FUNCTIONAL SAFETY MODEL FOR E/E COMPONENT OF AN AUTONOMOUS VEHICLE

by

Mukul Anil Gosavi

A thesis submitted to the faculty of
The University of North Carolina at Charlotte
in partial fulfillment of the requirements
for the degree of Master of Science in
Electrical Engineering

Charlotte

2018

Approved by:

_____

Dr. James M. Conrad

_____

Dr. Ronald Sass

_____

Dr. Arun Ravindran

ABSTRACT

MUKUL ANIL GOSAVI. Functional Safety Model for E/E component of an Autonomous Vehicle. (Under the direction of DR. JAMES M. CONRAD)

Currently there is extensive research and investment in safety technologies, such as Advanced Driver Assistance Systems (ADAS) for enabling road vehicles to become intelligent and safer, thus making them detect and prevent possible accidents, assist the driver in changing lanes efficiently and making more accurate turns. Almost every automotive company is researching and developing autonomous vehicles. This huge amount of investment in terms of money and efforts might soon make self-driving vehicles a reality and consumers might start seeing autonomous and non-autonomous vehicles running together on the road. Along with the functional benefits of these autonomous vehicles, some new risks are also introduced into the vehicle and road safety. The ISO 26262 standard deals with the functional safety of the Electric and Electronic (E/E) components of a road vehicle. As of now, there is no such standard that directly applies to the functional safety of autonomous vehicles and hence, many researchers have tried to use this ISO 26262 standard as a guideline for developing software/hardware models for making autonomous vehicles compatible to the functional safety standards.

This thesis conducts a survey of techniques used by different authors in order to develop architectural models for E/E components of vehicles that comply with functional safety standards and can be integrated in autonomous vehicles. This thesis uses the knowledge gathered from the survey to design a method to incorporate functional safety concept into the Intelligent Transportation System (ITS) project that has been developed by UNC Charlotte.

ACKNOWLEDGEMENTS

I would like to take this opportunity to express my gratitude and thank my advisor Dr. James M. Conrad. Without his guidance and support, the successful completion of this thesis would not have been possible. I would also like to thank committee members, Dr. Ronald Sass and Dr. Arun Ravindran for their insights and support. Also, I want to thank all the faculty members of Electrical and Computer Engineering Department for helping me throughout my Master's program at University of North Carolina at Charlotte.

I would like to specially thank Dr. Benjamin B. Rhoades who has helped me technically throughout this thesis. I would like to express my sincere appreciation and thank all the new and existing members of the Embedded and Robotics lab, especially Aishwarya and Jaydeep for their support.

I want to thank my mother Ashwini, who has been the main source of my inspiration throughout the journey of becoming an Engineer. I want to thank my father Anil and uncle Sunil for supporting me emotionally and financially. Lastly, I want to thank all members of the Gosavi and the Desai family for believing in me and standing beside me in hard times.

This thesis is dedicated to the memory of my maternal uncle Nandkishor S. Desai.

TABLE OF CONTENTS

LIST OF FIGURES viii

LIST OF TABLES x

LIST OF ABBREVIATIONS xi

CHAPTER 1: INTRODUCTION 1

1.1. Motivation 1

1.2. Functional Safety in Automotive and Author's Related Work 2

1.3. Completed Thesis Work 3

1.4. Organization 4

CHAPTER 2: ISO 26262: FUNCTIONAL SAFETY STANDARD FOR ROAD VEHICLES 6

2.1. Introduction to ISO 26262 6

2.2. Survey of Existing Methods 9

2.2.1. The Autonomous Vehicle Control (AVC) Module Strategy: Architectural Level Approach 9

2.2.2. Designing Safe and Secure Autopilot 11

2.2.3. Integrated Approach for Tackling Functional Safety and Cybersecurity 13

2.3. Why Present Functional Safety Standards are Not Enough 14

CHAPTER 3: SAFETY ANALYSIS PROCEDURE 17

3.1. V-Model of Automotive Product Development Cycle 17

3.1.1. System Engineering Process Group (SYS) 17

3.1.2. Software Engineering Process Group (SWE) 20

3.2. Hazard Analysis and Risk Assessment 22

3.2.1. Initiation of the HARA 23

3.2.2. Situation Analysis and Hazard Identification 23

3.2.3. Classification of Hazardous Event 24

3.2.4. Determination of ASIL and Safety Goals 26

3.2.5. Verification 26

3.3. Functional Safety Concept 26

3.3.1. Derivation of Functional Safety Requirements 27

3.3.2. Allocation of Functional Safety Requirements 28

3.3.3. Safety Concept Validation 28

3.3.4. Safety Concept Verification 29

3.4. Product Development at System Level 29

3.4.1. Initiation 29

3.4.2. Specification of the Technical Safety Requirements 29

3.4.3. System Design 30

3.4.4. Item Integration and Testing 31

3.4.5. Safety Validation 31

3.4.6. Functional Safety Assessment 31

3.5. Product Development at Software Level 31

3.5.1. Initiation 32

3.5.2. Specification of Software Safety Requirements 33

3.5.3. Software Architectural Design 33

3.5.4. Software Unit Design and Implementation 33

3.5.5. Software Unit Testing 34

3.5.6. Software Integration and Testing 34

3.5.7. Verification of Software Safety Requirements 35

CHAPTER 4: FUNCTIONAL SAFETY ANALYSIS: COMMUNICATION MODULE 36

4.1. Components of Intelligent Transportation System 36

4.1.1. Vehicle Partition 36

4.1.2. Infrastructure Partition 38

4.2. Functional Safety Analysis of the Vehicle Partition of the ITS Module 39

4.2.1. Assumptions 40

4.2.2. HARA of Vehicle Classification and Vehicle Telemetry module 42

4.2.3. ASIL Assignment 53

4.2.4. Defining Safety Goals 54

4.2.5. Defining Functional Safety Requirements 55

4.2.6. Defining Technical Safety Requirements 56

CHAPTER 5: RESULTS 62

5.1. Safety concept application for speed hazard 63

CHAPTER 6: CONCLUSIONS AND FUTURE SCOPE 70

6.1. Conclusions 70

6.2. Future Scope 71

REFERENCES 73

LIST OF FIGURES

FIGURE 2.1: Relation of IEC 61508 with ISO 26262 7

FIGURE 2.2: Safety Lifecycle as Viewed by ISO 26262 8

FIGURE 2.3: High Level AVC Module Structure 10

FIGURE 2.4: Autopilot Item Definition as per ISO 26262 12

FIGURE 2.5: Static Defense Layers of ESCL System 15

FIGURE 3.1: V-Model for Automotive Product Development 18

FIGURE 3.2: V-Model: Engineering Processes of Product Development 20

FIGURE 3.3: Hierarchy of Safety Goals and Functional Safety Requirements 28

FIGURE 3.4: Reference Phase Model for the Development of a Safety Related Item 32

FIGURE 3.5: Reference Phase Model for the Software Development 35

FIGURE 4.1: Components of an Intelligent Transportation System (ITS) 36

FIGURE 4.2: ELM327 Bluetooth Dongle for OBDII Port 37

FIGURE 4.3: ITS Framework Flowchart (ITS) 40

FIGURE 4.4: Steps for Performing of Safety Analysis of an E/E Component 41

FIGURE 4.5: Legend for components of potential collision scenario diagram 44

FIGURE 4.6: VIN Hazard 03 Scenario for Vehicle Behind the Host Vehicle 46

FIGURE 4.7: VIN Hazard 03 Scenario for Vehicle In Front the Host Vehicle 46

FIGURE 4.8: VIN Hazard 04 Scenario for Vehicle Behind the Host Vehicle 47

FIGURE 4.9: VIN Hazard 04 Scenario for Vehicle In Front the Host Vehicle 47

FIGURE 4.10: Potential Collision Scenario Caused when Transmitted Speed is Less than Actual Speed 52

FIGURE 4.11: Potential Collision Scenario Caused when Transmitted Speed is More than Actual Speed 53

FIGURE 4.12: High Level Block Diagram 57

FIGURE 5.1: Potential Collision Scenario Caused when Transmitted Speed is Less than Actual Speed 64

FIGURE 5.2: Potential Collision Scenario Caused when Transmitted Speed is Less than Actual Speed 65

FIGURE 5.3: Potential Collision Scenario Caused when Transmitted Speed is Less than Actual Speed 66

FIGURE 5.4: Potential Collision Scenario Caused when Transmitted Speed is Less than Actual Speed 67

FIGURE 5.5: Potential Collision Scenario Caused when Transmitted Speed is Less than Actual Speed 68

FIGURE 5.6: Potential Collision Scenario Caused when Transmitted Speed is Less than Actual Speed 69

LIST OF TABLES

TABLE 2.1: Vehicular safety / cybersecurity requirements analysis terms 13

TABLE 3.1: Classes of Severity 24

TABLE 3.2: Classes of Probability of Exposure 25

TABLE 3.3: Classes of Controllability 25

TABLE 3.4: ASIL determination 27

TABLE 4.1: Vehicle Characterization and Classification 43

TABLE 4.2: Hazard Analysis and Risk Assessment (HARA) for VIN Transmission Function Part A 48

TABLE 4.3: Hazard Analysis and Risk Assessment (HARA) for VIN Transmission Function Part B 49

TABLE 4.4: Hazard Analysis and Risk Assessment (HARA) for Transmission of Relative Speed Function Part A 60

TABLE 4.5: Hazard Analysis and Risk Assessment (HARA) for Transmission of Relative Speed Function Part B 61

LIST OF ABBREVIATIONS

ADAS	Advanced Driver Assistant Systems.
ASIL	Automotive Safety and Integrity Level.
ATC	Automatic Train Control.
ATO	Automatic Train Operation.
ATP	Automatic Train Protection.
ATS	Automatic Train Supervision.
AutoDL	Automotive Defense Level.
AUTOSAR	Automotive Open system Architecture.
AVC	Autonomous Vehicle Control.
AVO	Autonomous Vehicle Operation.
AVP	Autonomous Vehicle Protection.
BCM	Body Control Module.
CPS	Cyber Physical Systems.
E/E	Electric and Electronic.
ECU	Electronic Controller Unit.
ESCL	Electronic Steering Column Lock.
FLD	Fuel Level Display.
FMEA	Failures Modes and Effects Analysis.
FSR	Functional Safety Requirement.
GPS	Global Positioning System.
HARA	Hazard Analysis and Risk Assessment.
HIL	Hardware-In-the-Loop.
IEC	International Electrotechnical Commision.
IOT	Internet of Things.

ISO	International Organization for Standardization.
ITS	Intelligent Transportation System.
MIL	Model-In-the-Loop.
OBD	On-Board Diagnostic.
OBU	On-Board Unit.
PIL	Processor-In-the-Loop.
QM	Quality Management.
RSU	Road-Side Unit.
SecL	Security Level.
SIL	Software-In-the-Loop.
SWE	Software Engineering Process Group.
SYS	System Engineering Process Group.
TARA	Threat Analysis and Risk Assessment.
TSR	Technical Safety Requirement.
V2I	Vehicle-to-Infrastructure.
V2V	Vehicle-to-Vehicle.
VIN	Vehicle Identification Number.
WHO	World Health Organization.
WMI	World Manufacturer Identifier.

CHAPTER 1: INTRODUCTION

1.1 Motivation

According to the World Health Organization (WHO) "1.2 million people die each year on the world's roads, with millions more sustaining serious injuries and living with long-term adverse health consequences. Globally, road traffic crashes are a leading cause of death among young people, and the main cause of death among those aged 15-29 years [1]". Therefore, road and vehicle safety plays an important role in the automotive product development cycle. IEC 61508 defines Safety as "the freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or the environment [2]".

Many Electric and Electronic (E/E) components have been introduced in automobiles which has led to an increase in the amount of software needed to operate them. It is observed that, in recent years, software costs in cars will increase exponentially aligned with the amount of software enabled features [3]. A modern day premium car might consist of up to 90 Electronic Control Units (ECUs), 11 communication networks and might execute up to 1,000,000 Lines Of Code [4]. This increases the software complexity and with it the probability of failures. The task of verifying software to detect failures is thus becoming more and more difficult, time consuming and critical [5]. There are many similar problems faced by developers while developing software in automotive domain. More details about these problems can be found in [3].

IEC 61508 defines Functional Safety as "a subset of the overall vehicle safety that depends on a system or equipment operating correctly in response to its inputs [2]". Failure of even one of the various components inside an automobile is a major issue

as the life of the driver, passengers or pedestrians might be endangered because of it. For example, the sudden failure of headlamps when the car is in motion during night time might cause an accident. Therefore, one must ensure that these components are failsafe. ISO 26262 - "Road Vehicles - Functional Safety" is a standard for automotive industry, designed to prevent failure or malfunction of E/E components in a car.

With the introduction of various intelligent systems inside a road vehicle like advanced driver assistance systems (ADAS), we are transitioning from non-autonomous to semi- and eventually fully-autonomous vehicles. Soon we can expect to see vehicles with some level of autonomy running on the roads along with non-autonomous vehicles. This will increase the possibility of hazards and risks that can affect safety of the driver and vehicle. Unlike ISO 26262 there is no dedicated standard specially derived for autonomous vehicles / components. Therefore, it is essential to address the challenges faced while ensuring functional safety of the E/E components of any level of autonomous vehicle.

1.2 Functional Safety in Automotive and Author's Related Work

The V-model for product development is used extensively in the automotive industry. The product development cycle includes requirement elicitation, system architectural design, software design, implementation, verification test, integration, test and validation. However, there is a safety centric process that runs in parallel with the product development cycle: functional safety analysis, concept development and integration with the software requirements. The functional safety concept is developed to ensure that the component continues to work safely in the normal state of operation as well as in the state of failure.

The functional safety manager is responsible for carrying out the analysis. The responsibilities of a functional safety manager include identifying the importance of safety in different elements, carrying out the hazard analysis and risk assessment of the element, setting the requirements and establishing the necessary assurance for

safety of that element. An extension to the original ISO 26262 model that can be used to define safety concept for multiple vehicles has been proposed in this work. The end product of this thesis are the requirements that need to be incorporated in the models by their respective developer while using ITS on the road. These requirements need to be translated into software requirements later when an automotive original equipment manufacturer supplies the developers with their customer requirements and the software architect defines the software interfaces. Since the customer requirements are proprietary information, defining TSRs will be the last step of this thesis.

1.3 Completed Thesis Work

Many automotive professionals have tried to develop models for different E/E components used for autonomous vehicles which comply with the requirements stated by ISO 26262 to render them functionally safe. Many different systems that can make the vehicles more intelligent are being developed. One such model has been developed at UNC Charlotte called the Intelligent Transportation System (ITS) framework proposed by Dr. Benjamin Rhoades [6] in his PhD Dissertation. The work presented in this thesis aims at incorporating a safety model framework inside the vehicle partition of this ITS.

ISO 26262 is the standard dedicated to ensure functional safety in road vehicles. Therefore, in this thesis it is considered as a guideline while ensuring the safety of the modules under consideration. However, the ITS model is a framework that interacts with more than one vehicle on the road. ISO 26262 has no section dedicated to address such behavior. It only considers the safety of the vehicle in which our E/E component is being integrated and not about the other vehicles in the surroundings. This thesis proposes an extension to this standard that considers the hazards caused to the surrounding vehicles mainly the vehicle immediately in front and behind the host car. This thesis ignores concepts like lane change, multiple lanes, overtaking for

reducing the complexity and reserves them for future work.

A hazard analysis and a risk assessment is conducted in order to find out the level of criticality of the two modules and assign a Automotive Safety and Integrity Level (ASIL) to it. This analyses is used to define Safety Goals, Functional Safety Requirements (FSR) and Technical Safety Requirements (TSR) for the modules. Thus we define a failsafe mechanism for both the modules as per the ISO 26262 standard. Ultimately, this thesis shows how in theory a hazardous state is converted to a safer state by incorporating the model suggested by this thesis work.

1.4 Organization

This section gives an overview of the organization of this thesis report. This thesis is organized into following sections: Introduction, Literature Survey, Methodology, Author's Work, Results, Conclusions and Future Scope and References.

Chapter 2 gives an introduction to the ISO 26262 standard for functional safety of road vehicles and a survey of different models that are developed for autonomous vehicles by their respective authors using ISO 26262 as a guideline. This survey mainly discusses three models: model based on autopilot for trains, model based on autopilot for aircrafts and an integrated approach for safety and cyber-security.

Chapter 3 describes functional safety analysis method that is specified by the ISO 26262 and used to carry out the safety analysis of our selected automotive E/E component. This chapter mostly discusses the three processes: functional safety concept development, product development for safety at system level and at software level.

Chapter 4 gives an introduction to the previous "Intelligent Transportation System (ITS)" research and presents the safety analysis of E/E component of the vehicle telemetry and vehicle dynamics module of the vehicle partition of the ITS. This safety analysis includes Hazard Analysis and Risk Assessment (HARA), ASIL Assignment, Defining Safety Goals, Functional Safety Requirements (FSR) and Technical Safety Requirements (TSR) for the two modules.

Chapter 5 shows how the author's proposed model can be incorporated in the ITS vehicle partition and interprets the results.

Chapter 6 concludes the thesis and discusses the future scope of this work.

CHAPTER 2: ISO 26262: FUNCTIONAL SAFETY STANDARD FOR ROAD VEHICLES

Safety is one of the key issues in future automotive development, especially with the introduction of smart features like driver assistance (ADAS), active and passive safety systems, in vehicle dynamics control, etc. IEC 61508 [2] defines Safety as:

> "the freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment."

Many E/E have been introduced in the vehicles and thus the amount of software required to operate these components has increased. With an increase in software there is a need to add failsafe mechanisms to ensure its safety. Functional safety is that part of overall safety of a vehicle which deals with the correct operation of its E/E components. ISO 26262 is a standard derived from IEC 61508 especially for applications in automotive domain. Figure 2.1 shows all the safety standards that are derived using IEC 61508 and the domain in which they are used.

2.1 Introduction to ISO 26262

ISO 26262 standard has been developed to address potential hazards that might be caused due to the failure or malfunction of safety-related components. This is done by classifying the components into different Automotive Safety and Integrity Levels (ASILs). There are four levels of ASILs: A, B, C and D where A represents least critical and D represents the most critical component. For example, a component like Head-Lamps and Turn Indicators can be classified as ASIL A or B whereas, an Electronic Power Steering is very critical with respect to safety and hence it is

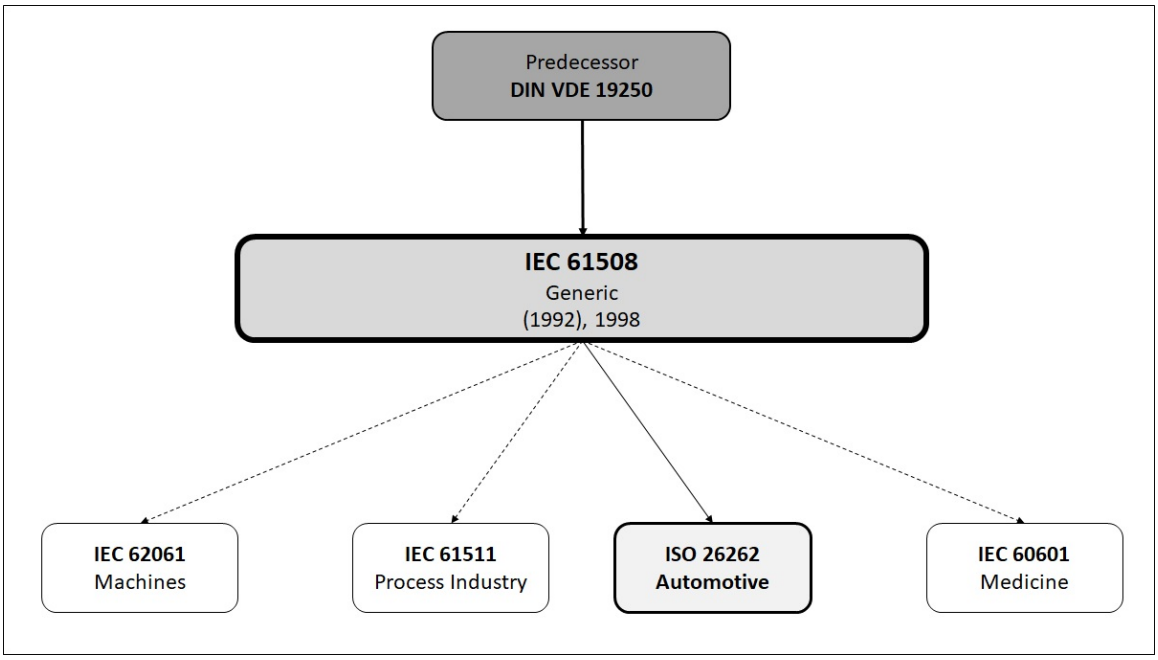

Figure 2.1: Relation of IEC 61508 with ISO 26262

classified as ASIL D. A survey of how to apply ISO 26262 in practice is covered by [7] using the experience gained by them in a pilot project at a German car manufacturer and other similar projects.

ISO 26262 standard consists of 10 parts or phases : Vocabulary (Part 1) [8], Management of Functional Safety (Part 2) [9], Concept Phase (Part 3) [10], Product Development at System Level (Part 4) [11], Hardware Level (Part 5) [12] and Software Level (Part 6) [13], Production and Operation (Part 7) [14], Supporting Processes (Part 8) [15], ASIL oriented and safety oriented analyses (Part 9) [16] and Guideline on ISO 26262 (Part 10) [17]. Based on Part 2, different phases of the product development lifecycle are assigned corresponding safety roles as shown in Figure 2.2. Most of the work discussed in this thesis is based on various levels (parts 3, 4 and 6) of the product development cycle.

To classify components into ASILs, one must do the HARA. For this purpose, a table is maintained that contains all the possible hazardous events that can occur. These events are then further classified based on factors such as: Frequency of

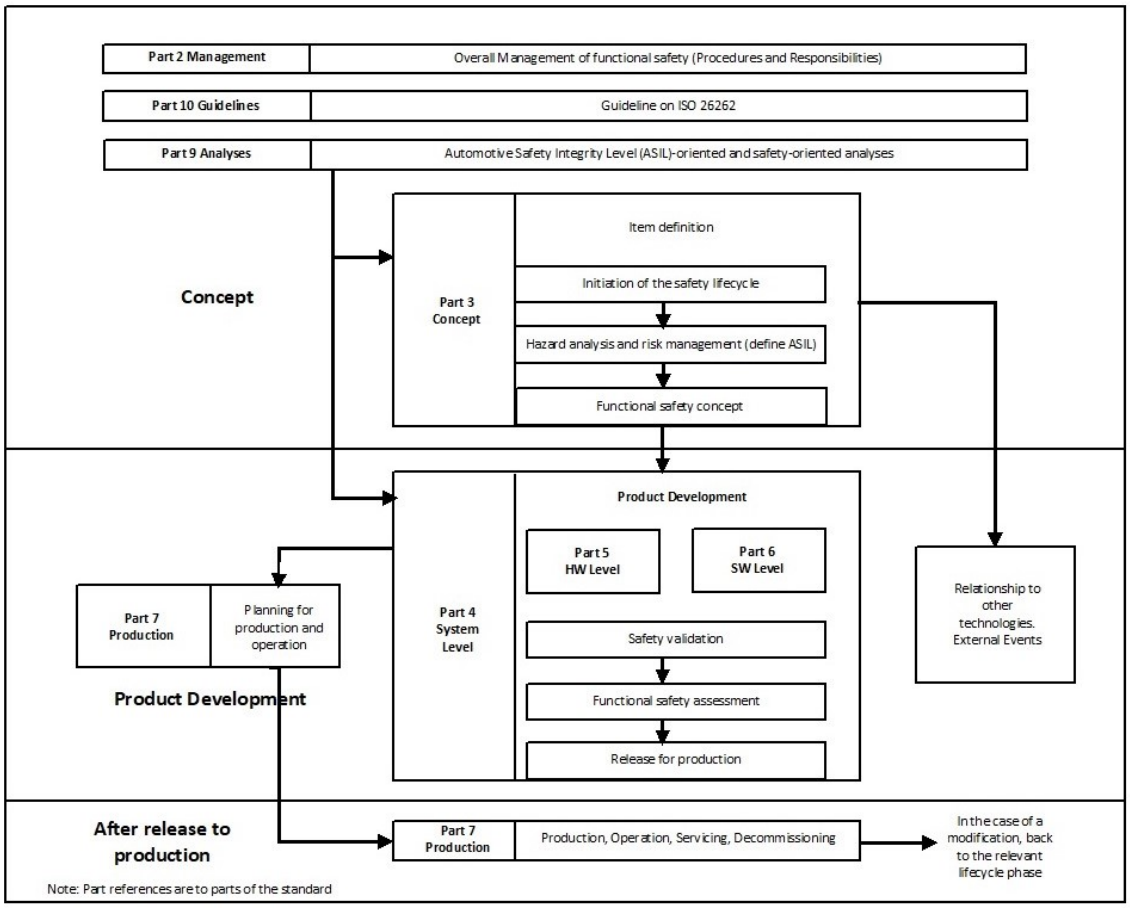

Figure 2.2: Safety Lifecycle as Viewed by ISO 26262 [20]

occurrence of that event, Human controllability to avoid an accident in case of its occurrence, and Potential severity of the resulting damage or harm. Each ASIL not only specifies a mechanism for detecting errors and handling them to make the residual risk minimum and acceptable but also defines confirmation measures including examination and assessment. A reference example for applying ISO 26262 in practice is shown in [18] using "Fuel Level Display (FLD) system". Authors of [19] introduce a safety-oriented process line-based methodological framework that will analyze the commonalities and differences between different safety models in order to enable reuse and derive a flexible model. HARA and ASIL assignment method is described in detail in Section 3.2.

2.2 Survey of Existing Methods

IEC 61508 [2] is an international standard for ensuring functional safety of E/E components in various industrial domains. ISO 26262 is derived from IEC 61508 especially for serving as functional safety standard for automotive applications. However, there is no particular standard dedicated to ensure safety for different levels of autonomous vehicles. Therefore many authors have tried different approaches on different levels of product lifecycle using guidelines from ISO 26262. Some of these approaches that make safety concepts applicable for E/E components of autonomous vehicles are summarized below:

2.2.1 The Autonomous Vehicle Control (AVC) Module Strategy: Architectural Level Approach

There is a massive investment in 'Intelligent' vehicle technologies which is going to turn autonomous vehicles into a reality in few years. Autonomous vehicles are highly safety critical. Even the ISO 26262 functional safety standard for road vehicles is not enough for autonomous vehicle scope. Therefore, [21] proposes a design strategy to design the autonomous vehicle at architectural level. The main idea of this design is to have an independent module that will aim at protecting the autonomous vehicle and increase the level of safety.

In this paper, the Autonomous Vehicle Control (AVC) module is discussed which is indeed very similar in approach to the Automatic Train Control (ATC) Module used in railway transportation systems. The ATC consists of three parts namely, Automatic Train Protection (ATP) which is responsible for maintaining fail-safe protection against collision and excessive speed; Automatic Train Operation (ATO) which is responsible for taking basic operation of the train like speed regulation and programmed stopping; and Automatic Train Supervision (ATS) that is responsible to adjust speed to maintain schedule and provide data for better service. Similar, to the ATC is the

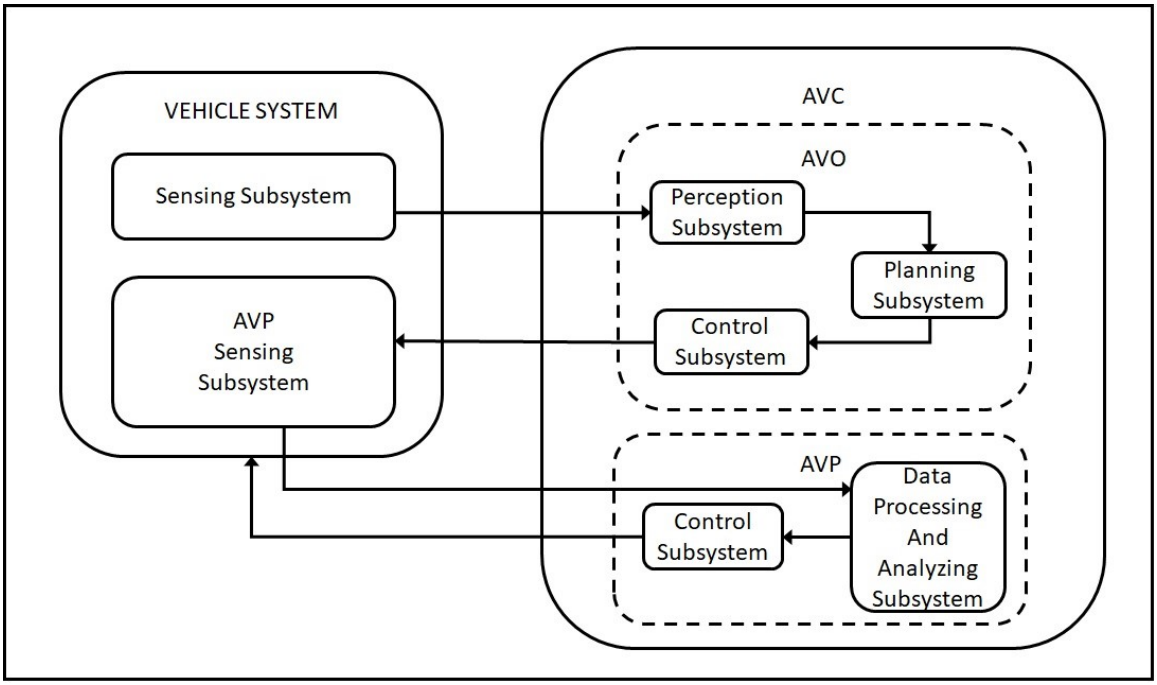

Figure 2.3: High Level AVC Module Structure [21]

AVC module, however, it consists of only two parts AVP and AVO. There is no AVS module.

Most autonomous vehicles decompose their architecture into four main subsystems: sensing, perception, planning and control. Introduction of AVC divides these subsystems amongst the vehicle system and the two sub-modules AVP and AVO as shown in the Figure 2.3. The sensing task is divided into two: normal sensing and sensing for AVP. Normal sensing data is provided to the AVO which is responsible Perception and Planning and generates control signals for the vehicle system. The AVP sensing system provides data to the AVP which also generates control signals for vehicle system but these are special ones which are intended to protect the vehicle from hazardous situations. Thus, different control systems can be generated from AVO and AVP based on sensor data from different sensors. These control signals are independent of each other and the system is aware of the priorities. AVP control signals are only generated based on hazardous situations but the AVO control signals are continuously generated. Thus, this design separates the operational layer from

the protection layer and will facilitate the following: AVP's safety levels analyzed separately, Possible errors detected and repaired and identification of critical points. The authors claim to circumvent the gap related to the safety of the autonomous vehicles conceptually. This paper only proposes this design and thus the future scope is to implement, test and validate it.

2.2.2 Designing Safe and Secure Autopilot

This approach [22] mainly involves analyses of safety and security risks posed by the introduction of the autopilot feature in a road vehicle thus making it semi-autonomous. Firstly, the authors gather lessons that are learned from the aviation industry which already has an autopilot feature in use since last 60 years. This paper considers different accidents that have taken place in the past due to human factors and analyses how humans fail to cope when the autopilot system malfunctions or shuts down. Vehicles can also be fully autonomous meaning that the car has full control over driving decisions or they can be manual meaning the driver has full control.

The paper further discusses the method suggested by the author to make this autopilot system stable in the urban environment. The first step is to define a modular functional architecture by identifying all the use cases and based on these use cases a list of functions is made. ISO 26262 defines an Autopilot Item Figure 2.4 which shows all the systems that perform these derived functions. The second step is to perform the Hazard Analysis. A generic and an extensive list of hazards is created. The third step is to form a technical architecture thus identifying the different components and functions that interface with the autopilot. The fourth step is to standardize the behavioral interface descriptions. The fifth step is to form a security architecture for the every component of the car to make it truly autonomous.

The author suggests following security measures: Authenticity of data that is sent from one entity to another, Integrity of data to prevent any alteration of data, Availability of any entity to all others that are authorized to access it, Confidentiality of

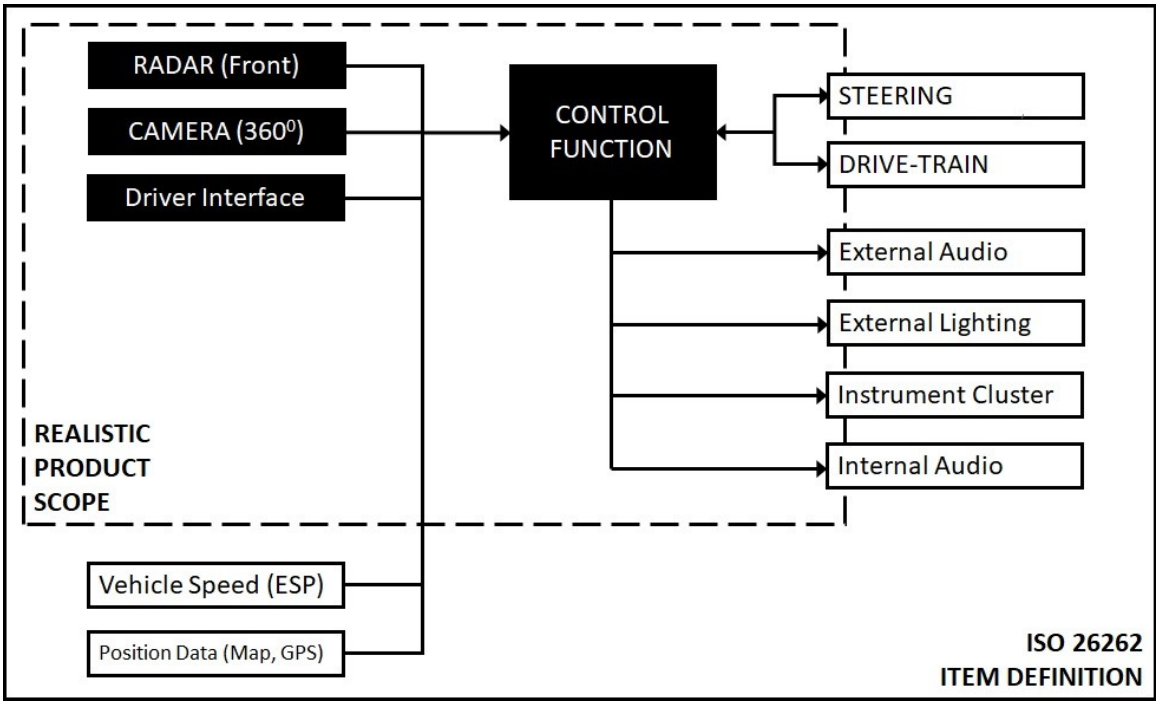

Figure 2.4: Autopilot Item Definition as per ISO 26262 [22]

data to prevent any unauthorized entity to read the data, Non-repudiation to maintain all the records of data transfer and authentications along with time stamps by one entity and transfer these records to the other one so that neither can deny the transfer of data that took place, Intrusion Detection mechanism, a second generation security measure that require a standardized protocol provided by Automotive Open System Architecture (AUTOSAR).

The authors conclude that the intended attacks on autopilot systems are certain to occur. We need to make sure that the autopilot systems are secure enough to block any intrusion by attackers. There is a possibility of unintended attacks as well and that needs to be dealt as well to make the vehicle fully autonomous. The two layers of defense suggested by this paper aim to buy time for the industry to develop more sophisticated methods in the future.

Table 2.1: Vehicular safety / cybersecurity requirements analysis terms [23]

Analysis	Safety	Cybersecurity
Subject		
Risk	Hazard	Threat
System inherent deficiency	Malfunction	Vulnerability
External enabling condition	Hazardous situation	Attack
Category		
Impact analysis	Severity	Threat criticality
External risk control analysis	Controllability	Attacker skills, know-how
Occurrence analysis	Exposure	Attack resources & surfaces
Result		
Design goal	Safety goal	Security target
Design goal criticality	ASIL	SecL

2.2.3 Integrated Approach for Tackling Functional Safety and Cybersecurity

The authors of [23] define a new integrated approach to make intelligent systems secure and safe. The main idea behind developing this integrated model is that the new E/E systems that are used in various domains like automotive, aeronautics and medical are becoming more and more smart and are close to becoming autonomous. Not only these systems are safety-critical i.e. failure of these systems can harm humans but also these are susceptible to cyber-attacks. There are standards defined for both functional safety (IEC 61508 and ISO 26262) and cybersecurity of cyber-physical systems (CPS). However, a functionally safe model may not be cyber secured and vice versa. Therefore, the idea is to combine both these standards and create an integrated model which aims ensuring safety and security. Since this approach is defined for intelligent cyber-physical systems, it can also be applied to autonomous vehicles and ADAS in automotive domain.

This paper uses the example of automotive Electronic Steering Column Lock system (ESCL) to develop a method and logic for integrating the functional safety and cyber security. This is done in the early design phase that is the requirement and constraint

analysis phase. The first step is to derive safety and security requirement and combine them. However, to do that we need a common vocabulary including vehicular terms which can be understood by experts in both the domains. Table 2.1 shows mapping of different terms relevant to safety and security domains. Using this vocabulary an integrated analysis is done instead of separate Hazard Analysis and Risk Assessment (HARA) and Threat Analysis and Risk Assessment (TARA) on ESCL. Then on architectural level a model is proposed. Instead of a single protective layer, multiple successive layers of failure or attack prevention / detection. Thus the concept of having ASILs in functional safety and Security Layers (SecLs) are combined into multiple Automotive Defense Layers (AutoDLs) at different levels. Assuming that the attacks on different security layers SecLs are in a particular order, a model containing the newly integrated Automotive Defense Layers is created for the ESCL system as shown in Figure 2.5. So for attacking any particular system the attacker would now have to go through the AutoDL that protects it.

Trust Boundary Violation is the last part that needs to be taken care of in order to complete our integrated model. The challenge is that the Trust Boundary Identification is completely different in safety than in security engineering. So the authors define a different method by which trust boundaries of both the domains can be identified and integrated into common boundaries. Thus this paper proposes a method to integrate functional safety and cybersecurity aspects in early phases of embedded system design. This method helps us to apply the cybersecurity concepts and methods used in cyber-physical systems and Internet Of Things (IOT) based systems to be applied to the automotive systems as well and the functional safety concepts used by automotive engineers to be applied to cyber-physical systems.

2.3 Why Present Functional Safety Standards are Not Enough

The functional safety standards like ISO 26262 and IEC 61508 judge the safety of a system based on the presence or absence of unacceptable and unreasonable risk. Thus,

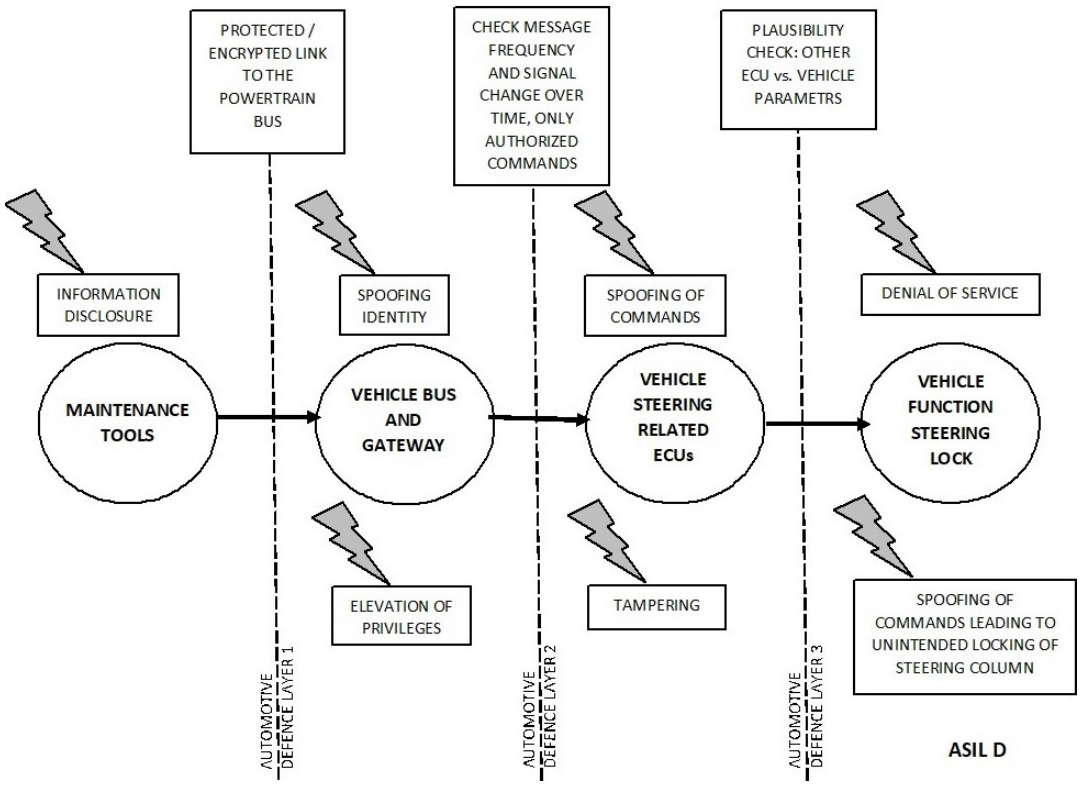

Figure 2.5: Static Defense Layers of ESCL System [24]

these risks in small acceptable amounts are ignored by these standards and hence they don't guarantee absolute safety. Since these standards are defined in such a way, there is a chance that there might be human error in judgments which might have catastrophic consequences. The authors of [25] analyze the morals concepts and issues related to functional safety together with common fallacies in risk perception. They use Kahneman's book "Thinking, Fast and Slow" [26] as a foundation for analysis of unreasonable risk judgments.

Following are the Functional Safety Ethics Issues that are critical to risk-related decision making processes within the area of functional safety. Diversity of judgments: There is a diversity of judgments because the amount of risk an individual judges might differ greatly amongst individuals. Vision Zero and Zero Tolerance are principles used by governments to behaviors that cause harm but are not used in functional safety. Wants vs. Needs: Flying, Driving etc are not human needs but are

human wants, therefore a question arises whether these wants need to be fulfilled at the cost of risks. Business: The main objective of developing safe systems must be safety and not profit, however most of the times developing safer systems is done for profits. Other ethical issues include Law, Regulations, Policies, Evolution, Innovation and Sustainability.

Thus addressing these issues is very important. With the current development in the domain of autonomous systems addressing these issues have become more urgent. Thus, these current existing standards are not enough and as a future scope of this domain one can exploit this topic. The above survey was conducted by the author of this thesis and presented in Southeast conference 2018 [27].

CHAPTER 3: SAFETY ANALYSIS PROCEDURE

ISO 26262 defines the safety analysis procedure in detail. This chapter is dedicated to discuss this procedure by referring to parts 3, 4 and 6 of ISO 26262 [10, 11, 13]. Part 5: Product development at the hardware level [12] is also relevant to the safety analysis, however, we are only concerned with the software part and hence will not discuss it in this chapter.

3.1 V-Model of Automotive Product Development Cycle

ISO 26262 follows the double V-model of automotive product development shown in Figure 3.1. The double V-model is split into two separate V-models each for hardware and software. Figure 3.1 shows various steps in safety analysis which can be correlated to different phases of v-model. Therefore, we will discuss the System and Software engineering process group of the v-model as per Automotive Spice guidelines [28] before moving to the first step (HARA) of functional safety analysis procedure.

3.1.1 System Engineering Process Group (SYS)

This group consists of five processes, described below:

1. Requirements Elicitation

   The main purpose of this process is to establish a requirements baseline that will serve as a basis for defining the work products. Communication with the stakeholder is very essential in this phase. The basis of this process are the stakeholder requirements. A mechanism of monitoring the changing needs of the stakeholder is established. By studying these requirements, the stakeholder expectations are understood and agreed upon. The requirements are then updated accordingly and a baseline is established.

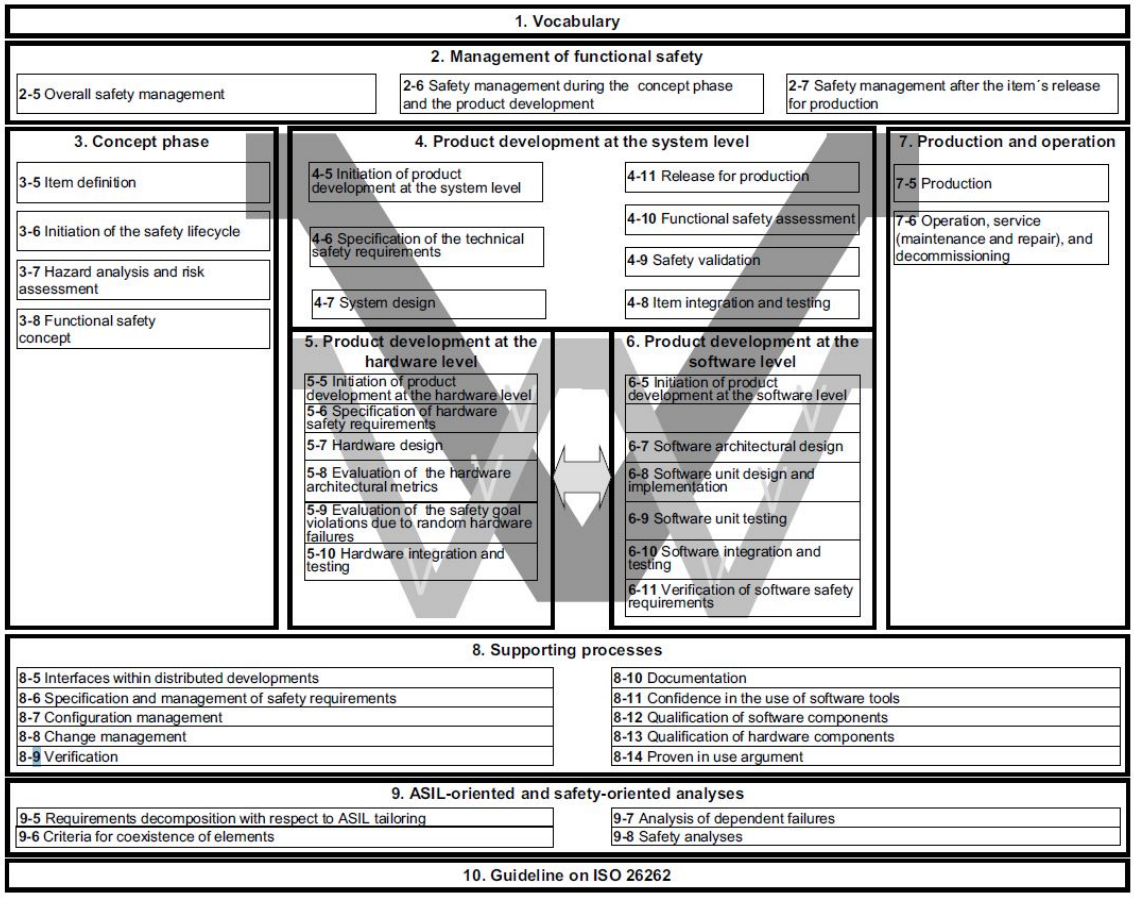

Figure 3.1: V-Model for Automotive Product Development [8]

2. System Requirements Analysis

   The final baseline version of the stakeholder requirements are then transformed into system requirements in this process. These requirements are used as guidelines while designing the system. Firstly, the system requirements are specified using the stakeholder requirements. These requirements are then grouped into relevant clusters, sorted in logical order for project and prioritized according to the stakeholder needs. These requirements are now analyzed to check their interdependencies, technical feasibility and correctness, etc.

3. System Architecture Design

   After the system requirements have been written, the next step is to identify

which system requirement is to be allocated to which elements of the system. Therefore, we need to create a system level architectural design. This design will identify all the elements of the system, allocate each system requirement to appropriate element, define interfaces of each system, define dynamic behaviors and establish backward traceability between system requirements and system architectural design. Thus a consistency between requirements and design is established. This system architectural design needs to be communicated and agreed upon by all the affected parties.

4. System Integration and Integration Test

   After all the system elements have been developed, it is required to integrate them into one system that is consistent with the system architectural design. This integrated system then needs to be tested for compliance with architectural design and system interfaces between each integrated item. Initially an integration strategy and a test strategy consistent with the project plan is prepared. A specification for integration test is developed that is suitable to provide proof of compliance of integrated system items with the system architectural design. Then the system items are integrated and tested using test cases that are selected according to the specifications. Then the results are summarized and communicated all the parties.

5. System Qualification Test

   This is the final test that is performed on the system to make sure that the system satisfies the system requirements and is ready for delivery to the customer. Firstly, a test strategy is prepared and a specification for system qualification test is developed that can serve as a proof of compliance of the system with the system requirements. Test cases are developed according to these specifications and the system is then tested. The results of this test procedure are shared

with all the affected parties.

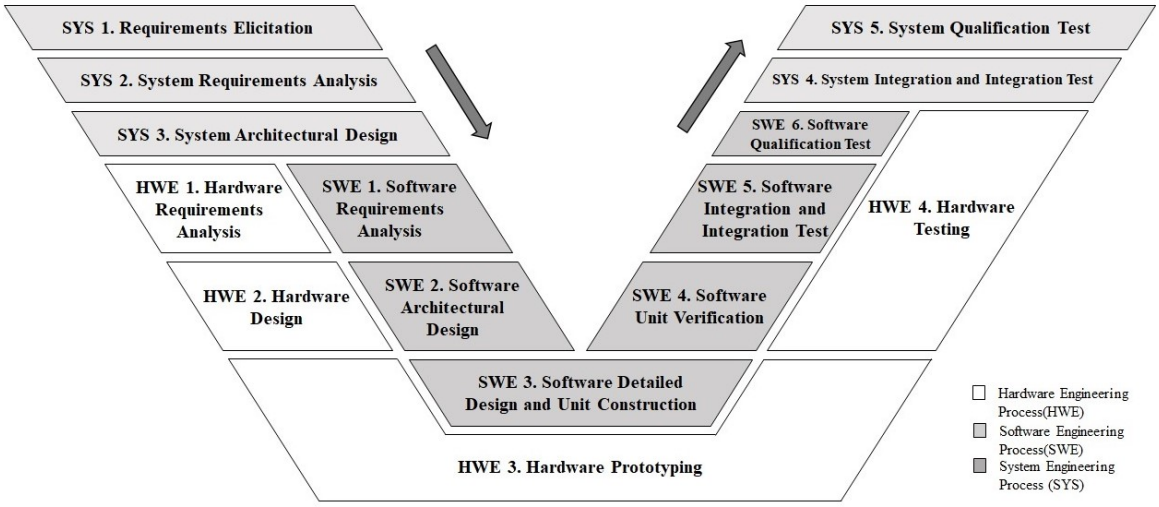

Figure 3.2: V-Model: Engineering Processes of Product Development

3.1.2 Software Engineering Process Group (SWE)

After developing a system architectural design i.e. SYS 3, we move to the software development and test phase that comes under the Software Engineering Process Group. This process group covers all the software related analysis, design, development and testing processes. The six sub-phases of this process group are discussed below:

1. Software Requirement Analysis

   The basic objective of this process is to convert software related parts from the list of system requirements into software requirements. Firstly, the software elements are identified and their corresponding software interfaces are defined. The system requirements related to those elements are converted into software requirements. These software requirements are then classified and grouped according to the subsystems and clusters they belong to. Next step is to define the order in which these software requirements need to be implemented because

of priorities. Throughout the process consistency and backward traceability is maintained and the results are communicated to the affected parties.

2. Software Architecture Design

   The software architectural design process is basically performed to develop a software architecture corresponding to the software requirements. This helps to allocate the software requirements to appropriate software elements and interfaces associated with them. Resource consumption is a very important factor and hence objectives related to resource consumption are defined. The software architecture must be consistent with the software requirements and must be bidirectionally traceable. All the affected parties are informed once the process is finished.

3. Software Detailed Design and Unit Construction

   This is basically the implementation phase. Based on the architectural design, a detailed design is created and interfaces and dynamic behaviors are defined for each of the individual software units. The software requirements that are classified in the previous phases are linked to their corresponding software unit designs in order to maintain consistency and establish bidirectional traceability. This design is conveyed to and agreed upon by affected parties and these units are then created. These units need to be consistent and bidirectionally traceable with their design.

4. Software Unit Verification

   The software units developed in the previous phase are verified in this phase. Firstly, a verification strategy along with a regression strategy is defined. Criteria for verification is defined that will ensure compliance of the software with the design and requirements. the the units are verified according to the strategy

and criteria. The results of the verification process are recorded and conveyed to the affected parties.

5. Software Integration and Integration Test

   This phase is basically for integrating the software units into larger ones to form a completed software. This software needs to be consistent with the architectural design and hence a test is also performed after the integration. This process begins by defining software integration consistent with project plan and the architectural design. A test strategy along with a regression strategy is also defined. A specification for software integration test is defined according to the test strategy. This specifications will ensure the consistency of the integrated software units and their interfaces with the software architectural design. Then the software units are finally integrated into one unit according to the strategy. Test cases that are included in the test specifications are then applied to this integrated software and results are recorded. These results are then conveyed to and agreed upon by affected parties.

6. Software Qualification Test

   This i the last level of testing that is done on the software and is done to ensure that the software is consistent with the software requirements. This is done by defining a strategy along with a regression test strategy. Specifications are defined according to the strategy. These test specification are considered enough for ensuring that the software is consistent with the requirements. Test cases are associated with each requirement. Ultimately the software is tested and results are recorded, conveyed to and agreed upon by all the affected parties.

3.2 Hazard Analysis and Risk Assessment

According to ISO 26262 - Concept Phase [10] "the main objective of the hazard analysis and risk assessment is to identify and to categorize the hazards that malfunc-

tions in the item can trigger and to formulate the safety goals related to the prevention or mitigation of the hazardous events, in order to avoid unreasonable risk."

The first step while initiating the functional safety analysis of any E/E component is to distinguish whether it is a new development or an update to an existing development. Due to several reasons like corrections of software, or the use of different development tools etc., implementation modifications can arise. For updating the already existing safety analysis, the process is continued using "Impact Analysis". In case of a new development, we proceed using Hazard Analysis and Risk Assessment (HARA).

Following are the steps for performing HARA:

3.2.1 Initiation of the HARA

The initialization of HARA starts by defining the item for which the analysis is performed. The item must be evaluated by determining whether a safety mechanism exist for it or not. These safety mechanisms are incorporated as a part of functional safety concept.

3.2.2 Situation Analysis and Hazard Identification

This step consists of two different sub-steps:

3.2.2.1 Situation Analysis

Situation analysis considers both correct and incorrect use of a vehicle and describes hazardous event that can result due to malfunctioning of the item. All such operational situations and modes are described in this analysis.

3.2.2.2 Hazard Identification

The first step in the HARA process is to identify different hazards. This is done systematically using different methods like brainstorming, FMEA, field studies etc. These hazards are defined considering various situations of a vehicle and its behavior. All operational conditions and their consequences are considered while determining

hazardous events. If the identified hazardous event is outside the scope of ISO 26262, it is considered important to highlight the need to take measures to control this hazard and to inform the person who is responsible for handling it.

3.2.3 Classification of Hazardous Event

After identifying hazards, it is important to classify them into classes based on three factors: severity, probability of exposure and controllability.

3.2.3.1 Severity

The term "Severity" is used throughout this context for referring to the severity of the given hazardous event. According to the ISO 26262 standard: Part 3 [10], severity is classified into four classes S0, S1, S2 and S3. The order of severity increases from S0 to S3. In order to determine which class of severity the given hazardous event belong to, all the potential injuries that can result because of this hazard are evaluated for the driver, passengers, people around the vehicle and the people who are in surrounding vehicles. Table 3.1 shows a defined rationale for classifying "Severity". If the hazard is assigned severity class S0 then no ASIL assignment is needed.

Table 3.1: Classes of Severity [10]

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

3.2.3.2 Probability of Exposure

The term "probability of exposure" is used for referring to the probability of occurrence of the hazard based on the exposure to various environmental factors considering the duration or the frequency of exposure. According to the ISO 26262 standard: Part 3 [10], probability of exposure is classified into five classes E0, E1, E2, E3 and E4.

The probability of exposure increases from E0 to E4. In order to determine which class of probability of exposure the given hazardous event belong to, all the environmental factors that can affect the occurrence of the hazard are considered. Some situations are evaluated using the duration for which the exposure exists and some are evaluated using the frequency of exposure. Table 3.2 shows a defined rationale for classifying "Probability of exposure". E0 class corresponds to those situations which are extremely unusual or uncertain or incredible. Such situations don?t require ASIL assignment.

Table 3.2: Classes of Probability of Exposure [10]

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

3.2.3.3 Controllability

The term "controllability" is used to refer to the probability of the driver to avoid hazardous situations by retaining or regaining control of the vehicle during a hazardous event. According to the ISO 26262 standard: Part 3 [10], controllability is classified into four classes C0, C1, C2 and C3. The ease in controllability decreases from C0 to C3. In order to determine which class of controllability the given hazardous event belong to, the likelihood that the representative driver will be able to retain or regain control of the vehicle if the hazard were to occur is considered. Table 3.3 shows a defined rationale for classifying "Controllability". If the hazard is assigned controllability class C0 then no ASIL assignment is needed.

Table 3.3: Classes of Controllability [10]

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

3.2.4 Determination of ASIL and Safety Goals

In this step an ASIL is defined for each hazardous event using the three parameters described in Section 3.2.3. There are four ASILs defined in ISO 26262 standard namely A, B, C and D. A is the lowest ASIL and D is the highest. In addition to the four ASILs, there is one more class Quality Management (QM) which denotes no requirement to comply with ISO 26262. Using the HARA performed in the previous step, a table is maintained. This table has all the possible hazardous situations classified on the basis of three parameter from Section 3.2.3. Using these classes, the ASIL for each hazardous event is determined by referring to the 3.4. ASIL assignment is a critical issue. It is important to ensure that the chosen level of operational situations and modes does not lead to an inappropriate lowering of the ASIL. Therefore, if one cannot arrive at a conclusion while selecting the ASIL, the appropriate higher ASIL is selected.

Along with the assignment of ASIL, it is required to assign a safety goal for each hazard and then make a list of all the safety goals for the component under analysis. If multiple safety goals are similar then they can be combined into one. Safety goals are the top level safety requirements and get converted into Functional Safety Requirements (FSRs) and eventually into Technical Safety Requirements (TSRs).

3.2.5 Verification

This step is basically a review procedure. This review is done to check the completeness and correctness of the Hazard Analysis and Risk assessment. The reviewer is supposed to be someone from outside the team of developers.

3.3 Functional Safety Concept

After performing HARA, the next step is to derive the functional safety concept for the component under consideration. After completing the HARA procedure we have the ASIL assigned to the component as well as safety goals defined and assigned

Table 3.4: ASIL determination [10]

Severity Class	**Probability Class**	**Controllability class**		
		C1	**C2**	**C3**
S1	**E1**	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	**E1**	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	**E1**	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

for the corresponding hazard. The hierarchy of safety goals and functional safety requirements is shown in Figure 3.3.

3.3.1 Derivation of Functional Safety Requirements

Next step is to derive functional safety requirements (FSRs) which will form the basis of the functional safety concept. There must be at least one FSR for each of the safety goals. One FSR can be valid for multiple safety goals. Operating mode, fault tolerant time interval, safe state and other such parameters specified in the standard shall be specifically considered while deriving every FSR. Architectural assumptions also need to be considered while deriving the FSRs. Normally, the way to handle an hazardous state is to transition into a safe state within an acceptable time interval. However, if this transition is not possible, emergency operations need to be defined for such hazardous situations. Warning and degradation concept is also defined as an FSR. Warning and degradation concept contains a description of transitions to and from a safe state and the conditions for transitioning.

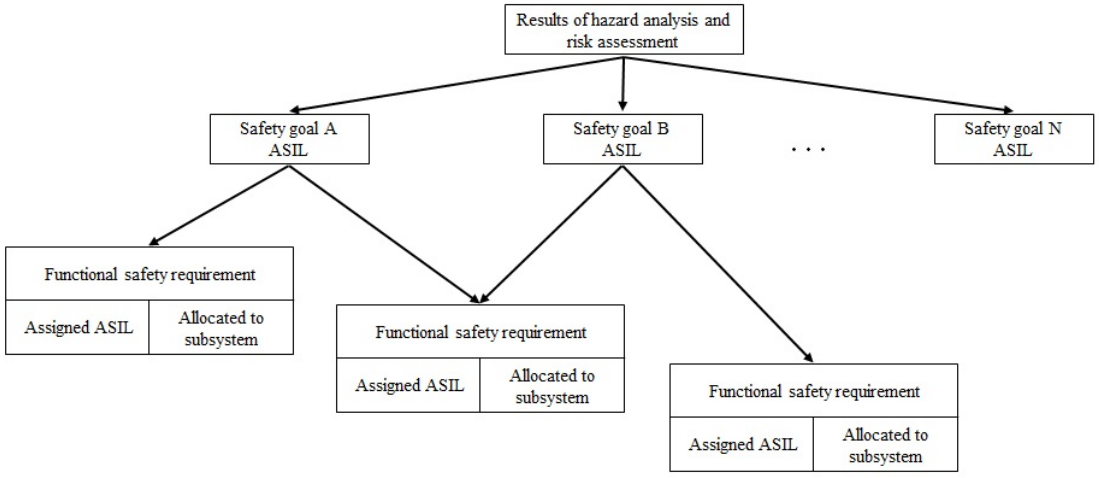

Figure 3.3: Hierarchy of Safety Goals and Functional Safety Requirements [10]

3.3.2 Allocation of Functional Safety Requirements

After deriving the FSRs, these requirements are allocated to respective architectural elements. During the allocation, the ASIL must be inherited from the respective safety goal. If several FSRs are assigned to same architectural element, then the highest ASIL out of them must be considered while developing that element. If the component consists of several architectural elements, then FSRs are defined for each system and their interfaces and these FSRs are allocated to these elements. The functional safety concept can be based on other technologies or external measures. If so, FSRs for architectural elements of those technologies / measures and for their interfaces need to be defined. If other technologies are used, specific measures that are outside the scope of ISO 26262 are needed and hence no ASIL is assigned to the FSRs related to them. On the contrary, if external measure are used, related FSRs are addressed using ISO 26262 and their implementation is ensured.

3.3.3 Safety Concept Validation

The safety concept that has been defined in the previous steps needs to be validated in order ensure its consistency and compliance with the preliminary architectural

assumptions. Therefore, acceptance criteria for the safety validation is specified by referring to the FSRs.

3.3.4 Safety Concept Verification

After validating the consistency and compliance of the functional safety concept with the architectural assumptions, this functional safety concept is verified. This done by checking its compliance and consistency with the FSRs and the ability to avoid or lessen the gravity of hazards.

3.4 Product Development at System Level

In the Section 3.1.1, system level development phase of the automotive product development cycle using V-model is explained. ISO 26262 follows the same model in order to develop safety related system level model. Thus we can draw analogy between the system level part of the V-model and functional safety system development reference model shown in Figure 3.4. Following are the sub-phases of system level production development cycle of ISO 26262:

3.4.1 Initiation

This is the initiation procedure of product development at system level. The main objective is to devise a plan to determine and execute the functional safety activities during the sub-phases of system level product development. This includes plan to determine methods and measures used for design and integration, validation activities and functional safety assessment. This plan must be in accordance with the Part 2 of ISO 26262 [9], which gives guidelines referring to the management phase.

3.4.2 Specification of the Technical Safety Requirements

This step can be related to the "Requirement Elicitation" and "System Requirements Analysis" steps of Section 3.1.1. The main objective is to specify technical safety requirements (TSRs) and to ensure that the TSRs comply with the FSRs. Therefore, TSRs are defined in accordance with the functional safety concept derived

in the previous phases. TSRs specify the safety-related dependencies between different elements of the system and between different systems. They also specify the response of system to various stimuli such as failures that may affect the achievement of safety goals. A TSR also specifies safety mechanisms like measures to detect or prevent faults inside the system or external devices that interact with the system, methods to achieve safe state from a hazardous state and measures for implementing warning and degradation concept. In order to ensure that a safe state is achieved, a TSR must also specify how the transition to safe state occurs, fault tolerant time interval, emergency operation interval (if safe state cannot be reached immediately), avoidance of latent faults and measures to maintain the safe state. TSRs must be specified for safety activities during production, maintenance, repair and decommissioning as per Part 7: ISO 26262 [14].

3.4.3 System Design

This step can be related to the "System Architecture Design" step of Section 3.1.1. The objective of this sub-phase is to develop and verify a system design and a technical safety concept that complies with the FSRs and the TSRs. First step in this process is to develop a system design specification and a technical safety concept. The TSRs are allocated to the system design elements and are implemented. Next step is to define system architectural design constraints. This includes maintaining compliance of the system design with the ASIL assigned to the TSR and defining internal and external interfaces of the safety-related elements. Next step is to develop measures for avoiding systematic failures. This is done by identifying internal and external causes of systematic failures using Deductive and Inductive analysis methods. The TSRs are then allocated to hardware, software or both and hardware-software interfaces are specified. Finally, the system design and technical safety concept is verified for consistency and compliance with previous safety phases.

3.4.4 Item Integration and Testing

This phase can be related with the "System Integration and Integration Test" step of Section 3.1.1. As we can see from Figure 3.2 and 3.4,in V-model of product development we have Section 3.5 between Section 3.4.3 and Section 3.4.4. So we assume that the Software Development and Test phase has been completed before explaining this Section. This phase has three sub-phases. The first sub-phase is integration of hardware and software of each element that the item comprises of. The second sub-phase is the integration of all the elements of the item. And the third sub-phase is the integration of the item with various systems inside the vehicle and the vehicle itself. The main objective of the integration process is to test compliance of the system as a whole unit with its safety requirements in accordance with the ASIL classification and to verify if the "system design" cover all the safety requirements.

3.4.5 Safety Validation

This phase can be related with the "System Qualification Test" step of Section 3.1.1. In the previous phase the integrated system design was verified and checked for consistency with the safety requirements. In this phase, the integrated system is checked for consistency with the safety goals and whether the safety goals are correct, complete and fully achieved. Firstly, a validation plan is specified and then executed. The safety goals are thus validated in accordance with their assigned ASILs.

3.4.6 Functional Safety Assessment

This is step is specific to functional safety and as the name states, the main objective of this phase is to assess if the developed item is functionally safe.

3.5 Product Development at Software Level

In the Section 3.1.2, software level development phase of the automotive product development cycle using V-model is explained. ISO 26262 follows the same model in order to develop safety related software level model. Thus we can draw analogy

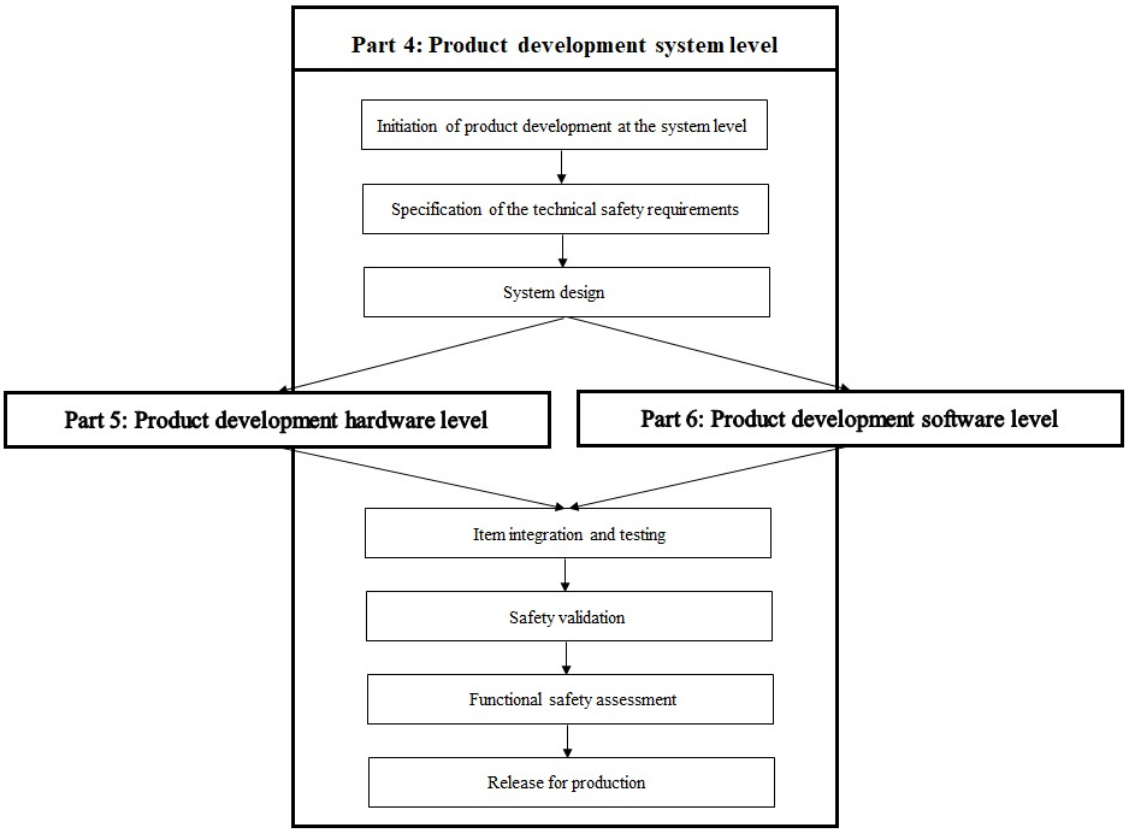

Figure 3.4: Reference Phase Model for the Development of a Safety Related Item [11]

between the software level part of the V-model and functional safety software development reference model shown in Figure 3.5. Following are the sub-phases of software level production development cycle of ISO 26262:

3.5.1 Initiation

This is the initiation procedure of product development at software level. The main objective is to devise a plan to determine and execute the functional safety activities during the sub-phases of software level product development. This includes plan to determine methods and measures used for design and integration, validation activities and functional safety assessment. This plan must be in accordance with the Part 2 of ISO 26262 [9], which gives guidelines referring to the management phase.

3.5.2 Specification of Software Safety Requirements

This phase can be related to the "Software Requirements Analysis" step of the V-model for product development in Section 3.1.2. The main objective of this phase is to derive software requirements from technical safety concept and system design specification. Other objective include detailing of software-hardware interface requirements and to verify if all the above specified requirements are consistent with the technical safety concept and system design specifications. Software Requirements address all the software-based functions which are prone to failure resulting in violation of TSR allocated to that system. Thus every software requirement is based on one or more TSRs. Complex requirements are decomposed into multiple simple software requirements using ASIL decomposition as specified in Part 9: ISO 26262 [16]. The hardware-software interface requirements are verified jointly by persons responsible for system, hardware and software development.

3.5.3 Software Architectural Design

This phase can be related to the "Software Architectural Design" step of the V-model for product development in Section 3.1.2. The objective of this phase is to design and verify a software architectural design based on the software safety requirements developed in the previous phase. In order to ensure that the software architectural design captures all the necessary information, the design is kept modular, encapsulated, simple and such that all the software units are identifiable. The design also specifies the static as well as dynamic design aspects of the software components. Every safety related component is classified as newly developed, reused with modifications or reused without modifications.

3.5.4 Software Unit Design and Implementation

This phase can be related to the "Software Detailed Design and Unit Construction" step of the V-model for product development in Section 3.1.2. The objective of this

phase is to specify and implement the software units and verify them in accordance to the architectural design developed in the previous phase. This is basically the implementation phase where the software for the item will be implemented in parts or software units keeping in mind the correct order of execution of those units, consistency of the software interfaces between those units, correctness of data and control flow between and within them, simplicity and testability. After the implementation is done, it must be verified in accordance with Part 8: ISO 26262 [15]. The compliance of the software units with the hardware-software interface specification must be verified. The developed software must satisfy all the software requirements and must comply with the software design specification.

3.5.5 Software Unit Testing

This phase can be related to the "Software Unit Verification" step of the V-model for product development in Section 3.1.2. The objective of this phase is to test whether the software units comply with the software unit design. Firstly a test plan is specified and then executed in accordance with Part 8: ISO 26262 [15]. Along with the specified functionality, compliance with software unit design, compliance with hardware-software interface requirements and robustness of the software are tested. A test is performed to make sure that there is no unintended functionality implemented by the software units.

3.5.6 Software Integration and Testing

This phase can be related to the "Software Integration and Integration Test" step of the V-model for product development in Section 3.1.2. The main objective of this phase is to integrate all the software units into one big unit. Another objective is to show that this integrated software is in compliance with the software architectural design. Firstly, an integration plan is prepared. This plan includes steps to integrate the individual software units into a complete embedded software that will be in accor-

dance with the software design and software requirements. This software integration plan will consider all the functional dependencies between different software units and also the hardware-software integration dependencies. The "Integration test" is then planned and executed to verify if the specified functionality is provided by the integrated software and to check for compliance between the integrated software and the software architectural design. Software integration testing can be performed in different environments like model-in-the-loop tests (MIL), processor-in-the-loop tests (PIL), software-in-the-loop tests (SIL) and hardware-in-the-loop tests (HIL).

3.5.7 Verification of Software Safety Requirements

This phase can be related to the "Software Qualification Test" step of the V-model for product development in Section 3.1.2. The only objective is to check if the software fulfills the software safety requirements. A verification test plan is developed. Specifications for compliance with and coverage of software safety requirements and pass-fail criteria are defined. Test cases are run and plan is executed.

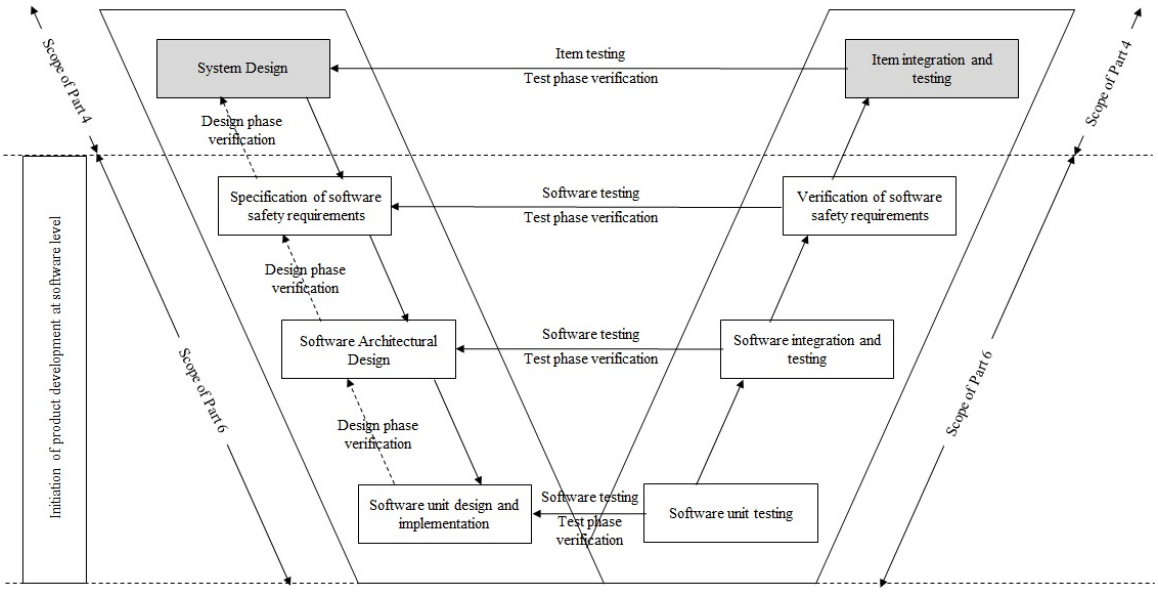

Figure 3.5: Reference Phase Model for the Software Development [13]

CHAPTER 4: FUNCTIONAL SAFETY ANALYSIS: COMMUNICATION MODULE

The previous chapter described the functional safety analysis procedure. This chapter will discuss the previous research on the "Intelligent Transportation System (ITS)" [6] and author's software model to incorporate functional safety inside the ITS. Main components of an ITS are shown in Figure 4.1. More information about the work at UNC Charlotte can be found in [29] and [30].

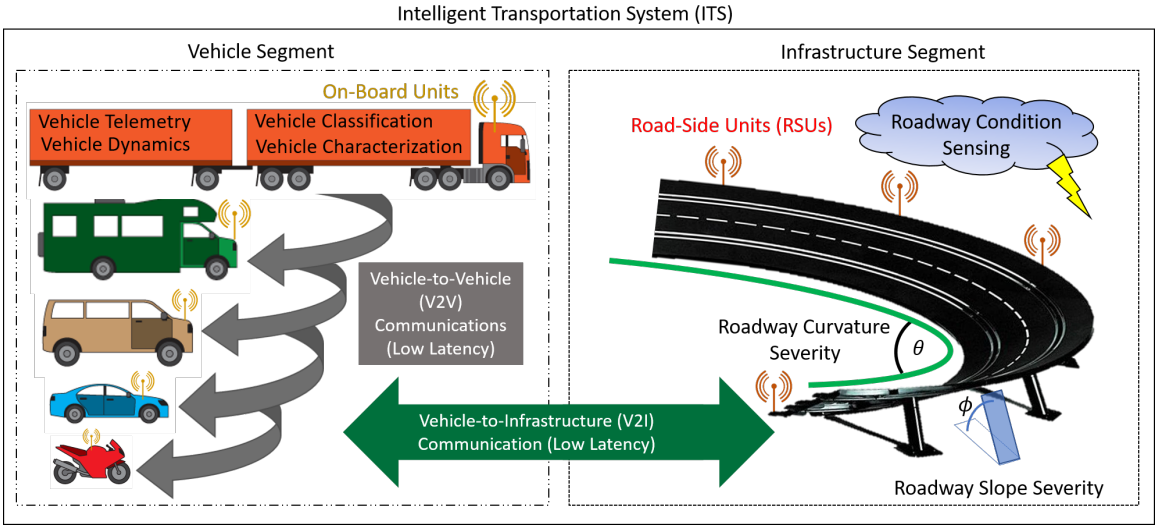

Figure 4.1: Components of an Intelligent Transportation System (ITS) [6, 31, 32]

4.1 Components of Intelligent Transportation System

The ITS is divided into two main partitions, namely : Vehicle and Infrastructure partition.

4.1.1 Vehicle Partition

This partition is responsible for vehicle data collection and dispersion. This data includes crucial information such as relative speed, location and direction that are

then communicated to all the other vehicles on the roadway and to the infrastructure. Following are different blocks that constitute the vehicle partition.

1. Vehicle Classification and Characterization

   This is the first challenge presented by the vehicle partition. The objective is to quickly identify and classify the vehicle into one of the classes discussed in Table 4.1 in real-time. A central database is to be maintained in order to help identify and classify the vehicles on the basis of their VIN as suggested by the ITS framework [6].

2. Vehicle Telemetry and Dynamics

   This block is responsible for gathering all vehicle data and transmitting it. Patent information in [33] shows how a small device can be used to transmit vehicle telemetry data. On-Board Diagnostic (OBD) port is present in all vehicles produced after 1996 and is used to extract the vehicle diagnostics and real-time data from the vehicle. The author in [6] uses a Bluetooth Dongle, shown in Figure 4.2 to connect to the OBD II port. After classifying and characterizing the vehicle the next challenge is to correctly extract the vehicle telemetry and dynamics data to transmit to other vehicles on the roadway.

Figure 4.2: ELM327 Bluetooth Dongle for OBDII Port [6, 34]

3. Vehicle-to-Vehicle (V2V) Communication

   Important information such as vehicle relative speed, vehicle dynamics, etc. are available with the vehicle and hence a direct V2V communication can be used in real-time. This block represents the V2V communication module. The main objective of this block is to establish a successful V2V communication link between the vehicles that are in its range. In this thesis, it is assumed that a successful V2V is already establish for purpose of study.

4. On-Board Units (OBUs)

   OBUs are devices that are required in order to communicate via V2V communication. Many companies are trying to develop an OBU that will require less space so that the car manufacturers will be able to add it to their cars without consuming much space and the customers won't have to compromise on their limited cargo space.

4.1.2 Infrastructure Partition

Another important part of the ITS is to receive and pass on information about the surrounding infrastructure and roadway conditions. The infrastructure partition of the ITS is responsible for establishing this communication.

1. Roadway Characterization

   The first challenge in the infrastructure partition is to characterize the roadway. Many GPS navigation systems presently provide navigation services however, none of them provide a comprehensive snapshot of the roadway. The following two parts constitute a roadway characterization system.

   1.1. Roadway Curvature and Slope Classification

   The two main parameters of a roadway are its slope and the curve / banking. The first step in roadway classification therefore involves classifying

its slope and curvature. There currently exists no direct method that can relay this information directly to the ITS. A data collection based method is used by the rally car racing and the previous work also uses similar method.

1.2. Roadway Condition Sensing

Along with the classification, condition sensing is also important to provide a complete characterization of a roadway. For example, factors like speed and braking distance will differ for the same vehicle on different road conditions.

2. Vehicle-to-Infrastructure (V2I Communication)

Once the gathering and classification of the roadway information is done, this information needs to be transfered to the vehicles on the roads. This is where the Vehicle-to-Infrastructure (V2I) comes into picture. The main objective of this module is to make sure the vehicle can transmit and receive real-time traffic and roadway condition information to and from the centralized system.

3. Road-Side Units (RSU)

The RSUs are the units that help in accomplishing the V2I communication. All the data about the roadway conditions that is collected needs to be transmitted to the centralized ITS server. This is done using th RSUs.

A high level block diagram of the previous work is shown in Figure 4.12.

4.2 Functional Safety Analysis of the Vehicle Partition of the ITS Module

ISO 26262 is a standard dedicated to ensure functional safety of road vehicles. This standard has no section dedicated to autonomous vehicle or for handling smart systems like the ITS. The ISO 26262 standard performs the entire safety analysis procedure focusing only on the vehicle and the factors like roadway conditions, traffic,

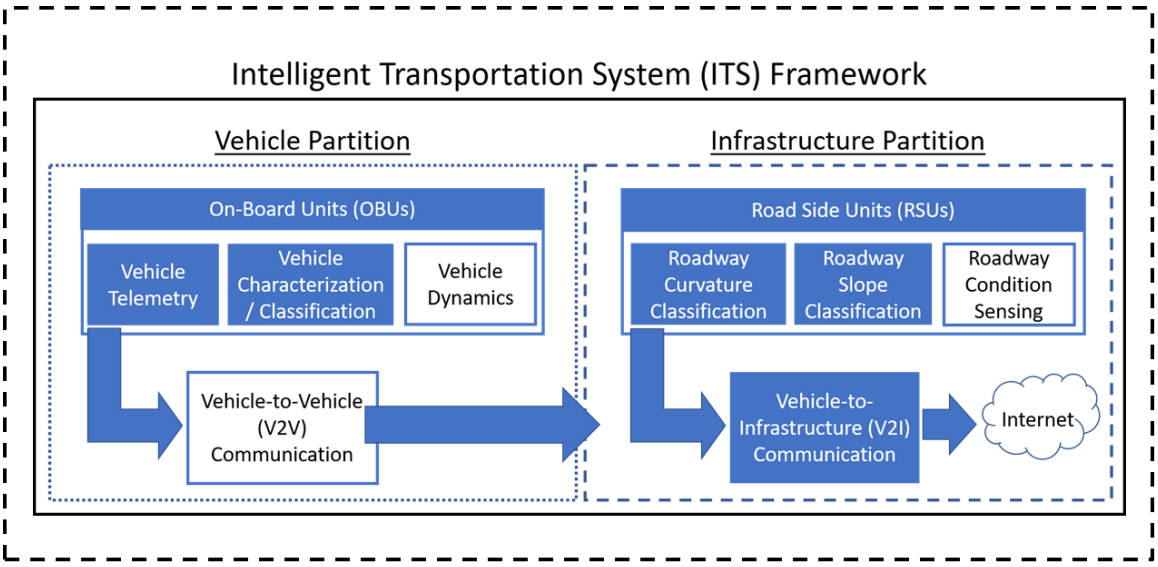

Figure 4.3: ITS Framework Flowchart (ITS) [6]

speed, climate conditions, etc. It fails to consider concepts like V2V communication, where other vehicle's safety is also affected and can indeed affect safety of our vehicle. This thesis tries to establish a model that will serve as an extension to the ISO 26262 standard. The entire procedure is discussed in Chapter 3 and can be summarized as shown in Figure 4.4.

4.2.1 Assumptions

The author is developing a safety model for a single module which is part of an ITS and is connected to a vehicle during runtime. Thus this module interacts not only with the different parts of the ITS but also with the different components of the vehicle's Body Control Module (BCM). Therefore, the safety of these modules will be dependent on each other. So in order to limit the scope of this thesis to a single module we make some assumptions that are discussed further in this paragraph. One such assumption is to completely rely on the data provided by the Vehicle Diagnostics Module that is responsible to provide data via the OBD II port in vehicles manufactured after 1996. For vehicles that are manufactured before 1996 there is no OBD II port and therefore the driver will manually input the data to be transmitted by the

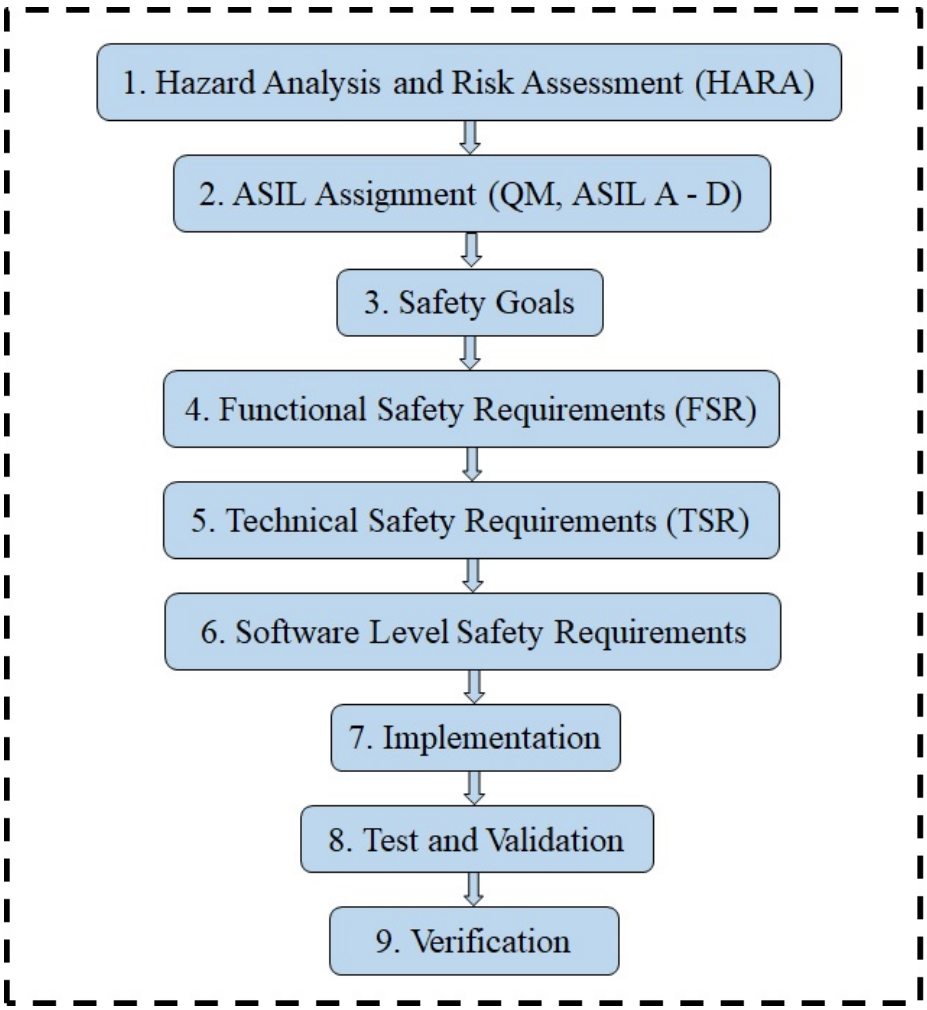

Figure 4.4: Steps for Performing of Safety Analysis of an E/E Component

V2V communication module. This will be considered during our safety analysis as one of the factors affecting the safety.

This thesis is basically trying to develop an extension to the present ISO 26262 standard by which it can start considering the safety of surrounding vehicles along with the host vehicle. We therefore need to define the term "surrounding vehicle". Currently we limit this term to be used only for those vehicles that are in the range of the V2V communication range. To further reduce the complexity, we consider a single lane roadway therefore the surrounding vehicle can be either in front or behind the host vehicle. Also we assume the V2V range to be large enough to communicate with only one vehicle in front and behind the host vehicle. Single lane also eliminates the

possibility of lane change assistance module and thus eliminates any interdependency on that module.

The previous author also has made some assumptions while developing the ITS module and the related algorithms. Since this thesis is a safety analysis model for the previous author's work, this thesis will make assumptions that are consistent with the ITS model. One such assumption of the previous work is that V2V communication module has been already established and will be used by the ITS. This thesis will not only assume that the V2V communication has been successfully established but also that it is consistent with the requirements of the ISO 26262 standard. In the previous work, the author has defined criteria for classifying all the road vehicles into six different classes as shown in Table 4.1. In this work, the author neglects the sixth class that consists of the emergency vehicles like police vehicles, ambulance, fire-truck, etc. which have to be handled specially. A police vehicle in pursuit of a suspect or an ambulance rushing to the hospital etc. cannot be handled like normal road vehicles. Therefore, we keep class six vehicles aside for time being and will consider them as a part of our future work.

4.2.2 HARA of Vehicle Classification and Vehicle Telemetry module

The steps to perform the HARA are discussed in the Section 3.2. We follow the same steps and perform the analysis for our Vehicle classification and Vehicle Telemetry module.

4.2.2.1 Analysis of Vehicle Classification Module Using VIN

One of the most important information that will be transmitted from the host vehicle and received by the surrounding vehicle is the Vehicle Identification Number(VIN). ISO 3779:2009 standard for Road Vehicles : World Manufacturer Identifier (WMI) [35] defines a VIN as a unique code, including a serial number, used by the automotive industry to identify individual motor vehicles, towed vehicles, motorcy-

cles, scooters and mopeds. Thus by transmitting the VIN to surrounding vehicles, the surrounding vehicles can get data related to the dynamics of our vehicle. The author of [6] classifies all the vehicles into 6 main types shown in Table 4.1. Thus a lot of information can be derived from VIN. Incorrect transmission of VIN can lead to derivation incorrect dynamics information. The HARA shown in Table 4.2 and Table 4.3 discusses four cases in which incorrect transmission can cause hazard.

Table 4.1: Vehicle Characterization and Classification

Class	**Length(in)**	**Weight(lbs)**	**Height(in)**	**Example**
1	$x < 100$	$x < 1000$	$x < 50$	**Motorcycle:** BMW 1200R
2	$100 < x < 185$	$1000 < x < 3500$	$50 < x < 60$	**Coupe:** Nissan GT-R
3	$185 < x < 200$	$2500 < x < 4500$	$55 < x < 65$	**Sedan:** Honda accord
4	$200 < x < 215$	$4500 < x < 7000$	$60 < x < 75$	**truck:** RAM 2500
5	$x > 215$	$x > 7000$	$x > 75$	**Bus:** Volvo Tour Bus
6A	$x < 100$	$x < 1000$	$x < 50$	**Emergency Vehicle:** Police Motor Bike
6B	$100 < x < 215$	$1000 < x < 7000$	$50 < x < 75$	**Emergency Vehicle:** Ambulance
6C	$x > 215$	$x > 7000$	$x > 75$	**Emergency Vehicle:** Fire Truck

Figures 4.6 - 4.9 depict the collision scenario that may result due the hazards 03 and 04. This paragraph provides instructions so as to how to read these diagrams in order to understand the scenario its depicting. These diagrams have 3 parts labeled A, B and C and four different types of vehicles namely : the host car labeled "4" if its a motorbike (relatively smaller vehicle) and labeled "5" if its a truck (relatively larger vehicle), green car labeled "3" is the vehicle behind the host vehicle and blue car labeled "2" is the vehicle in front of the host as shown in Figure 4.5. The direction in which the vehicles are traveling is from left to right denoted by the gray arrow. Part A is the initial state of the scenario which shows V2V communication (VIN transmission)

taking place between the host and the surrounding vehicle. This communication is indicated by the curved red arrow as mentioned in the legend in Figure 4.5. This communication is presumed to be erroneous and hence the vehicle behind the host will get the wrong VIN. Therefore, the surrounding vehicle will incorrectly interpret the dynamics of the host. Part B shows this wrong interpretation and Part C shows the actual scenario which might show a traffic jam or unnecessary speeding (hazard 03) or collision (hazard 04).

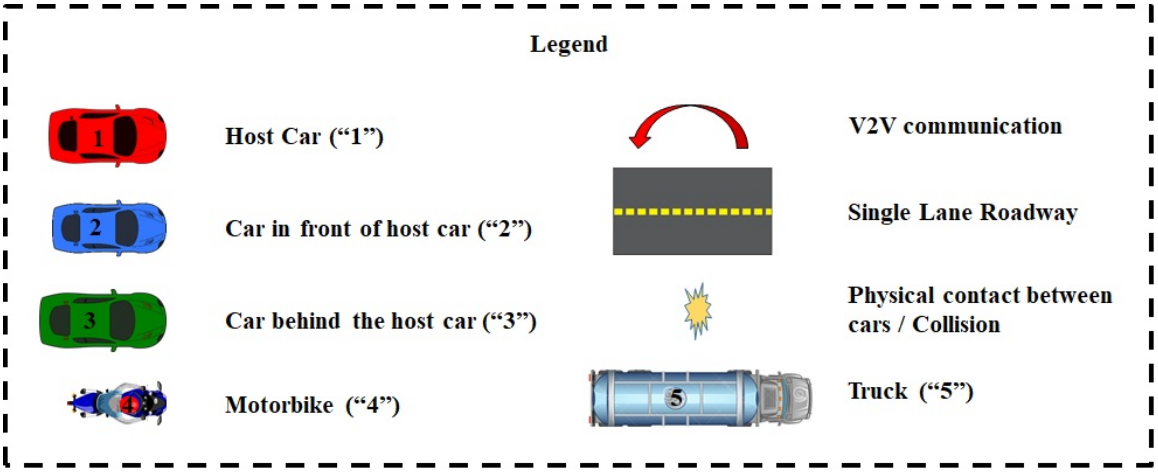

Figure 4.5: VIN Hazard 03 Scenario

1. Hazard 01

   In this case, the VIN that is transmitted by the host car is not only incorrect but also invalid, which means that this VIN number does not belong to any valid car. Invalid VINs can be easily detetcted by the surrounding vehicles and necessary actions can be taken.

2. Hazard 02

   In this case, the VIN that is transmitted is incorrect, but coincidently it corresponds to a valid car other than the host car, but this other car also belongs to the same type as the host car. For example, both the host car and the misinterpreted car are Honda Accords or the host car is a Honda Accord and

the misinterpreted car is a Toyota Camry or a Honda Civic Sedan. Since both the cars are of same type, even the misinterpreted dynamics won't make much difference and hence avoid any serious accidents.

3. Hazard 03

   In this case, the VIN that is transmitted is incorrect, but coincidently it corresponds to a valid car other than the host car and this other car belongs to some other type of car that is smaller than the host car. For example, the host car is a motorcycle and the misinterpreted car is a truck. Since both the cars are of different types, there will be a large difference between the actual and misinterpreted dynamics. The surrounding car will think that the host car is a motorcycle instead of a truck. The dimensions of a truck are larger than that of a motorcycle and hence the surrounding car will maintain a larger distance between itself and the host as shown. The vehicle behind the host will slow down and maintain a much lager distance ad thus blocking traffic behind it as shown in the Figure 4.6. The vehicle in front will think that a truck is speeding towards it and hence will increase its own speed to maintain a safe distance as shown in Figure 4.7.

4. Hazard 04

   In this case, the VIN that is transmitted is incorrect, but coincidently it corresponds to a valid car other than the host car and this other car belongs to some other type of car that is smaller than the host car. For example, the host car is a truck and the misinterpreted car is a motorcycle. Since both the cars are of different types, there will be a large difference between the actual and misinterpreted dynamics. The surrounding car will think that the host car is a motorcycle instead of a truck. The dimensions of a motorcycle are smaller than that of a truck and hence the surrounding car will come closer to the host.

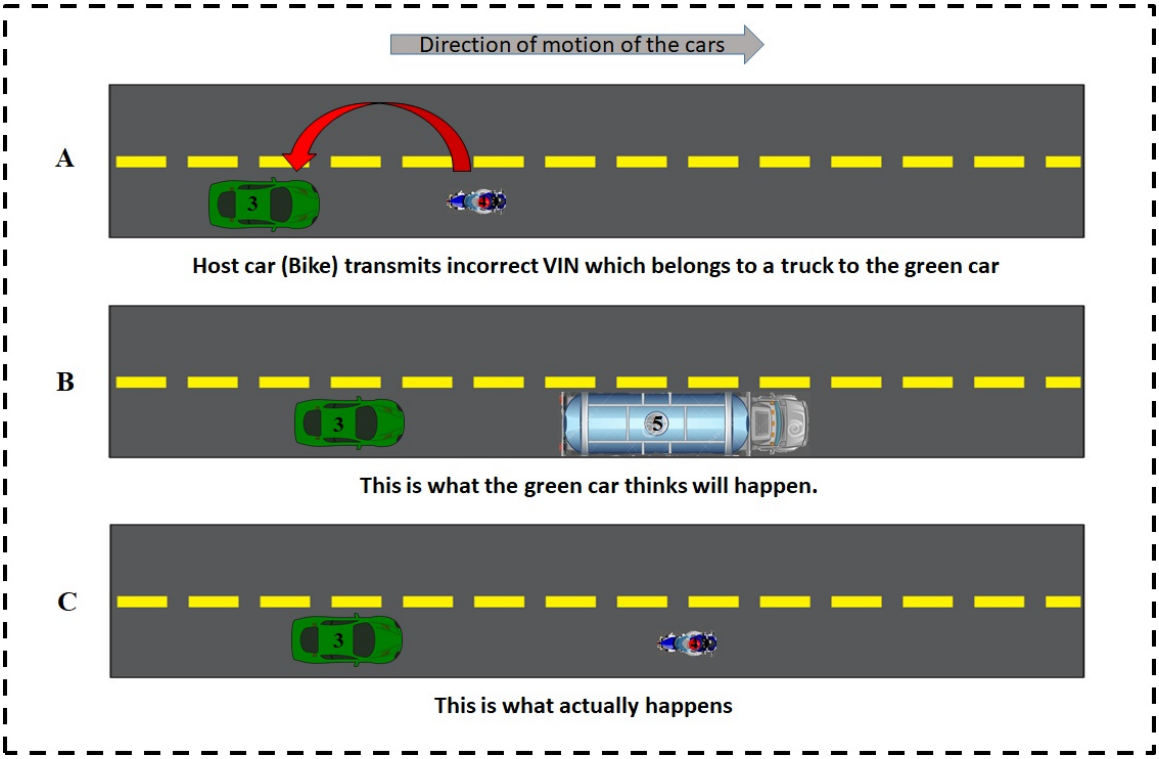

Figure 4.6: VIN Hazard 03 Scenario for Vehicle Behind the Host Vehicle

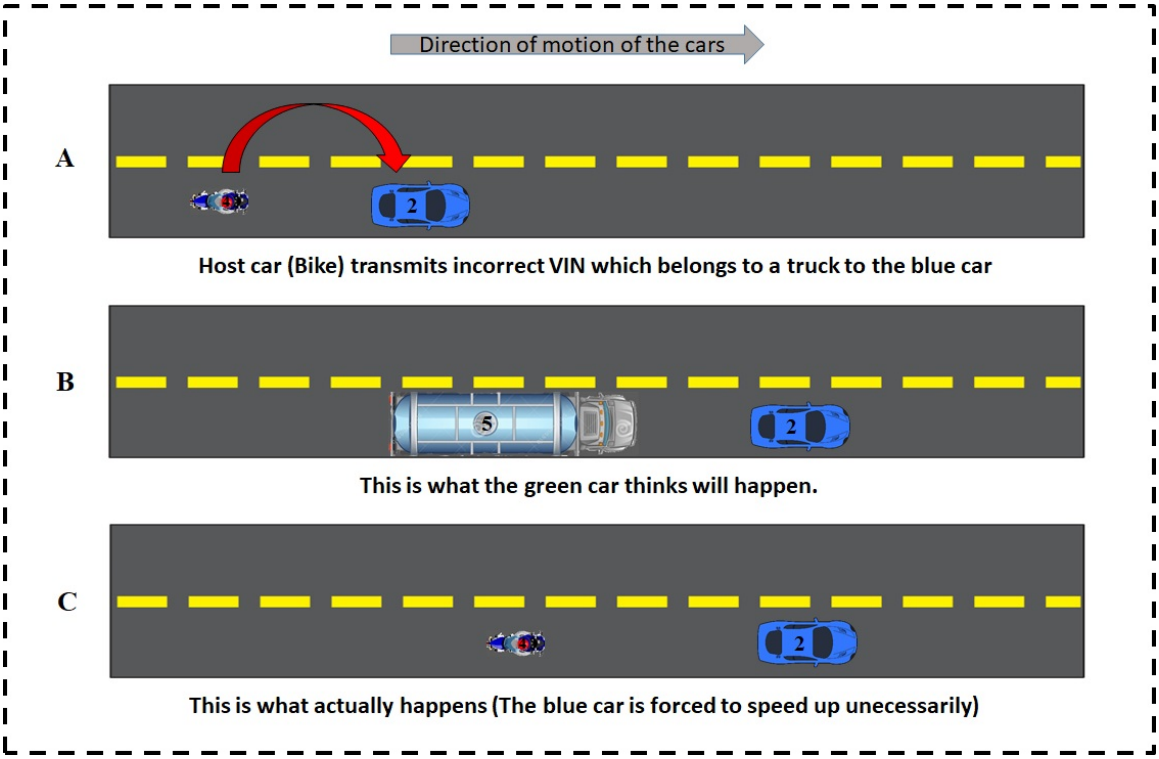

Figure 4.7: VIN Hazard 03 Scenario for Vehicle In Front the Host Vehicle

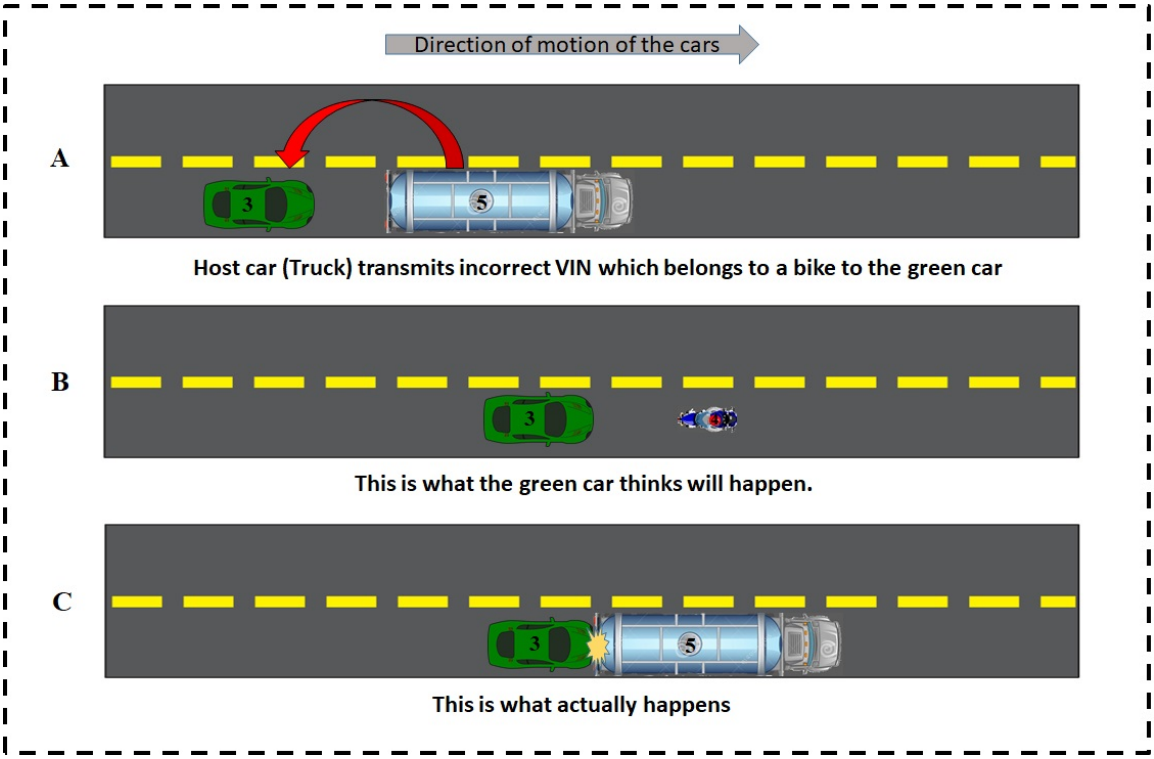

Figure 4.8: VIN Hazard 04 Scenario for Vehicle Behind the Host Vehicle

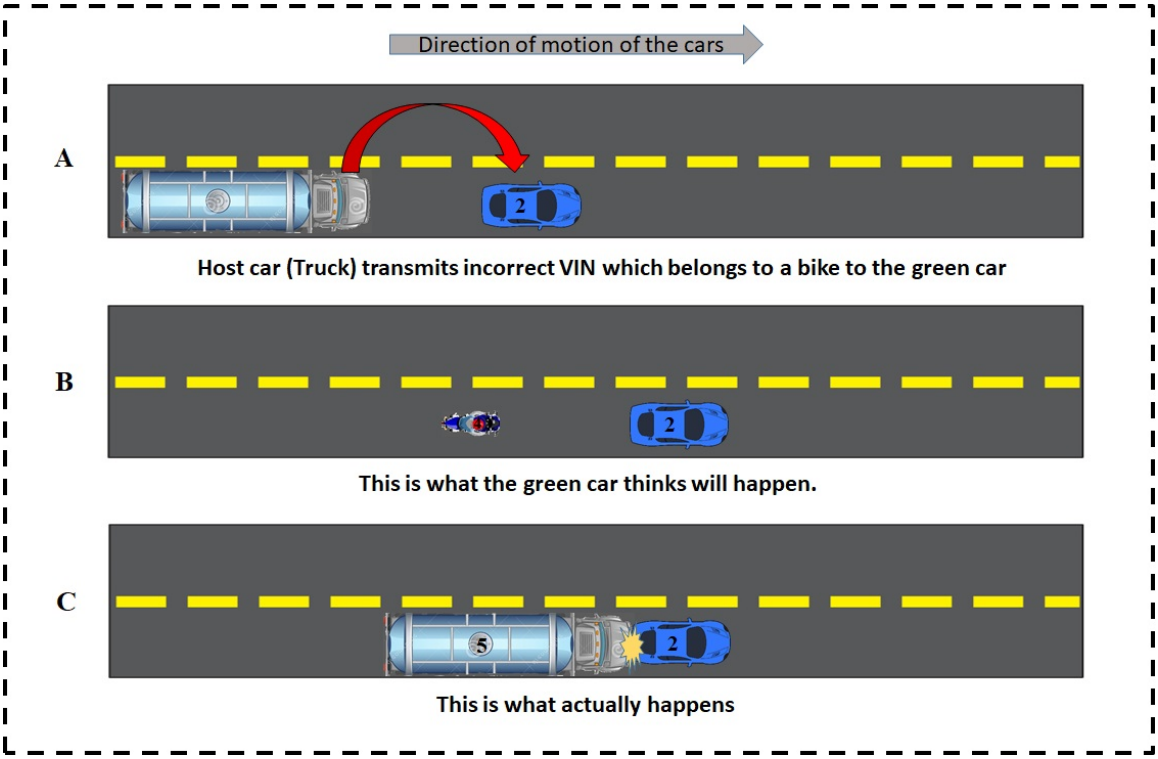

Figure 4.9: VIN Hazard 04 Scenario for Vehicle In Front the Host Vehicle

Table 4.2: Hazard Analysis and Risk Assessment (HARA) for VIN Transmission Function Part A

Name of Component : Intelligent Transport System (ITS) - V2V Communication					
Situation analysis and Hazard identification					
Hazard Situation No.	**Function**	**Hazard**	**Driving & Operation Situation**	**Details about failure**	**Effect of failure (and description of the possible hazard)**
HZ_01	Transmit VIN number from one vehicle to another	VIN is not transmitted by host / received by surrounding vehicles correctly	Driving on country / secondary road with traffic behind in short distance	The incorrect VIN that is transmitted does not correspond to any valid vehicle	Surrounding vehicles receive an invalid VIN and hence cannot extract further information like telemetry and dynamics
HZ_02				The incorrect VIN that is transmitted coincidently corresponds to some other valid vehicle of the same type as the host vehicle	Surrounding vehicles receive an incorrect but valid VIN and hence extract further information like telemetry and dynamics
HZ_03				The incorrect VIN that is transmitted coincidently corresponds to some other valid vehicle of different type than the host vehicle	Surrounding vehicles receive an incorrect but valid VIN and hence extract further information like telemetry and dynamics of a bigger vehicle than host
HZ_04					Surrounding vehicles receive an incorrect but valid VIN and hence extract further information like telemetry and dynamics of a smaller vehicle than host

Table 4.3: Hazard Analysis and Risk Assessment (HARA) for VIN Transmission Function Part B

Name of Component : Intelligent Transport System (ITS) - V2V Communication									
Hazard Classification							Determination of Safety Goal		
Severity	Justification - S	Probability of Exposure	Justification - E	Controllability	Justification - C	Resulting ASIL	Safety Goal No.	Safety Goal	Explanation
0 - 3		0 - 4		0 - 3		QM, ASIL A-D			
0	Other vehicles will detect error easily and hence will avoid collision	2	Due to multiple factors like software error or communication error this kind of hazard can occur	3	Transmittion in vehicles manufactured after 1996 is done by software and hence cannot be controlled by driver.	QM	SG_01	VIN must be correctly transmitted from the host vehicle and correctly received by surrounding vehicles	Invalid VIN number will have no information associated with it, and hence the software in other vehicles will detect the error and take necessary actions
0	Since the vehicle type corresponding to the incorrect VIN is same as host, therefore the telemetry & dynamics information, although errornous, is tolerable					QM			Since the vehicle type corresponding to the incorrect VIN is same as host, therefore the telemetry & dynamics information, although errornous, is tolerable
0	Since the vehicle type of the misinterpreted vehicle is larger in size than the host, a larger distance will be maintained between he two and hence no collision is possible					QM			A small (host) vehicle will be misinterpreted as a larger one by the surrounding vehicles, thus maintaining a larger distance. This will only lead to blocking of the traffic behind the host, but wont cause any harm to any individual.
3	Since the vehicle type of the misinterpreted vehicle is smaller in size than the host, a collision is possible					ASIL A			A large (host) vehicle will be misinterpreted as a smaller one by the surrounding vehicles, thus maintaining a smaller or no distance leading to collision which can be severe depending on the speed of the vehicle.

The vehicle behind the bike may come closer and cause a collision as shown in the Figure 4.8. Similarly, the vehicle in front may slow down thinking that its within the safe distance limit and cause a collision as show in Figure 4.9.

4.2.2.2 Analysis of Vehicle Telemetry Module Using Vehicle Relative Speed

Another piece of important information that will be transmitted from the host vehicle and received by the surrounding vehicle is the vehicle relative speed. Speed is a critical parameter and the surrounding vehicles adjust their relative speed according to the value received from the host vehicle. If this speed value received from the host vehicle is erroneous, then the surrounding vehicles will miscalculate the relative speed and positions and will either cause a collision or block the traffic behind. Speed also affects other dependent parameters like braking distance. Therefore we need to perform a HARA on the vehicle telemetry module. The HARA shown in Table 4.4 and Table 4.5 discusses four cases in which incorrect transmission of the speed value can cause hazards.

While performing HARA on the Vehicle Classification module, we didn't consider different roadway conditions, this was because the VIN number is not dependent on the roadway or climate conditions. However, for the vehicle telemetry values like speed, braking distance etc depend on the surface of the roadway, climate condition, etc. For example, a snow covered road might be slippery (less friction) and hence more braking distance. So while performing HARA we will consider two different types of roadway conditions. Hazards 05 and 06 will be considered on a secondary / country road, whereas the remaining hazards are on a highway where the speed of the cars will be very high.

Figures 4.10 and 4.11 depict the probable collision scenario that may result due the hazards 05-08. This paragraph provides instructions so as to how to read these diagrams in order to understand the scenario its depicting. These diagrams have 2 parts labeled A and B and three different types of vehicles namely : the host car labeled "1" and colored "red", the car in front of the host car labeled "2" and colored "blue" and the car behind the host car labeled "3" and colored "green" as shown in Figure 4.5. The direction in which the vehicles are traveling is from left to right.

Part A is the initial state of the scenario which shows V2V communication (vehicle speed transmission) taking place between the host and the surrounding vehicle. This communication is indicated by the curved red arrow as mentioned in the legend in Figure 4.5. This communication is presumed to be erroneous and hence the surrounding vehicles will get the wrong speed value from the host. Therefore, the surrounding vehicles will incorrectly interpret the speed of the host. Part B shows the hazardous scenario later in time which might result in a collision.

1. Hazard 05

   In this case, the speed value transmitted by the host car is less than its actual speed. When the surrounding cars receive this erroneous speed value, they miscalculate the speed and position of the host car with respect to them. Therefore, the surrounding cars slow down or maintain a low speed to avoid collision with the host. However, as the actual speed of the host is more than the transmitted speed value, the actual position of the host will be farther than the value calculated by the surrounding cars. Thus the car behind the host will block traffic behind it and the car in front of the host may collide with the host car as shown in the Figure 4.10.

2. Hazard 06

   In this case, the speed value transmitted by the host car is more than its actual speed. When the surrounding cars receive this erroneous speed value, they miscalculate the speed and position of the host car with respect to them. Therefore, the surrounding cars may speed up trying to keep up with the host. However, as the actual speed of the host is less than the transmitted speed value, the actual position of the host will be behind the position value calculated by the surrounding cars. Thus the car in front of the host will drive away from the host and will not be affected much. However, the car behind the host car may

speed up and collide with the host car as shown in the Figure 4.11.

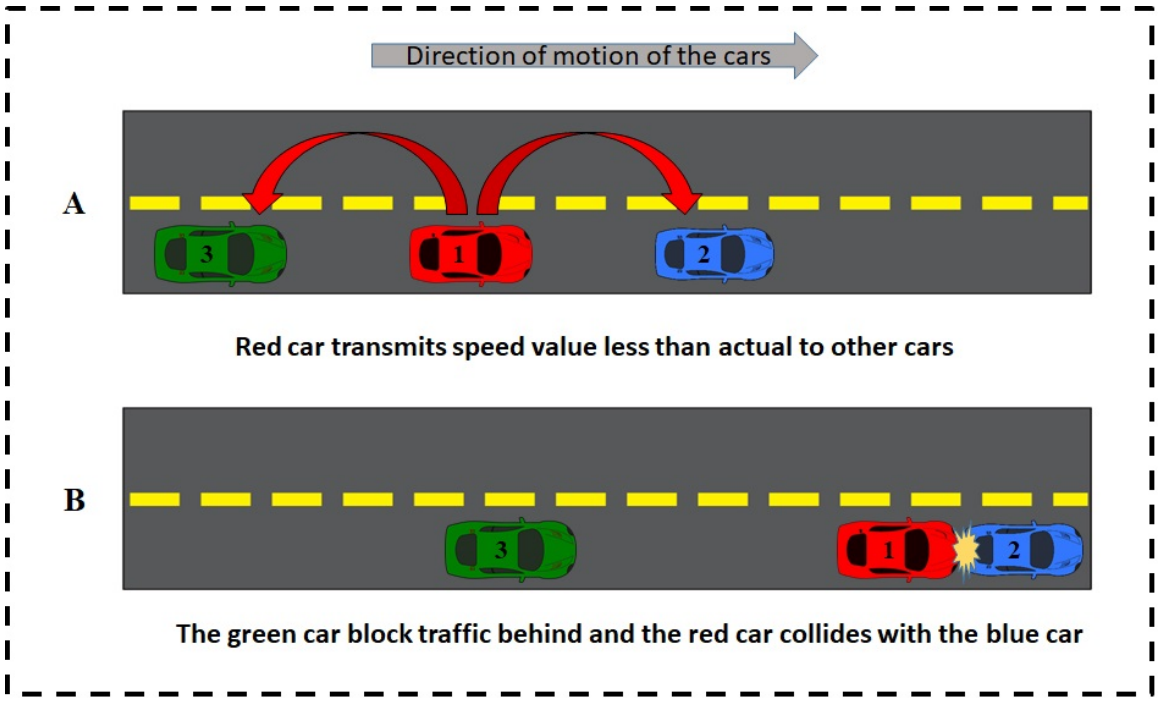

Figure 4.10: Potential Collision Scenario Caused when Transmitted Speed is Less than Actual Speed

3. Hazard 07

   This case is very similar to Hazard 05, the only difference is that the roadway conditions are different. Hazard 05 is on a secondary / country road and Hazard 07 is on a highway which will be more severe. This is because, vehicles are at a high speed and therefore, controllability and severity factors go one level up and so does the ASIL assignment value. An explanation to this can be found in Table 4.5.

4. Hazard 08

   This case is very similar to Hazard 06, the only difference is that the roadway conditions are different. Hazard 06 is on a secondary / country road and Hazard 08 is on a highway which will be more severe. This is because, vehicles are at a high speed and therefore, controllability and severity factors go one level up

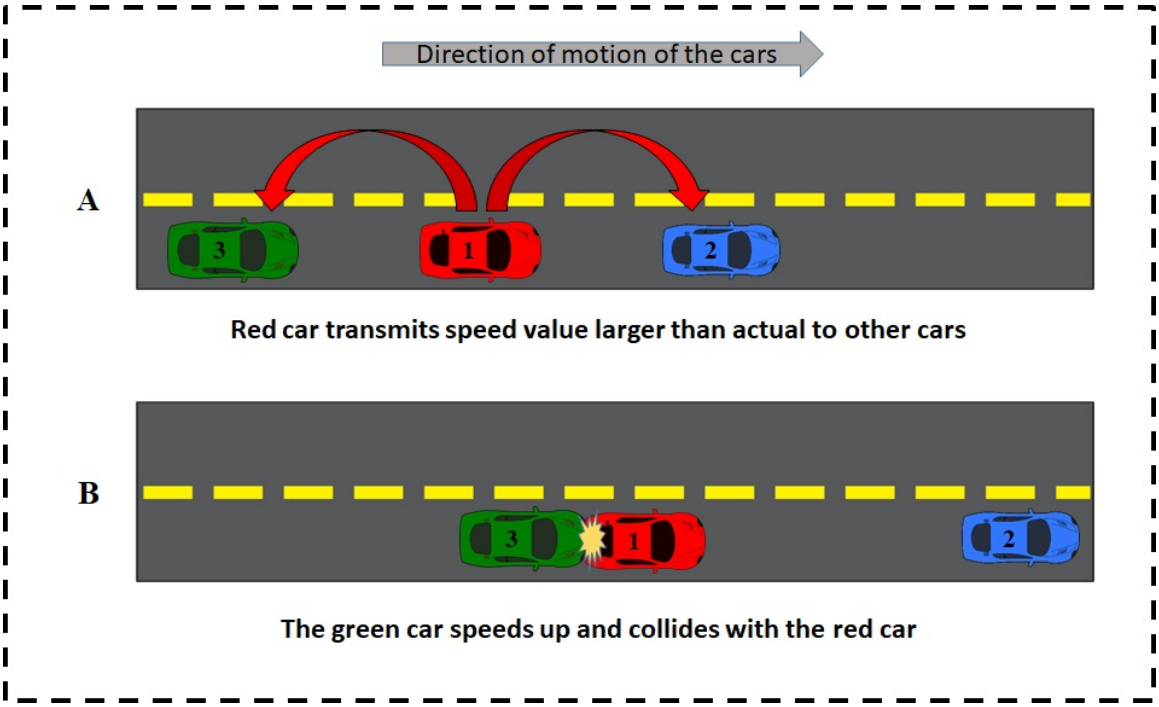

Figure 4.11: Potential Collision Scenario Caused when Transmitted Speed is More than Actual Speed

and so does the ASIL assignment value. An explanation to this can be found in Table 4.5.

4.2.3 ASIL Assignment

This section is dedicated to determine the ASIL of the hazards discussed in Section 4.2.2. The ASIL levels have been assigned to each of these hazards while performing HARA.

4.2.3.1 ASIL Assignment for the Vehicle Classification Module

ASIL for hazards 01-04 can be found in Table 4.3. It is observed that the hazards 01-03 are assigned QM and therefore they are not critical with respect to safety standards. However, hazard 04 is a critical scenario and there is a possibility of collision. The magnitude of damage caused due to his collision will vary depending on the speed of the vehicles, condition and type of roadway and other such factors. Therefore, hazard 04 is assigned ASIL A. According to the ISO 26262 standard, when

different hazards are assigned different ASILs then the overall component is assigned the highest level amongst them. Since ASIL A is higher than QM, therefore the Vehicle Classification Module is assigned ASIL A.

4.2.3.2 ASIL Assignment for the Vehicle Telemetry Module

ASIL for hazards 05-08 can be found in Table 4.5. It is observed that the hazards 05 and 07 are very identical and the only difference between them is the type of roadway. Same is the case with hazards 06 and 08. The hazards 05 and 06 are on a secondary roadway, where the speed is relatively low and therefore the controllability of driver is good. On the other hand, hazards 07 and 08 occur when the roadway is a highway, speed of the vehicles is high and controllability is bad as compared to the former case. Therefore, hazards 05 and 06 are assigned ASIL A and the hazards 07 and 08 are assigned ASIL B. According to the ISO 26262 standard, when different hazards are assigned different ASILs then the overall component is assigned the highest level amongst them. Since ASIL B is higher than ASIL A, therefore the Vehicle Telemetry Module is assigned ASIL B.

4.2.4 Defining Safety Goals

Safety Goals can be derived from each hazards. Sometimes multiple hazards can have same safety goals and hence can be grouped together. For example, hazards 01-04 have the same safety goals and hence are grouped together. We have determined two safety goals, one of each of the Classification (refer Table 4.3) and the Telemetry module (refer Table 4.5).

1. Safety Goal 01

   The vehicle classification module must classify the vehicle correctly after receiving the VIN from it.

2. Safety Goal 02

Vehicle telemetry module must determine the value of its safe speed correctly after receiving the relative speed from the host vehicle.

4.2.5 Defining Functional Safety Requirements

Now based on the Safety Goals defined in Section 4.2.4, we will determine FSRs for the Vehicle Classification and Vehicle Telemetry Modules.

4.2.5.1 FSR for Vehicle Classification Module

1. FSR 01

   The vehicle after the receiving the VIN via V2V communication, must correctly determine te type of vehicle.

2. FSR 02

   Once the type is determined, the Vehicle Classification Module must extract information corresponding to that particular type / model of vehicle from the centralized server.

4.2.5.2 FSR for Vehicle Telemetry Module

1. FSR 03

   The vehicle after the receiving the front vehicle's relative speed via V2V communication, must correctly determine the speed of the vehicle.

2. FSR 04

   The vehicle after the receiving the rear vehicle's relative speed via V2V communication, must correctly determine the speed of the vehicle.

3. FSR 05

   Once the front vehicle's speed is determined, the Vehicle Telemetry Module must determine the minimum speed that it should maintain to avoid blocking traffic behind or causing a collision with the rear vehicle.

4. FSR 06

   The Vehicle Telemetry Module must determine the maximum speed that it can attain while avoiding collision with the vehicle in front of it.

4.2.6 Defining Technical Safety Requirements

Now based on the Safety Goals and FSRs defined in Sections 4.2.4 and 4.2.5 respectively, we will determine TSRs for the Vehicle Classification and Vehicle Telemetry Modules.

4.2.6.1 TSR for Vehicle Classification Module

Considering the Vehicle Classification module from a technical point of view, we observe that it is largely dependent on the V2V communication module and the centralized database. There is one more factor on which the correct transmission of VIN is dependent: the source that provides VIN to the V2V communication module. For vehicle manufactured after 1996, this source is the vehicle diagnostic module for which the functional safety standards already exist and hence can be handled easily. However, for legacy vehicles the source of VIN is the manual input given by the driver. The High Level Block Diagram in Figure 4.12 shows ITS model for legacy vehicles.

From this above information we determine the following TSRs:

1. TSR 01

   For vehicle that are manufactured after 1996, the vehicle diagnostic module provide correct VIN to the V2V communication module for transmission.

2. TSR 02

   For vehicle that are manufactured before 1996, the vehicle must prompt a confirmation message before accepting the VIN value from the driver.

3. TSR 03

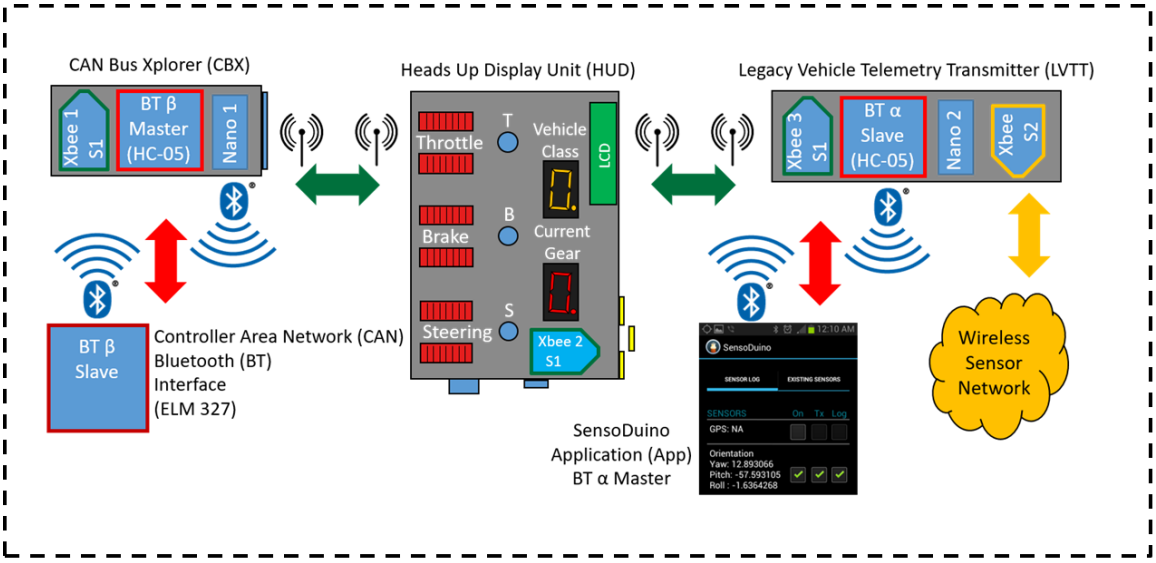

Figure 4.12: High Level Block Diagram [6]

The V2V communication module must transmit the VIN correctly to the surrounding vehicles.

4. TSR 04

   The V2V communication module must receive the VIN correctly from the surrounding vehicles.

5. TSR 05

   The centralized database must return correct information about the vehicle dynamics corresponding to the VIN provided by the vehicle classification module.

As we can see from the above TSR, they belong to different modules and therefore need to be taken care by their developers. According to ISO 26262 Part 2 [10], since these TSR rely on other modules, they must be allocated to their respective modules.

4.2.6.2 TSR for Vehicle Telemetry Module

For converting the FSRs related to this module into TSRs. We need to do a technical analysis of the hazard scenarios. Therefore, we will consider two different approaches. The first approach will be based on type of vehicle (with and without

collision detector sensors) and second by considering type of roadway. TSRs 06-09 follow first approach and rest follow second approach.

1. TSR 06

   If the vehicle is equipped with collision detector sensors, the vehicle must not completely rely on the speed calculated by the vehicle telemetry module alone. It must also consult collision detect module for safe distance clearance check between front and rear vehicles before speeding up or slowing down.

2. TSR 07

   If the vehicle sensors detect presence of a vehicle within the safe distance limit then a warning is to be issued in the form of visual warning such as light flashes or audio warning like honking the horn or both.

3. TSR 08

   If the vehicle is not equipped with collision detector sensors, the vehicle must follow a speed value that is a little less that the value calculated by the vehicle telemetry module.

4. TSR 09

   If the vehicle is not equipped with collision detector sensors, the vehicle must prompt the driver to check if proper distance is being maintained between both the front and the rear vehicle.

5. TSR 10

   If the vehicle is on a secondary or a relatively slower roadway it must follow TSRs 06-09 to maintain safe distance.

6. TSR 11

If the vehicle is on a highway and equipped with collision detector sensors, it must follow TSRs 06 and 07. If it detects presence of vehicle within the safe distance limit then a warning is to be sent to it via V2V communication.

7. TSR 12

   If the vehicle is on a highway and is not equipped with collision detector sensors, it must follow TSRs 08 and 09. It must inform the surrounding vehicles that it is without collision detection mechanism via V2V communication.

In this way we have developed our Functional Safety Concept in this Chapter. The next will discuss the result on applying this concept to our ITS modules.

Table 4.4: Hazard Analysis and Risk Assessment (HARA) for Transmission of Relative Speed Function Part A

Name of Component : Intelligent Transport System (ITS) - V2V Communication					
Situation analysis and Hazard identification					
Hazard Situation No.	**Function**	**Hazard**	**Driving & Operation Situation**	**Details about failure**	**Effect of failure (and description of the possible hazard)**
HZ_05	Transmit vehicle relative speed from one vehicle to another	Vehicle relative speed is not transmitted by host / received by surrounding vehicles correctly	Driving on country / secondary road with traffic behind in short distance	The speed that is transmitted is less than the actual speed of the host vehicle	Surrounding vehicle thinks that the host vehicle is slower than the actual speed
HZ_06				The speed that is transmitted is more than the actual speed of the host vehicle	Surrounding vehicle thinks that the host vehicle is faster than the actual speed
HZ_07		Vehicle relative speed is not transmitted by host / received by surrounding vehicles correctly	Driving on a highway with high speed traffic behind in short distance	The speed that is transmitted is less than the actual speed of the host vehicle	Surrounding vehicle thinks that the host vehicle is slower than the actual speed
HZ_08				The speed that is transmitted is more than the actual speed of the host vehicle	Surrounding vehicle thinks that the host vehicle is faster than the actual speed

Table 4.5: Hazard Analysis and Risk Assessment (HARA) for Transmission of Relative Speed Function Part B

Name of Component : Intelligent Transport System (ITS) - V2V Communication									
Hazard Classification							Determination of Safety Goal		
Severity	Justification - S	Probability of Exposure	Justification - E	Controllability	Justification - C	Resulting ASIL	Safety Goal No.	Safety Goal	Explanation
0 - 3		0 - 4		0 - 3		QM, ASIL A-D			
3	The vehicle in front of host vehicle can fail to maintain distance and may cause collision	2	Due to multiple factors like software error or communication error this kind of hazard can occur	2	Host driver has to pay attention when speeding, other driver has to pay attention and increase distance between the vehicles if possible. Normally controllable; majority of drivers are able to avoid accident	ASIL A	SG_02	Vehicle relative speed must be correctly transmitted from the Host vehicle to another vehicles	In this case, the vehicle behind the host thinks that the host is slow and maintains a slow speed thereby blocking the traffic behind it. The vehicle in front of the host is in more danger of getting hit by the host which is approaching at a higher speed than what is interpreted.
3	The vehicle behind the host vehicle can fail to maintain distance and may cause collision			2	Host driver has to pay attention on vehicles approaching from behind, other driver has to pay attention while speeding. Normally controllable; majority of drivers are able to avoid accident	ASIL A			In this case, the vehicle behind the host thinks that the host is faster than it actually is and may increase its speed which may cause an accident. The vehicle in front of the host is relatively safe.
3	The vehicle in front of host vehicle can fail to maintain distance and may cause collision	3	Due to multiple factors like software error or communication error this kind of hazard can occur	2	Vehicles are very fast on the highway, a very skilled driver may control this situation but it is required for all the surrounding drivers to have same level of skill which is very rare.	ASIL B	SG_02	Vehicle relative speed must be correctly transmitted from the host vehicle to another vehicles	In this case, the vehicle behind the host thinks that the host is slow and maintains a slow speed thereby blocking the traffic behind it. The vehicle in front of the host is in more danger of getting hit by the host which is approaching at a higher speed than what is interpreted.
3	The vehicle behind the host vehicle can fail to maintain distance and may cause collision			2	Vehicles are very fast on the highway, a very skilled driver may control this situation but it is required for all the surrounding drivers to have same level of skill which is very rare.	ASIL B			In this case, the vehicle behind the host thinks that the host is faster than it actually is and may increase its speed which may cause an accident. The vehicle in front of the host is relatively safe.

CHAPTER 5: RESULTS

This chapter shows the results after implementing the safety requirements in the framework. Figures 5.4, 5.5, 5.1, 5.2, 5.6 and 5.3 depict the probable collision scenario that may result due the hazards 05-08. This paragraph provides instructions so as to how to read these diagrams in order to understand the scenario its depicting. These diagrams have 3 parts labeled A, B and C and three different types of vehicles namely: the host car labeled "1" and colored "red", the car in front of the host car labeled "2" and colored "blue" and the car behind the host car labeled "3" and colored "green" as shown in Figure 4.5. Some cars have collision detect sensors represented by blue beams in front and rear of the that car. The direction in which the vehicles are traveling is from left to right. Part A is the initial state of the scenario which shows V2V communication (vehicle speed transmission) taking place between the host and the surrounding vehicle. This communication is indicated by the curved red arrow as mentioned in the legend in Figure 4.5. This communication is presumed to be erroneous and hence the surrounding vehicles will get the wrong speed value from the host. Therefore, the surrounding vehicles will incorrectly interpret the speed of the host.

For figures 5.4, 5.5, 5.1 and 5.2 part B shows a state in which two vehicles come close to each other and the vehicle with collision detect sensors detect the other vehicle. Part C shows the how the collision is avoided. Whereas, for figures 5.6 and 5.3 part B shows a state in which two vehicles collide when the surrounding vehicles follow the received (erroneous) value of speed. Part C shows how the collision can be delayed if the surrounding vehicles apply the safety adjustment to the received speed value.

5.1 Safety concept application for speed hazard

Following are the different approaches based on the type of vehicles under consideration, suggested by the author to tackle the hazardous situations discussed in Chapter 4. Vehicle can be divided into two major types, one with collision detect sensors and others without the sensors. Usually, the latest models of many vehicles are equipped with ADAS which has variety of sensors associated with them.

1. When transmitted speed is less than actual

   This hazardous situation is discussed in Section 4.2.2.2 as Hazards 05 and 07. The surrounding vehicle receives a speed value that is less than the actual speed of the host vehicle via the V2V communication from the host vehicle. The calculations done by the vehicle telemetry module are based on this erroneous value. This may encourage the surrounding vehicle to maintain a relatively low speed. As shown in Figure 4.10, the vehicle that is behind of the host will slow down and block the traffic behind it. However, the vehicle in front of the host vehicle might speed up with respect to the host and cause a collision with the host.

   1.1. If only the host vehicle has collision detect sensors:

   If the host vehicle is equipped with collision detect sensors, the surrounding vehicle can be detected by the host if the distance between them decreases. Thus when the host approaches the blue car, it detects the blue car and a warning is issued in the form of a visual signal like flashing of lights or an audio signal like sounding the horn. A telltale signal is also sent to the blue car via V2V to alert the driver and the host car reduces its speed. Thus a potential hazard is avoided as shown in Part C of Figure 5.1. This solution is based on the TSRs 06 and 07.

   1.2. If only the surrounding vehicle has collision detect sensors:

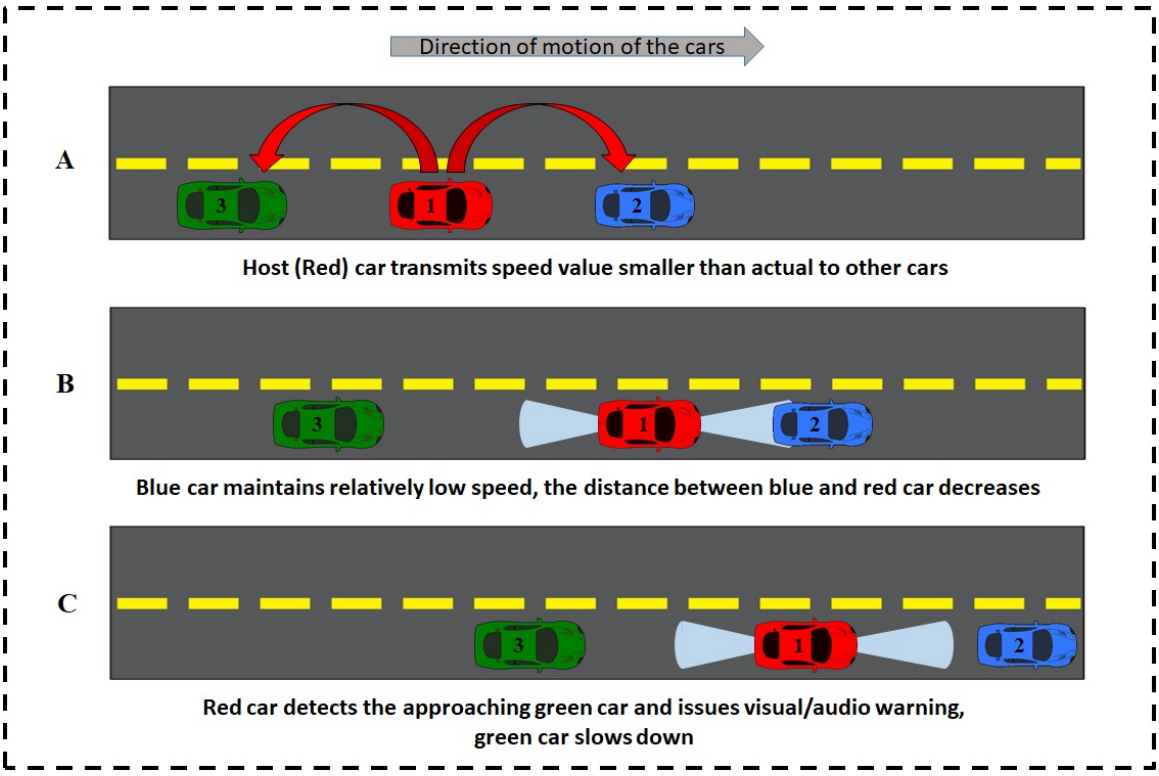

Figure 5.1: Potential Collision Scenario Caused when Transmitted Speed is Less than Actual Speed

If the surrounding vehicle is equipped with collision detect sensors, the host can be detected by it if the distance between them decreases. Thus when the host approaches the blue vehicle from the rear end, the host is detected by the blue car and warning is issued in the form of a visual signal like flashing of lights or an audio signal like sounding the horn and the host is asked to reduce its speed. A telltale signal is also sent to the host car via V2V to alert the driver. Thus a potential hazard is avoided as shown in Part C of Figure 5.2. This solution is based on the TSRs 06 and 07.

1.3. If only the both the vehicles have collision detect sensors:

If both the host and the surrounding vehicle is equipped with collision detect sensors, the first one who detects the other one issues a warning. Thus a potential hazard is avoided.

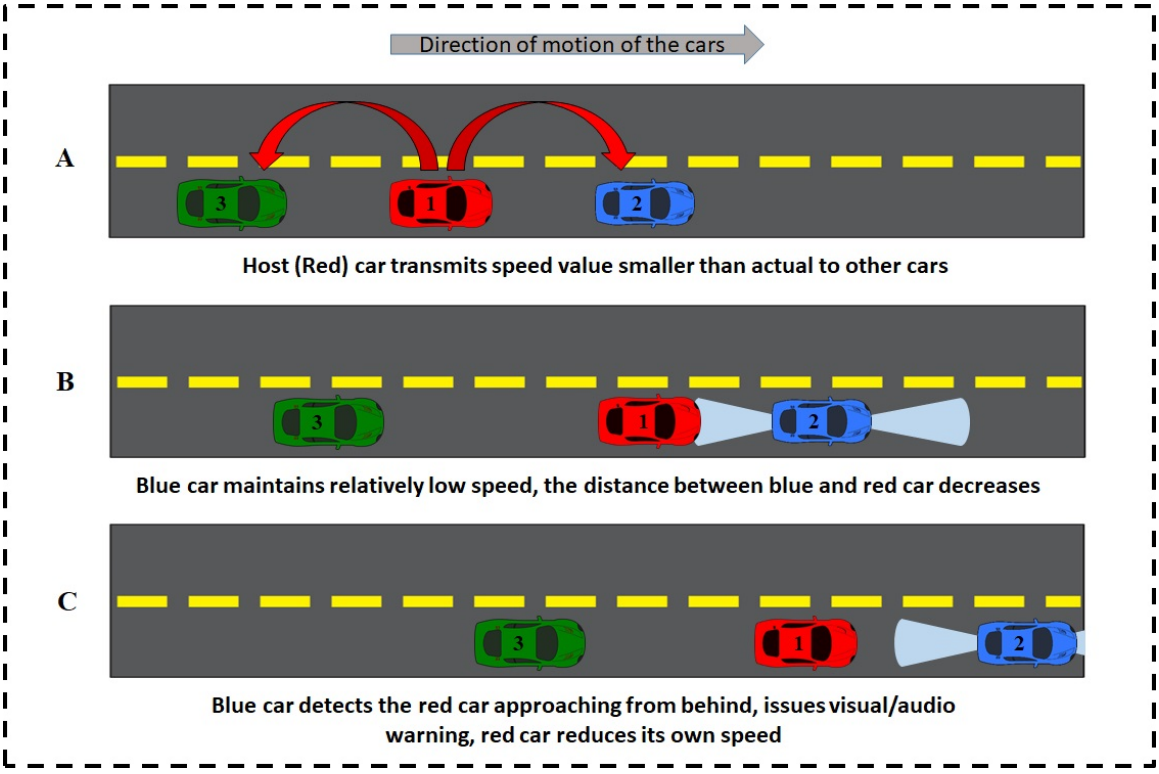

Figure 5.2: Potential Collision Scenario Caused when Transmitted Speed is Less than Actual Speed

1.4. If only the both the vehicles don't have collision detect sensors:

This is a worst case scenario where both the host and the surrounding vehicle are without collision detect sensors. Therefore, according to TSR 09 the surrounding vehicle informs the host that it is a vehicle without collision detection mechanism. Therefore, the host must follow a speed less than the value transmitted. The difference between the transmitted value and this value is termed as safety speed adjustment by the author. Therefore, the time to collision is extended. This time is utilized by the driver to retake the control over the speed and avoid collision. This solution is shown in Figure 5.3, Part B shows the situation if a safety speed adjustment suggested by the author is not used and Part C shows if the safety speed adjustment is used.

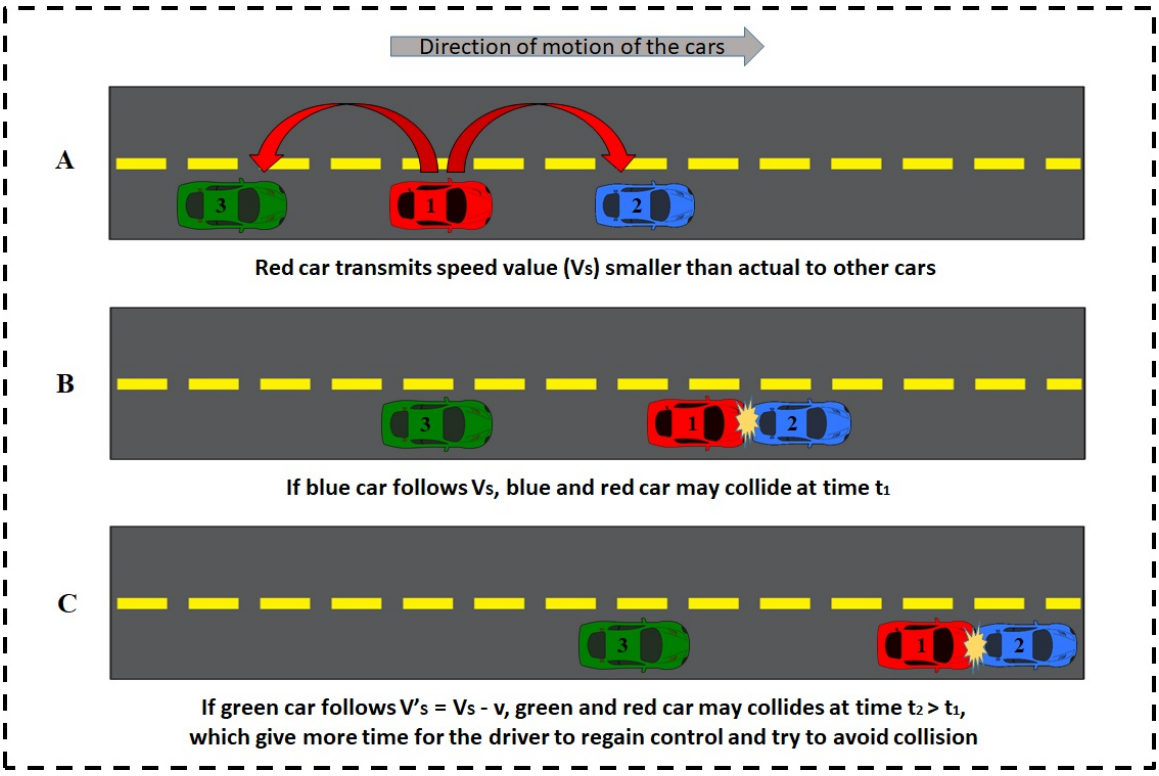

Figure 5.3: Potential Collision Scenario Caused when Transmitted Speed is Less than Actual Speed

2. When transmitted speed is more than actual:

   This hazardous situation is discussed in Section 4.2.2.2 as Hazards 06 and 08. The surrounding vehicle receives a speed value that is less than the actual speed of the host vehicle via the V2V communication from the host vehicle. Now the calculations done by the vehicle telemetry module are based on this erroneous value. This may encourage the surrounding vehicle to increase its own speed. As shown in Figure 4.11, the host vehicle will not be affected by the vehicle in front, because it will speed up and drive away from the host. However, a collision may be caused due to the vehicle behind the host vehicle as it speeds up towards the host vehicle.

   2.1. If only the host vehicle has collision detect sensors:

   If the host vehicle is equipped with collision detect sensors, the vehicles

approaching from the rear or the vehicles blocking the way in the front of host can be detected. Thus when the green vehicle approaches the host from the rear end, it is detected by the host and a warning is issued in the form of a visual signal like flashing of lights or an audio signal like sounding the horn. A telltale signal is also sent to the green car via V2V to alert the driver and the green car is asked to reduce its speed. Thus a potential hazard is avoided as shown in Part C of Figure 5.4. This solution is based on the TSRs 06 and 07.

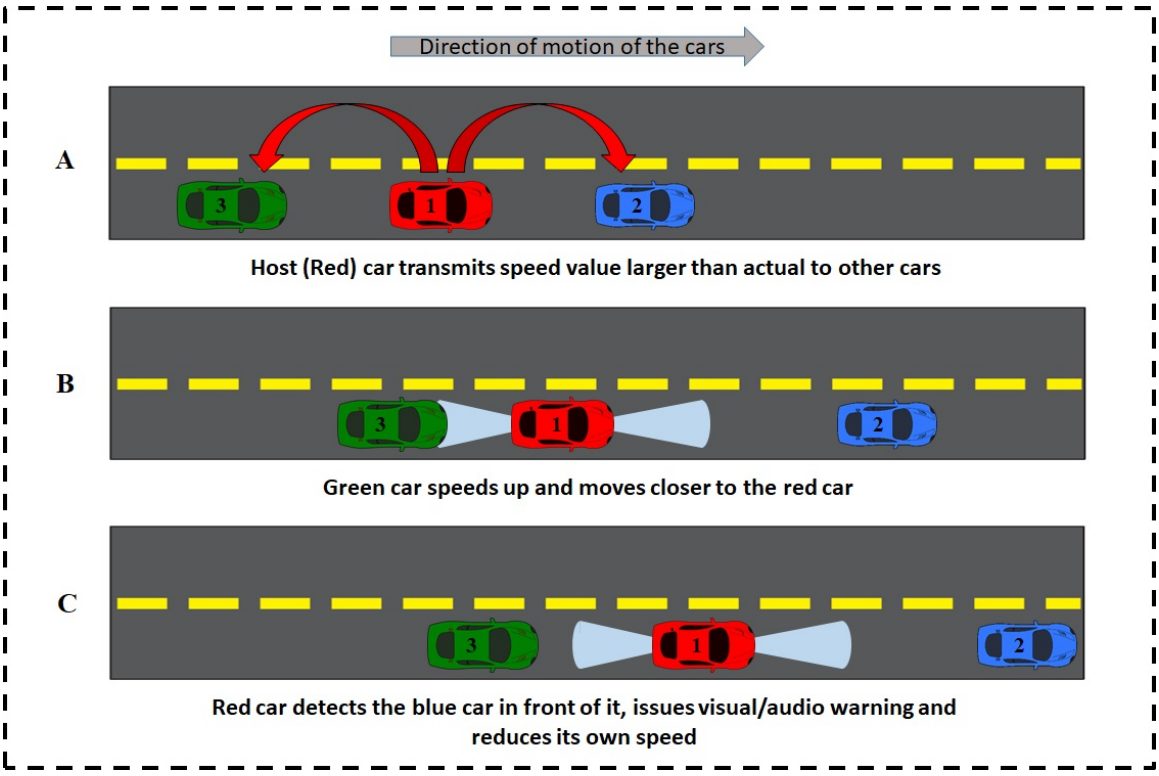

Figure 5.4: Potential Collision Scenario Caused when Transmitted Speed is Less than Actual Speed

2.2. If only the surrounding vehicle has collision detect sensors:

If the surrounding vehicle is equipped with collision detect sensors, the host can be detected by it if the distance between them decreases. Thus when the green vehicle approaches the host from the rear end, the host is detected by the green car and warning is issued in the form of a visual

signal like flashing of lights or an audio signal like sounding the horn. The speed of the green vehicle is also reduced. A telltale signal is also sent to the host car via V2V to alert the driver. Thus a potential hazard is avoided as shown in Part C of Figure 5.5. This solution is based on the TSRs 06 and 07.

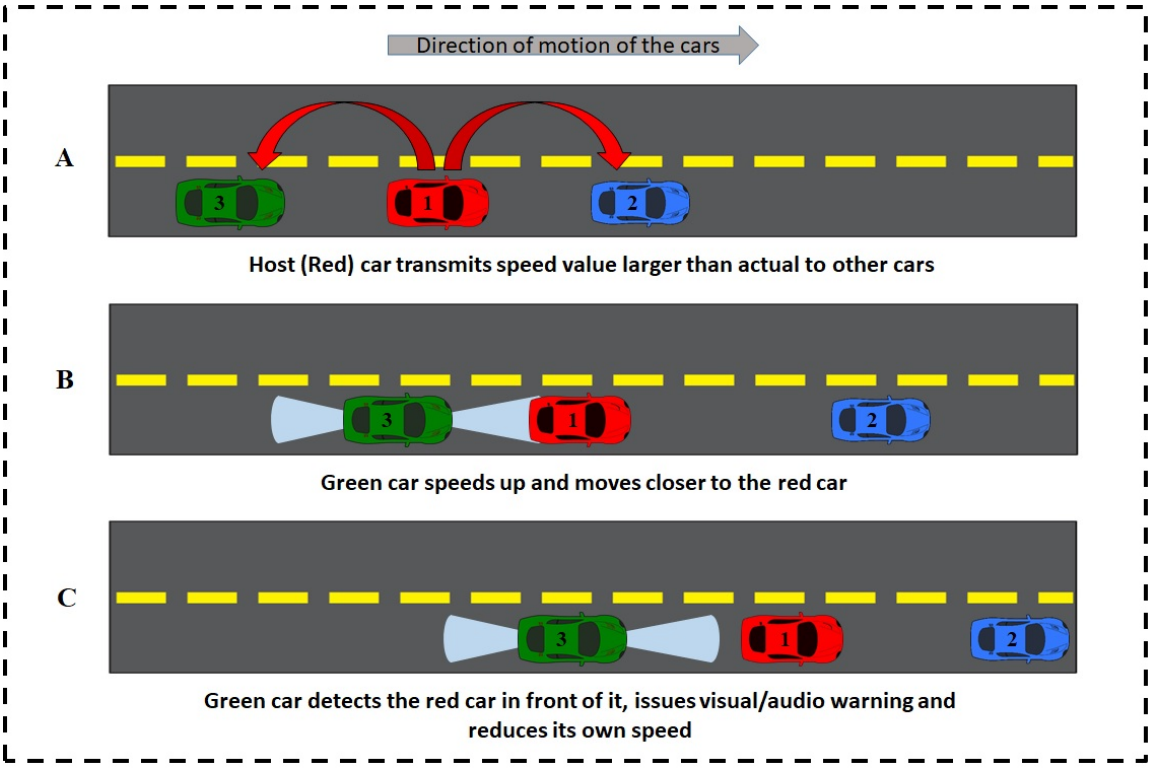

Figure 5.5: Potential Collision Scenario Caused when Transmitted Speed is Less than Actual Speed

2.3. If only the both the vehicles have collision detect sensors:

If both the host and the surrounding vehicle is equipped with collision detect sensors, the first one who detects the other one issues a warning. Thus a potential hazard is avoided.

2.4. If only the both the vehicles don't have collision detect sensors:

This is a worst case scenario where both the host and the surrounding vehicle are without collision detect sensors. Therefore, according to TSR 08 the

surrounding vehicle follows a speed value less than the value transmitted by the host. The difference between the transmitted value and this value is termed as safety speed adjustment by the author. Therefore, the time to collision is extended. This time is utilized by the driver to retake the control over the speed and avoid collision. This solution is shown in Figure 5.6, Part B shows the situation if a safety speed adjustment suggested by the author is not used and Part C shows if the safety speed adjustment is used.

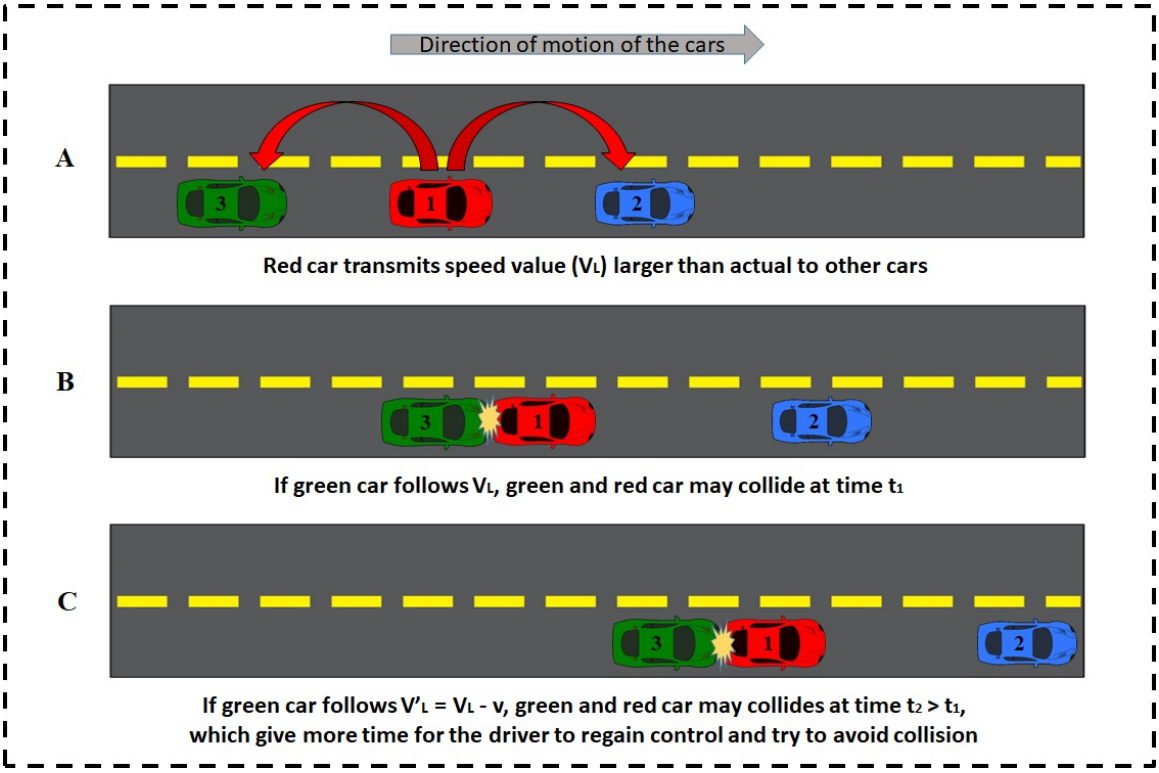

Figure 5.6: Potential Collision Scenario Caused when Transmitted Speed is Less than Actual Speed

CHAPTER 6: CONCLUSIONS AND FUTURE SCOPE

6.1 Conclusions

The review phase of this thesis involved a detailed study of the ISO 26262 standard and different methods used for incorporating this standard in autonomous vehicles. The survey consisted of a study of three different techniques used to make the autonomous vehicle functionally safe. The first method discussed about the AVC module which is based on the study of the ATC module used in trains. The second method was based on the study of autopilot and their failure scenarios for airplanes. And the third method was an approach that discussed the integrated and incorporation of functional safety and cyber security in the vehicle. This survey also discussed how the present safety standards were insufficient for autonomous vehicles.

This thesis also discussed the ITS framework developed at UNC Charlotte. A HARA analysis was performed on the vehicle partition of this ITS framework. The analysis discussed about the different hazards that may be caused due to the incorrect transmission of the VIN and the vehicle speed from the host vehicle to the surrounding vehicles via the V2V communication. The VIN transmission affected the vehicle classification module whereas the speed transmission affected the vehicle telemetry moduel. Safety goals were defined and assigned to each of the hazard. This helped to determine the level of criticality and therefore decide the level of ASIL that was assigned to the two modules. The vehicle classification module was assigned ASIL A and the vehicle telemetry module was assigned ASIL B. The safety goals were then converted into the FSRs and then into the TSRs. Based on the TSRs a solution to the problem was suggested.

This thesis work comprised four different approaches to incorporate safety in the

ITS framework. The first approach increased the number of vehicles under consideration. The traditional way of performing the safety analysis was to consider one vehicle's safety only. This thesis adapted a three vehicle approach: a host vehicle which is the main vehicle and two other vehicles that may be affected due to the incorrect data forwarded by the host vehicle. The second approach is based on classifying the vehicles into different classes based on the dynamics of the car. The third approach considers different types of roadways on basis of the speed limits. Based on the speed of the vehicle, parameters like braking distance, time of collision, force of impact during collision may be different. And finally while suggesting the failsafe measure, the vehicle are classified again, but on the basis of availability of collision detection mechanism in the vehicles. This is discussed in Section 5.1.

6.2 Future Scope

This thesis was based on various primary assumptions mentioned in Section 4.2.1 that helped reduce the complexity and limit the scope of this thesis. However, there are a few things that the author of this thesis plans on adding in the future. This thesis was primarily based on the fact that an ITS framework is established and multiple vehicles communicate with each other. Therefore, a safety analysis was performed on a multiple vehicle system. However, only two vehicles, one in front and the other in the rear of the host vehicle were considered. The vehicles on adjacent lanes were not considered. In future the author wishes to eliminate this assumption and consider multiple lanes and hazards that maybe caused during lane change. The solutions to avoid collision discussed in this thesis involves adjusting the speed, alert messages etc. Lane changes can also be considered as a way to avoid collisions when two vehicle travel at different speeds.

The hazard analysis that was performed on the vehicle classification module indicated that the proper transmission of the VIN depended on the data transmission from the V2V communication module. Thus the safety of one module is dependent

on the reliability of the data transmitted from a communication module. This communication module is vulnerable to cyber attacks. This thesis is mainly concerned with the functional safety and not the cyber security. However, if an integrated model of safety-security as discussed in the research by the authors of [23] and the survey [27] conducted by the author of this thesis then the reliability of the data received or transmitted by this V2V module increases.

In the previous work [6], the author classifies the vehicles into six different types. This thesis considers only the first five types and reserves type six vehicle as a part of the future scope. Type six vehicles include the emergency vehicles like a police vehicle, an ambulance, or a fire truck. Such vehicles are priority vehicles and therefore they need to be handled separately. The hazards may include an escape of a felon from the hands of police, delay in providing medical facilities to a patient inside an ambulance, etc. Therefore, these type six vehicle need to be specially addressed in the future work. The ITS framework also has a second partition called the "Infrastructure Partition". The author may also analyze this partition as a part of the future work.

REFERENCES

[1] "WHO | Global status report on road safety 2015," *WHO*, 2016.

[2] R. Bell, "Introduction to IEC 61508," in *Conferences in Research and Practice in Information Technology Series*, 2005.

[3] M. Broy and Manfred, "Challenges in automotive software engineering," in *Proceeding of the 28th international conference on Software engineering - ICSE '06*, (New York, New York, USA), ACM Press, May 2006.

[4] H. Altinger, Y. Dajsuren, S. Siegl, J. J. Vinju, and F. Wotawa, "On Error-Class Distribution in Automotive Model-Based Software," in *2016 IEEE 23rd International Conference on Software Analysis, Evolution, and Reengineering (SANER)*, pp. 688–692, IEEE, mar 2016.

[5] G. Bahig and A. El-Kadi, "Formal Verification of Automotive Design in Compliance With ISO 26262 Design Verification Guidelines," *IEEE Access*, vol. 5, pp. 4505–4516, 2017.

[6] B. B. Rhoades, *A novel framework for integrating legacy vehicles into an intelligent transportation system.* PhD thesis, University of North Carolina at Charlotte, May 2018.

[7] M. Born, J. Favaro, and O. Kath, "Application of ISO DIS 26262 in practice," in *Proceedings of the 1st Workshop on Critical Automotive applications Robustness & Safety - CARS '10*, (New York, New York, USA), p. 3, ACM Press, 2010.

[8] "ISO 26262-1:2011 - Road vehicles – Functional safety – Part 1: Vocabulary."

[9] "ISO 26262-2:2011 - Road vehicles – Functional safety – Part 2: Management of functional safety."

[10] "ISO 26262-3:2011 - Road vehicles – Functional safety – Part 3: Concept phase."

[11] "ISO 26262-4:2011 - Road vehicles – Functional safety – Part 4: Product development at the system level."

[12] "ISO 26262-5:2011 - Road vehicles – Functional safety – Part 5: Product development at the hardware level."

[13] "ISO 26262-6:2011 - Road vehicles – Functional safety – Part 6: Product development at the software level."

[14] "ISO 26262-7:2011 - Road vehicles – Functional safety – Part 7: Production and operation."

[15] "ISO 26262-8:2011 - Road vehicles – Functional safety – Part 8: Supporting processes."

[16] "ISO 26262-9:2011 - Road vehicles – Functional safety – Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses."

[17] "ISO 26262-10:2012 - Road vehicles – Functional safety – Part 10: Guideline on ISO 26262."

[18] J. Westman and M. Nyberg, "A Reference Example on the Specification of Safety Requirements using ISO 26262," p. NA, sep 2013.

[19] B. Gallina, S. Kashiyarandi, H. Martin, and R. Bramberger, "Modeling a Safety- and Automotive-Oriented Process Line to Enable Reuse and Flexible Process Derivation," in *2014 IEEE 38th International Computer Software and Applications Conference Workshops*, pp. 504–509, IEEE, jul 2014.

[20] C. MacNamee, D. Heffernan, and P. Fogarty, "Runtime verification monitoring for automotive embedded systems using the ISO 26262 Functional Safety Standard as a guide for the definition of the monitored properties," *IET Software*, vol. 8, pp. 193–203, oct 2014.

[21] C. B. S. T. Molina, J. R. de Almeida, L. F. Vismari, R. I. R. Gonzalez, J. K. Naufal, and J. B. Camargo, "Assuring Fully Autonomous Vehicles Safety by Design: The Autonomous Vehicle Control (AVC) Module Strategy," in *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, pp. 16–21, IEEE, jun 2017.

[22] S. Norton and H. Akram, "Designing safe and secure autopilots for the urban environment," in *11th International Conference on System Safety and Cyber-Security (SSCS 2016)*, pp. 4 (6 .)–4 (6 .), Institution of Engineering and Technology, 2016.

[23] A. Riel, C. Kreiner, G. Macher, and R. Messnarz, "Integrated design for tackling safety and security challenges of smart products and digital manufacturing," *CIRP Annals*, vol. 66, pp. 177–180, jan 2017.

[24] C. Kreiner, R. Messnarz, A. Riel, D. Ekert, M. Langgner, D. Theisens, and M. Reiner, "Automotive Knowledge Alliance AQUA - Integrating Automotive SPICE, Six Sigma, and Functional Safety," pp. 333–344, Springer, Berlin, Heidelberg, 2013.

[25] A. Johnsen, G. D. Crnkovic, K. Lundqvist, K. Hanninen, and P. Pettersson, "Risk-Based Decision-Making Fallacies: Why Present Functional Safety Standards are Not Enough," in *2017 IEEE International Conference on Software Architecture Workshops (ICSAW)*, pp. 153–160, IEEE, apr 2017.

[26] D. Kahneman, "Thinking, fast and slow," 2011.

[27] M. A. Gosavi, B. B. Rhoades, and J. M. Conrad, "Application of Functional Safety in Autonomous Vehicles Using ISO 26262 Standard: A Survey," in *Proceedings of 2018 IEEE SoutheastCon, Tampa, FL*, April 2018.

[28] "Quality Management in the Automotive Industry Automotive SPICE ® Process Reference Model Process Assessment Model Title: Automotive SPICE Process Assessment / Reference Model Copyright Notice," 2015.

[29] B. B. Rhoades and J. M. Conrad, "A Novel Terrain Topology Classification and Navigation for an Autonomous CAN Based All-Terrain Vehicle," in *Proceedings of 2018 IEEE SoutheastCon, Tampa, FL*, April 2018.

[30] B. B. Rhoades, V. Katariya, and J. M. Conrad, "A Novel RF (XBee) and IR LoS (Line-of-Sight) Collaborative Vehicle-to-Vehicle Navigation Technique," in *Proceedings of 2018 IEEE SoutheastCon, Tampa, FL*, April 2018.

[31] NHTSA, "U.s. department of transportation releases policy on automated vehicle development | national highway traffic safety administration (nhtsa)," May 2013. (Accessed on 10/07/2016).

[32] ChicagoLandToysandHobby, "6 high banked curve 2/30 deg - chicagoland toys and hobbies." (Accessed on 05/04/2017).

[33] T. Harrington, D. Bowman, W. Johnson, R. Benner, R. Capener, and H. Han, "Vehicle tag used for transmitting vehicle telemetry data," Dec. 9 2004. US Patent App. 10/855,871.

[34] Kersen, "Xr7 elm327 bluetooth obdii scan tool for honda / toyota / ford rover/ audi / opel," 2015. (Accessed on 09/30/2016).

[35] "ISO 3780:2009 - Road vehicles – World manufacturer identifier (WMI) code."