasons for delivering low assistance include:

- High friction events and material deterioration.
    - Inadequate assembly control / geometrical tolerances.
    - Corrosion is formed and assistance is deteriorated.
    - Lack of lubrication.
- Mechanical failure of components (physical deformation).
- Steering lock-up
- Power supply is insufficient to meet the required power by the motor. (Low voltage event) In the case of low voltage, providing assistance would cause voltage drain, impeding the right functioning of other systems.

- External factors prevents from steering to turn the wheels (i.e., departing from a parking position and wheels are unable to turn because of an obstruction).

Possible requirements

UCA2-SC1-R1: Vehicle speed signal shall have higher hierarchy than other signals

UCA1-S4-R1: High friction conditions shall be able to be estimated by the algorithm.

UCA1-S2-R1: Ensure that enough power is available to provide assistance to the speed of the vehicle. Prioritization shall be enforced to ensure that vehicle control actuators receive the required power to operate the vehicle under safe conditions.

UCA16-S1-R3: If assistance is stopped being provided, audible chimes and warnings shall be made available to the driver. Driver shall be informed state of vehicle and instructed for correct actions to follow (i.e. allow system temperature to lower and take vehicle for service and inspection)

UCA1-S4-R4: System shall be guarded against foreign components and environmental conditions that could detriment performance

UCA8: Too much turning force provided when the driver executes a steering maneuver (over assist) (H-1,2,3,4,5)

Scenario1: SCM incorrectly believes that incremental assistance is required for low speed conditions (incorrect process model). The SCM might believe that incremental assistance is required because:
The SCM incorrectly believes that vehicle speed is lower than actual vehicle speed. The SCM could incorrectly believe there is low speed because:

- Vehicle speed feedback is incorrect. Causes include:
    - Failed vehicle speed sensor
    - Wheel speed is used to determine vehicle speed, but wheel speed doesn't match vehicle speed
        - Acceleration in uneven or slippery surface could cause wheel speed to differ from vehicle speed

        - Anti-lock brakes affect wheel speeds
        - System is too sensitive to differential speed measurements
        - Connection or assembly improperly made.
    - Electromagnetic disturbance interferes with signal from wheel speed sensors (high signal to noise ration)
    - Internal components overheat causing degradation of the system and false readings.
    - A pervious value for vehicle speed is used to determine the vehicle speed.
- Inadequate external speed feedback could explain incorrect SCM process model (sensor calibration, sensor failure, signal delays).
- Maximum torque threshold is set up too high in algorithm.
- SCM does not update change in speed fast enough. Using an old (high) speed value to provide assistance at low speed.

SCM provides high assistance because SCM incorrectly believes vehicle turning angle is too small. SCM believes turning angle is too small because:

- Vehicle turning angle feedback is incorrect. Causes include:
    - Failed turning angle sensor.
    - Shorted harness, open circuit.
    - Signal delay in the BUS.
    - Sensor degrades over time.
    - Electromagnetic disturbance interferes with signal from sensor.
    - A pervious value for vehicle turning angle is used to determine real angle.
- Vehicle turning angle threshold or calibration is incorrect. Causes include:
    - Incorrect factory calibration.
    - Changes or modifications to vehicle's steering system without recalibration

SCM provides high assistance because the torque sensor feedback incorrectly indicates low torque. The incorrect feedback could be due to:

- SCM electronic failure (circuit internal failure).
- Steering wheel/Torque sensor failure.
- Shorted harness, open circuit.
- Delayed signal information provided by sensor, in the BUS.
- Algorithm minimum or maximum threshold for torque is incorrect and assistance is not provided.

- Sensors degrade over time (incorrect assembly, corrosion).
- Incorrect sensors calibration for vehicle architecture and geometry.
- Electromagnetic disturbance interferes with signal from sensor.
- An old value or parameter is used to calculate the input torque form the driver.

Requirements applicable:

> SC-R6: Assistance shall be delivered following a ramp proportional to vehicle speed. Such ramp function shall be estimated according to the vehicle architecture and dynamic targets.

UCA9: Assistance is provided in a direction not commanded by the driver (H-1,2,3,4,5)

Scenario1: SCM provides assistance in the opposite direction because SCM incorrectly believes vehicle-turning angle is changing in opposite direction than real turning angle. SCM believes turning angle is incorrect because:

- Vehicle turning angle feedback is incorrect. Causes include:
  - Failed turning angle sensor.
  - Shorted harness, open circuit.
  - Signal delay in the BUS.
  - Steering angle sensor installed in inverted position.
  - Incorrect connection in motor (inverted polarity).
  - Electromagnetic disturbance interferes with signal from sensor.
  - A pervious value for vehicle turning angle is used to determine real angle.
- Vehicle turning angle threshold or calibration is incorrect. Causes include:
  - Algorithm measurement error. (Includes units conversion error)
  - Changes or modifications to vehicle's steering system without recalibration

Requirements:

> UCA1-S4-R4: System shall be guarded against foreign components and environmental conditions that could detriment performance.

UCA5-S1-R3: Wheel speed signal shall be updated in TBD [ms] intervals to avoid signal delays.

UCA9-S1-R1: Steering wheel angle shall be received each TBD [ms] to avoid delay in signal.

UCA1-S4-R2: Control plan and quality assurance plans shall be in place to ensure parts meet design tolerances and material specifications called in part prints, as well they are installed as designed.

Control action provided but not followed

Scenario3: SCM provides command of assistance accordingly to the steering angle but is not effective because assistance is provided in opposite direction. Reasons why assistance can be provided in opposite direction include:

- Inverted polarity in motor.
- Incorrect assembly of components.
- Delayed signal information provided by sensors.

Requirements

UCA9-S1-R1: Steering wheel angle shall be received each TBD [ms] to avoid delay in signal.

UCA9-S3-R2: Motor terminals assembly and sensor assembly shall have means ensuring correct assembly and provide traceability (Critical operation in production plan). Quality control shall ensure correct assembly before installing into the vehicle.

UCA5-S1-R3: Wheel speed signal shall be updated in TBD [ms] intervals to avoid signal delays.

UCA9-S1-R1: Steering wheel angle shall be received each TBD [ms] to avoid delay in signal.

UCA1-S4-R2: Control plan and quality assurance plans shall be in place to ensure parts meet design tolerances and material specifications called in part prints, as well they are installed as designed.

UCA10: Assistance is provided in a manner that discomforts the driver (H4, 5)

Scenario1: Assistance coming from the EPS discomforts the driver because vehicle conditions enable erratic feeling. Vehicle conditions may enable erratic feeling because:

- Assembly connections improperly made or do not retain torque/ torqued out of specification or alignment.
- Degraded mounts or isolators in subframe.
- Nibbling effect caused by incorrect mount of wheel and tire assembly.
- Gear reverse efficiency is too high.
- Suspension geometry or tuning does not correspond with the performance target of vehicle. Suspension might be too sensitive to road conditions, or response too harsh causing the steering system to react accordingly.
- Function provided but noises or vibrations are experienced by the driver, caused by:
    - Packaging interference
    - Assemblies having excessive friction or without proper lubrication
    - Isolation material not properly installed or selected (steering boot, steering gear mounts)
    - Improper geometry selected causing moan.
    - Improper alignment of components.
    - System natural frequency incompatible with geometry.
    - Incorrect assembly of components.
- Hardware failure. Includes:
    - Gear damaged
    - Wear in pinion or rack assembly
    - Ball joint degraded or making noise.
    - Belt assembly failure (rupture)
    - Electric Motor internal failure

Scenario2: SCM delivers an incorrect level of assistance providing low steering efforts (excessive dampening). The SCM provides excessive dampening because:

- Thresholds for dampening are out of specification or do not match vehicle characteristics.
- Algorithm is too sensitive to friction conditions and may detect high friction and over compensate.

Requirements applicable:

> UCA1-S4-R1: High friction conditions shall be able to be estimated by the algorithm. If high friction conditions are detected, driver shall be informed so vehicle can be taken for inspection.
>
> UCA1-S4-R2: Control plan and quality assurance plans shall be in place to ensure parts meet design tolerances and material specifications called in part prints, as well they are installed as designedUCA3: Assistance is provided too late when steering is required by the driver (H-1,2,3,4,5)

UCA3: Assistance is provided too late when driver executes a steering maneuver (H-1,2,3,4,5)

Scenario1: SCM does not provide assistance command because incorrectly believes that the driver has not initiated a steering. The SCM may not perceive that the driver has initiated a steering action because:
SCM provides high assistance because SCM incorrectly believes vehicle turning angle is too small. SCM believes turning angle is too small because:

- Vehicle turning angle feedback is incorrect. Causes include:
  - Failed turning angle sensor.
  - Shorted harness, open circuit.
  - Signal delay in the BUS.
  - Sensor degrades over time.
  - Electromagnetic disturbance interferes with signal from sensor.
  - A pervious value for vehicle turning angle is used to determine real angle.
  - Degradation of sensors due to high temperature condition.
- Vehicle turning angle threshold or calibration is incorrect. Causes include:
  - Incorrect factory calibration.

    - Changes or modifications to vehicle's steering system without recalibration
- SCM low processing efficiency.

Requirements

UCA3-S1-R1: SCM shall have enough processing capability to process signals at the required speed.

UCA9-S1-R1: Steering wheel angle shall be received each TBD [ms] to avoid delay in signal.

UCA9-S2-R2: Motor terminals assembly and sensor assembly shall have means ensuring correct assembly and provide traceability (Critical operation in production plan). Quality control shall ensure correct assembly before installing into the vehicle.

UCA3-S1-R4: System components shall meet manufacturing specifications and dimensional control such it can't prevent items to assemble or cause end play.

<u>Control action is provided but not followed</u>

Scenario2: SCM provides steering signal but not followed or followed too late when driver has initiated steering command. The SCM may provide late assistance command because:

- Short or grounded circuit in the power supply to the motor.
- Insufficient power in the system to provide desired assistance when is requested.
- Corrosion formed in the system causes erratic assistance delivery.
- Fault in motor, obstruction in the steering gear
- Excessive endplay with travel limiters.

Requirements that apply include:

UCA3-S1-R2: Algorithm shall be able to detect if there is a shorted ground in the circuit that provides power to SCM or steering motor.

UCA3-S1-R5: If a shorted ground or sensor failure is detected, the system shall enter a protection mode and provide TBD [Nm] auxiliary assistance. The algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware that the vehicle requires inspection.

UCA1-S4-R4: System shall be guarded against foreign components and environmental conditions that could detriment performance.

UCA3-S1-R4: System components shall meet manufacturing specifications and dimensional control such it can't prevent items to assemble or cause end play.

Scenario3: SCM resets due to a fault condition and provides assistance after the driver requests it.

- SCM detects a fault in the system (motor not providing enough assistance, faulty sensor)

Requirements

UCA3-S1-R6: SCM shall not reset while operating. Accepted reset conditions are key-on/key-off events.

UCA6: Assistance is provided intermittently when driver executes a steering maneuver (H-1,2,3,4,5)

Scenario1: SCM provides intermittent assistance command because vehicle speed is sent intermittently to the SCM. The speed signal may be sent intermittently to the SCM because:

- Measurement errors, corrosion in sensors, delayed signal, sensor faults.
- Voltage provided to the motor fluctuates (current available drained by other module, grounded circuit).
- High friction conditions.
- Electromagnetic disturbance provides a high signal to noise ratio.

Requirements that apply

UCA1-S1-R1: Provide additional feedback for determining vehicle speed and steering angle.

UCA1-S2-R1: Ensure that enough power is available to provide assistance to the speed of the vehicle. Prioritization shall be enforced to ensure that vehicle control actuators receive the required power to operate the vehicle under safe conditions.

UCA1-S4-R2: Control plan and quality assurance plans shall be in place to ensure parts meet design tolerances and material specifications called in part prints, as well they are installed as designed.

Scenario2: SCM intermittently provides assistance because it keeps rebooting while in operation due to a fault condition. The SCM may reboot while in operation because:

- SCM detects a fault in the system (motor not providing enough assistance, faulty sensor, signal out of frequency, etc.) and resets.
- Voltage provided to the motor fluctuates (current available drained by other module, grounded circuit), which causes the SCM to reset.

Requirements that apply:

UCA3-S1-R6: SCM shall not reset while operating. Accepted reset conditions are key-on/key-off events.

UCA1-S2-R1: Ensure that enough power is available to provide assistance to the speed of the vehicle. Prioritization shall be enforced to ensure that vehicle control actuators receive the required power to operate the vehicle under safe conditions.

<u>Control action provided but not followed:</u>

Scenario3: SCM sends assistance command but is not effective because it feels intermittent. Assistance may feel intermittent because:

- Current provided to the motor is intermittent. Could be due to:
    - Grounded circuit
    - Corrosion accumulates in motor terminals

- Hardware failure
    - Steering gear internal components premature wear
    - Travel limiters adjustment fail
- Foreign objects lodge in the system.
- Excessive free play in gear or linkage system.
- Joint torque specified incorrectly.
- Joints in the system are degraded over time.
- Improper geometry selected (gear ratio, rack travel distance).

Requirements:

UCA6-S1-R1: System shall guard components to withstand corrosion during the duty cycle of vehicle and comply with corporate corrosion requirements.

UCA3-S1-R2: Algorithm shall be able to detect if there is a shorted ground in the circuit that provides power to SCM or steering motor.

UCA6-S3-R1: System components shall withstand designed duty cycle defined by corporate requirements.

UCA1-S4-R2: Control plan and quality assurance plans shall be in place to ensure parts meet design tolerances and material specifications called in part prints, as well they are installed as designed.

UCA1-S4-R4: System shall be guarded against foreign components and environmental conditions that could detriment performance

UCA10-S3-R1: Joints that are deemed critical to ensure correct performance of the system shall be traceable. Correct joint analysis, materials and finishes shall be studied to ensure joint integrity under operational duty cycle of the vehicle

UCA3-S1-R5: If a shorted ground or sensor failure is detected, the system shall enter a protection mode and provide TBD [Nm] auxiliary assistance. The algorithm shall include

logic to display MIL and sonorous chimes to the driver so he can be made aware that the vehicle requires inspection.

UCA4: Assistance is interrupted while driver executes a steering maneuver (H-1,2,3,4)

Scenario1: The SCM stops sending assistance command while the driver is requiring aid because SCM incorrectly believes that assistance is no longer needed. SCM believes that assistance is no longer needed because:

- Sensor measurement incorrect or missing.
- SCM believes that the steering wheel angle has changed and returned to zero position. (Lost signal from sensor, intermittent fault, incorrect connection of sensor)
- Grounded circuit.
- Competing actuators in the system to be powered by vehicle (low power).
- Incorrect information sent from sensors (intermittent speed command)

Requirements

UCA1-S1-R1: Provide additional feedback for determining vehicle speed and steering angle.

UCA3-S1-R5: If a shorted ground or sensor failure is detected, the system shall enter a protection mode and provide TBD [Nm] auxiliary assistance. The algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware t aware that the vehicle requires inspection.

UCA1-S1-R4: Algorithm shall include logic to detect if signals from sensors are not being sent with the periodic timing the system requires.

UCA1-S2-R5: Auxiliary power in vehicle shall be capable to maintain road lights and minimum of TBD [V] to provide assistance in the event of engine stall and vehicle speed is higher than TBD [kph].

Control action is provided but not followed

Scenario2: SCM provides steering command but not followed because something prevents the motor to provide assistance. Reasons that prevent the motor to provide assistance include:

- Motor does not receive the current required to provide assistance due to a shorted circuit in the system.
- Electrical ground not connected correctly.
- Communication bus error.
- Incorrect connection in motor.
- External elements lodge in the system (debris) or prevent the system to operate.

Requirements

UCA1-S4-R4: System shall be guarded against foreign components and environmental conditions that could detriment performance

UCA3-S1-R2: Algorithm shall be able to detect if there is a shorted ground in the circuit that provides power to SCM or steering motor.

UCA1-S2-R1: Ensure that enough power is available to provide assistance to the speed of the vehicle. Prioritization shall be enforced to ensure that vehicle control actuators receive the required power to operate the vehicle under safe conditions.

UCA9-S2-R2: Motor terminals assembly and sensor assembly shall have means ensuring correct assembly and provide traceability (Critical operation in production control). Quality control shall ensure correct assembly before installing into the vehicle.

UCA7: Assistance continues being provided when safe angle has been reached (H-1,2,3,4,5)

Scenario1: SCM continues providing steering command after required angle has been reached because SCM incorrectly believes that assistance is still being required. SCM believes that assistance is still required because:
SCM incorrectly believes vehicle turning angle is too small. SCM believes turning angle is too small because:

- Vehicle turning angle feedback is incorrect. Causes include:
  - Failed turning angle sensor.

- Shorted harness, open circuit.
- Signal delay in the BUS.
- Sensor degrades over time.
- Electromagnetic disturbance interferes with signal from sensor.
- A pervious value for vehicle turning angle is used to determine real angle.

- Vehicle turning angle threshold or calibration is incorrect. Causes include:
    - Incorrect factory calibration.
    - Changes or modifications to vehicle's steering system without recalibration

Requirements:

UCA1-S1-R2: System level validation shall ensure that electric sensors, actuators and modules does not irradiate electromagnetic noise that could cause improver behavior of modules, actuators and sensors of the system and the vehicle.

UCA1-S1-R3: System level validation shall ensure that electric sensors, actuators and modules signal to noise ratio remains functional during vehicle operation and through common (environmental) electro-magnetic noises.

UCA1-S4-R5: System shall provide service required light and proper chimes when detects failure of actuators such as motor, sensors or SCM. System shall store fault codes for inspection and service.

UCA5-S1-R3: Wheel speed signal shall be updated in TBD [ms] intervals to avoid signal delays.

UCA9-S1-R1: Steering wheel angle shall be received each TBD [ms] to avoid delay in signal.

UCA3-S1-R1: SCM shall have enough processing capability to process signals at the required speed.

<u>Control action provided but not followed</u>

Scenario2: SCM stops providing steering command but something prevents self-centering of the system. This could be caused by:

- Steering locks-up due to lodging of external elements.
- Steering is not able to return from corner event to neutral position due to degraded condition of steering system:
    - Suspension geometry tampered.
    - High friction condition due to degraded system components, high corrosion.
- High torque being demanded during steering, causing the system to overheat and desist providing assistance.
- Travel limiters failure.

Requirements:

UCA1-S4-R1: High friction conditions shall be able to be estimated by the algorithm.

UCA1-S4-R2: Control plan and quality assurance plans shall be in place to ensure parts meet design tolerances and material specifications called in part prints, as well they are installed as designed.

UCA1-S4-R4: System shall be guarded against foreign components and environmental conditions that could detriment performance.

UCA6-S1-R1: System shall guard components to withstand corrosion during the duty cycle of vehicle and comply with corporate corrosion requirements.

UCA6-S3-R1: System components shall withstand designed duty cycle defined by corporate requirements.

UCA3-S1-R4: System components shall meet manufacturing specifications and dimensional control such it can't prevent items to assemble or cause end play.

Driver

This section analyzes the role of the driver in ensuring as safe operation of the vehicle as a main element of control of the system. The section will analyze commands not given or missing as well as commands not followed. Commands not given are shown as part of the control structure loop highlighted in Figure 3.

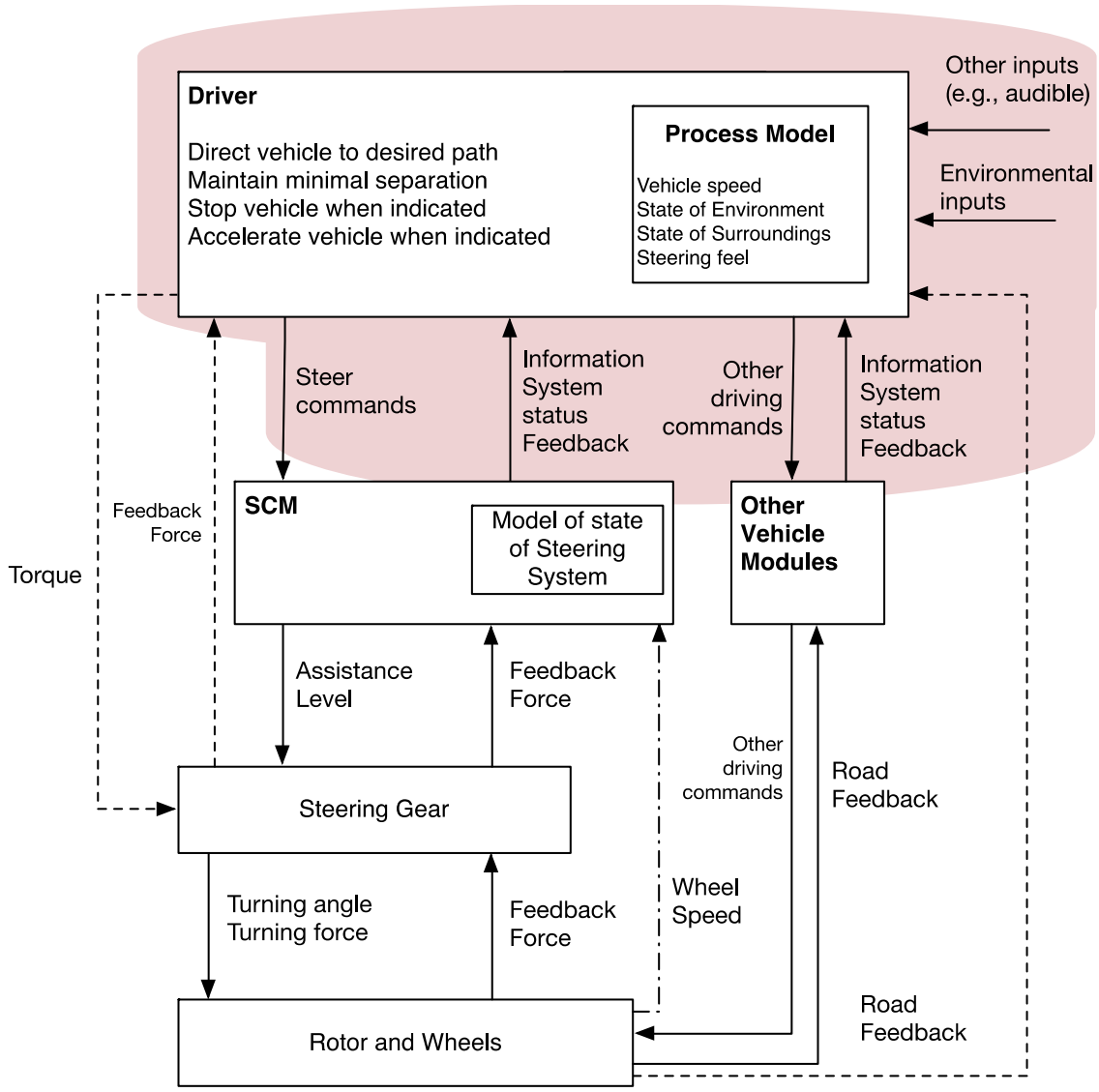

Figure 14 - Driver section

When analyzing commands given but not followed, the causes of leading to those scenarios will be analyzed by the loop shown in Figure 4.

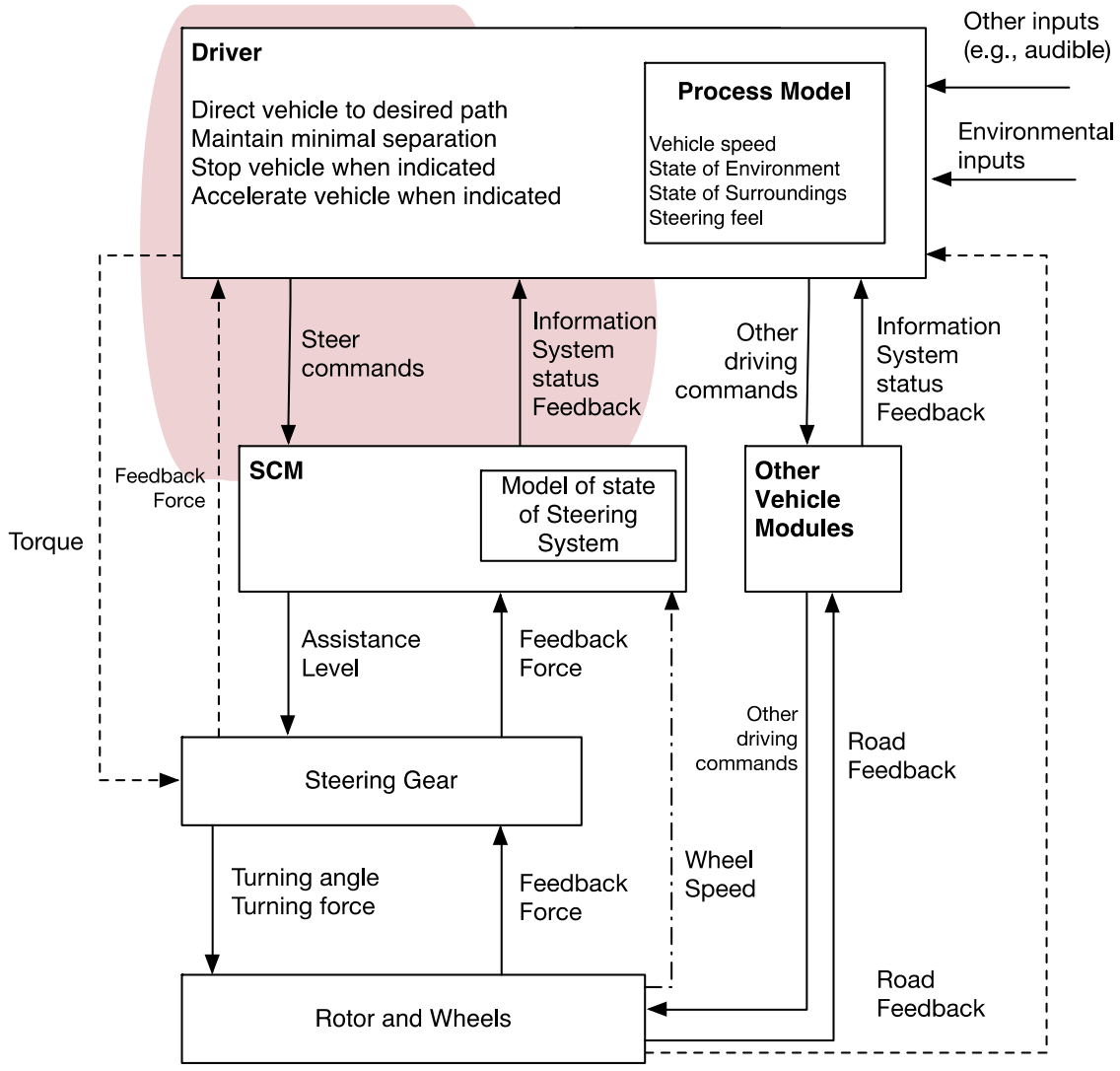

Figure 15 - Control structure command not followed

UCA11: Driver does not provide steering command when there are people or objects in his/her path (H-1,2,3,4,5)

Scenario1: Driver incorrectly believes that there is no need of changing path (process model flaw) because something prevents driver awareness. Reasons that the driver process model can be flawed include:

- Harsh environmental conditions that impede the driver to have a clear visibility of road and environment.
- Vehicle is not aligned properly, causing to follow a different direction than provided by the steering wheel. Vehicle alignment also could have been degraded over time.

Requirements that can be defined from this scenario include:

> UCA10-S1-R1: Design shall be able to hold alignment (Toe, Camber, Caster) under vehicle's duty cycle.
>
> UCA10-S2-R1: If assistance corresponding to the vehicle speed can't be provided, chime above TBD [dB] and discernable display that ensures the driver is aware of reduced assistance shall be provided.

Scenario2: Driver believes that certain amount of assistance will be provided but is unable to provide correct steering angle due to lack of assistance. Assistance may not match Driver's believed assistance because:

- Driver is not made aware that assistance won't be provided (UCA1)
- Notification has no great impact on driver to provide awareness of reduced assistance.
- Driver gets distracted while driving.
- Engine shuts off, making power steering unavailable (lack of power)

Requirements applicable to this scenario include:

> UCA10-S2-R1: If assistance corresponding to the vehicle speed can't be provided, chime above TBD [dB] and discernable display that ensures the driver is aware of reduced assistance shall be provided.
>
> UCA1-S4-R5: System shall provide service required light and proper chimes when detects failure of actuators such as motor, sensors or SCM. System shall store fault codes for inspection and service.
>
> UCA1-S2-R5: Auxiliary power in vehicle shall be capable to maintain road lights and minimum of TBD [V] to provide assistance in the event of engine stall and vehicle speed is higher than TBD [kph].

<u>Control action provided but not followed</u>

Scenario3: Driver provides steering command but vehicle does not turn because the vehicle is unable to provide assistance. Possible causes include:

- Joints in the system are degraded over time. Possible joint degradation between the input shaft and the steering column, or tie rods to knuckle.
- Alignment degrades over time.
- Steering locks-up.
- Foreign objects lodge in the system.
- Assistance is not provided. See SCM not providing assistance for detail.
- Pinion gears failure, rack gear failure, bearing failure.

Requirements that apply:

> UCA10-S3-R1: Joints that are deemed critical to ensure correct performance of the system shall be traceable. Correct joint analysis, materials and finishes shall be studied to ensure joint integrity under operational spectrum of the vehicle.
>
> UCA1-S4-R3: Alignment (Toe) shall be maintained during all types of operation cycles of the vehicle.
>
> UCA1-S4-R4: System shall be guarded against foreign components and environmental conditions that could detriment performance.
>
> UCA6-S3-R1: System components shall withstand designed duty cycle defined by corporate requirements.

UCA12: Driver provides steering command towards a static or moving object (H-1,2,3,4)

Scenario1: Vehicle is directed incorrectly because vehicle does not allow for self-center when driver departs from cornering maneuver. Possible causes include:

- Degraded connections in the system prevent the vehicle to recover from turn.
- Excessive friction impedes the system to return to zero position.
- Foreign material lodges in the system and prevents the gear to return to zero position.

Requirements that apply

UCA10-S3-R1: Joints that are deemed critical to ensure correct performance of the system shall be traceable. Correct joint analysis, materials and finishes shall be studied to ensure joint integrity under operational duty cycle of the vehicle.

UCA1-S4-R1: High friction conditions shall be able to be estimated by the algorithm. And be informed to the driver for verification of state of system components.

UCA1-S4-R4: System shall be guarded against foreign components and environmental conditions that could detriment performance.

Scenario2: Vehicle is directed to an unwanted path because wheels pull to one side upon heavy acceleration. Wheels may pull to an unwanted path during heavy acceleration because:

- Heavy acceleration (intended or unintended) from the engine while losing grip to the steering wheel.
- Torque steer is higher than anticipated by the driver (mental model) that in turn can't direct the vehicle into a desired path.
- SCM receives incorrect high torque information from the engine that reduces assistance and may cause vehicle difficult to maneuver (See UCA2).

Requirements that apply

UCA11-S2-R1: SCM shall communicate with Engine Control Module to identify situations that could lead to high torque steer.

UCA11-S2-R2: Torque steer compensation shall not be enabled when there is a reported engine fail.

<u>Control action provided but not followed</u>

Scenario3: Driver provides steering command away from objects but vehicle does not follow the commanded direction. Possible causes:

- Joints in the system are degraded over time. Possible joint degradation between the input shaft and the steering column, or tie rods to knuckle.

- Alignment degrades over time
- Steering locks-up
- Foreign objects lodge in the system.
- Assistance is not provided. See SCM not providing assistance for detail.
- Pinion gear failure, rack gear failure, bearing failure.

Requirements that apply

UCA10-S3-R1: Joints that are deemed critical to ensure correct performance of the system shall be traceable. Correct joint analysis, materials and finishes shall be studied to ensure joint integrity under operational spectrum of the vehicle.

UCA1-S4-R3: Alignment (Toe) shall be maintained during all types of operation cycles of the vehicle.

UCA1-S4-R4: System shall be guarded against foreign components and environmental conditions that could detriment performance.

UCA6-S3-R1: System components shall withstand designed duty cycle defined by corporate requirements.

UCA14: Driver provides abrupt steering command while traveling at degraded road conditions (H-1,2,3,4,5)

Scenario1: Vehicle cannot be controlled because driver demands high assistance while traveling in degraded road conditions. Driver may require high assistance in degraded road conditions because:

- Driver is not aware that high assistance is demanded from the system, or expects that the system shall provide such assistance under harsh situations (mental model).
- System is operated under degraded state (e.g. high internal temperature) without the driver being notified.

Requirements that apply:

UCA14-S1-R1: Means of acquiring system temperature shall be obtained to avoid using the system in degraded conditions.

UCA4-S3-R1: If high system temperature is detected, the system shall provide minimum TBD [Nm] limp home mode assistance to ensure the driver can take the vehicle for inspection. Algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware that the vehicle is in a reduced performance mode.

UCA13: Driver leaves safe path before steering maneuver is being completed (H-1,2,3,4,5)

Scenario1: Driver might expect low assistance (mental model) and system provides high assistance level to perform a cornering event. The system may provide different assistance level because:

- Driver is unaware that assistance varies with speed.
- While performing a heavy acceleration, the driver steers the vehicle. He/She would be expecting low assistance (mental model) but the vehicle turns more than the driver commands through the steering wheel. (Torque steer)
- See SCM UCA2.

Requirements

UCA11-S2-R1: SCM shall communicate with Engine Control Module to identify situations that could lead to high torque steer.

UCA11-S2-R2: Torque steer compensation shall not be enabled when there is a reported engine fail.

Scenario2: Driver performs a steering maneuver in a desired direction but is unable to maintain a desired path because assistance perceived is too low. The driver may experience that the assistance is too low because:

- Assistance is not provided (loss of assistance) and the driver is not informed or neglects a low sound warning (See UCA1)
- Torque steer event opposite to the driver commanded direction.

- See SCM UCA5.

Requirements

> UCA10-S2-R1: If assistance corresponding to the vehicle speed can't be provided, chime above TBD [dB] and discernable display that ensures the driver is aware of reduced assistance shall be provided.

Scenario3: Driver provides steering command in the incorrect direction to follow desired path. May be due to:

- Driver gets distracted while driving.
- Driver not being familiar with steering assistance and/or responsiveness of system.

Scenario4: Driver stops providing a steering command before a safe path has been reached while performing a turning command.

- The corner is not designed properly.
- The driver gets distracted.
- Driver not familiar with steering assistance. The driver could think that high assistance will be provided to maintain turning curve and relaxes force applied, allowing the vehicle dynamics to recover from turn (zero position).

Scenario5: Driver counter-steers fast or too aggressive while performing parking lot maneuvers and finds an obstruction or hard to provide direction. Possible causes:

- Actuation is delayed.
- Signal delay or not received.
- Steering lock-up.
- High friction in the system prevents the motor to provide the assistance commanded by the SCM, making difficult for the driver to reach desired path.

Requirements

> UCA3-S1-R1: SCM shall have enough processing capability to process signals at the required speed.

UCA1-S4-R1: High friction conditions shall be able to be estimated by the algorithm. And be informed to the driver for verification of state of system components.

UCA5-S1-R3: Wheel speed signal shall be updated in TBD [ms] intervals to avoid signal delays.

UCA9-S1-R1: Steering wheel angle shall be received each TBD [ms] to avoid delay in signal.

Control action provided but not followed

Scenario6: Driver provides correct steering command but vehicle follows an unsafe path. The vehicle may follow an unsafe path because:

- Possible joint degradation between the input shaft and the steering column, or tie rods to knuckle.
- Alignment degrades over time
- Steering locks-up
- Foreign objects lodge in the system.
- Assistance is not provided. See SCM not providing assistance for detail.
- Pinion gears failure, rack gear failure, bearing failure.

Requirements

UCA10-S3-R1: Joints that are deemed critical to ensure correct performance of the system shall be traceable. Correct joint analysis, materials and finishes shall be studied to ensure joint integrity under operational spectrum of the vehicle.

UCA1-S4-R3: Alignment (Toe) shall be maintained during all types of operation cycles of the vehicle.

UCA1-S4-R4: System shall be guarded against foreign components and environmental conditions that could detriment performance.

UCA6-S3-R1: System components shall withstand designed duty cycle defined by corporate requirements

Scenario7: Assistance stops being provided while driver continues executing a steering maneuver.

- Conflicting signals or missing.
- Overheat in the system and enters a protection mode.
- System resets while turning or in a curve.
- System enters a high friction condition while turning, making harder to provide assistance.
- Hardware failure while turning (disconnect due to joint torque relaxation).

Requirements affected

UCA4-S3-R1: If high system temperature is detected, the system shall provide minimum TBD [Nm] limp home mode assistance to ensure the driver can take the vehicle for inspection. Algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware that the vehicle is in a reduced performance mode.

UCA14-S1-R1: Means of acquiring system temperature shall be obtained to avoid using the system in degraded conditions.

UCA3-S1-R6: SCM shall not reset while operating. Accepted reset conditions are key-on/key-off events.

UCA1-S4-R1: High friction conditions shall be able to be estimated by the algorithm. And be informed to the driver for verification of state of system components.

UCA6-S3-R1: System components shall withstand designed duty cycle defined by corporate requirements.

Scenario8: Assistance continues being when driver finishes executing a steering maneuver.

- System does not update signals.
- High torque provided due to improper calibration of sensors or input data about suspension geometry.

- EMC noise affects signal input.
- Rotor and wheels assembly lock-up in one direction.
- Steering gear system locks-up or get stuck.
- SCM continues providing assistance. See UCA7

Requirements affected

UCA5-S1-R3: Wheel speed signal shall be updated in TBD [ms] intervals to avoid signal delays.

UCA3-S1-R6: SCM shall not reset while operating. Accepted reset conditions are key-on/key-off events.

UCA1-S1-R2: System level validation shall ensure that electric sensors, actuators and modules do not irradiate electromagnetic noise that could cause improver behavior of modules, actuators and sensors of the system and the vehicle.

UCA1-S1-R3: System level validation shall ensure that electric sensors, actuators and modules signal to noise ratio remains functional during vehicle operation and through common (environmental) electro-magnetic noises.

Second iteration of STPA

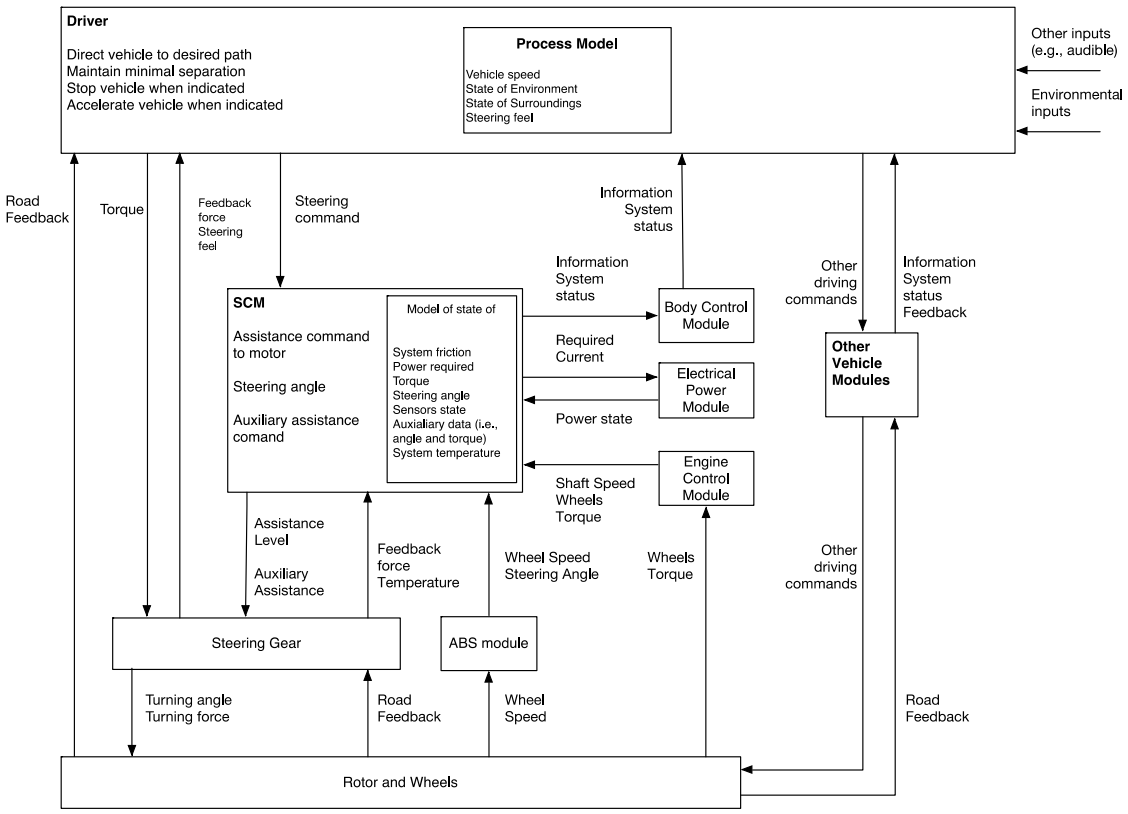

Figure 16 - Control structure second iteration

STEP 1: Identifying Unsafe Control Actions

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing or Order	Stopped Too Soon/ Applied Too Long
SCM provides assistance command to the motor	UCA1: Assistance is not provided when driver executes a steering maneuver (H-1,2,3,4)	UCA2: High assistance is provided while traveling at high speeds (H-1,2,3,4,5)	UCA3: Assistance is provided too late when driver executes a steering maneuver (H-1,2,3,4,5)	UCA4: Assistance is interrupted while driver executes a steering maneuver (H-1,2,3,4)
		UCA5: Low assistance is provided while traveling at low speeds (H-1,2,3,4)	UCA6: Assistance is provided intermittently when driver executes a steering maneuver (H-1,2,3,4,5)	UCA7: Assistance continues being provided when safe angle has been reached (H-1,2,3,4,5)
		UCA8: Too much turning force provided when the driver executes a steering maneuver (over assist) (H-1,2,3,4,5)		UCA16: Assistance continues being provided when system has reached an internal temperature above TBD [C] (H4,5)
		UCA9: Assistance is provided in opposite direction than commanded by driver (H-1,2,3,4,5)		UCA17: Assistance continues being provided when voltage available is below TBD [V] (H-2,3,5,6)
		UCA10: Assistance is provided in a manner that discomforts the driver (H4, 5)		

Driver provides commands steering (force and direction) to steering wheel	UCA11: Driver does not provide steering command when there are people or objects in his/her path (H-1,2,3,4,5)	UCA12: Driver provides steering command towards a static or moving object (H-1,2,3,4)	UCA15: Driver performs a steering maneuver before or after safe path direction (H-1,2,3,4,5)*	UCA13: Driver leaves safe path before steering maneuver is being completed (H-1,2,3,4,5)
		UCA14: Driver provides abrupt steering command while traveling at degraded road conditions (H-1,2,3,4,5)		
Command auxiliary assistance mode when fault is detected or high temperature is detected	UCA18: SCM does not command limited assistance when fault is detected or there is a high temperature event (H-4,5)	UCA19: SCM sends auxiliary assistance command when there is no fault or high temperature event (H-4)	UCA20: SCM commands auxiliary assistance but driver is not made aware (H-1,2,3,4)	UCA21: Stops providing auxiliary assistance command when is safe to provide it (H-1,2,3,4,5)
			UCA22: SCM intermittently commands auxiliary assistance (H-1,2,3,4,5)	

New UCA's identified based on required feedback, sensors and interactions:

UCA16: Assistance continues being provided when system has reached an internal temperature above TBD [C] (H4,5)

Scenario1: SCM continues providing assistance command when temperature threshold has been reached because incorrectly believes that temperature is below the design threshold. SCM may believe that the system temperature is below the design threshold because:

- Temperature sensor failure or incorrect feedback (measurement error) or delay, degradation such as corrosion in terminals.
- Incorrect connection of temperature sensor or shorted connection.
- Incorrect temperature threshold selected, or equated incorrectly in algorithm.
- Power variance affects sensitivity of sensor.
- Electromagnetic disturbance interferes with temperature signal.
- Driver keeps requesting high assistance (high traffic condition, stop-start events and changing lanes abruptly)

Requirements

UCA4-S3-R1: If high system temperature is detected, the system shall provide minimum TBD [Nm] auxiliary assistance to ensure the driver can take the vehicle for inspection. Algorithm shall include logic to display MIL and sonorous chimes to the driver so he or she can be made aware that the vehicle is in a reduced performance mode.

UCA10-S2-R1: If assistance corresponding to the vehicle speed can't be provided, chime above TBD [dB] and discernable display that ensures the driver is aware of reduced assistance shall be provided.

UCA16-S1-R1: Once the system has entered to an auxiliary assistance mode, it can only be taken out by a key cycle event or technician prior diagnose.

UCA16-S1-R1: Auxiliary assistance of TBD [Nm] shall be commanded when system detects internal temperature above TBD1 [C] and below TBD2 [C]. If system reaches or surpasses TBD2 [C] assistance shall stop being provided to avoid further degradation of system.

UCA16-S1-R3: If assistance is stopped being provided, audible chimes and warnings shall be made available to the driver. Driver shall be informed state of vehicle and instructed for correct actions to follow (i.e. allow system temperature to lower and take vehicle for service and inspection)

<u>Control action provided but not followed</u>

Scenario2: The driver receives high assistance when high system temperature has been reached because SCM commands auxiliary assistance that is set too high. SCM may command a high auxiliary assistance because:

- Incorrect thresholds selected for auxiliary assistance.
- Motor failure, only provides one type of assistance (high).

Requirements

UCA16-S1-R1: Auxiliary assistance of TBD [Nm] shall start when system detects internal temperature above TBD1 [C] and below TBD2 [C]. If system reaches or surpasses TBD2 [C], assistance shall stop being provided.

UCA6-S3-R1: System components shall withstand designed duty cycle defined by corporate requirements.

UCA9-S2-R2: Motor terminals assembly and sensor assembly shall have means ensuring correct assembly and provide traceability (Critical operation in production control). Quality control shall ensure correct assembly before installing into the vehicle.

UCA3-S1-R4: System components shall meet manufacturing specifications and dimensional control such it can't prevent items to assemble or cause end play.

UCA17: Assistance is provided when voltage available is below TBD [V] threshold (H-2,3,5)

Scenario1: The driver does not receive the required assistance for the vehicle speed because the SCM incorrectly believes that the correct level of assistance is provided for vehicle speed. The SCM may believe (incorrectly) that the correct assistance is being provided because:

- System does not detect voltage is low or does not receive information that there is low voltage in the system.
- Low voltage in the system that is not monitored by the SCM.
- There is no prioritization for critical operation components if there is low voltage available.
- Driver continues to request high output from the vehicle contributing to vehicle's low voltage state.

- Engine stalls while driving (unrelated to EPS) and power is insufficient to command the vehicle.

Requirements

UCA1-S2-R1: Ensure that enough power is available to provide assistance to the speed of the vehicle. Prioritization shall be enforced to ensure that vehicle control actuators receive the required power to operate the vehicle under safe conditions.

UCA17-S1-R1: System shall measure voltage available in the system to ensure assistance requested is capable to be provided. When there is an event of low voltage, driver shall be informed.

Control action provided but not followed

Scenario2: SCM provides assistance command but it is not effective because there is low voltage in the system. The system voltage may be low because:

- Power is not being supplied because the system is not capable (Engine stall, harness unplugged)
- System measures correctly power available but is unable to power the motor and driver is not communicated.
- Driver is not informed that vehicle might be operated in a degraded state and continues to request high output from the vehicle contributing to vehicle's low voltage state.

Requirements

UCA1-S2-R1: Ensure that enough power is available to provide assistance to the speed of the vehicle. Prioritization shall be enforced to ensure that vehicle control actuators receive the required power to operate the vehicle under safe conditions.

UCA17-S1-R1: System shall measure voltage available in the system to ensure assistance requested is capable to be provided. When there is an event of low voltage, driver shall be informed.

One mitigation strategy that could be implemented in the system is to command auxiliary assistance mode when fault is detected (low voltage, conflicting signals for speed, angle and torque, high temperature, high friction). A typical auxiliary assistance would be such that it can assist the driver during low speeds maneuvers when more assistance is required and also could avoid over assist in high-speed circumstances such that it could disturb the driver's belief (mental model) of the expected assistance. Such assistance should be in line of the vehicle architecture and derived from the ergonometric perspective from the demographic pool of drivers. For analysis sake, an arbitrary 75 kph assistance correspondent the vehicle traveling in a highway road type of situation would be selected.

With this new control action, Iteration 1 UCA's are revisited and subsequently analyze causes that could lead to the system hazards.

UCA18: SCM does not command auxiliary assistance when fault is detected or there is a high temperature event (H4, H5)

Scenario1: SCM does not command auxiliary assistance because SCM believes there is high friction but the speed is low. If high friction is detected at low speed SCM should not command auxiliary assistance because the amount of assistance provided at low speed should be higher than the auxiliary assistance. Possible causes include:

- False detection of high temperature at high speed. Possible contributors:
    - Temperature sensor incorrect measurements.
    - Incorrect thresholds selected for high temperature.
- Torque sensor failure, measurement error or false signal (contributor to miscompute high friction)
- Steering wheel angle sensor failure. If Steering wheel angle can't be estimated any other way than with its sensor, it might be hazardous providing assistance since it could lead to scenarios analyzed in UCA7.
- Temperature sensor incorrect measurement, indicating high friction in system.
- Wheel speed sensor failure or speed can't be estimated. It might be hazardous for the SCM to provide assistance when speed can't be estimated.
- Shorted harness, open circuit.
- Algorithm threshold for high friction is incorrectly specified
- Detection algorithm is not sensible enough to identify high friction conditions.

- Electromagnetic disturbance interferes with signals from sensors.
- Old values are used to calculate friction (e.g. The SCM would believe that low assistance is required when using a high value for speed previously stored, but if the actual state of vehicle speed is low, the input torque from the driver will be higher. The SCM would believe that higher torque input is required for certain level of assistance, hence interpreting that there is high friction in the system).

Scenario2: SCM does not command auxiliary assistance because SCM incorrectly believes there is high temperature and high speed. If high temperature is detected at high speed, SCM should not command auxiliary assistance because that would deliver more assistance, contributing to increase in temperature. Possible contributors

- Torque sensor failure, measurement error or false signal (contributor to miscompute high friction)
- Temperature sensor calibration set incorrectly.
- SCM reads the correct temperature but incorrectly thinks that the vehicle speed is high. SCM believes vehicle speed is too high because:
    - Vehicle speed feedback is incorrect. Causes include:
        - Failed vehicle speed sensor
        - Wheel speed is used to determine vehicle speed, but wheel speed doesn't match vehicle speed
        - Acceleration in uneven or slippery surface could cause wheel speed to differ from vehicle speed
        - Anti-lock brakes affect wheel speeds
        - System is too sensitive to differential speed measurements
        - Connection or assembly improperly made.
    - Electromagnetic disturbance interferes with signal from wheel speed sensors (high signal to noise ration)
    - Internal components overheat causing degradation of the system and false readings.
    - A pervious value for vehicle speed is used to determine the vehicle speed

Thomas [13] proposed a new method for identifying unsafe control actions. Thomas observed that the UCA's derived from STPA often exhibit a common structure. Such structure may be formalized in four-part construction: A source, a type, a control action, and a context.

The *source* and *control action* are found in the relevant system control structure developed as part of the system engineering foundation. The *type* refers as if the control action is provided or not provided, following four ways a control action may be unsafe (provided, not provided, out of order or timing and applied too soon or too long). A context could be defined by a set of process model variables (PMV) – variables that describe the system state [13].

An example of PMV is exemplified using high friction in Figure 7.

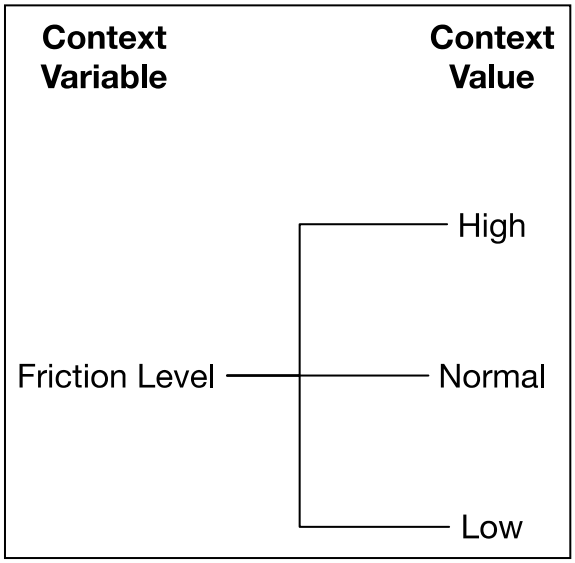

Figure 17 - PMV of Auxiliary Assistance

Context variables	**State**
Friction Level High: Above TBD threshold Normal: Within TBD range Low: Below TBD threshold	[High, Normal, Low]
Temperature High: Above TBD threshold Normal: Within TBD range Low: Below TBD threshold	[High, Normal, Low]
Vehicle Speed High: TBD range for high speed Low: TBD range for low speed	[High, Low]

Table 21 - Context variables for auxiliary assistance

Once PMV is formalized, a context table may be constructed to identify unsafe control actions and generate applicable requirements. The requirements specify when a control action must be commanded and when it must not be commanded to ensure safety and prevent the system hazards.. Following Thomas proposal, functional requirements for Auxiliary Assistance are provided in Table 10**.**

SC: Source controller that can issue the control action of the system
T: is the type of control action (Provided or not provided)
CA: Control Action (i.e.) command that is output by the controller.
Co: Context in which the control action is or is not provided

For Auxiliary Assistance command:
SC= SCM
T= Provided, left blank are specified as don't care or wildcards.
CA= Command Auxiliary assistance
Co= Friction condition, temperature condition, speed.

Provide auxiliary assistance command

		S-F	S-F
Friction =	High	T	
	Normal		
	Low		
Temperature =	High		T
	Normal	T	
Vehicle Speed =	High	T	
	Low		T

Table 22 - SpecTRM-RL of Auxiliary Assistance

STPA Requirements for auxiliary assistance

Following the method for determining when auxiliary assistance that was described in the section before, STPA analysis continues to determine the applicable requirements.

Requirements

UCA16-S1-R1: Auxiliary assistance of TBD [Nm] shall start when system detects internal temperature above TBD1 [C] and below TBD2 [C]. If system reaches or surpasses TBD2 [C], assistance shall stop being provided.

UCA4-S3-R1: If high system temperature is detected, the system shall provide minimum TBD [Nm] auxiliary assistance to ensure the driver can take the vehicle for inspection. Algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware that the vehicle is in a reduced performance mode.

UCA3-S1-R3: If discrepancy is constant among correlated signals, the algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware that the vehicle requires inspection. When discrepancy occurs, the system shall provide minimum TBD [Nm] auxiliary assistance to ensure the driver can take the vehicle for inspection.

Control action is provided but not followed

Scenario2: SCM provides limited assistance command when fault is detected but is not effective because high assistance is provided. High assistance may be provided because:

- Signal interference to command motor (Electromagnetic noise)
- Motor incorrect thresholds.
- Value for auxiliary assistance provided too high.

Requirements affecting this scenario:

UCA4-S3-R1: If high system temperature is detected, the system shall provide minimum TBD [Nm] auxiliary assistance to ensure the driver can take the vehicle for inspection. Algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware that the vehicle is in a reduced performance mode.

UCA1-S1-R2: System level validation shall ensure that electric sensors, actuators and modules does not irradiate electromagnetic noise that could cause improver behavior of modules, actuators and sensors of the system and the vehicle.

UCA1-S1-R3: System level validation shall ensure that electric sensors, actuators and modules signal to noise ratio remains functional during vehicle operation and through common (environmental) electro-magnetic noises.

UCA19: SCM sends auxiliary assistance command when there is no fault or high temperature event (H5)

Scenario1: SCM sends auxiliary assistance because it incorrectly believes that conditions are met to provide auxiliary assistance. Possible causes include:

- High friction event is detected at low speed. If auxiliary assistance is provided at low speed (75 kph in this case), the assistance received would be less, contributing to the difficulty of steering. The algorithm might not be detecting high friction condition and there might be a high temperature event. Causes for not detecting a high friction condition include:
    - Friction coefficients changes with the weather (low temperature may cause incorrect readings and change the friction coefficient of the road)
    - The driver provides high inputs too fast (changing lanes quickly, high steering inputs when it is not required, keep providing force beyond rack stop)
    - Vehicle characteristic changes (GVW, wrong tires/wheels)
    - Signals variability too high.
    - Algorithm threshold for high friction is incorrectly specified
    - Detection algorithm is not sensible enough to identify high friction conditions.
- Not detecting high temperature at high speed. If high temperature is detected at high speed, SCM should not command auxiliary assistance because assistance from the motor would be higher, contributing to increase in temperature. Possible contributors:
    - Temperature sensor failure
    - Algorithm logic sends auxiliary assistance when vehicle speed can’t be determined. Incorrect speed signals could lead to scenarios described in UCA2, UCA5 and UCA 8.

- Steering wheel angle sensor failure. If Steering wheel angle can't be estimated any other way than with its sensor, it might be hazardous providing auxiliary assistance since it could lead to scenarios analyzed in UCA7.

Control action provided but not followed

Scenario2: SCM provides auxiliary assistance but is ineffective because something prevents assistance to be delivered. Possible causes include:

- Motor failure, degraded terminals, steering lock-up, friction is too high.
- Foreign objects lodged in the system.

Requirements applicable:

UCA19-S1-R1: When SCM has commanded auxiliary mode, vehicle speed controllers (if equipped) shall be prevented to enable.

UCA19-S2-R1: Assistance or Auxiliary Assistance cannot be provided in the event of not having confidence of detecting speed.

UCA19-S2-R2: Assistance or Auxiliary Assistance cannot be provided in the event not having certainty of steering wheel angle signal.

UCA3-S1-R3: If discrepancy is constant among correlated signals, the algorithm shall include logic to display MIL and audible chimes to the driver so he can be made aware that the vehicle requires inspection. When discrepancy occurs, the system shall provide minimum TBD [Nm] auxiliary assistance to ensure the driver can take the vehicle for inspection.

UCA16-S1-R3: If assistance is stopped being provided, audible chimes and warnings shall be made available to the driver. Driver shall be informed state of vehicle and instructed for correct actions to follow (i.e. allow system temperature to lower and take vehicle for service and inspection)

UCA20: SCM commands auxiliary assistance command but driver is not made aware (H1, 2, 3, 4, 5)

Scenario1: There is an event of either hot temperature or high friction, which provides limited assistance behavior, but driver is not made aware. Possible causes include:

- Missing communication to BCM.
- BCM is in fault mode, not receiving information.
- Signal delay.
- Chimes are not audible.
- Driver gets distracted or something prevents the driver to be made aware, e.g., music volume too high.

Requirements

UCA20-S1-R1: System shall inform when there is no communication with other modules.

UCA20-S1-R2: SCM shall send the BCM a signal that has entered to an auxiliary mode within TBD [ms] of entering to such mode.

Control action provided but not followed

Scenario2: SCM commands auxiliary assistance and BCM sends signal to inform the driver, but he is not made aware

- Chime does not come off due to a shorted ground.
- Chime is not laud enough or displayed in a way it is easily noticeable by the driver.

Requirements

UCA1-S4-R5: System shall provide service required light and proper chimes when detects failure of actuators such as motor, sensors or SCM. System shall store fault codes for inspection and service.

UCA4-S3-R1: If high system temperature is detected, the system shall provide minimum TBD [Nm] auxiliary assistance to ensure the driver can take the vehicle for inspection.

Algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware that the vehicle is in a reduced performance mode.

UCA3-S1-R3: If discrepancy is constant among correlated signals, the algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware that the vehicle requires inspection. When discrepancy occurs, the system shall provide minimum TBD [Nm] auxiliary assistance to ensure the driver can take the vehicle for inspection.

UCA22: SCM intermittently commands auxiliary assistance (H-1,2,3,4,5)

Scenario 1: SCM does not provide the required assistance for vehicle speed because the assistance fluctuates, confusing the driver. The assistance command from the SCM may fluctuate because:

- Intermittent matching of signals due to one sensor fault, misconnected or error measurement.
- Electromagnetic noise allowed in the system providing erratic behavior of sensors.
- Voltage variance in the system is too high, making the system to send erratic signals and SCM to provide erratic commands.
- Temperature sensor failure, intermittent.
- Power is supplied intermittently.

Requirements

UCA4-S3-R1: If high system temperature is detected, the system shall provide minimum TBD [Nm] auxiliary assistance to ensure the driver can take the vehicle for inspection. Algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware that the vehicle is in a reduced performance mode.

UCA3-S1-R3: If discrepancy is constant among correlated signals, the algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware that the vehicle requires inspection. When discrepancy occurs, the system shall provide minimum TBD [Nm] auxiliary assistance to ensure the driver can take the vehicle for inspection.

UCA1-S1-R2: System level validation shall ensure that electric sensors, actuators and modules does not irradiate electromagnetic noise that could cause improver behavior of modules, actuators and sensors of the system and the vehicle.

UCA1-S1-R3: System level validation shall ensure that electric sensors, actuators and modules signal to noise ratio remains functional during vehicle operation and through common (environmental) electro-magnetic noises.

UCA1-S2-R1: Ensure that enough power is available to provide assistance to the speed of the vehicle. Prioritization shall be enforced to ensure that vehicle control actuators receive the required power to operate the vehicle under safe conditions.

UCA17-S1-R1: System shall measure voltage available in the system to ensure assistance requested is capable to be provided. When there is an event of low voltage, driver shall be informed.

UCA16-S1-R1: Once the system has entered to an auxiliary assistance mode, it can only be taken out by a key cycle event or technician prior diagnose.

Control action provided but not followed

Scenario2: SCM provides auxiliary command but there is only intermittent assistance received by the driver because the motor provides fluctuating force to the Outer tie rod. The motor may provide fluctuating force to the outer tie rod because:

- Shorted ground or low voltage where there is not enough power to feed the system
- High friction condition.
- Hardware failure. Includes:
    - Gear damaged
    - Wear in pinion or rack assembly
    - Ball joint degraded or making noise.
    - Belt assembly failure (rupture)
    - Electric Motor internal failure

Requirements that apply

UCA3-S1-R2: Algorithm shall be able to detect if there is a shorted ground in the circuit that provides power to SCM or steering motor.

UCA1-S4-R1: High friction conditions shall be able to be estimated by the algorithm. If high friction conditions are detected, driver shall be informed so vehicle can be taken for inspection.

UCA6-S3-R1: System components shall withstand designed duty cycle defined by corporate requirements.

UCA21: Stops providing auxiliary assistance command while in fault mode or high temperature (H1, 2, 3, 4, 5)

Scenario1: The SCM cannot maintain auxiliary assistance command because the system is incorrectly believed to be in high friction or high temperature condition. Possible causes include:

- SCM stops providing signal due to an error state or system reset.
- Temperature signal provides incorrect signal, sensor degrades over time providing false readings.
- Intermittent signals, or signals for speed or angle does not correlate.

Requirements

UCA16-S1-R1: Auxiliary assistance of TBD [Nm] shall start when system detects internal temperature above TBD1 [C] and below TBD2 [C]. If system reaches or surpasses TBD2 [C], assistance shall stop being provided.

UCA4-S3-R1: If high system temperature is detected, the system shall provide minimum TBD [Nm] auxiliary assistance to ensure the driver can take the vehicle for inspection. Algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware that the vehicle is in a reduced performance mode.

UCA16-S1-R1: Once the system has entered to an auxiliary assistance mode, it can only be taken out by a key cycle event or technician prior diagnose.

Control action provided but not followed

Scenario2: SCM sends auxiliary assistance command but it is not effective because the system keeps degrading. Possible causes include:

- Auxiliary power selected is too high that keeps making the situation worst.
- Communication error, conflict with signal information.

Requirements

UCA3-S1-R3: If discrepancy is constant among correlated signals, the algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware that the vehicle requires inspection. When discrepancy occurs, the system shall provide minimum TBD [Nm] auxiliary assistance to ensure the driver can take the vehicle for inspection.

UCA16-S1-R1: Once the system has entered to an auxiliary assistance mode, it can only be taken out by a key cycle event or technician prior diagnose.

UCA16-S1-R3: If assistance is stopped being provided, audible chimes and warnings shall be made available to the driver. Driver shall be informed state of vehicle and instructed for correct actions to follow (i.e. allow system temperature to lower and take vehicle for service and inspection)

Revision of prior iteration including findings in iteration 2

In the second iteration, the revised control structure can be analyzed to identify any additional accident scenarios that have been introduced. This section revises accident scenarios from the first iteration to include additional causes that may have been introduced. The next section will identify scenarios for any new UCAs that were not analyzed in the first iteration.

UCA1: Assistance is not provided when driver executes a steering maneuver (H-1,2,3,4)

Scenario1: SCM does not provide assistance because SCM incorrectly believes that assistance is not needed (incorrect process model). The SCM may not know assistance is needed because:

- ABS and transmission output shaft does not match the actual vehicle speed. ABS vehicle speed does not match the actual vehicle speed because:
    - Failed vehicle speed sensor
    - Acceleration in uneven or slippery surface could cause wheel speed to differ from vehicle speed
    - Anti-lock brakes affect wheel speeds
    - System is too sensitive to differential speed measurements
    - Connection or assembly improperly made.
    - Electromagnetic disturbance interferes with signal from wheel speed sensors (high signal to noise ration)
    - Internal components overheat causing degradation of the system and false readings.
    - A pervious value for vehicle speed is used to determine the vehicle speed.
    - Errors in the calculation from the ABS Control Module.
- The transmission output shaft speed does not match the actual vehicle speed because:
    - Failed transmission speed sensor
    - Transmission shaft speed at turning is too different between Right and Left hand side causing conflict between measured speed and actual speed.
    - Connection or assembly improperly made.
    - Electromagnetic disturbance interferes with signal from transmission speed sensors (high signal to noise ration)
    - Internal components overheat causing degradation of the system and false readings.
    - Errors in the calculation from the transmission module.
    - The ABS module goes to error estate and last value of vehicle speed keeps being sent.

Additional Requirements:

UCA1-S1-R7: The system shall provide a minimum assistance of TBD [Nm] to help the driver bring the vehicle to a safe state when vehicle speed does not match the calculated vehicle speed by other modules. Assistance shall be available when the SCM detects that system is in

error state, or other modules are sending information that does not match with the model of SCM.

Given that an additional control action is identified, a new scenario is derived that could not be justified before since there were no interaction with other vehicle modules. New causes are identified from Scenario 4:

Scenario4: SCM does not provide assistance command because SCM incorrectly believes that it is not safe to provide assistance. SCM believes it is unsafe because:

- There is no correlation between steering wheel angle measured by sensor and provided by ABS module.
- Incorrectly reported high temperature (sensor failure).
- Incorrectly reported high friction.
- Incorrectly reported low voltage.

Control action is provided but not followed:

Scenario2: SCM provides assistance command but it is not effective because the current to power the motor is low. The current may be too low because:

- Electrical power module commands shutting down power to prevent battery drain.

Scenario3: SCM provides steering command but it is insufficient due to steering lock condition. The system could be locked because:

- Friction detection algorithm does not account correctly for high friction in the system. This could be because:
    - Thresholds for friction are too low.
    - Driving in low friction or split friction roads.
    - Changing vehicle conditions (Process model) (i.e., GVW, tires)
    - Input signals variability (Angle, torque, speed)
    - High torque events that could provide false readings (i.e., High lateral acceleration, aggressive take off, aggressive maneuvers)

Additional requirements:

UCA1-S4-R1: High friction conditions shall be able to be estimated by the algorithm. If high friction conditions are detected, driver shall be informed so vehicle can be taken for inspection.

The rationale for this requirement is to avoid false readings and trigger false high friction conditions when in reality the vehicle is being driven in a context where it could be inferred as high friction, such as off-road situation or partially dampen roads.

UCA2: High assistance is provided while traveling at high speeds (H-1,2,3,4,5)

Scenario1: SCM incorrectly provides high assistance when vehicle speed is high. SCM incorrectly believes that vehicle speed is low because:

- There is no correlation between speed signals and vehicle speed, SCM computes high speed (incorrectly)

New requirements

> UCA2-S1-R3: Vehicle speed received from the wheel speed sensor and correlation with speed received from Engine Control Module shall match before providing assistance command.
>
> UCA3-S1-R3: If discrepancy is constant among correlated signals, the algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware that the vehicle requires inspection. When discrepancy occurs, the system shall provide minimum TBD [Nm] auxiliary assistance to ensure the driver can take the vehicle for inspection.

<u>Control action provided but not followed</u>

Scenario2: The SCM provides a low assistance command but it is not effective because high assistance remains being delivered. Possible reasons for remain providing high assistance include:

Additional Requirements that apply:

UCA5-S1-R3: Wheel speed signal shall be updated in TBD [ms] intervals to avoid signal delays.

UCA9-S1-R1: Steering wheel angle shall be received each TBD [ms] to avoid delay in signal.

UCA3-S1-R1: SCM shall have enough processing capability to process signals at the required speed.

UCA2-S1-R3: Vehicle speed received from the wheel speed sensor and correlation with speed received from Engine Control Module shall match before providing assistance command.

UCA3-S1-R3: If discrepancy is constant among correlated signals, the algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware that the vehicle requires inspection. When discrepancy occurs, the system shall provide minimum TBD [Nm] auxiliary assistance to ensure the driver can take the vehicle for inspection.

UCA5: Low assistance is while traveling at low speeds (H-1,2,3,4)

Scenario 1: SCM provides low assistance because incorrectly believes that the vehicle speed is high. SCM might incorrectly believe that vehicle speed is high because:

- There is no correlation between speed signals and vehicle speed, SCM computes low speed (incorrectly)

Additional requirements:

UCA2-S1-R3: Vehicle speed received from the wheel speed sensor and correlation with speed received from Engine Control Module shall match before providing assistance command.

UCA3-S1-R3: If discrepancy is constant among correlated signals, the algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware that the vehicle requires inspection. When discrepancy occurs, the system shall provide minimum TBD [Nm] auxiliary assistance to ensure the driver can take the vehicle for inspection.

Control action provided but not followed

Scenario 2: SCM provides high assistance command correctly but assistance delivered to turn the wheels is low. Possible reasons for delivering low assistance include:

- Algorithm does not calculate high friction condition.

Additional Requirements

UCA1-S4-R1: High friction conditions shall be able to be estimated by the algorithm. If high friction conditions are detected, driver shall be informed so vehicle can be taken for inspection.

UCA9: Assistance is provided in opposite direction than commanded by driver (H1, 2, 3, 4,5)

Scenario1: SCM provides assistance in the opposite direction as commanded by the driver because signal is provided opposite to where assistance is being required. Reasons for why the assistance signal is provided in opposite direction include:

- Conflicting information between steering angle signal and that provided by ABS module.
- Steering angle failure and inferred steering wheel angle from wheel speed sensors provided out of synchronization or out of sequence, inferring a steering maneuver.

Requirements that apply:

UCA3-S1-R3: If discrepancy is constant among correlated signals, the algorithm shall include logic to display MIL and audible chimes to the driver so he can be made aware that the vehicle requires inspection. When discrepancy occurs, the system shall provide minimum TBD [Nm] auxiliary assistance to ensure the driver can take the vehicle for inspection.

Scenario2: Driver experience unwanted assistance while driving the vehicle.

- Steering angle failure and inferred steering wheel angle from wheel speed sensors provided out of synchronization or out of sequence, inferring a steering maneuver.

UCA3: Assistance is provided too late when steering is required by the driver (H-1,2,3,4,5)

Scenario1: SCM does not provide assistance command because incorrectly believes that the driver has not initiated a steering. The SCM may not perceive that the driver has initiated a steering action because:

- Steering angle sensor failure and WSS failure would make the SCM infer that no steering request has been made by the driver.

Additional Requirements

> UCA3-S1-R3: If discrepancy is constant among correlated signals, the algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware that the vehicle requires inspection. When discrepancy occurs, the system shall provide minimum TBD [Nm] auxiliary assistance to ensure the driver can take the vehicle for inspection.

UCA4: Assistance is interrupted while driver executes a steering maneuver (H-1,2,3,4)

Scenario1 The SCM stops sending assistance command while the driver is requiring aid because SCM incorrectly believes that assistance is no longer needed.

- Vehicle speed signal and engine speed signal do not correlate causing a conflict.

Additional Requirements

> UCA3-S1-R3: If discrepancy is constant among correlated signals, the algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware that the vehicle requires inspection. When discrepancy occurs, the system shall provide minimum TBD [Nm] limp home mode assistance to ensure the driver can take the vehicle for inspection.

UCA3-S1-R5: If a shorted ground or sensor failure is detected, the system shall enter a protection mode and provide TBD [Nm] auxiliary assistance. The algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware t aware that the vehicle requires inspection.

UCA4-S3-R1: If high system temperature is detected, the system shall provide minimum TBD [Nm] limp home mode assistance to ensure the driver can take the vehicle for inspection. Algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware that the vehicle is in a reduced performance mode.

UCA16-S1-R3: If assistance is stopped being provided, audible chimes and warnings shall be made available to the driver. Driver shall be informed state of vehicle and instructed for correct actions to follow (i.e. allow system temperature to lower and take vehicle for service and inspection).

UCA6: Assistance is provided intermittently when driver executes a steering maneuver (H-1,2,3,4,5)

Scenario1: SCM provides intermittent assistance command because vehicle speed is sent intermittently to the SCM. The speed signal may be sent intermittently to the SCM because:

- Conflicting signals about steering angle or vehicle speed.
- System temperature measurement oscillates between thresholds for auxiliary mode and no assistance provided.

Additional requirements

UCA3-S1-R3: If discrepancy is constant among correlated signals, the algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware that the vehicle requires inspection. When discrepancy occurs, the system shall provide minimum TBD [Nm] limp home mode assistance to ensure the driver can take the vehicle for inspection.

UCA3-S1-R5: If a shorted ground or sensor failure is detected, the system shall enter a protection mode and provide TBD [Nm] auxiliary assistance. The algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware t aware that the vehicle requires inspection.

UCA16-S1-R1: Auxiliary assistance of TBD [Nm] shall start when system detects internal temperature above TBD1 [C] and below TBD2 [C]. If system reaches or surpasses TBD2 [C], assistance shall stop being provided.

UCA16-S1-R1: Once the system has entered to an auxiliary assistance mode, it can only be taken out by a key cycle event or technician prior diagnose.

Control action provided but not followed

Scenario3: SCM sends assistance command but is not effective because it feels intermittent. Assistance may feel intermittent because:

- Wheel speed sensor and angle sensor provide conflicting signal causing the SCM to factor information and provide assistance with the rate it receives.

Additional Requirements

UCA3-S1-R3: If discrepancy is constant among correlated signals, the algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware that the vehicle requires inspection. When discrepancy occurs, the system shall provide minimum TBD [Nm] limp home mode assistance to ensure the driver can take the vehicle for inspection.

UCA7: Assistance continues being provided when safe angle has been reached (H-1,2,3,4,5)

Scenario1: SCM continues providing steering command after required angle has been reached because SCM incorrectly believes that assistance is still being required. SCM believes that assistance is still required because:

- Conflicting signals with Wheel Speed sensor and steering wheel angle.
- Torque sensor failure (false reading or measurement)

Additional Requirements

UCA3-S1-R3: If discrepancy is constant among correlated signals, the algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware that the vehicle requires inspection. When discrepancy occurs, the system shall provide minimum TBD [Nm] limp home mode assistance to ensure the driver can take the vehicle for inspection.

Driver

This section revises the driver section with additional causes derived from Iteration 2 and additional requirements that apply for the scenarios selected. Only additional information is displayed:

UCA11: Driver does not provide steering command when there are objects or people in their path (H-1,2,3,5)

Scenario1: Driver incorrectly believes that there is no need of changing path (process model flaw) because something prevents driver awareness. Reasons that the driver process model can be flawed include:

- Driver believes (mental model) that assistance will be provided, but is not aware that is under protected assistance mode (not informed, or display is not visible or audible)

Additional Requirements

UCA10-S2-R1: If assistance corresponding to the vehicle speed can't be provided, chime above TBD [dB] and discernable display that ensures the driver is aware of reduced assistance shall be provided.

UCA16-S1-R1: Once the system has entered to an auxiliary assistance mode, it can only be taken out by a key cycle event or technician prior diagnose.

UCA16-S1-R1: Auxiliary assistance of TBD [Nm] shall start when system detects internal temperature above TBD1 [C] and below TBD2 [C]. If system reaches or surpasses TBD2 [C], assistance shall stop being provided.

UCA16-S1-R3: If assistance is stopped being provided, audible chimes and warnings shall be made available to the driver. Driver shall be informed state of vehicle and instructed for correct actions to follow (i.e. allow system temperature to lower and take vehicle for service and inspection).

Scenario2: Driver believes that certain amount of assistance will be provided but is unable to provide correct steering angle due to lack of assistance.

Requirements that apply

UCA10-S2-R1: If assistance corresponding to the vehicle speed can't be provided, chime above TBD [dB] and discernable display that ensures the driver is aware of reduced assistance shall be provided.

UCA1-S2-R5: Auxiliary power in vehicle shall be capable to maintain road lights and minimum of TBD [V] to provide assistance in the event of engine stall and vehicle speed is higher than TBD [kph]

UCA13: Driver leaves safe path before steering maneuver is being completed (H-1,2,3,4,5)

Scenario1: Driver might expect low assistance (mental model) and system provides high assistance level to perform a cornering event. The system may provide different assistance level because:

- System shows a limited assistance display due to high temperature in the system that changes the driver mental model. If the system comes back to normal temperature without alerting the driver, the prior mental model would remain expecting a reduced assistance.

Additional requirements that apply:

UCA16-S1-R1: Once the system has entered to an auxiliary assistance mode, it can only be taken out by a key cycle event or technician prior diagnose.

Scenario5: Driver counter-steers fast or too aggressive while performing parking lot maneuver and finds an obstruction or hard to provide direction. Possible causes:

- Assistance would not be provided because there is a conflict between steering angle and speed signals.

Additional requirements that apply

UCA3-S1-R3: If discrepancy is constant among correlated signals, the algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware that the vehicle requires inspection. When discrepancy occurs, the system shall provide minimum TBD [Nm] limp home mode assistance to ensure the driver can take the vehicle for inspection.

Scenario7: Assistance stops being when driver finishes executing a steering maneuver.

- Conflicting signals with Wheel Speed sensor and steering angle

Additional Requirements

UCA3-S1-R3: If discrepancy is constant among correlated signals, the algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware that the vehicle requires inspection. When discrepancy occurs, the system shall provide minimum TBD [Nm] limp home mode assistance to ensure the driver can take the vehicle for inspection.

Scenario8: Assistance continues being when driver finishes executing a steering maneuver.

- Conflicting signals with Wheel Speed sensor and steering wheel angle

UCA3-S1-R3: If discrepancy is constant among correlated signals, the algorithm shall include logic to display MIL and sonorous chimes to the driver so he can be made aware that the vehicle requires inspection. When discrepancy occurs, the system shall provide minimum TBD [Nm] limp home mode assistance to ensure the driver can take the vehicle for inspection.

Appendix 2: FMEA analysis of EPS system

Category (Product)	Criteria: Severity of Effect (Effect on Product) – DFMEA & PFMEA	Rank	Category (Process)	Criteria: Severity of Effect (Effect on Process) - PFMEA
Safety and/or Regulatory Compliance	Potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulation without warning.	**10**	**Safety and/or Regulatory Compliance**	May endanger operator (machine or assembly) without warning.
	Potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulation with warning.	**9**		May endanger operator (machine or assembly) with warning.
Primary Function *Essential*	Loss of primary function (vehicle inoperable, does not affect safe vehicle operation)	**8**	**Major Disruption**	100% of product may have to be scrapped. Line shutdown or stop ship.
	Degradation of primary function (vehicle operable, but at reduced level of performance)	**7**	**Significant Disruption**	A portion of the production run may have to be scrapped. Deviation from primary process; decreased line speed or added manpower.
Secondary Function *Convenient*	Loss of secondary function (vehicle operable, but comfort / convenience functions inoperable)	**6**	**Rework out-of-station**	100% of production run may have to be reworked off line and accepted.
	Degradation of secondary function (vehicle operable, but comfort / convenience functions at reduced level of performance)	**5**		A portion of the production run may have to be reworked off line and accepted.
Annoyance	Appearance or Audible Noise, vehicle operable, item does not conform. Defect noticed by most customers (> 75%)	**4**	**Rework in-station**	100% of production run may have to be reworked in station before it is processed.
	Appearance or Audible Noise, vehicle operable, item does not conform. Defect noticed by many customers (50%)	**3**		A portion of the production run may have to be reworked in-station before it is processed.
	Appearance or Audible Noise, vehicle operable, item does not conform. Defect noticed by discriminating customers (< 25%)	**2**	**Minor Disruption**	Slight inconvenience to process, operation, or operator
No effect	No discernible effect.	**1**	**No effect**	No discernible effect

Figure 18 - Suggested Severity criteria from SAE J1739 [8]

Likelihood of Failure	Criteria: Occurrence of Cause – DFMEA (Design life/reliability of item/vehicle)	Rank	Criteria: Occurrence of Cause – PFMEA (Incidents per 1000 items/vehicles)
Very High	New technology/new design with no history.	**10**	≥ 100 per thousand pieces >/= 1 in 10
High	Failure is inevitable with new design, new application, or change in duty cycle/operating conditions.	**9**	50 per thousand pieces 1 in 20
	Failure is likely with new design, new application, or change in duty cycle/operating conditions.	**8**	20 per thousand pieces 1 in 50
	Failure is uncertain with new design, new application, or change in duty cycle/operating conditions.	**7**	10 per thousand pieces 1 in 100
Moderate	Frequent failures associated with similar designs or in design simulation and testing.	**6**	2 per thousand pieces 1 in 500
	Occasional failures associated with similar designs or in design simulation and testing.	**5**	.5 per thousand pieces 1 in 2,000
	Isolated failures associated with similar design or in design simulation and testing.	**4**	.1 per thousand pieces 1 in 10,000
Low	Only isolated failures associated with almost identical design or in design simulation and testing.	**3**	.01 per thousand pieces 1 in 100,000
	No observed failures associated with almost identical design or in design simulation and testing.	**2**	≤.001 per thousand pieces 1 in 1,000,000
Very Low	Failure is eliminated through preventative control.	**1**	Failure is eliminated through preventative control.

Figure 19 - Suggested Occurrence evaluation criteria from SAE J1739 [8]

Category (Product)	DFMEA Criteria: Likelihood of Detection by Design Control	Rank	Category (Process)	PFMEA Criteria: Likelihood of Detection by Process Control
Absolute Uncertainty	No current design control; Cannot detect or is not analyzed	10	Absolute Uncertainty	No current process control; Cannot detect or is not analyzed
Difficult to Detect	Design analysis/detection controls have a weak detection capability; Virtual Analysis (e.g. CAE, FEA, etc.) is **not correlated** to expected actual operating conditions.	9	Difficult to Detect	Defect (Failure Mode) and/or Error (Cause) is not easily detected (e.g. Random audits)
Post Design Freeze and Prior to Launch	Product verification/validation after design freeze and prior to launch with **pass/fail** testing (Sub-system or system testing with acceptance criteria e.g. Ride & handling, shipping evaluation, etc.)	8	Defect Detection Post Processing	Defect (Failure Mode) detection post-processing by operator through visual/tactile/audible means.
	Product verification/validation after design freeze and prior to launch with **test to failure** testing (Sub-system or system testing until failure occurs, testing of system interactions, etc.)	7	Defect Detection at Source	Defect (Failure Mode) detection in-station by operator through visual/tactile/audible means or post-processing through use of attribute gauging (go/no-go, manual torque check/clicker wrench, etc.)
	Product verification/validation after design freeze and prior to launch with **degradation** testing (Sub-system or system testing after durability test e.g. Function check)	6	Defect Detection Post Processing	Defect (Failure Mode) detection post-processing by operator through use of variable gauging or in-station by operator through use of attribute gauging (go/no-go, manual torque check/clicker wrench, etc).
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.)	5	Defect Detection at Source	Defect (Failure Mode) or Error (Cause) detection in-station by operator through use of variable gauging or by automated controls in-station that will detect discrepant part and notify operator (light, buzzer, etc.). Gauging performed on setup and first-piece check (for set-up causes only)
	Product validation (reliability testing, development or validation tests) prior to design freeze using **test to failure** (e.g. until leaks, yields, cracks, etc.)	4	Defect Detection Post Processing	Defect (Failure Mode) detection post-processing by automated controls that will detect discrepant part and lock part to prevent further processing.
	Product validation (reliability testing, development or validation tests) prior to design freeze using **degradation** testing (e.g. data trends, before/after values, etc.)	3	Defect Detection at Source	Defect (Failure Mode) detection in-station by automated controls that will detect discrepant part and automatically lock part in station to prevent further processing.
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.	2	Error Detection and/or Defect Prevention	Error (Cause) detection in-station by automated controls that will detect error and prevent discrepant part from being made
Detection not applicable; Failure Prevention	Failure cause or failure mode can not occur because it is fully prevented through design solutions (e.g. Proven design standard/best practice or common material, etc.)	1	Detection not applicable; Error Prevention	Error (Cause) prevention as a result of fixture design, machine design or part design.

Figure 20 - Suggested Detection evaluation criteria from SAE J1739 [8]

Subsystem	Electric Power Steering Gear	Responsible	Rodrigo Sotomayor								FMEA ID	Hardware FMEA
Model	2017 -X	Prepared by	Rodrigo Sotomayor								FMEA date	9/1/2014

Function	Potential Failure Mode	Potential Effect(s) of Failure	SEV	Class	Potential Cause(s) of Failure	OCC	Prevention Controls	Detection Controls	DET	RPN	Recommended Action	Responsibility & Target completion Date
(1) Transfer diver input (torque and	(1.1) EPS does not convert angular displacement/torque to linear displacement/force	(1.1.1) Unable to control direction of vehicle	10	YC	(1.1.1.1) Incompatibility between gears assembly (1.1.1.2) Internal components failure (ICF) (1.1.1.3) Incorrect internal components assembly (Packaging)	2	-Fatigue Test at system level - GD&T - Wear to failure test - Impact test at system level - No assist wear test - Standards for Packaging Clearance	- Durability test at vehicle level - Component supplier quality control plan - Component FMEA - Virtual design aid clearance check	3	60		
		(1.1.2) Customer dissatisfaction	10	YC	(1.1.1.4) Corrosion	2	- Material Specification - Corrosion Protection specification	- Corrosion test at vehicle level (XX cycles) - Raw material supplier control testing	3	60		
		(1.1.3) Driver input is not enough to turn EPS input shaft	10	YC	(1.1.1.5) External objects stuck in the system or contiguous components	4	- System Isolation Specification - Standards for Packaging Clearance	- Corrosion test at vehicle level - Durability test at vehicle level	5	200		
			10	YC	(1.1.1.6) Steering gear lock up	2	- Static torsional test at system level - Fatigue test at system level	- Durability test at vehicle level	3	60		
			10	YC	(1.1.1.7) Adjustment travel limiters failure/improper set up	2	- Static torsional test at system level - Fatigue test at system level - Mechanical stop test at system level - Component design validation	- Durability test at vehicle level - Component FMEA	3	60		
			10	YC	(1.1.1.8) Improper connections made at system interface: I-shaft to gear, gear to frame, tie rod to knuckle	2	- Joint design - Fastener design validation - Fastener audit torque	- Joint analysis - Road load data at vehicle level - Fasteners torque and angle tests	3	60		
			10	YC	(1.1.1.9) Gear/linkage system not adequately designed to handle wear, impact & fatigue	4	- Fatigue test at system level - Static torsional test at system level - Mounting test at system level - Impact test at system level	- Durability test at vehicle level	4	160		
			10	YC	(1.1.1.11) Motor fails to allow rotation of input shaft under driver input	1	- Fatigue test at component level - Standards for Packaging Clearance	- Durability test at vehicle level - Electrical hardware design review Vehicle level electrical CAE - EMC testing	3	30		
			10	YC	(1.1.1.12) Rack and ball nut assembly does not permit axial movement of the rack	2	- Fatigue test at component level - Standards for Packaging Clearance	- Corrosion test at vehicle level (XX cycles) - Durability test at vehicle level	3	60		
	(1.2) Convert angular displacement to linear displacement and force intermittently	(1.2.1) Vehicle response inconsistent (non-linear)	10	YC	(1.2.1) Incorrect internal components assembly (Packaging)	3	- Standards for Packaging Clearance	- Virtual design aid clearance check	2	60		
		(1.2.2) Degraded vehicle control	10	YC	(1.2.2) Internal component failure	4	- Fatigue test at system level - Static torsional test at system level - Impact test at system level	- Durability test at vehicle level	3	120		
		(1.2.3) Damage to contiguous components	10	YC	(1.2.3) Adjustment travel limiters failure/improper set up	3	- Static torsional test at system level - Fatigue test at system level - Mechanical stop test at system level - Component design validation	- Durability test at vehicle level - Component FMEA	5	150		

Function	Potential Failure Mode	Potential Effect(s) of Failure	SEV	Class	Potential Cause(s) of Failure	OCC	Prevention Controls	Detection Controls	DET	RPN	Recommended Action	Responsibility & Target completion Date
angular displacement) to linear displacement and force to knuckle assembly		(1.2.4) Blocked system relative to steering wheel position	10	YC	(1.2.4) Gear/linkage system not adequately designed to handle wear, impact & fatigue	4	- Fatigue test at system level - Static torsional test at system level - Mounting test at system level - Impact test at system level	- Durability test at vehicle level	4	160		
		(1.2.5) Customer dissatisfaction	10	YC	(1.2.5) External objects stuck in the system or contiguous components	4	- System Isolation Specification - Standards for Packaging Clearance	- Corrosion test at vehicle level - Durability test at vehicle level	5	200		
			10	YC	(1.2.6) Motor fails to allow rotation of input shaft under driver input	4	- Fatigue test at component level - Standards for Packaging Clearance	- Durability test at vehicle level - Electrical hardware design review Vehicle level electrical CAE - EMC testing	5	200		
	(1.3) Degraded conversion of angular displacement to linear displacement	(1.3.1) Degraded vehicle control	7		(1.3.1) Gear/linkage system stiffer than required for vehicle architecture	6	- Rigidity and compliance test at system level - Torsional bar rate definition	- Durability test at vehicle level - Gear FMEA	4	168		
		(1.3.2) Degraded center feel	8		(1.3.2) Free play in gear / linkage system	5	- Rigidity and compliance test	- Durability test at vehicle level - Gear FMEA	4	160		
		(1.3.3) Function delivered but outside the expected performance for vehicle segment	8		(1.3.3) Excessive lash in torque sensor	5	- GD&T - Torque sensor calibration testing - Component FMEA	- Durability test at vehicle level - Vehicle calibration to comply with DNA targets - Component FMEA	4	160		
		(1.3.4) Vehicle pulls and/or drifts	7	YS	(1.3.4) Column joint, outer tie rod to knuckle looseness	5	- Joint validation - Fastener audit torque - Assembly plant control	- Durability test at vehicle level - Joint analysis	3	105		
		(1.3.5) Noise while steering	7	YS	(1.3.5) Steering shaft looseness	5	- Static Torsional test at system level - Fatigue test at system level - Rigidity and compliance test at system level	- Durability test at vehicle level - Gear FMEA	3	105		
		(1.3.6) Excessive tire wear	8		(1.3.5) Improper gear ratio	5	- GD&T	- Development test at vehicle level	2	80		
			8		(1.3.6) Does not maintain Toe self adjustment while driving	5	- Component design validation and testing	- Durability test at vehicle level - Development test at vehicle level	2	80		
	(1.4) Degraded conversion of angular displacement to linear displacement Single-sided disconnect - directional control maintained	(1.4.1) Degraded vehicle directional control	7		(1.4.1) Linkage disconnected on one side	3	- Fatigue test at system level - Impact test at system level - Component design validation and testing	Vehicle durability test Ref: Gear FMEA	3	63		
		(1.4.2) Degraded center feel	7	YS	(1.4.2) Position of Torque sensor moves rack in wrong direction	4	- GD&T	- Development test at vehicle level - Package Design Review	3	84		
		(1.4.3) Excessive tire wear										
		(1.4.4) Vehicle pulls/drifts										
	(1.5) Degraded conversion of input torque to linear force. (excessive friction)	(1.5.1) No self centering	6	YS	(1.5.1) Excessive gear/linkage friction	4	- Fatigue test at system level - Torque testing at system level	Development test at vehicle level Durability test at vehicle level	3	72		
		(1.5.2) No road feedback	10	YC	(1.5.2) Electric motor failure	4	- Electric motor FMEA	- Electrical Hardware Design Review - Vehicle Level Electrical CAE	4	160		
		(1.5.3) Degraded center feel	6	YS	(1.5.3) Torque Sensor + IPA Assembly moves rack in wrong direction	4	- Torque Sensor FMEA	- Development test at vehicle level - Durability test at vehicle level	3	72		
		(1.5.4) Increased efforts										
		(1.5.5) Steering in wrong direction										

Function	Potential Failure Mode	Potential Effect(s) of Failure	SEV	Class	Potential Cause(s) of Failure	OCC	Prevention Controls	Detection Controls	DET	RPN	Recommended Action	Responsibility & Target completion Date
(2) Convert linear displacement/force of the steering knuckle to angular displacement/torque of the steering column to provide feedback	(2.1) Does not convert linear displacement/force to angular displacement/torque	(2.1) Degraded vehicle control	10	YC	(2.1.1) Incompatibility between gears assembly	3	- GD&T - Wear to failure test - Impact test at system level - No assist wear test	- Durability test at vehicle level - Component supplier quality control plan - Component FMEA	4	120		
			10	YC	(2.1.2) Internal components failure (ICF)	3	-Fatigue Test at system level - GD&T - Wear to failure test - Impact test at system level - No assist wear test	- Durability test at vehicle level - Component supplier quality control plan - Component FMEA	3	90		
			10	YC	(2.1.3) Incorrect internal components assembly (Packaging)	3	- Standards for Packaging Clearance	- Virtual design aid clearance check	3	90		
			10	YC	(2.1.4) Corrosion	2	- Material Specification - Corrosion Protection specification	- Corrosion test at vehicle level (XX cycles) - Raw material supplier control testing	3	60		
			10	YC	(2.1.5) External objects stuck in the system or contiguous components	4	- System Isolation Specification - Standards for Packaging Clearance	- Corrosion test at vehicle level - Durability test at vehicle level	5	200		
			10	YC	(2.1.6) Steering gear lock up	3	- Static torsional test at system level - Fatigue test at system level	- Durability test at vehicle level	3	90		
			10	YC	(2.1.7) Adjustment travel limiters failure/improper set up	4	- Static torsional test at system level - Fatigue test at system level - Mechanical stop test at system level - Component design validation	- Durability test at vehicle level - Component FMEA	4	160		
			10	YC	(2.1.8) Improper connections made at system interface: I-shaft to gear, gear to frame, tie rod to knuckle	2	- Joint design - Fastener design validation - Fastener audit torque	- Joint analysis - Road load data at vehicle level - Fasteners torque and angle tests	4	80		
			10	YC	(2.1.9) Gear/linkage system not adequately designed to handle wear, impact & fatigue	4	- Fatigue test at system level - Static torsional test at system level - Mounting test at system level - Impact test at system level	- Durability test at vehicle level	3	120		
	(2.2) Does not provide feedback from knuckle	(2.2.1) No road feedback	6	YS	(2.2.1) Excessive gear / linkage friction	4	- Fatigue test at system level - Static torsional test at system level	- Development test at vehicle level - Durability test at vehicle level	3	72		
		(2.2.2) Driver requires to provide force to recover from turn	6	YS	(2.2.2) Excessive steering system damping	3	- Tuning development at component level	- Development test at vehicle level - Durability test at vehicle level	3	54		
		(2.2.3) No self-centering	6	YC	(2.2.3) Gear system self-locks	3	- Fatigue test at system level - Impact test at system level	- Development test at vehicle level - Durability test at vehicle level	4	72		
		(2.2.4) Degraded system function	10	YC	(2.2.4) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level	4	160		
		(2.2.5) Customer dissatisfaction										
	(2.3) Degraded / non-linear / uneven conversion of linear force to torque	(2.3.1) No or slow self-centering	6	YS	(2.3.1) Excessive gear / linkage friction	4	- Fatigue test at system level - Static torsional test at system level	- Development test at vehicle level - Durability test at vehicle level	3	72		
		(2.3.2) Degraded road feedback / center feel	6	YS	(2.3.2) Excessive steering system damping	3	- Tuning development at component level	- Development test at vehicle level - Durability test at vehicle level	3	54		
		(2.3.3) Degraded system function	10	YC	(2.3.4) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level	4	160		
		(2.3.4) Driver requires to provide force to recover from turn	8		(2.3.5) Free play in gear / linkage system	5	- Rigidity and compliance test	- Durability test at vehicle level - Gear FMEA	4	160		

Function	Potential Failure Mode	Potential Effect(s) of Failure	SEV	Class	Potential Cause(s) of Failure	OCC	Prevention Controls	Detection Controls	DET	RPN	Recommended Action	Responsibility & Target completion Date
from road to driver and allow self centering of the steering		(2.3.5) Customer dissatisfaction	7	YS	(2.3.6) Column joint, outer tie rod to knuckle looseness	5	- Joint validation - Fastener audit torque - Assembly plant control	- Durability test at vehicle level - Joint analysis	3	105		
	(2.4) EPS does not self return	(2.4.1) Driver requires to provide force to recover from turn	8		(2.4.1) Damage / Wear of the gear system	4	-Fatigue Test at system level - Wear to failure test - Impact test at system level - No assist wear test	- Durability test at vehicle level	4	128		
		(2.4.2) Customer dissatisfaction	8		(2.4.2) Improper use of gear to vehicle geometry	4	- CAD - CAE	- Development testing at vehicle level	4	128		
			6	YS	(2.4.3) Friction above the designed ranges in the system	4	-Fatigue Test at system level - Wear to failure test	- Development test at vehicle level - Durability test at vehicle level	3	72		
			7		(2.4.4) Foreign objects allowed in the gear system	6	- System Isolation Specification - Contamination specification	- Development test at vehicle level - Durability test at vehicle level - Gear FMEA	4	168		
			10	YC	(2.4.5) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level	4	160		
	(2.5) EPS self return slowly	(2.5.1) Driver requires to provide force to recover from turn	8		(2.5.1) Damage / Wear of the gear system	4	-Fatigue Test at system level - Wear to failure test - Impact test at system level - No assist wear test	- Durability test at vehicle level	4	128		
		(2.5.2) Customer dissatisfaction	8		(2.5.2) Improper use of gear to vehicle geometry	4	- CAD - CAE	- Development testing at vehicle level	4	128		
			6	YS	(2.5.3) Friction above the designed ranges in the system	4	-Fatigue Test at system level - Wear to failure test	- Development test at vehicle level - Durability test at vehicle level	3	72		
			7		(2.5.4) Foreign objects allowed in the gear system	6	- System Isolation Specification - Contamination specification	- Development test at vehicle level - Durability test at vehicle level - Gear FMEA	4	168		
			10	YC	(2.5.5) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level	4	160		
	(2.6) EPS self return too fast	(2.6.1) customer dissatisfaction	6	YS	(2.6.1) Inadequate Motor to gear / linkage system friction	4	- Fatigue Test at system level - Wear to failure test	- Development test at vehicle level - Durability test at vehicle level	3	72		
			6	YS	(2.6.2) Inadequate gear / linkage system friction	4	- Fatigue Test at system level - Wear to failure test	- Development test at vehicle level - Durability test at vehicle level	3	72		
			6		(2.6.3) Excessive suspension restoring force	4	- Development test at vehicle level	- Development test at vehicle level - Durability test at vehicle level	5	120		
	(2.7) Excessive feedback from knuckle (nibble & wheel fight)	(2.7.1) Wheel fight / nibble	10	YC	(2.7.1) Improper or defective gear installation on vehicle	4	- Mounting test at system level	- Development test at vehicle level - Durability test at vehicle level - NVH development test at vehicle level	4	160		
		(2.7.2) Customer dissatisfaction	6	YS	(2.7.2) Inadequate gear / linkage system friction	4	- Fatigue Test at system level - Wear to failure test	- Development test at vehicle level - Durability test at vehicle level	3	72		
		(2.7.3) Degraded road feedback	6	YS	(2.7.3) Excessive steering system damping	3	- Tuning development at component level	- Development test at vehicle level - Durability test at vehicle level	3	54		
			6	YS	(2.7.4) Tire imbalance	3	- Component design validation and testing	- Development test at vehicle level - Durability test at vehicle level	3	54		
			10	YC	(2.5.5) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level	4	160		
			6		(2.7.6) Excessive suspension sensitivity	4		- Development test at vehicle level - Durability test at vehicle level	5	120		

Function	Potential Failure Mode	Potential Effect(s) of Failure	SEV	Class	Potential Cause(s) of Failure	OCC	Prevention Controls	Detection Controls	DET	RPN	Recommended Action	Responsibility & Target completion Date
(3) Provide damping to isolate the driver from road harshness and driveline input	(3.1) Insufficient damping	(3.1.1) Wheel fight / nibble	6	YS	(3.1.1) Mounting isolators failure	4	- Fatigue Test at system level - Wear to failure test - Mounting test at system level	- Development test at vehicle level - Durability test at vehicle level - Nibble sensitivity study - Road load vehicle - Isolator tuning	5	120		
			10	YC	(3.1.2) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level	4	160		
			6		(3.1.3) Gear reverse efficiency too high	4	- Fatigue Test at system level	- Development test at vehicle level - Durability test at vehicle level	4	96		
		(3.1.2) Customer dissatisfaction	7	YS	(3.1.4) Torque sensor provides wrong torque command	5	- Sensor FMEA	- Development test at vehicle level - Durability test at vehicle level	5	175		
			6		(3.1.5) Electric Motor provides lower than required torque to belt assembly	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level	4	96		
			10	YC	(3.1.6) Power supply harness does not supply required current to Electric motor	4	- Power Supply Harness FMEA	- Development test at vehicle level - Durability test at vehicle level	6	240		
	(3.2) Excessive damping	(3.2.1) Degraded center feel	6	YS	(3.2.1) Isolator material out of specification	4	- Fatigue Test at system level - Wear to failure test - Mounting test at system level	- Development test at vehicle level - Durability test at vehicle level - Nibble sensitivity study - Road load vehicle - Isolator tuning	5	120		
		(3.2.2) Customer dissatisfaction	6		(3.2.2) Gear reverse efficiency too low	4	- Fatigue Test at system level	- Development test at vehicle level - Durability test at vehicle level	4	96		
			6	YS	(3.2.3) Excessive gear/linkage friction	4	- Fatigue test at system level - Torque testing at system level	Development test at vehicle level Durability test at vehicle level	3	72		
			10	YC	(3.2.4) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level	4	160		
			8		(3.2.5) Torque sensor provides wrong torque command	4	- Sensor FMEA	- Development test at vehicle level - Durability test at vehicle level	4	128		
			6		(3.2.6) Electric Motor provides lower than required torque to belt assembly	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level	4	96		
	(4.1) No assistance - Full loss of power assist	(4.1.1) Increased steering efforts due to complete loss of power assist	10		(4.1.1) Belt assembly does not transmit torque between Electric Motor and rack	4	- Belt assembly FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	6	192		
		(4.1.2) Increased brake effort due to complete loss of power assist to the boost system	8		(4.1.2) Electric motor does not provide torque to belt assembly	5	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out - Electrical hardware testing review - Vehicle steering communications message design review	6	240		
		(4.1.3) Customer dissatisfaction	8		(4.1.3) Torque sensor does not provide torque measurement to Electric motor ECU	5	- Torque sensor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	6	240		

Function	Potential Failure Mode	Potential Effect(s) of Failure	SEV	Class	Potential Cause(s) of Failure	OCC	Prevention Controls	Detection Controls	DET	RPN	Recommended Action	Responsibility & Target completion Date
(4) Provide assistance to reduce driver's steering efforts to levels that match the functional requirements of the vehicle			8		(4.1.4) Torque sensor cover assembly does not protect outboard housing assembly	5	- Torque sensor cover FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	6	240		
			10	YC	(4.1.5) Power supply harness does not supply required current to Electric motor	4	- Power Supply Harness FMEA	- Development test at vehicle level - Durability test at vehicle level	6	240		
			8		(4.1.6) Damage / wear of gear system	4	- Fatigue test at system level - Component DVP&R - Material Specification	- Development test at vehicle level - Durability test at vehicle level	4	128		
			8		(4.1.7) Stalled engine	5	- Component DVP&R (Engine)	- Development test at vehicle level - Durability test at vehicle level	6	240		
			8		(4.1.8) Connector / fittings /attachment failure	5	- Component DVP&R (Connectors)	- Development test at vehicle level - Durability test at vehicle level - Cold room vehicle testing	6	240		
	(4.2) Intermittent loss of power assist	(4.2.1) Uneven efforts	10		(4.2.1) Electric motor does not provide correct torque to Belt assembly	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	160		
		(4.2.2) Customer dissatisfaction	7		(4.2.2) Torque sensor provides unbalanced torque command	4	- Torque sensor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	5	140		
			7		(4.2.3) Torque sensor provides erratic torque command	4	- Torque sensor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	5	140		
			6		(4.2.4) Gear housing interferes with rack movement or misaligned Electric motor and ball nut assembly	4	- Ball nut assembly FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	96		
			7	YS	(4.2.5) Failure of steering wheel rotational sensor to send input signal to control module	4	- Component testing verification	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	5	140		
	(4.3) System provides more assistance than required	(4.3.1) System degradation	8		(4.3.1) Damage / wear of internal components	4	- Fatigue test at system level - Torque testing at system level	- Development test at vehicle level - Durability test at vehicle level	4	128		
		(4.3.2) Low steering efforts	6		(4.3.2) Torque sensor outputs incorrect torque command signal	4	- Torque Sensor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	5	120		
		(4.3.3) Customer dissatisfaction	6		(4.3.3) Electric motor provides incorrect torque to rack	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	96		
			7		(4.3.4) Torque sensor provides torque command opposite to driver input	4	- Torque Sensor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	5	140		

Function	Potential Failure Mode	Potential Effect(s) of Failure	SEV	Class	Potential Cause(s) of Failure	OCC	Prevention Controls	Detection Controls	DET	RPN	Recommended Action	Responsibility & Target completion Date
	(4.4) System provides less assistance than required	(4.4.1) Increased steering efforts	7		(4.4.1) Torque sensor outputs lower than required torque command signal	4	- Torque Sensor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	5	140		
		(4.4.2) Increased breaking efforts	6	4	(4.4.2) Electric motor provides lower than required torque to rack	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	96		
		(4.4.3 Degraded system function	10	YC	(4.4.3) Belt assembly foes not transmit all of torque from Electric motor to ball nut assembly	3	- Belt assembly FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	5	150		
		(4.4.4) Customer dissatisfaction	10	YC	(4.4.4) Rack and ball nut assembly internal component failure	3	- Rack and Ball nut assembly FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	120		
			10	YC	(4.4.5) Power supply harness does not supply required current to Electric motor	4	- Power Supply Harness FMEA	- Development test at vehicle level - Durability test at vehicle level	6	240		
			8		(4.4.6) Damage / wear of internal components	4	- Fatigue test at system level - Torque testing at system level	- Development test at vehicle level - Durability test at vehicle level	4	128		
	(5.1) Under assist at low speed only	(5.1.1) Steering efforts high	10	YC	(5.1.1) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Effort test at system level	4	160		
		(5.1.2) Customer discomfort	6		(5.1.2) Electric motor provides incorrect torque to belt assembly	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	96		
	(5.2) Under assist at high speed only	(5.2.1) Steering efforts high	10	YC	(5.2.1) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Effort test at system level	4	160		
		(5.2.2) Customer discomfort	6		(5.2.2) Electric motor provides incorrect torque to belt assembly	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	96		
	(5.3) Over assist at low speed only	(5.3.1) Steering efforts low	10	YC	(5.3.1) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Effort test at system level	4	160		
		(5.3.2) Customer discomfort	6		(5.3.2) Electric motor provides incorrect torque to belt assembly	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	96		
		(5.4.1) Steering efforts low	10	YC	(5.4.1) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Effort test at system level	4	160		

Function	Potential Failure Mode	Potential Effect(s) of Failure	SEV	Class	Potential Cause(s) of Failure	OCC	Prevention Controls	Detection Controls	DET	RPN	Recommended Action	Responsibility & Target completion Date
(5) Vary power assist with vehicle speed	(5.4) Over assist at high speed only	(5.4.2) Customer discomfort	6		(5.4.2) Electric motor provides incorrect torque to belt assembly	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	96		
	(5.5) Intermittent assistance during/after deceleration	(5.5.1) Steering efforts unpredictable	10	YC	(5.5.1) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Effort test at system level	4	160		
		(5.5.2) Customer dissatisfaction	6		(5.5.2) Electric motor provides incorrect torque to belt assembly	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	96		
	(5.6) Inconsistent assist at constant speed	(5.6.1) Steering efforts unpredictable	10	YC	(5.6.1) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Effort test at system level	4	160		
		(5.6.2) Customer dissatisfaction	6		(5.6.2) Electric motor provides incorrect torque to belt assembly	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	96		
	(5.7) Steering assist changes abruptly during acceleration & deceleration	(5.7.1) Steering efforts quick transition	10	YC	(5.7.1) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Effort test at system level	4	160		
		(5.7.2) Customer dissatisfaction	6		(5.7.2) Electric motor provides incorrect torque to belt assembly	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	96		
	(5.8) Under assist during evasive maneuvers	(5.8.1) Steering efforts high	10	YC	(5.8.1) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Effort test at system level	4	160		
		(5.8.2) Customer discomfort	6		(5.8.2) Electric motor provides incorrect torque to belt assembly	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	96		
	(5.9) Over assist during evasive maneuvers	(5.9.1) Steering efforts low	10	YC	(5.9.1) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Effort test at system level	4	160		
		(5.9.2) Customer discomfort	6		(5.9.2) Electric motor provides incorrect torque to belt assembly	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	96		
		(6.1.1) Customer dissatisfaction due	7		(6.1.1) Gear housing interfering with other adjacent components	4	- CAD	- Static clearance reviews - NVH testing at vehicle level	4	112		
			6		(6.1.2) Pinion assembly makes unwanted noise	4	- Pinion FMEA	- Durability test at vehicle level - NVH Testing at vehicle level	4	96		
			6		(6.1.3) Incorrect assembly at interface with I-shaft Incorrect assembly of boot allowing seal vibration	4	- Installation manual - GD&T	- Virtual design aid clearance check - Prototype build	4	96		

Function	Potential Failure Mode	Potential Effect(s) of Failure	SEV	Class	Potential Cause(s) of Failure	OCC	Prevention Controls	Detection Controls	DET	RPN	Recommended Action	Responsibility & Target completion Date
(6) Provide function under the NVH targets	(6.1) Does not meet / Intermittingly meets program targets	to noises Moan Whine Grunt Hiss Whistle Clonk Rattle ZIP noise Squeal Squeak	6	YS	(6.1.4) Inadequate isolation causing noise	4	- Component design validation - CAE	- Durability test at vehicle level - NVH Testing at vehicle level	5	120		
			6		(6.1.5) Improper assembly procedure followed	4	- Installation manual	- NVH Testing at vehicle level	4	96		
			6		(6.1.6) Improper pulley ratio causing moan	3	- CAE	- NVH Testing at vehicle level	4	72		
			4		(6.1.7) Engine idle speed and fluctuation causing noise	3	- CAE	- NVH Testing at vehicle level	4	48		
			6		(6.1.8) Roll restrictor design causing noise	3	- CAE	- NVH Testing at vehicle level	4	72		
			6		(6.1.9) Power steering lines causing squeal noise in engine compartment	3	- CAD - Installation manual	- NVH Testing at vehicle level	4	72		
			6		(6.1.10) Improper yoke clearance/ yoke spring load causing rattle	4	- Component design validation - Standards for Packaging Clearance	- Durability test at vehicle level	4	96		
		(6.1.2) Customer dissatisfaction due to vibrations Shudder Buzz/Grungy Wheel fight Nibble Steering wheel vibrations	6		(6.2.1) Pulley ratio causing vibration Pulley alignment	4	- CAE - Installation manual	- NVH Testing at vehicle level - Durability test at vehicle level	4	96		
			7	YS	(6.2.2) Large forcing function - Engine torque pulses causing vibration	5	- CAE - Insulation design	- NVH Testing at vehicle level - Durability test at vehicle level	5	175		
			6		(6.2.3) System components mis-assembled during production	4	- CAD - Installation manual	- CAD - Virtual builds - Prototype builds	4	96		
(7) Meet Electromagnetic Compatibility requirements (EMC)	(7.1) Interference with other systems, loss of function	(7.1.1) Degraded vehicle performance	10	YC	(7.1.1) Torque sensor signal interference by other vehicle systems	2	- Torque sensor FMEA - Electrical CAE	- EMC testing at Vehicle level - Electrical breadboard testing - Electrical Hardware design review	5	100		
		(7.1.2) Customer dissatisfaction										
	(7.2) Generates more than XX dBuV/m Function affected by XX dBuV/m	(7.2.1) Interference with other electronic equipment in vehicle Not immune to external EMC inputs Loss of function	10	YC	(7.2.1) Electric motor emissions exceed required levels	3	- Electric motor FMEA	- EMC testing at Vehicle level - Electrical breadboard testing - Electrical Hardware design review	5	150		
			10	YC	(7.2.2) Electric motor affected by XX dBuV/m of EMC	3	- Electric motor FMEA	- EMC testing at Vehicle level - Electrical breadboard testing - Electrical Hardware design review	5	150		
			10		(7.2.3) Sensors emits more than XX dBuV/m	2	- Sensor FMEA	- EMC testing at Vehicle level - Electrical breadboard testing - Electrical Hardware design review	5	100		
			10	YC	(7.2.4) Sensors shields does not provides enough isolation for incoming dBuV/m	2	- Sensor FMEA	- EMC testing at Vehicle level - Electrical breadboard testing - Electrical Hardware design review	5	100		
			10	YC	(7.2.4) Sensors shields does not provides enough isolation for outgoing dBuV/m	2	- Sensor FMEA	- EMC testing at Vehicle level - Electrical breadboard testing - Electrical Hardware design review	5	100		
	(7.3) EMC performance degrades over time	(7.3.1) Reduced immunity to external EMC. EMC interference with other electronic systems in vehicle over time	10	YC	(7.3.1) Electric Motor failure	4	- Electric motor FMEA	- EMC testing at Vehicle level - Electrical breadboard testing - Electrical Hardware design review	4	160		
			10	YC	(7.3.2) Electric harness loss of function	4	- Power Supply Harness FMEA	- EMC testing at Vehicle level - Electrical breadboard testing - Electrical Hardware design review	6	240		
		(7.4.1) Intermittent	10		(7.4.1) Motor intermittently emits excess EMC or is effected by EMC over time	2	- Electric motor FMEA	- EMC testing at Vehicle level - Electrical breadboard testing - Electrical Hardware design review	5	100		

Function	Potential Failure Mode	Potential Effect(s) of Failure	SEV	Class	Potential Cause(s) of Failure	OCC	Prevention Controls	Detection Controls	DET	RPN	Recommended Action	Responsibility & Target completion Date
	(7.4) Intermittently meets EMC performance	EMC interference with other electronic systems in vehicle. Not immune to external EMC. Intermittent function	10		(7.4.2) Steering Control Module (SCM) intermittently emits excess EMC or is effected by EMC over time	3	- SCM FMEA	- EMC testing at Vehicle level - Electrical breadboard testing - Electrical Hardware design review	5	150		
			10	YC	(7.4.3) Wiring harness intermittently emits excess EMC or picks up external EMC over time	4	- Power Supply Harness FMEA	- EMC testing at Vehicle level - Electrical breadboard testing - Electrical Hardware design review	6	240		
(8) Meet power consumption targets	(8.1) Power draw exceeds (XX) Amps	(8.1.1) Electric motor fuse blows deriving to manual steering efforts (loss of assist)	6		(8.1.1) Electric motor electric requirement is more that intended Loss of function of Electric motor	4	- Electric motor FMEA	- Electric draw testing at vehicle level - Electrical breadboard at system level	4	96		
	(8.2) Functional draw exceeds duty cycle specified amps	(8.2.1) Increased load on vehicle electrical system Decreased fuel economy Dimming lights Slow blower motor Degraded battery life Customer dissatisfaction	6		(8.2.1) Electric motor electric requirement is more that intended Loss of function of Electric motor	4	- Electric motor FMEA	- Electric draw testing at vehicle level - Electrical breadboard at system level	4	96		
	(8.3) Vehicle off current draws exceeds (XX) amps	(8.3.1) Drained battery	6		(8.3.1) Electric motor electric requirement is more that intended Loss of function of Electric motor	4	- Electric motor FMEA	- Electric draw testing at vehicle level - Electrical breadboard at system level	4	96		
	(8.4) Lock end stop current does not drop below (XX) amps after Y seconds	(8.4.1) Dropping of battery current	6		(8.4.1) Electric motor electric requirement is more that intended Loss of function of Electric motor	4	- Electric motor FMEA	- Electric draw testing at vehicle level - Electrical breadboard at system level	4	96		
(9) Position the inner and outer ball joint centers for correct suspension geometry	(9.1) Does not position Inner ball joint and Outer ball joint properly	(9.1.1) Degraded vehicle directional control	8		(9.1.1) Steering gear or linkage geometrical tolerances set incorrectly	4	- CAD - GD&T	- Development test at vehicle level - Durability test at vehicle level	4	128		
		(9.1.2) Degraded center feel	7	YS	(9.1.2) Torque of Outer ball joint lock nut not specified correctly	5	- Joint assembly studies - Fastener design validation	- Development test at vehicle level - Durability test at vehicle level	3	105		
		(9.1.3) Vehicle pulls/drifts	10	YC	(9.1.3) Corrosion	2	- Corrosion protection specification	- Salt spray testing	3	60		
		(9.1.4) Excessive tire wear	8		(9.1.4) Wear of components	4	- Material specification - Torque specification	- Fatigue test at system level - Durability test at vehicle level	4	128		
	(9.2) Does not maintain position during driving	(9.2.1) Degraded vehicle directional control	8	YS	(9.2.1) Insufficient stiffness of steering gear linkage	3	- Material specification	- Development test at vehicle level - Durability test at vehicle level	2	48		
		(9.2.2) Degraded center feel	7	YS	(9.2.2) Torque of Outer ball joint lock nut not specified correctly	5	- Joint assembly studies - Fastener design validation	- Development test at vehicle level - Durability test at vehicle level	3	105		
		(9.2.3) Vehicle pulls/drifts	10	YC	(9.2.3) Corrosion	2	- Corrosion protection specification	- Salt spray testing	3	60		
		(9.2.4) Excessive tire wear	8		(9.2.4) Wear of components	4	- Material specification - Torque specification	- Fatigue test at system level - Durability test at vehicle level	4	128		
(10) Position EPS system properly to ensure correct column routing and steering uniformity	(10.1) Does not position steering column coupling	(10.1.1) Excessive steering non-uniformity	7		(10.1.1) Incorrect position/orientation of input shaft end	3	- CAD - GD&T	- Development testing at vehicle level - Durability test at vehicle level - Service sign off	2	42		
	(10.2) Does not position steering column coupling with tolerances temporarily while driving	(10.1.2) Degraded center feel	8	YS	(10.2.1) Insufficient input shaft bending stiffness	3	- Material specification - CAE - GD&T	- Development testing at vehicle level - Durability test at vehicle level - Service sign off	2	48		
		(10.1.3) Steering wheel position not centered	6		(10.2.2) Connection to extension shaft twisted	2	- Installation manual	- Development testing at vehicle level - Prototype build at vehicle level	2	24		
		(10.1.4) Squeeze noise from floor seal										

Subsystem	Electric Power Steering Gear	Responsible	Rodrigo Sotomayor	FMEA ID	Software FMEA
Model	2017 -X	Prepared by	Rodrigo Sotomayor	FMEA date	9/1/2014

Function	Potential Failure Mode	Potential Effects of Failure	SEV	Class	Potential Cause	OCC	Prevention Controls	Detection Controls	DET	RPN	Recommended Action	Responsibility & Target completion Date
(1) Provide damping to isolate the driver from road harshness and driveline input	(1.1) Insufficient damping	(1.1.1) Wheel fight / nibble	6	YS	(1.1.1) Electric motor failure	5	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level	5	150		
		(1.1.2) Customer dissatisfaction	6	YS	(1.1.2) Torque sensor provides wrong torque command	3	- Sensor FMEA	- Development test at vehicle level - Durability test at vehicle level	5	90		
			6	YS	(1.1.3) Electric Motor provides lower than required torque to belt assembly	5	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level	5	150		
	(1.2) Excessive damping	(1.2.1) Degraded center feel	10	YC	(1.2.4) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level	4	160		
		(1.2.2) Customer dissatisfaction	7	YS	(1.2.5) Torque sensor provides wrong torque command	3	- Sensor FMEA	- Development test at vehicle level - Durability test at vehicle level	5	105		
			6	4	(1.2.6) Electric Motor provides lower than required torque to belt assembly	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level	4	96		
(2) Provide assistance to	(2.1) No assistance provided by software - Full loss of power assist	(2.1.1) Increased steering efforts due to complete loss of power assist	8		(2.1.1) Incorrect thresholds values set for assistance curve	4	- Calibration testing at system level - Calibration testing at vehicle level	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	3	96		
		(2.1.2) Increased brake effort due to complete loss of power assist to the boost system	8		(2.1.2) Torque sensor does not provide torque measurement to Electric motor SCM	3	- Torque sensor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	3	72		
		(2.1.3) Customer dissatisfaction	8		(2.1.3) Steering Wheel angle sensor does not provide angle change to SCM	3	- Steering Wheel Angle sensor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	3	72		
	(2.2) Intermittent loss of power assist	(2.2.1) Uneven efforts	10	YC	(2.2.1) Electric motor does not provide correct torque to Belt assembly	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	5	200		
		(2.2.2) Customer dissatisfaction	7	YS	(2.2.2) Torque sensor provides unbalanced torque command	3	- Torque sensor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	5	105		
			7	YS	(2.2.3) Torque sensor provides erratic torque command	3	- Torque sensor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	5	105		
			6	YS	(2.2.4) Steering wheel angle sensor does not send input signal to control module	3	- Component testing verification	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	5	90		

Function	Potential Failure Mode	Potential Effects of Failure	SEV	Class	Potential Cause	OCC	Prevention Controls	Detection Controls	DET	RPN	Recommended Action	Responsibility & Target completion Date
assistance to reduce driver's steering efforts to levels that match the functional requirements of the vehicle	(2.3) System provides more assistance than required	(2.3.1) System degradation	6		(2.3.1) Incorrect or no signal provided of vehicle speed	4	- Redundancy - Inform user/governing module lack of signal	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	96		
		(2.3.2) Low steering efforts	6		(2.3.2) Torque sensor outputs incorrect torque command signal	4	- Torque Sensor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	96		
		(2.3.3) Customer dissatisfaction	6		(2.3.3) Electric motor provides incorrect torque to rack	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	96		
			8		(2.3.4) Torque sensor provides torque command opposite to driver input	4	- Torque Sensor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	128		
	(2.4) System provides less assistance than required	(2.4.1) Increased steering efforts	6		(2.4.1) Torque sensor outputs lower than required torque command signal	4	- Torque Sensor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	96		
		(2.4.2) Increased breaking efforts	6		(2.4.2) Electric motor provides lower than required torque to rack	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	96		
		(2.4.3 Degraded system function	5		(2.4.3) Belt assembly foes not transmit all of torque from Electric motor to ball nut assembly	4	- Belt assembly FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	80		
		(2.4.4) Customer dissatisfaction	5		(2.4.4) Incorrect or no signal provided of vehicle speed	4	- Redundancy - Inform user/governing module lack of signal	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	80		
	(3.1) Under assist at low speed only	(3.1.1) Steering efforts high	10	YC	(3.1.1) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Effort test at system level	4	160		
		(3.1.2) Customer discomfort	6		(3.1.2) Electric motor provides incorrect torque to belt assembly	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	96		
			7		(3.1.3) Incorrect module command (too high)	3	- Electric breadboard testing at system level - Calibration settings	- Development test at vehicle level - Durability test at vehicle level - SW testing	5	105		

Function	Potential Failure Mode	Potential Effects of Failure	SEV	Class	Potential Cause	OCC	Prevention Controls	Detection Controls	DET	RPN	Recommended Action	Responsibility & Target completion Date
(3) Vary power assist with vehicle speed	(3.2) Under assist at high speed only	(3.2.1) Steering efforts high	6		(3.2.1) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Effort test at system level	4	96		
		(3.2.2) Customer discomfort	6		(3.2.2) Electric motor provides incorrect torque to belt assembly	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	96		
			6		(3.2.3) Incorrect module command (too low)	4	- Electric breadboard testing at system level - Calibration settings	- Development test at vehicle level - Durability test at vehicle level - SW testing	3	72		
	(3.3) Over assist at low speed only	(3.3.1) Low Steering effort	6		(3.3.1) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Effort test at system level	3	72		
		(3.3.2) Customer discomfort	6		(3.3.2) Electric motor provides incorrect torque to belt assembly	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	96		
			6		(3.3.3) Incorrect module command (too low)	4	- Electric breadboard testing at system level - Calibration settings	- Development test at vehicle level - Durability test at vehicle level - SW testing	4	96		
	(3.4) Over assist at high speed only	(3.4.1) Steering efforts low	6		(3.4.1) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Effort test at system level	4	96		
		(3.4.2) Customer discomfort	6		(3.4.2) Electric motor provides incorrect torque to belt assembly	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	96		
			6		(3.4.3) Incorrect module command (too low)	4	- Electric breadboard testing at system level - Calibration settings	- Development test at vehicle level - Durability test at vehicle level - SW testing	4	96		
	(3.5) Intermittent assistance during/after deceleration	(3.5.1) Steering efforts unpredictable	7		(3.5.1) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Effort test at system level	6	168		
		(3.5.2) Customer dissatisfaction	8		(3.5.2) Electric motor provides incorrect torque to belt assembly	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	5	160		
			8		(3.5.3) Incorrect vehicle signal (too high)	4	- Electric breadboard testing at system level - Calibration settings	- Development test at vehicle level - Durability test at vehicle level - SW testing	5	160		
		(3.6.1) Steering efforts unpredictable	8		(3.6.1) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Effort test at system level	5	160		

Function	Potential Failure Mode	Potential Effects of Failure	SEV	Class	Potential Cause	OCC	Prevention Controls	Detection Controls	DET	RPN	Recommended Action	Responsibility & Target completion Date
	(3.6) Inconsistent assist at constant speed	(3.6.2) Customer dissatisfaction	8		(3.6.2) Electric motor provides incorrect torque to belt assembly	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	5	160		
			8		(3.6.3) Incorrect module command	4	- Electric breadboard testing at system level - Calibration settings	- Development test at vehicle level - Durability test at vehicle level - SW testing	5	160		
	(3.7) Steering assist changes abruptly during acceleration & deceleration	(3.7.1) Steering efforts quick transition	8		(3.7.1) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Effort test at system level	5	160		
		(3.7.2) Customer dissatisfaction	8		(3.7.2) Electric motor provides incorrect torque to belt assembly	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	5	160		
			8		(3.7.3) Incorrect vehicle signal	4	- Electric breadboard testing at system level - Calibration settings	- Development test at vehicle level - Durability test at vehicle level - SW testing	5	160		
	(3.8) Under assist during evasive maneuvers	(3.8.1) Steering efforts high	8	YS	(3.8.1) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Effort test at system level	5	160		
		(3.8.2) Customer discomfort	8		(3.8.2) Electric motor provides incorrect torque to belt assembly	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	128		
	(3.9) Over assist during evasive maneuvers	(3.9.1) Steering efforts low	8		(3.9.1) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Effort test at system level	5	160		
		(3.9.2) Customer discomfort	6	4	(3.9.2) Electric motor provides incorrect torque to belt assembly	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	96		
	(3.10) Steering assist increases & decreases quickly and unpredictably	(3.10.1) Steering efforts unpredictable	10	YC	(3.10.1) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Effort test at system level	5	200		
		(3.10.2) Customer discomfort	6		(3.10.2) Electric motor provides incorrect torque to belt assembly	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	4	96		
			6		(3.10.3) Incorrect vehicle signal	4	- Electric breadboard testing at system level - Calibration settings	- Development test at vehicle level - Durability test at vehicle level - SW testing	4	96		

Function	Potential Failure Mode	Potential Effects of Failure	SEV	Class	Potential Cause	OCC	Prevention Controls	Detection Controls	DET	RPN	Recommended Action	Responsibility & Target completion Date
(4) Allow service of the system	(4.1) Not being able to service steering system components	(4.1.1) Degradation of system function	5	YS	(4.1.1) System does not allow for display codes when an error state occurs	4	- SCM FMEA	- Development test at vehicle level - Durability test at vehicle level	5	100		
		(4.1.2) Customer dissatisfaction (4.1.3) Increased maintenance cost	5	YS	(4.1.2) System does not allow for codes to be stored	4	- SCM FMEA	- Development test at vehicle level - Durability test at vehicle level	5	100		
	(4.2) Does not communicate with generic diagnostic tool	(4.2.1) Increased cost of diagnostics and ownership (4.2.2) Customer dissatisfaction	5	YS	(4.2.1) Software installed incorrectly or corrupted	4	- SCM FMEA	- Servie evaluation and sign off at vehicle level	5	100		
		(4.2.3) Vehicle being used in public roads when there is a service concern	5	YS	(4.2.2) Latest Software level not installed	4	- Electric motor FMEA	- Servie evaluation and sign off at vehicle level	5	100		
(5) Provide electrical signals to other system	(5.1) Does not transmit steering wheel position	(5.1.1) Degraded vehicle directional control	8	YC	(5.1.1) SCM does not transmit steering wheel position over vehicle network	5	- Electric motor FMEA	- Electric hardware design review at system level -Software design review - Electrical breadboard testing at system level - Communication testing at vehicle level	6	240		
		(5.1.2) Brake system does not receive relative steering wheel position										
		(5.1.3) Reduced functionality of vehicle										
	(5.2) Steering wheel position is intermittently transmitted	(5.2.1) Degraded vehicle directional control	8		(5.2.1) SCM failure	5	- SCM FMEA	- Electric hardware design review at system level -Software design review - Electrical breadboard testing at system level - Communication testing at vehicle level	5	200		
		(5.2.2) Brake system does not receive relative steering wheel position										
		(5.2.3) Reduced functionality of vehicle										
	(5.3) Steering wheel position is transmitted incorrectly	(5.3.1) Brake system performance is degraded	8		(5.3.1) SCM transmits erroneous signal with indication that ABS signal is valid	4	- SCM FMEA	- Electric hardware design review at system level -Software design review - Electrical breadboard testing at system level - Communication testing at vehicle level	4	128		
		(5.3.2) Brake system does not receive relative steering wheel position										
		(5.3.3) Reduced functionality of vehicle										
	(6.1) Does not detects high friction condition	(6.1.1) High efforts to steer to driver	6		(6.1.1) Thresholds set too low	2	- Road load calculations	- Development testing at vehicle level - Fatigue test at system level	3	36		
		(6.1.2) Premature ware of components	6		(6.1.2) Road friction coefficient is too low	2	- Road load calculations	- Development testing at vehicle level	3	36		
		(6.1.3) Customer dissatisfaction	6		(6.1.3) Vehicle characteristic changes (installation of out-of-spec tires, changes in GVW, modification to vehicle)	2	- Include aftermarket variants in development and testing - CAE	- Development testing at vehicle level	3	36		
			6		(6.1.4) Steering wheel position variability larger than set tolerances	2	- Determination of function characteristic of steering wheel - Variation stack up study	- Development testing at vehicle level	3	36		
			6		(6.1.5) Vehicle speed variability larger than tolerances	2	- Variation stack up study	- Development testing at vehicle level	3	36		
			6		(6.1.6) Assist torque variability larger than tolerances	2	- Variation stack up study	- Development testing at vehicle level	3	36		
			6		(6.1.7) Impact events	4		- Software validation - Development testing at vehicle level	4	96		
			6		(6.1.8) Internal Electric motor events	2	- Electric motor FMEA	- Software validation - Development testing at vehicle level	4	48		

Function	Potential Failure Mode	Potential Effects of Failure	SEV	Class	Potential Cause	OCC	Prevention Controls	Detection Controls	DET	RPN	Recommended Action	Responsibility & Target completion Date
(6) Diagnose high friction condition in system			6		(6.1.9) Aggressive driving (delay in friction calculation time)	2		- Software validation - Development testing at vehicle level	4	48		
			6		(6.1.10) Variable friction coefficient driving surfaces	2	- Communication with other modules to determine if variable friction coefficient exists - Limit friction calculation when such condition exists	- Software validation - Development testing at vehicle level	4	48		
	(6.2) Detects high friction condition incorrectly (false high friction)	(6.2.1) Warns the driver when there is no fault	6		(6.2.1) Thresholds set too high	2	- Road load calculations	- Development testing at vehicle level - Fatigue test at system level	3	36		
		(6.2.1) Customer dissatisfaction	6		(6.2.2) Road friction coefficient is too high	3	- Road load calculations	- Development testing at vehicle level	4	72		
		(6.2.3) Higher maintenance cost	4		(6.2.3) Vehicle characteristic changes (installation of out-of-spec tires, changes in GVW, modification to vehicle)	3	- Include aftermarket variants in development and testing - CAE	- Development testing at vehicle level	4	48		
			6		(6.2.4) Steering wheel position variability larger than set tolerances	2	- Determination of function characteristic of steering wheel - Variation stack up study	- Development testing at vehicle level	4	48		
			5		(6.2.5) Vehicle speed variability larger than tolerances	2	- Variation stack up study	- Development testing at vehicle level	4	40		
			6		(6.2.6) Assist torque variability larger than tolerances	2	- Variation stack up study	- Development testing at vehicle level	4	48		
			4		(6.2.7) Cold temperature temporarily cause a different friction calculation	2	- CAE	- Development testing at vehicle level	4	32		
			4		(6.2.8) Variable friction coefficient driving surfaces	2	- Communication with other modules to determine if variable friction coefficient exists - Limit friction calculation when such condition exists	- Software validation - Development testing at vehicle level	4	32		
			6		(6.2.9) Internal Electric motor events	4	- Electric motor FMEA	- Software validation - Development testing at vehicle level	4	96		
	(6.3) Detects high friction condition intermittently	(6.3.1) Driver may be confused by chime and message in cluster	6		(6.3.1) Internal Electric motor events	4	- Electric motor FMEA	- Software validation - Development testing at vehicle level	4	96		
		(6.3.2) Driver may learn to drive under high friction condition	4		(6.3.2) Unwanted interaction with other system signal	4	- Electric Breadboard testing at system level	- Software validation - Development testing at vehicle level	5	80		
		(6.3.3) Premature ware of system components	6		(6.3.4) Steering wheel position variability larger than set tolerances	4	- Determination of function characteristic of steering wheel - Variation stack up study	- Development testing at vehicle level	5	120		
		(6.3.4) Increased maintenance cost of vehicle	4		(6.3.5) Vehicle speed variability larger than tolerances	4	- Variation stack up study	- Development testing at vehicle level	4	64		
			4		(6.3.6) Assist torque variability larger than tolerances	4	- Variation stack up study	- Development testing at vehicle level	4	64		
(7) Transfer diver input	(7.1) EPS does not convert angular displacement/torque to linear displacement/force	(7.1.1) Unable to control direction of vehicle	10	YC	(7.1.1) Electric motor does not allow rotation of input shaft when commanded by driver	3	- Electric motor FMEA	- Durability test at vehicle level - Electrical hardware design review -Electrical CAE at vehicle level	5	150		
		(7.1.2) Customer dissatisfaction										
		(7.1.3) Driver input is not enough to turn EPS input shaft										
	(7.2) Convert angular displacement to linear displacement and force intermittently	(7.2.1) Vehicle response inconsistent (non-linear)	6		(7.2.1) Electric motor does not allow rotation of input shaft when commanded by driver	4	- Electric motor FMEA	- Durability test at vehicle level - Electrical hardware design review -Electrical CAE at vehicle level	5	120		
		(7.2.2) Degraded vehicle control										
		(7.2.3) Damage to contiguous components										

Function	Potential Failure Mode	Potential Effects of Failure	SEV	Class	Potential Cause	OCC	Prevention Controls	Detection Controls	DET	RPN	Recommended Action	Responsibility & Target completion Date
driver input (torque and angular displacement) to linear displacement and force to knuckle assembly		(7.2.4) Blocked system relative to steering wheel position										
		(7.2.5) Customer dissatisfaction										
	(7.3) Degraded conversion of angular displacement to linear displacement Single-sided disconnect - directional control	(7.3.1) Degraded vehicle directional control	8		(7.3.2) Position of Torque sensor moves rack in wrong direction	4	- Torque Sensor FMEA	- Development test at vehicle level - Package Design Review	4	128		
		(7.3.2) Degraded center feel										
		(7.3.3) Excessive tire wear										
		(7.3.4) Vehicle pulls/drifts										
	(7.4) Degraded conversion of input torque to linear force. (excessive friction)	(7.4.1) No self centering	6		(7.4.1) Electric motor does not allow rotation of input shaft when commanded by driver	4	- Electric motor FMEA	- Durability test at vehicle level - Electrical hardware design review -Electrical CAE at vehicle level	5	120		
		(7.4.2) No road feedback										
		(7.4.3) Degraded center feel										
		(7.4.4) Increased efforts	8		(7.4.2) Torque Sensor + IPA Assembly moves rack in wrong direction	3	- Torque Sensor FMEA	- Development test at vehicle level - Durability test at vehicle level	4	96		
		(7.4.5) Steering in wrong direction										
(8) Convert linear displacement/force of the knuckle arms to angular displacement/torque of the steering column to provide feedback from road to driver and allow self centering of the steering	(8.1) Does not provide feedback from knuckle	(8.1.1) No road feedback	4		(8.1.1) Excessive steering system dampening	3	- Tuning development at component level	- Development test at vehicle level - Durability test at vehicle level	3	36		
		(8.1.2) Driver requires to provide force to recover from turn	8		(8.1.2) Electric motor failure	3	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level	3	72		
		(8.1.3) No self-centering										
		(8.1.4) Degraded system function										
		(8.1.5) Customer dissatisfaction										
	(8.2) Degraded / non-linear / uneven conversion of linear force to torque	(8.2.1) No or slow self-centering	4		(8.2.1) Excessive steering system dampening	3	- Tuning development at component level	- Development test at vehicle level - Durability test at vehicle level	2	24		
		(8.2.2) Degraded road feedback / center feel	8		(8.2.2) Electric motor failure	3	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level	2	48		
		(8.2.3) Degraded system function										
		(8.2.4) Driver requires to provide force to recover from turn										
		(8.2.5) Customer dissatisfaction										
	(8.3) EPS does not self return	(8.3.1) Driver requires to provide force to recover from turn	8		(8.3.1) Electric motor failure	4	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level	3	96		
		(8.3.2) Customer dissatisfaction										
	(8.4) EPS self return slowly	(8.4.1) Driver requires to provide force to recover from turn	8		(8.4.1) Electric motor failure	2	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level	3	48		
		(8.4.2) Customer dissatisfaction										
	(8.5) EPS self return too fast	(8.5.1) customer dissatisfaction	8		(8.5.1) Electric motor failure	2	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level	3	48		
	(8.6) Excessive feedback from knuckle (nibble & wheel fight)	(8.6.1) Wheel fight / nibble	8		(8.6.1) Electric motor failure	2	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level	3	48		
		(8.6.2) Customer dissatisfaction										
		(8.6.3) Degraded road feedback										

Function	Potential Failure Mode	Potential Effects of Failure	SEV	Class	Potential Cause	OCC	Prevention Controls	Detection Controls	DET	RPN	Recommended Action	Responsibility & Target completion Date
(9) Provide function under the NVH targets	(9.1) Does not meet / Intermittingly meets program targets	(9.1.1) Customer dissatisfaction due to noises Moan Whine Grunt Hiss Whistle Clonk Rattle ZIP noise Squeal Squeak	8	YS	(9.1.1) Wrong controlling of the Electronic motor module	4	- Electric motor FMEA	- NVH testing at vehicle level	5	160		
		(9.1.2) Customer dissatisfaction due to vibrations Shudder Buzz/Grungy Wheel fight Nibble Steering wheel vibrations	8	YS	(9.2.1) Wrong controlling of the Electronic motor module	4	- Electric motor FMEA	- NVH testing at vehicle level	5	160		
(10) Meet power consumption targets	(10.1) Vehicle off current draws exceeds (XX) amps	(10.1.1) Drained battery	10	YC	(10.1.1) Electric motor failure	4	- Electric motor FMEA	- Electric draw testing at vehicle level - Electrical breadboard at system level	5	200		