TECHNISCHE UNIVERSITÄT
CHEMNITZ

Systematic Development for SAE Level 4 City Driving

Master Thesis

Submitted in Fulfilment of the

Requirements for the Academic Degree

M.Sc.

Dept. of Computer Science

Chair of Computer Engineering

Submitted by: Muhammad Aashir Ayaz

Student ID: 448046

Date: 06.09.2019

Supervising tutor: Prof. Dr. Wolfram Hardt (TU Chemnitz)

External supervisor: Alina Chelea (1ACUE Consulting and Engineering GmbH)

Acknowledgement

I would like to express my gratitude to my supervisors Prof. Dr. Wolfram Hardt and Dr. Ariana Heller for their patience, advice, guidance and support throughout my thesis.

I would like to thank Mr. Peter Müller for providing me platform in 1ACUE Consulting and Engineering GmbH to test my capabilities. His Wisdom, knowledge and Commitment to the highest standard has inspired and motivated me. I would like to thank Miss. Alina Chelea for her help, support and supervision in this work. She is always supporting and being a wonderful source of creative ideas. I also thank Mr. Danial Paula for his valuable entries in my thesis.

I would like to express my sincere and heartfelt attitude towards my parents for their love and faith in me. Their support and attention helped me overcome delays and stay focused on my study in all these years of my master.

I would like to thank my brother and sisters for their support and guidance in hard times and cheering me up.

Abstract

Autonomous driving technologies for autonomous cars have advanced to be one of the most important innovations within the automotive industry in recent years. The benefits for the client and the autonomous driving society are many, such as greater safety, lower fuel consumption and more efficient road systems. In the field of high automation driving, the complete Dynamic Driving Task (DDT) must be performed by the automated driving system (ADS) itself.

In this thesis the possibilities of using autonomous driving technologies for autonomous driving in the city are studied. For that, the City Pilot feature is taken into consideration at the item level. City Pilot must be an automatic driving function according to SAE Level 4, which performs the full DDT in the city environment.

The feature was developed with systems engineering methods, such as the V model, a top-down approach, the system modeling language (SysML) and in accordance with international standards such as SAE J3016, ERTRAC, NHTSA and ISO 26262.

The result of this work is an assumption at the City Pilot item level, which is capable of performing different driving scenarios. It contains a description of the feature with an Operational Design Domain (ODD) and a description of the driving scenario, as well as use case diagrams, derived from the scenarios, and its functional principle. A Hazard Analysis and Risk Assessment were run to examine the functional safety objectives of the feature. Finally, a functional City Pilot architectures were created.

The thesis gives an idea of a system engineering development process for a high automatic driving characteristic and can be used for other steps, such as further software/hardware development and technical solutions.

Keywords: Automated Driving System (ADS), Dynamic Driving Task (DDT), System Modelling Language (SysML), Operational Design Domain (ODD

Table of Contents

List of Figure

List of Tables

List of Abbreviations

ADAS	Advance Driving Assistance System
ADS	Automated Driving System
ASIL	Automotive Safety Integrity Level
CP	City Pilot
DDT	Dynamic Driving Task
E/E	Electrical/Electronic
ERTRAC	European Road Transport Research Advisory Council
ESV	Enhanced Vehicle Safety
FO	Fail-Operational
FS	Fail-Safe
FTTI	Fault Tolerant Time Interval
HAD	High Automated Driving
HARA	Hazards Analysis and Risk Assessment
MRC	Minimum Risk Condition
NHTSA	National Highway Traffic Safety Administration
ODD	Operational Design Domain
OEDR	Object Event Detection and Response
SAE	Society of Automotive Engineers
SysML	System Modelling Language
UML	Unified Modelling Language

1 Introduction

Since the 1990s – a time when autonomous driving was still only found in science fiction books or films, engineers and technicians have been working on driver assistance systems. In the next decade, the car industry will change more drastically than it has over the past 30 years, because today we are standing at the entrance to a new era of highly automated driving. [1]

Society of Automotive Engineers (SAE) has defined five levels in the evolution of autonomous driving. Each level describes the extent to which a car takes over tasks and responsibilities from its driver, and how the car and driver interact.

SAE levels 0 to 5 are defined according to their relative extent of automation. Where level 0 represents no sustained automated control of vehicle. Level 5 on the other hand represents a robotic car where even a steering wheel is not required. Level 3 and above are labelled as automated driving where a complex system is responsible of monitoring the driving environment. Human intervention is limited in these levels and vehicles are considered to be autonomous vehicles. [2] But these levels are still in testing phase.

However currently, in the year 2019, many companies are involved in the race for the market leadership in the field of autonomous driving cars. One of the most advanced options is the Audi A8, which has been called a Level 3 autonomous vehicle. For now, the closest to Level 5 autonomy in North America is Waymo's Robo-taxi service, which can claim Level 3 or maybe approach Level 4. A Level 4 vehicle only requires human control when the vehicle indicates that it needs a driver to intervene. Unfortunately, Waymo's system is still experiencing delays. [3]

In the field of highly automated driving such as level 4, the complete driving tasks must be fulfilled by the automated driving system itself. There are many situations the automated driving system must react on in a very short period, especially while driving inside the city.

This master thesis covers, systematic development for high automated city driving. For that, City Pilot SAE level 4 is taken in consideration.

1.1 Motivation

Self-driving technology is perhaps the most debated technology in the automotive industry right now and many companies are developing autonomous driving features to be added on their production cars. The motivation behind this technology showdown is to improve car safety and efficiency.

Sebastian Thrun, the leading engineer of Google's self-driving car project, wrote in his blog that the goal of developing self-driving car is to "help prevent traffic accidents, free up people's time and reduce carbon emissions." [4]

Autonomous Driving technologies for self-driving cars have advanced to be one of the most important innovations within the automotive industry during the last couple of years. There are many benefits of Autonomous Driving to customers and society, such as increased safety, decreased number of accidents and more efficient road systems.

As the system takes over the control, the driver has spare time to continue work without having fear about road safety. Furthermore, Senior citizens and disabled personnel, who have difficulty in driving, are assisted by Autonomous vehicles towards safe and accessible transportation.

1.2 Problem Statement

Safety is of paramount importance for operating autonomous vehicles. That doesn't mean the safety of just the riders and passengers, but also other vehicles on the road, pedestrians, and bicycle traffic. At this point autonomous driving cars still suffer from a lot of problems regarding the safety.

The main challenge for autonomous vehicles is to detect its surroundings and various objects (e.g. traffic signs, pedestrians etc.) especially while driving in a city. Other challenges are to detect the internal state of the car, understand, predict the current events and make a decision according to the predicted events. Developing a systematic strategy and a completely traceable Top-Down approach, capable of responding to its surrounding, by monitoring both the environment and ego vehicle internal state, is a solution to resolve these problems and increase safety.

Therefore, the goal of thesis is to develop a systematic approach and completely traceable strategy for autonomous driving SAE level 4 cars on city roads. To fulfil above goal, initial step should be defining of high automation driving according to global standards, high automation driving feature “City Pilot” and its operational design domain (ODD). This thesis ends with complete functional architecture of SAE level 4 City Pilot. This systematic approach should be developed in such a way that it can be continued and detailed further in future. Furthermore, it must be suitable to be extended with the necessary functional safety.

1.3 Structure of Thesis

The thesis starts with the detailed discussion of the international standards such as SAE J3016, European Road Transport Research Advisory Council (ERTRAC) and National Highway Traffic Safety Administration (NHTSA) which is used for realizing and developed autonomous driving approach for modern cities. Later, in this chapter explained V Model, the left side of the V model represents system requirements, its architecture and design along with implementation plans whereas the right side shows the system integration and testing. This work focuses on the left side of the V model which has been used to produce functional architecture of feature functions, which are meant to be deployed in the City Pilot (CP) mode of level 4 autonomous vehicles. Also explained current level of autonomous driving, functional safety standards ISO 26262 and systems engineering methods.

Chapter 3 covers the methods which are used to develop a complete systematic approach for City Pilot and explains V Model approach going top to down on the left side of V model which includes Idea Phase and Concept Phase. In Idea Phase analyzed the initials of City Pilot feature, driving scenarios and in Concept Phase doing the modelling for use cases, activity diagrams as well as functional architecture for City Pilot functions.

Chapter 4 is focused on the results which obtained by approach implementation of Idea Phase in V Model. City Pilot level 4 description and driving scenarios results are introduced in this chapter. The events and driving scenarios faces by City Pilot system are defined in this work through road track, OEDR (Object and Event Detection and Response) and ODD (Operational Design Domain). A number of use cases and activity diagrams have been modelled for this system and functional architecture are made on the basis of the results from Concept Phase approach in the chapter 5. In addition Hazards Analysis and Risk Assessment are also proposed for level 4 City Pilot.

Chapter 6 concludes this thesis with summary of all achievement along with the suggestion of the potential extensions of this work in future.

2 State of the Art

The work presented in this chapter were discussed, some research documents such as Levels of Driving Automation standard (SAE J3016), European Road Transport Research Advisory Council **(**ERTRAC)**,** National Highway Traffic Safety Administration (NHTSA), which were considered in this thesis as a vehicle and traffic safety standards to develop a Systematic Approach and also current status of level of driving automation. Later described functional safety, a high-level introduction to V -Model, along with Systems Engineering and its methods.

2.1 Levels of Driving Automation standard (SAE J3016)

SAE International (Society of Automotive Engineers) has defined levels of automation under their standard SAE J3016 and according to SAE there are six driving automation levels, reaching from no driving automation (level 0) to full driving automation (level 5) [2]. These levels and their definitions are well defined in the figure 2.1 below.

SAE level	Name	Narrative Definition	Execution of Steering and Acceleration/ Deceleration	*Monitoring* of Driving Environment	Fallback Performance of *Dynamic Driving Task*	System Capability *(Driving Modes)*
***Human driver* monitors the driving environment**						
0	No Automation	the full-time performance by the *human driver* of all aspects of the *dynamic driving task*, even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a
1	Driver Assistance	the *driving mode*-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	Human driver and system	Human driver	Human driver	Some driving modes
2	Partial Automation	the *driving mode*-specific execution by one or more driver assistance systems of both steering and acceleration/ deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	**System**	Human driver	Human driver	Some driving modes
***Automated driving system* ("system") monitors the driving environment**						
3	Conditional Automation	the *driving mode*-specific performance by an *automated driving system* of all aspects of the dynamic driving task with the expectation that the *human driver* will respond appropriately to a *request to intervene*	System	**System**	Human driver	Some driving modes
4	High Automation	the *driving mode*-specific performance by an automated driving system of all aspects of the *dynamic driving task*, even if a *human driver* does not respond appropriately to a *request to intervene*	System	System	**System**	Some driving modes
5	Full Automation	the full-time performance by an *automated driving system* of all aspects of the *dynamic driving task* under all roadway and environmental conditions that can be managed by a *human driver*	System	System	System	**All driving modes**

Figure 2.1 Levels of Driving Automation [2]

SAE J3016 standard also defines “Dynamic driving task” related to vehicle. According to the J3016 International the dynamic driving tasks consist of:

- Lateral and longitudinal vehicle motion control
- Monitoring the driving environment
- Object and event response execution
- Manoeuvre planning
- Enhancing conspicuity

Furthermore, standard also defines the role of driver and automated driving system while feature is engaged [2]. This thesis focuses on SAE Level 4 features which is known as highly automated driving. Vehicle operating at Level 4 contains a lot of features which are well-defined according to SAE Levels, these features can be driving highly automated car within a city or in rural areas as well as on highway but each feature has its own limitations, this work mainly covers City Pilot features where a car moves on a city road with high level of automation. More detailed about City Pilot feature can be found in chapter 3.

2.2 Vehicle and Traffic Safety Standards

In this section explain two important vehicle and traffic safety standards such as European Road Transport Research Advisory Council (ERTRAC) and National Highway Traffic Safety Administration (NHTSA) which later used to develop approach and help to understand events, functions and scenarios for level 4 City Pilot.

2.2.1 European Road Transport Research Advisory Council (ERTRAC)

ERTRAC is European technology platform which brings together road transport investors to develop a common vision for road transport research in Europe. It has three versions of research paper published 2015, 2017 and 2019 until now. The goal of the ERTRAC Roadmap is to provide a view and useful information on the development of connected automated driving in Europe. The Roadmap starts with common definitions of automation levels and systems, and then identifies the challenges for the implementation of higher levels of automated driving functions. ERTRAC discussed the levels of driving automation referenced by SAE J3016, Operational Design Domain, regularities and connectivity in terms of vehicle and infrastructure. It’s also discussed important factors for higher levels of driving automation such as, safety, transport system efficiency, comfort and social inclusion etc. In short, it states that, by 2050 vehicle should be electrified, automated and shared [5] [6].

Furthermore, main tasks supported by ERTRAC are listed below;

- Provide a strategic view for road transport research and innovation in Europe.
- Determine strategies and roadmaps to achieve this view through research and definitions.
- Contribute to increase coordination between the European, national, regional public and private Research and Development activities on road transport.
- Improving the networking and clustering of Europe’s research and innovation capabilities. Figure 2.2 showing all actors of road transport system which represent by ERTRAC [5] [6].

Figure 2.2 Illustrate the structure of ERTRAC [8]

2.2.2 National Highway Traffic Safety Administration (NHTSA)

The Enhanced Vehicle Safety (ESV) program began more than 40 years ago as part of the North Atlantic Treaty Organization (NATO) to control the challenges of modern society, and has been put in place through a mutual agreement between the governments of the United States, France and the Federal Republic Germany, Italy, the United Kingdom, Japan and Sweden. Participating nations agreed to develop experimental safety vehicles to advance the state-of-the-art technology in the automotive sector safety engineering and meet periodically to exchange information on their progress. After that agreement, the number of international partners have grown to include the governments of Canada, Australia, Netherlands, Hungary, Poland, Republic of Korea and two international organizations, the European Committee for Enhanced Safety for Vehicles and the European Commission. One representative from each country / organization serves as a government head person in support of the program [7].

The aim is to exchange information between all countries, National Highway Traffic Safety Administration (NHTSA), US Department of Transportation, distributes this technical document containing the proceedings of the 23rd International Technical Conference on ESV. The technical document included in this publication contain current safety research efforts around the world, share the common interest of reducing the number of motor vehicles fatalities and injuries [7].

The NHTSA analyses aspects of automated driving system (ADS) tests and develops test examples and evaluation methods for specific ADS L3 to L5 features. An example of a test framework has been developed to further support safety improvement objectives for all users of the transportation system. Furthermore, paper is based on seven tasks, which is described in seven chapters, these chapters' help to understand, later used to develop concept and systematic approach in this thesis [8].

Chapter 1: Explained comprehensive introduction and main objectives of NHTSA; objectives further described in different chapters in detailed in this research paper [8].

Chapter 2: Describes tactical maneuvers behaviors for assumed ADS feature, levels of driving automation according to SAE J3016 and furthermore, some steps of defining feature definition i.e. ODD and OEDR etc. [8].

ADS Features and Tactical and Operational Maneuvers (X = demonstrated, ? = speculated)	Commercially Available? (Y/N)	Level of Automation (SAE 1-5)	Parking	Maintain Speed	Car Following	Lane Centering	Lane Switching/Overtaking	Enhancing Conspicuity	Merge	Navigate On/Off Ramps	Follow Driving Laws	Navigate Roundabouts	Navigate Intersection	Navigate Crosswalk	Navigate Work Zone	N-Point Turn	U-Turn	Route Planning
Olli Local Motors *(Tampa, FL 2018)*	Y	4	X	X	X	X	X	X	?		X	?	X	?	?	X	X	X
CityMobil2 *(demo in multiple European cities, 2014-2016)*	N	4	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X
Navya Arma Shuttle *(France/ Switzerland)*	Y	4	X	X	X	X	X	X	?		X	?	X	?	?	X	X	X
Auro Self-Driving Shuttle	N	4	X	X	X	X	X	X	?		X	?	X	?	?	X	X	X
Varden Labs Self-Driving Shuttles	N	4	X	X	X	X	X	X	?		X	?	X	?	?	X	X	X
EZ10 Self-Driving Shuttle	N	4	X	X	X	X	X	X	?		X	?	X	?	?	X	X	X

Figure 2.3 Sample of Highly Automated Low Speed Shuttle Features [8]

Chapter 3: This chapter explains the identification of attributes that can be used to define Operational Design Domain (ODD) for ADS. An ODD describes the specific operating domains in which an ADS feature is designed to function, which are listed below; [8]

- Review ODD for assumed ADS feature
- Define ODD classification i.e. roadway type, weather, lighting etc.
- Characterized ODDs in which assumed ADS features may function

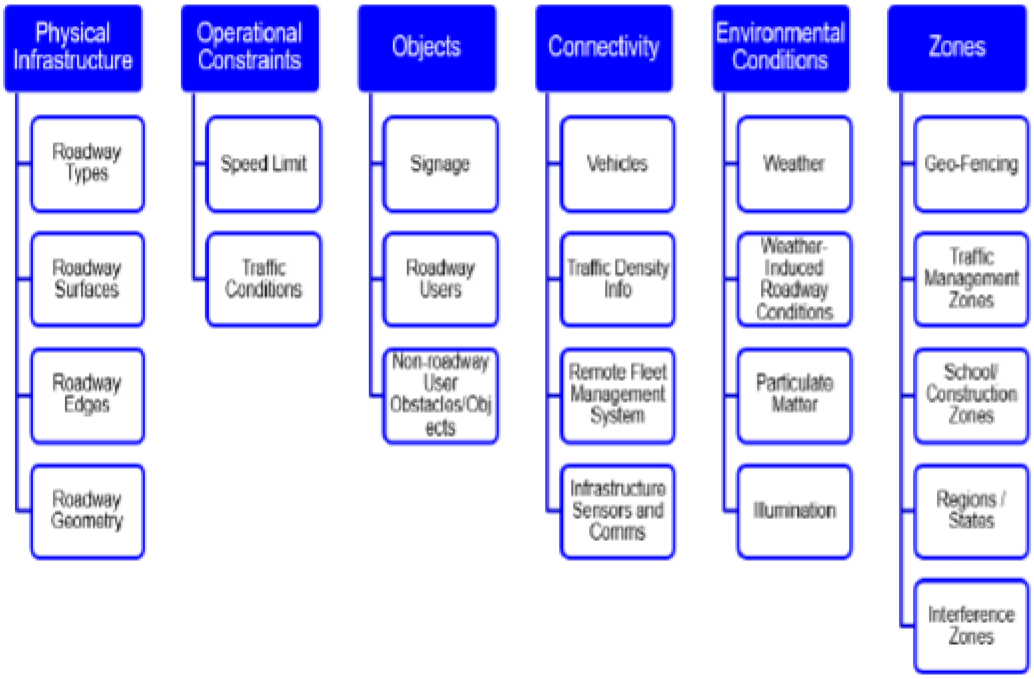

Figure 2.4 ODD Levels Framework

Chapter 4: Explains the recognition of Object, Event Detection and Response Analyses (OEDR) functions that enable ADS to operate safely within the prescribed operating ODD [8].

OEDR process explained into the following steps:

- Review the literature and research.
- Identify operational descriptions for features.
- Perform analysis to identify baseline ODDs.
- Perform driving scenario analysis.
- Perform analysis to identify OEDR behaviors and corresponding responses.

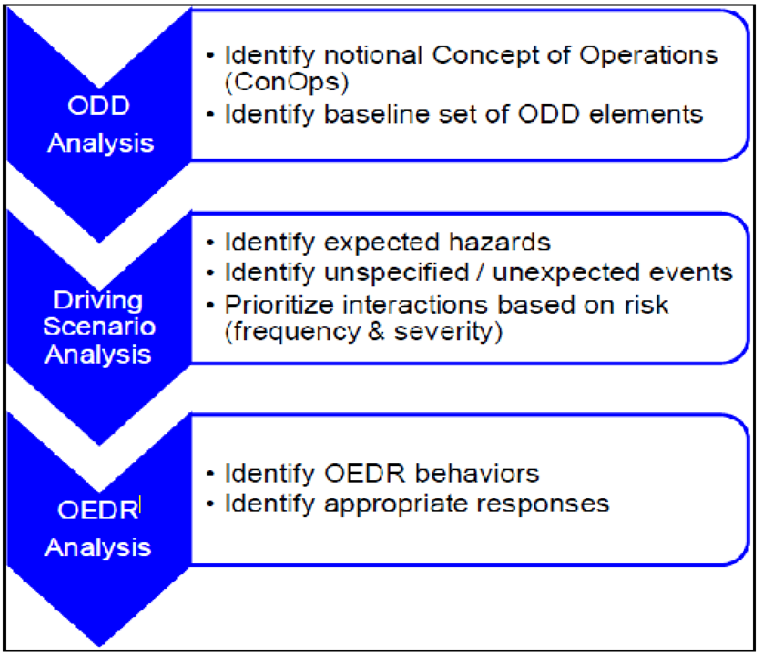

Figure 2.5 OEDR Capability Identification Process [8]

Chapter 5: Defines development of preliminary tests and evaluation methods to support the assessment of ADS for safe placement, based on components description in Chapter 2 (feature description), Chapter 3 (Operational Design Domain), and Chapter 4 (Object, Event Detection and Response Analyses). Further explained test scenarios for ADS feature such as, Tactical maneuvers behaviors, ODD elements, OEDR capabilities and Failure mode behaviors, also testing challenges. [8]

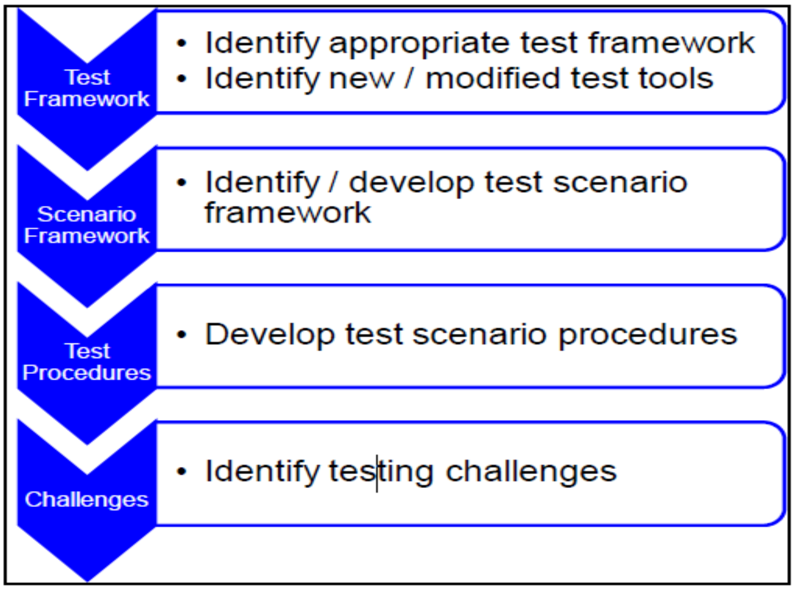

Figure 2.6 ADS Test and Evaluation Method Development Process [8]

Chapter 6: This chapter describes valuation approach to Fail-Operational and Fail-Safe (FO) and (FS) Mechanisms for an ADS. ADSs will use FO and FS mechanisms when the system does not function as supposed to be planned. These mechanisms enable ADS to achieve a Minimum Risk Condition (MRC) that removes the vehicle and its tenants from hazards to the safest extent possible. Defining, testing, and validating FO and FS strategies for achieving an MRC are important steps in ensuring the safe operation and utilization of ADS [8].

The last chapter is a concise summary and conclusion of technical paper.

2.3 Current level of Driving Automation

The increase in driver less cars will have a great influence on companies and professionals. Automated driving could replace corporate fleets for deliveries or transport of employees and workers could earn productive hours on the day by working instead of driving during daily commutes. Innovations in this field also completely change the vehicles insurance industry by reducing accidents, a new report predicts that accidents will decrease by 80% by 2040 [9].

But road to autonomy is long and extremely complicated. It can also be dangerous: two high profile efforts, from Uber Technologies and Tesla, were involved in crashes that caused the death of a pedestrian. One of Waymo's autonomous vans was involved in a collision in May 2018. However, the perceived interests are so huge, with the promise that transport companies need little in labor costs that many companies compete to master the technology and put it working [10].

In the next three years, almost all these contenders such as General Motors, Uber, Tesla and Waymo’s etc will be able to show cars capable of navigating the streets of the city at casual speeds along fixed routes.

“Waymo has developed a phenomenal system and is ahead of the pack,” said Brian Collie, head of Boston Consulting Group’s U.S [10].

The main objective of this thesis is to develop a systematic approach for level 4 automated driving, but goal line is not only to reach Level 4 on the scale of five steps of autonomous driving. Level 4 is the threshold at which a car can drive on pre-mapped routes and handle anything in its planned course without the intervention of a driver. Only Waymo has tested Level 4 vehicles on passengers other than their employees, and those people volunteered to be test subjects. No one has yet demonstrated at Level 5, where the car is so independent that there is no steering wheel, or no more driver presence is required. Without drivers, operating margins could be more than twice what carmakers generate at the moment [10]

2.4 Introduction to V Model

V Model organizes the system development process in phases, show in figure 2.7. V stands for verification and validation; V Model is used to develop a system with verification and validation.

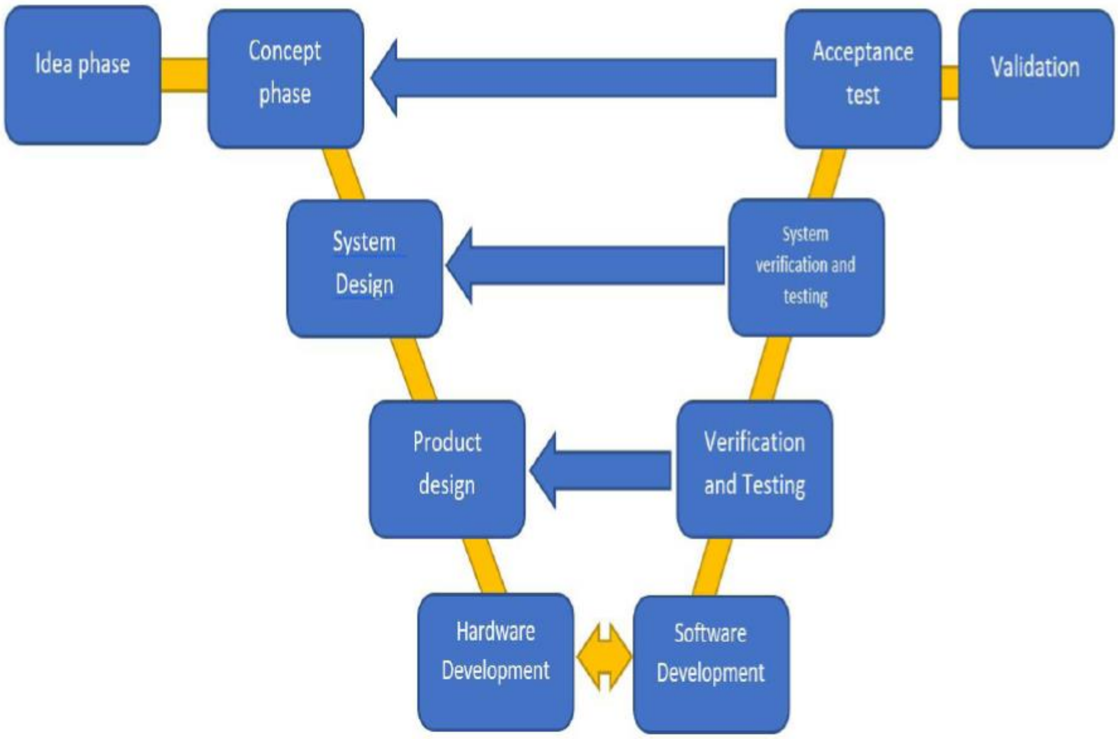

Figure 2.7 V Model and its phases

To the left of the V Model as shown in figure 2.7, the system definition develops from a general user view of system in Idea phase to a detailed specification of Concept phase. The system is decomposed into subsystems and the subsystems are dismantled into elements in System Design phase. Beside the decomposition of the system, the requirements are also explained into more specific specifications that are assigned to the system elements. After that Product Design phase is executed. While the hardware and software are implemented at the bottom of the V Model, the components of the systems are verified and examined on the right. Lastly, the complete system is validated to measure how well it corresponds with the requirements.

One of the significant things about V Model is the symmetry between the left and right side of the model. It reflects the relationship between the steps on the left and steps on the right. On the left side, a functional specification is started, which is expanded in more detail to a technical specification and implementation basis. At the right top of V model is the validation phase, which is tested according to specifications one left side. The connection between left side and right side of V Model ensure, that the focus is same from beginning to end of the system development process. This thesis covers the Idea phase and Concept phase of the model.

- **Idea Phase**

Idea is the establishment of any system; without a practical and well considered idea a system cannot be conceived as per end-user requirements. So, in the first thoughtful phase an idea is introduced which has potential of developing assumptions into a real system. Idea phase includes all initial requirements, cost analysis as well as planning of the system. It also includes milestones and different stages of the system. Once the initial phase is completed the idea is launched into the concept phase. In this thesis idea phase contain feature definition approach for SAE level 4 City Pilot development, which is described in more detailed in section 3.3.1.

- **Concept phase**

Concept phase is associated to the complete functionality of the system or product to be develop. To successfully conceive the conceptual complexity a brief knowledge about the ongoing research in the market relevant to the system or similar system/product is compulsory. This phase also includes the assessment of the alternative concepts which could be more effective in future as far as that particular system idea is concerned. Functionality of a system must cover following aspects, such as item definition, functional architecture and its requirements along with functional safety concept according to ISO 26262 standard. In this thesis concept phase of V Model evaluate the above-mentioned aspects of system, which are defined comprehensive by ISO 26262 standard. Functional safety and its standard ISO 26262 along with concept phase development can found in next section 2.5 and item level definition approach execution described in section 3.3.2 respectively.

2.5 Functional Safety

Safety is one of the key issues in development process of automotive industries. Development and integration of automotive functionalities strengthen the need for functional safety. As increasing of technological complexity, software content and mechatronic implementation, risk is increasing from systematic failures and random hardware failures. To deal with these issues and to ensure that best solution has been applied during the development of the systems, the ISO 26262 standard provides guidance to resolve these risks by determining appropriate requirements and processes [11].

2.5.1 Definition of Functional Safety

Functional Safety is defined in ISO 26262 as follows; "Absence of unreasonable risk due hazards caused by malfunctioning behaviour of E/E systems "[11]. A malfunction is a "function that does not behave as specified for customer operation e.g., due to systematic or random errors" [11]. While the "Safety in use" prevents hazards from nominal working functions, on the other hand, "Functional Safety" has the task to prevent hazardous malfunctions. Furthermore, hazards are potential source of harm caused by faulty behaviour of the item whereas risk is combination of the probability of occurrence of harm and severity of that harm [11].

Figure 2.8 Safety in use vs Functional Safety [12]

2.5.2 The ISO 26262 Standard

The ISO 26262, named “Road vehicles – Functional safety”. This norm is created for safety relevant electric/electronic systems in automobiles. It defines a procedure model with corresponding activities, work products and methods in development and production [11]. This procedure model is shown in figure 2.9 and ISO 26262 is consisting on several parts which are summarized below.

ISO 26262 starts with vocabulary part, which contain terms and definitions according to standard requirements and specification. Management of functional safety part defines the requirements for functional safety management and concept phase part specifies the requirements for the concept phase for automotive applications. After that product development at system level, hardware level and software level parts describe necessary activities and processes needed to develop product that meets the safety requirements along with integration, testing and validation. Production and operation part have two main objectives, to develop and maintain a production process for safety-related elements planned to be installed in road vehicles and second one is to achieve functional safety during the production process. Interfaces within distributive developments, qualification and evaluation of hardware/software components, overall safety requirements management, documentation and more describe in supporting processes part. The second last part of ISO 26262 describe Automotive Safety Integrity Level-oriented & Safety-oriented analysis requirements. The last part is guideline on ISO 26262 standard [11].

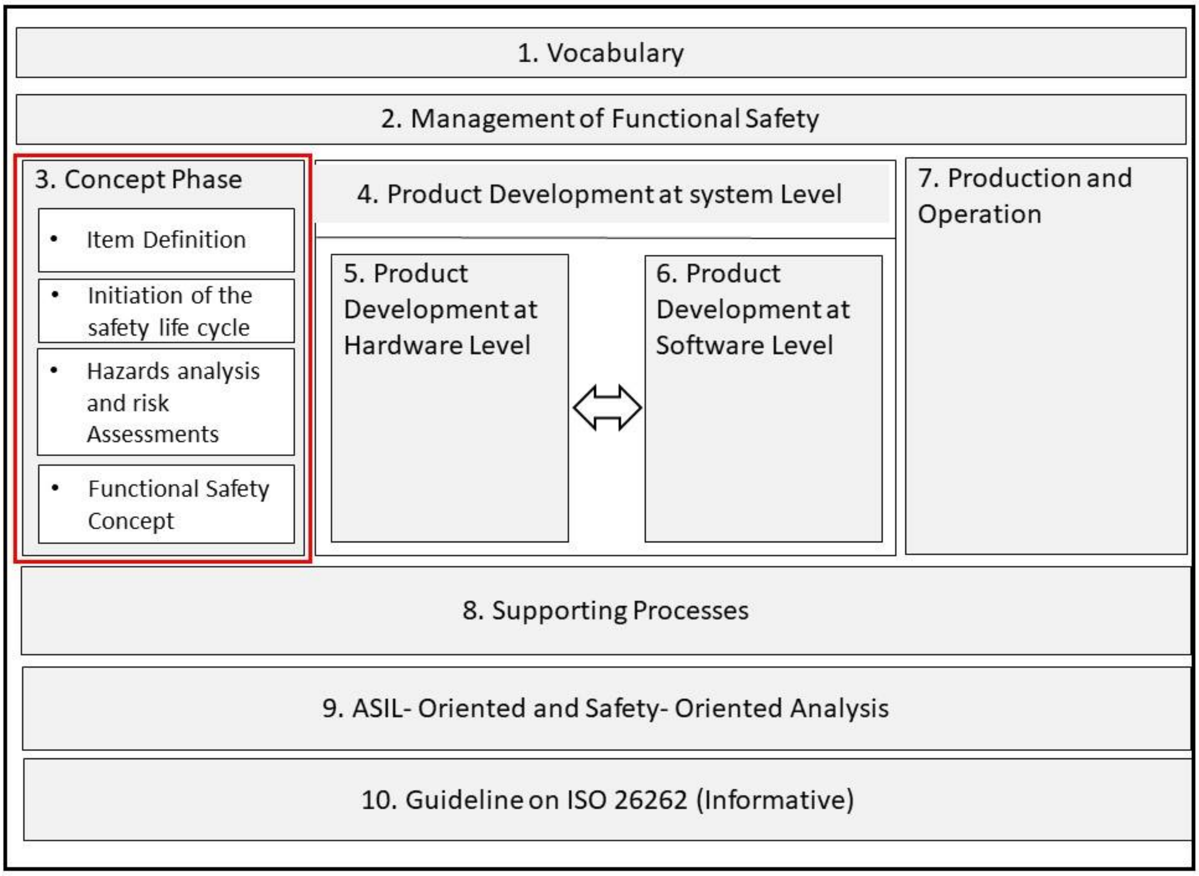

Figure 2.9 Overview of ISO 26262 [11]

This thesis covers concept phase part of ISO 26262, shown left side in figure 2.9. Furthermore, concept phase consists of following parts

- **Item definition**

It has two important objectives, first aim is to define and describe the functionality of the component, its dependencies and interaction with environment and other elements and second objective is to support a sufficient understanding of the functionality of the component so that the activities in following phases can be performed. ISO 26262 lists the requirements for establishing the definition of the item regarding its functionality, interfaces, environmental conditions, legal requirements, hazards, etc [11].

This definition serves to provide enough information about the component to the persons who conduct the consecutive sub phases define below and more detail about item level definition approach development process for SAE level 4 city driving can found under section 3.3.2.

- **Initiation of the safety lifecycle**

The purposes of the initiation of the safety lifecycle is to make the differences between a new component development and a modification to an existing component or item. Another purpose is to define the safety lifecycle activities that will be carried out in the case of a modification of the component [11].

- **Hazards Analysis and Risk Assessments**

The goal of risk analysis and risk assessment is to identify and classify the hazards caused by product malfunction and formulate safety objectives related to the prevention or mitigation of hazardous events, in order to avoid excessive risks.

Hazard analysis, risk assessment and Automotive Safety Integrity Level determination are used to determine the safety goals for the item to avoid unreasonable risk. For this, the item is evaluated regarding its potential risky events. Safety goals and their assigned ASIL are determined by a systematic valuation of dangerous events [11].

Classification of Hazards Events and Automotive Safety Integrity Level (ASIL)

The level of safety integrity of the automobile (ASIL) is a risk classification scheme defined by ISO 26262: Functional safety for road vehicles. This is an adaptation of the level of safety integrity used in automotive industry. This classification helps to define the safety requirements. The ASIL is established when performing a risk analysis of a potential hazard by observing the severity, exposure and controllability of the vehicle's operating scenario. The first step is classification of hazardous events [11].

The severity describes how serious an accident will be in case of a malfunction. It is classified from S0 to S3 in accordance to Table 1.

Table 1 Classes of Severity [11]

	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

The probability of exposure determines how often the situation occurs. The probability classes go from E0 to E4, as listed in Table 2.

Table 2 Classes of Probability of Exposure regarding Operational Situations [11]

	Class					
	E0	**E0***	**E1**	**E2**	**E3**	**E4**
Description	Incredible	Combination of very low probabilities	Very low probability	Low probability	Medium probability	High probability

The controllability describes the driver can control or not control the vehicle in case of a malfunction. The controllability classes go from C0 to C3 in accordance with Table 3.

Table 3 Classes of Controllability [11]

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

After classification is done the ASIL is determined in Table 4. For each hazardous event a safety goal should be set. The result of ASIL is calculated by summing the exposure with controllability and severity;

ASIL = E + C + S

ASIL A is the lowest safety integrity level where as ASIL D the highest one. Hazards that are identified as QM (Quality Management) do not dictate any safety requirements [11].

Table 4 ASIL Determination [11]

Severity class	Probability class	Controllability class		
		C1	C2	C3
S1	E0*	QM	QM	QM
	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E0*	QM	QM	QM
	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E0*	QM	QM	QM
	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

- **Functional safety concept**

The purpose of the functional safety concept is to originate the functional safety requirements, from the safety goals and assign them the initial architectural elements of the component or to external measurements.

In order to meet the safety objectives, the functional safety concept contains safety measures, including safety mechanisms, which must be implemented in the item's architectural elements and are stated in the functional safety requirements [11].

2.6 Systems Engineering and its Methods

Systems engineering is an interdisciplinary approach with the aim of achieving successful complex systems realize. Systems engineering focuses on the definition and documentation of the requirements of the system in the initial phase of development, the development of a system design and the review of the system for fulfilment with the requirements, taking into account the general problem: time, testing, creation, cost, planning, training , support and provision [12][13][14][15].

Systems engineering integrates all disciplines and forms a structured development process from the concept to the production phase. Both technical and economic aspects are considered to develop a system that meets the needs of users. Some of the systems engineering tools and methods made it possible to reach the goals for this thesis. These is explained in the following sections below.

2.6.1 Top-Down-Approach

In the context of the design of a system, the "Top-down approach" means that a high-level abstract, general description of the system is first created. Concluding with this high-level description, the system will be designed at lower and more detailed levels. In contrast to this, the "Bottom-up approach" does the opposite. At the beginning the pieces of the lowest level of the system are designed in detail and then they will be joined to the whole system [14].

2.6.2 Modelling Languages

A modelling language is an artificial language that can be used to express information or knowledge or systems in a structure defined by a consistent set of rules. The rules are used to interpret the meaning of components in the structure.

Besides modelling languages are used to describe systems necessities and conduct functionality. A modelling language can be graphical or textual;

Graphical modeling languages use a diagrams technique with named symbols that represent concepts and lines that connect the symbols, represent relationships and various other graphical notes to represent constraints.

Whereas Text modeling languages can use standardized keywords accompanied by parameters or natural language conditions and phrases to make computer interpretable expressions [16].

The most useful advantage of modelling languages is envisioned to enhance the productivity of skilled programmers so that they can handle more challenging problems. For this thesis work system modelling language (SysML) is used to develop the model of SAE level 4 city driving.

- ## Unified Modelling Language (UML)

The Unified Modelling Language (UML) is a general purpose, development modelling language in the field of software engineering. UML is intended to provide a standard way to visualize the design of a system [18].

- ## System Modelling Language (SysML)

A system modelling language (SysML) is used to define systems requirements and systems behavior with the help of different modeled diagrams. It is a standardized modelling language and graphic language used for systems engineering and for various complex system modelling. With SysML structures, behaviours and requirements of a system can be described and brought into a relationship. The goal of working with SysML is to create a standardized syntax for the presentation of system connections and their common understanding amongst participants [18][19].

- ## UML and SysML

SysML is not a completely new development language. It is based on the software modelling language UML. SysML is defined as a UML-Profile, which means that the UML model is adapted with new types casts and characteristics. Figure 2.10 shows the schematic connection between SysML and UML.

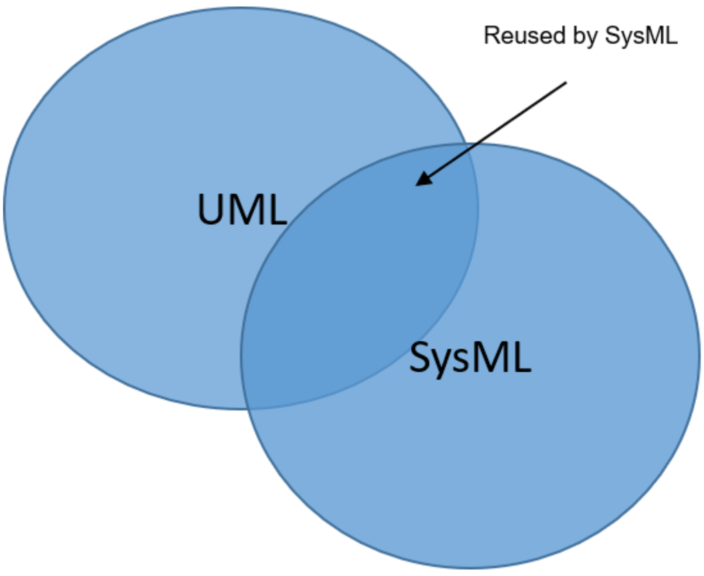

Figure 2.10 Schematic connection between SysML and UML

Creation of models done with Enterprise Architect – UML Development Tool (with SysML 1.4 plugin).

2.6.3 Types of Modelled Diagrams

SysML contains different types of diagrams. These diagrams are the interface between the user and the model. Figure 2.11 demonstrate summary of the diagrams and the new modifications in UML. Diagrams have different types which describe the behaviour or the structure of a system.

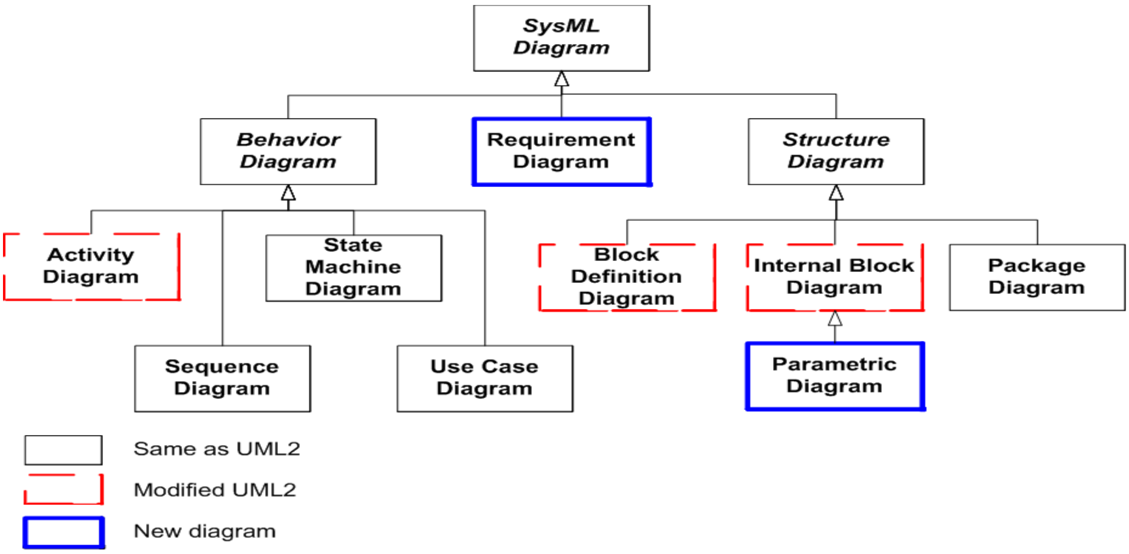

Figure 2.11 SysML Diagram Taxonomy [17]

In this thesis, SysML is used to explain use cases, activity diagrams and block definition diagrams regarding different scenarios of City Pilot.

- ### Use Case Diagrams

The use case diagram is one of SysML´s diagrams to model the systems behaviour. Amongst all it is the simplest one and is easy to understand. The diagram only portrays which use case has to do with which actor.

The use cases are represented by ellipses. The actors are pictured by human stick figures. Lines between the use cases and the actors show the relation between them in figure 2.12 [18][19][20].

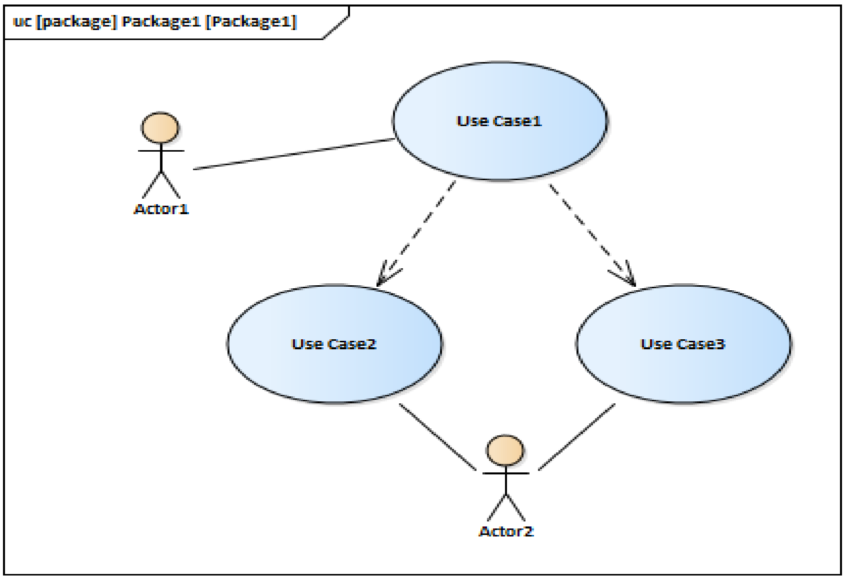

Figure 2.12 Use Case Diagram

- ## Activity Diagrams

The activity diagram is another diagram to model the system´s behaviour and defines a functional principle. It shows in which order different activities are executed. The activities are represented by rectangles with rounded corners. Arrows between these shows the flow of the activities are executed [18][19].

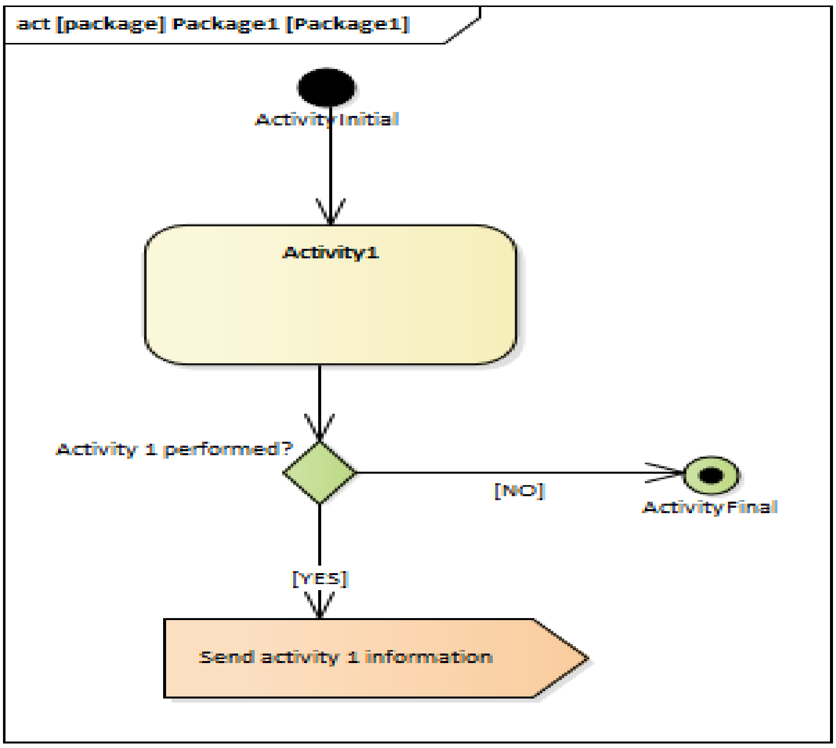

Figure 2.13 Activity Diagram

- ## Block Definition Diagrams

The block definition diagrams in SysML defines functions of blocks and relationships between them such as associations, generalizations and dependencies. It captures the definition of blocks in terms of properties, operations, further relationships between systems and subsystems [18][19].

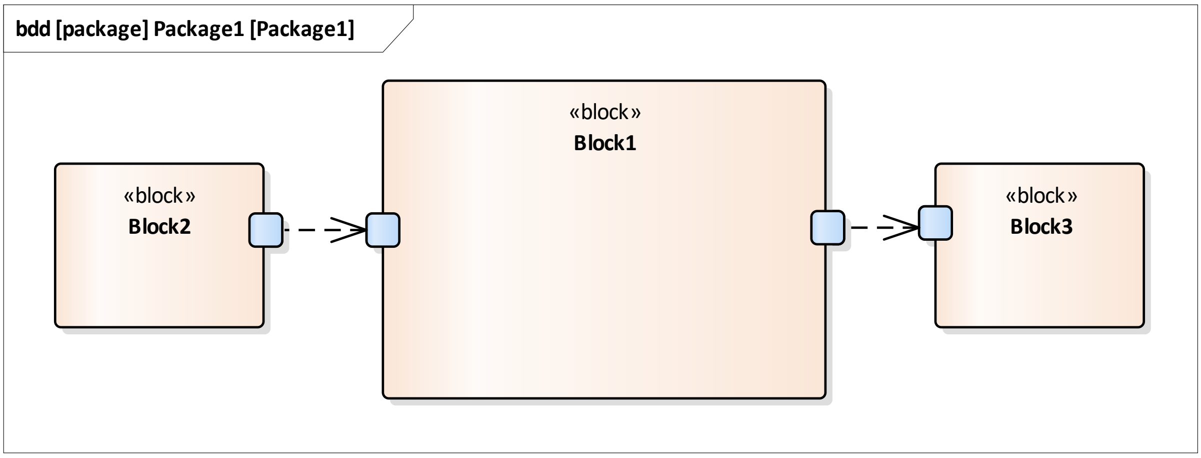

Figure 2.14 Block Definition Diagram

3 Methods

This chapter explains the execution and development process for systematic approach of SAE level 4 city driving. This chapter also explains the role and importance of Top-Down approach along with system modelling language. Explanation of overall systematic development Top-Down approach, which is already in use for different features is now reused and modified with more research to develop level 4 City Pilot. After by using overall systematic approach going from Top to Down on V Model that defines and describes a new approach for level 4 City Pilot in detail in idea phase and concept phase besides with definitions, references and explanations. Last but not the least, most important part is the driving routines and boundaries for SAE level 4 city driving development.

3.1 Systems Engineering

Systems engineering approach is interdisciplinary as explained in chapter 2 section 2.6. Furthermore, it is iterative in nature and focuses on optimal construction of the entire system in connection with its life cycle and its planned operational environment. Understanding and utilizing the right approach at the right time is an essential system engineering skill that can have a significant impact on the system schedule and success. Commonly, there are three classes of approaches that are addressed in systems engineering but mostly used top-down engineering and bottom-up engineering. City Pilot systematic approach is based on Top-Down engineering [20][21].

3.1.1 Top-Down Approach

Bottom-Up-Approach has the advantage that different system parts can be created immediately. Time and cost for Top-Down-Approach planning is saved. On the other hand, Bottom-Up Approach has several risks when it comes to placing the different components together in one system. If the components may not fit together, the system does not meet the necessary requirements or unnecessary components are created. As a conclusion, Bottom-Up-Approach is suitable for upgrading or replacing existing systems. The already existing system can be used as a template that saves the time and cost while the risks are low.

In the case of new, complex and unprecedented systems, the Top-Down-Approach is inevitable. In order to meet the requirements and create an overall work system, the general functionality must be planned before entering the details. If this is not done, the risks with Bottom-Up-Approach will arise [20].

3.1.2 Importance of Top-Down Approach in a systematic way

When the nonconcrete high-level descriptions of the Top-Down approach are changed, these can result in changes to all detailed lower-level descriptions of the system. This means that the time and cost saved on lower detailing can be wasted if Top-Down approach was not done in the right order and in a systematic way. On the other hand, changes at lower and detailed levels do not affect higher levels [20].

3.1.3 Model-based development

Model-based development was an emerging and promising design method. This process is part of the system technology that has found application not only in the automotive and aerospace industries, but also in industries that are part of mechatronic systems such as consumer electronics, interdisciplinary systems and more. Actually Model-based development is the solution of Document-based process problems and difficulties.

Document-based development means that the different development areas exchange specification only in the form of a written document. Each development area has its own individual specification. This means that they often do not know why requirements are written as they are, as the context for the entire system is missing. It can be very complicated to define all relevant requirements without making unnecessary information. When you read the specification, it can also be complicated to find all the relevant information, as they can be hidden in the text.

On the other hand, model-based development uses a single model for all development areas, rather than multiple written documents. The model is used to draw requirements from it and to add new requirements. The model also contains all other technical information and can be further developed by the various development areas. Within the framework of a complex system, this has the great advantage that the different development areas can always see the context of the requirement. In addition, no translation into other media where written documents need to be done. This saves time for translation and reduction of the risk of misunderstood claims [21].

3.1.4 Significance of SysML

The System Modeling Language (SysML) has emerged as a main factor of standard system architecture modeling language for Model Based Systems Engineering (MBSE) applications. SysML is a dialect of UML 2 that extends the standard Unified Modeling Language (UML) for software-intensive applications so that it can be successfully applied to system-technical applications. One more important reason to work with SysML is that systems engineering consists of three components: System requirements, system architecture and system behaviour. SysML provides for each of these components diagrams and the possibility to link these diagrams together. Furthermore, SysML allows multiple persons to access, modify and expand these diagrams. This gives the possibility to detail the model step by step further, in accordance with the Top-Down development process [20][21].

3.2 Overall Systematic Development Approach

High Automated Driving (HAD) must fulfill the standards of functional safety ISO 26262 known as functional safety for road vehicles standard and automotive industry also considered V Model as big reference to system development of automated vehicles. Any system development goes with different phases and has many components, elements and work products etc. Therefore, needed traceability between each phase of system development process or approach. This thesis aims to provide complete traceable and systematic development approach for SAE level 4 city driving. This thesis also focuses on overall systematic development approach shown in figure 3.1 and support to describe Top-Down composition steps for City Pilot L4 approach. It is worth mentioning that this thesis covers only upper part of overall systematic development approach mentioned with red line box in figure 13 that includes assumed item definition, assumed functional architecture on vehicle level and assumed vehicle architecture. Furthermore, approach is based on many standards and published papers like;

- SAE J3016
- NHTSA
- ERTRAC
- ISO 26262

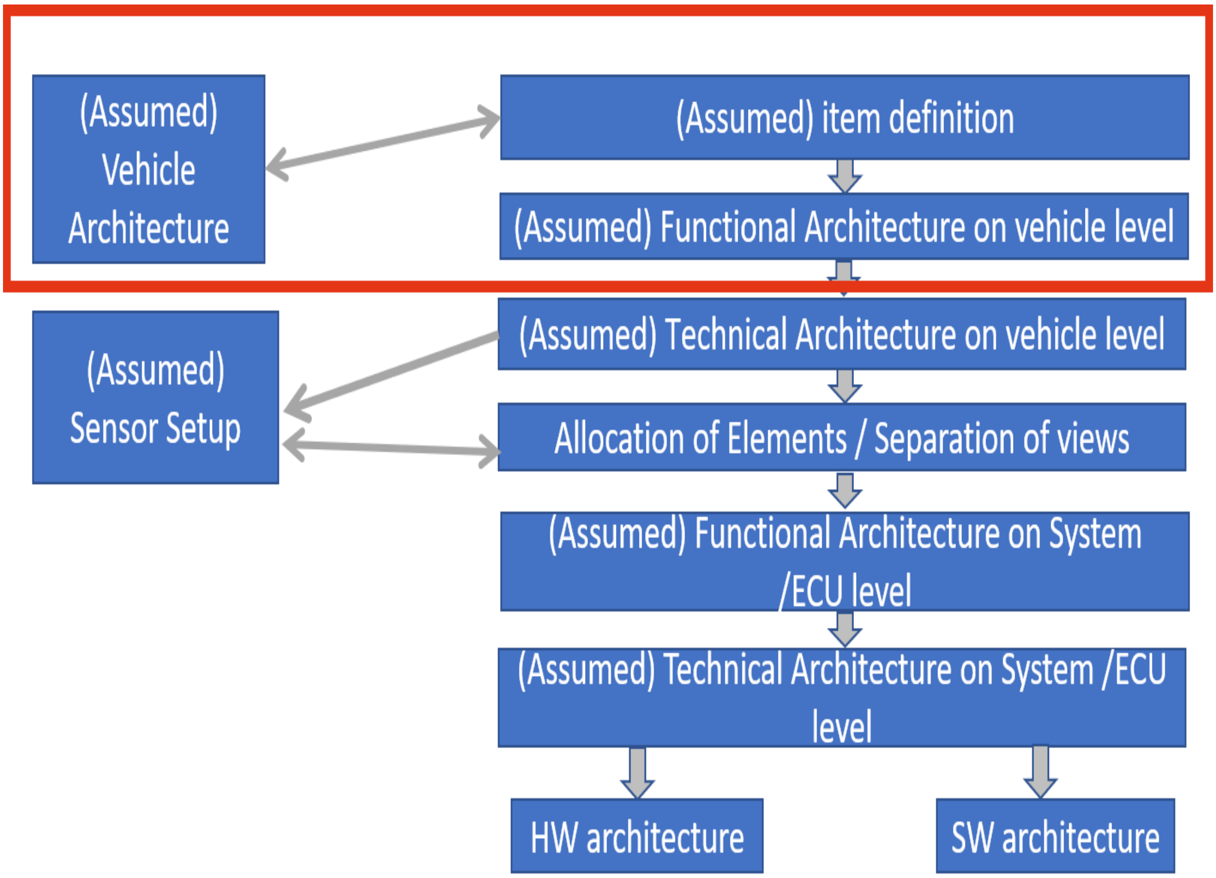

Figure 3.1 Overall Systematic Development Approach

3.2.1 Significances of Overall Systematic Approach

Overall systematic approach fulfills the standards and regulation for Advance Driving Assistance System (ADAS) and High Automated Driving (HAD) for automotive. It automatically generates the traceability between the different needed work products. A complete reasoning is given for all the content in information exchange between the work products. It makes reviews, assessments as well as certification easier. It could be used for all levels of automation (e.g. SAE Level 0-5). Approach is modular build, so that the different functions on different levels can be re-used. Easier identification of errors/faults an early stage of system development.

3.2.2 Overall Systematic Approach Classification for City Pilot Strategy

As mentioned above, this thesis work includes only upper part of overall systematic development approach which contains these points;

Assumed Item Definition: City Pilot item definition has the following main contents:

- Feature Description
- Road Track Scenarios
- Operational, Environmental and Functional Driving Scenarios
- Object & Event Detection & Response (OEDR) Analysis
- Operational Design Domain (ODD)
- Use Cases
- Activity Diagrams

Assumed functional Architecture on Vehicle Level: It is an architectural model that identifies system functions and their interactions with each other. Functional requirements of the system are an important basis for creating a functional architecture. The functional requirements of the feature City Pilot were worked out with the definition of the use cases explained in section 3.3.2.1. These use cases functions were later described by creating the associated activity diagrams.

Assumed Vehicle Architecture: This architecture describes vehicle dynamics model and it is intended to establish useful conventions for vehicle dynamics, maintaining compatibility with SAE and ISO when practical. Exceptions are noted when they occur.

Later, described all definitions and reuse this upper part of overall systematic approach going top to down on V Model to establish idea phase and concept phase. More detailed explanation about overall approach establishment can found in next section 3.3.

3.3 V Model Approach

This topic explains how general Top-Down-Approach with help of overall systematic development approach is established on V Model to provide a traceable strategy for SAE level 4 City Pilot. As described above in section 3.2.2, by using this definition and breaking into two parts to organize fitted in V Model to create and expand information for idea phase and concept phase. Furthermore, it describes the definitions for all terms related to approach and execution steps for results of systematic development of City Pilot.

3.3.1 Idea Phase

As described in section 2.4, idea is the first thoughtful phase in the establishment of any system because without a practical and well-considered idea, a system cannot be conceived as per end-user requirements. In idea phase feature definition approach is developed under consideration of SAE J3016 and NHTSA. According to these standards feature definition approach fulfilled all basics of systematic approach development process for level 4 city driving which is High Automated Driving (HAD) declared by Society of Automotive Engineers. Feature definition approach of City Pilot follows following structure shows in figure 3.2 step by step in order to achieve complete item level definition and functional architecture in concept phase.

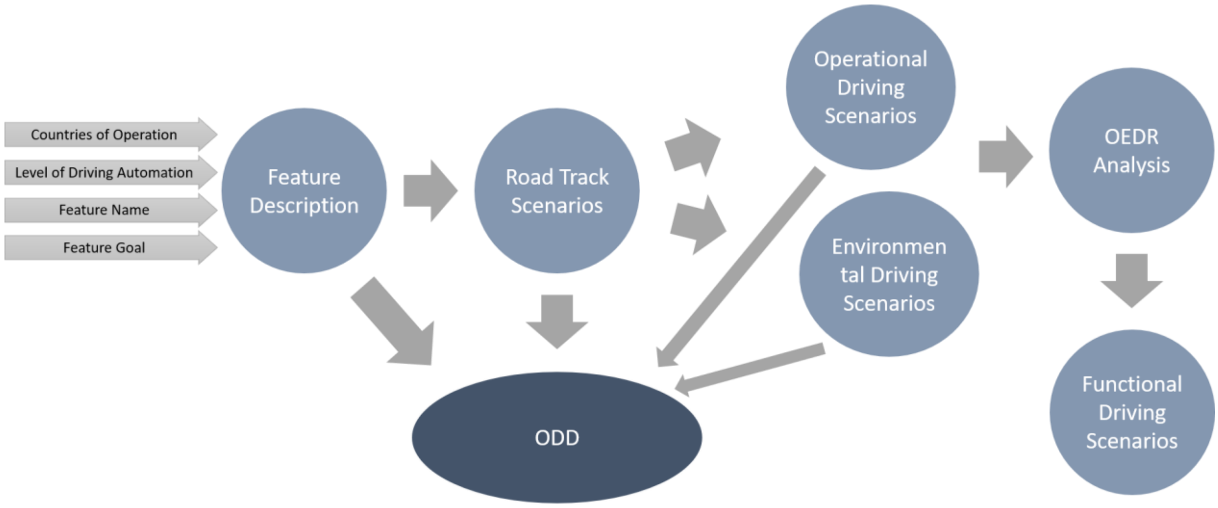

Figure 3.2 Feature Definition Approach

3.3.1.1 Feature Description

Feature description describes which tactical and operational maneuvers can be achieved as shown in figure 2.3 section 2.2. Feature description is developed by analyzed the important characteristics as well as feature functionality explained according to SAE J3016, vehicle and traffic safety standards defined in sections 2.1

and 2.2 respectively. Furthermore, Standard J3016 also explains the role of driver and feature (system) included in feature description as follow;

- Role of driver while the feature is not engaged
- Role of driver while the feature is engaged
- Role of feature while not engaged
- Role of feature while engaged

3.3.1.2 Definition of Driving Scenarios

Feature description gives a general overview of City Pilot, its functions and application area. In order to explain these functions and create use cases out of them, the exact driving scenarios had to be defined. This thesis covers and explains different aspects of driving scenarios which should help automotive engineers to develop a high automated vehicle to drive easily and deal with all scenarios which could happen in a city. The possible driving scenarios realized by City Pilot has four categories defined below with respective definitions;

- **Road Track Driving Scenarios**

Road Track explains the road scenarios for driving without objects, participant vehicles, pedestrian etc. for driving. The road track for city driving can include for example;

- City straight lane driving
- City roundabouts
- City intersections
- City curved lane turning left/right driving
- City tunnel driving etc.

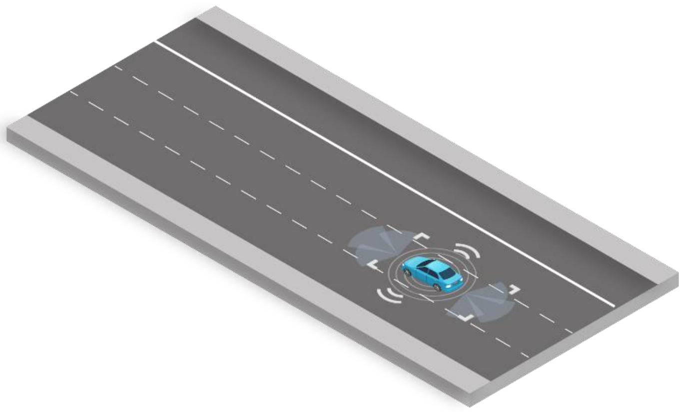

Figure 3.3 Example – City straight lane driving (piece of complete track)

A complete road track for city driving can be find in section 3.4 named as "driving routine" for City Pilot.

- **Operational Driving Scenarios**

Operational Driving Scenarios will be derived from Road Track Scenarios with the support of adding elements to the track. There are several operational constraints that need to be considered when designing and testing HAD feature applications such as City Pilot. Therefore, include elements e.g. traffic signs, participant vehicles etc. and elements must be taken from the considered elements list. Additionally, a selection needs to be done that either the element needs to be handled inside of Operational Design Domain or will outside an ODD which consider as a boundary. Table 5 shows an example of elements list whereas Figure 3.4 shows an element e.g. traffic sign and participant vehicle put in Road Track in order to drive Operational Driving Scenarios.

Table 5 Elements List Sample

Elements Lists	Inside of CP ODD?
Speed limit traffic sign	Yes
Vehicle in frontal zone	Yes
Animal in frontal zone	Yes
Vehicle in side zone	Yes
U-Turn traffic sign	No
....	

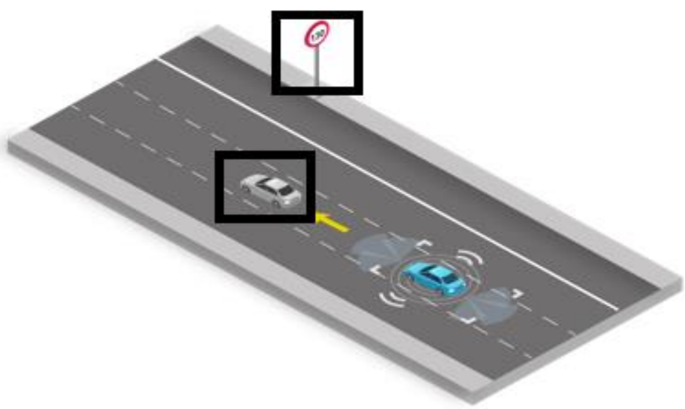

Figure 3.4 Elements on Road Track

There are many elements, like vehicles, traffic signs, traffic lights etc. which can be added to each single road track scenario. This will result in a huge amount of operational driving scenarios. For that reason, a main road track scenario is derived. Figure 3.5 shows formation of main road track scenario in order to manage all elements in operational driving scenarios.

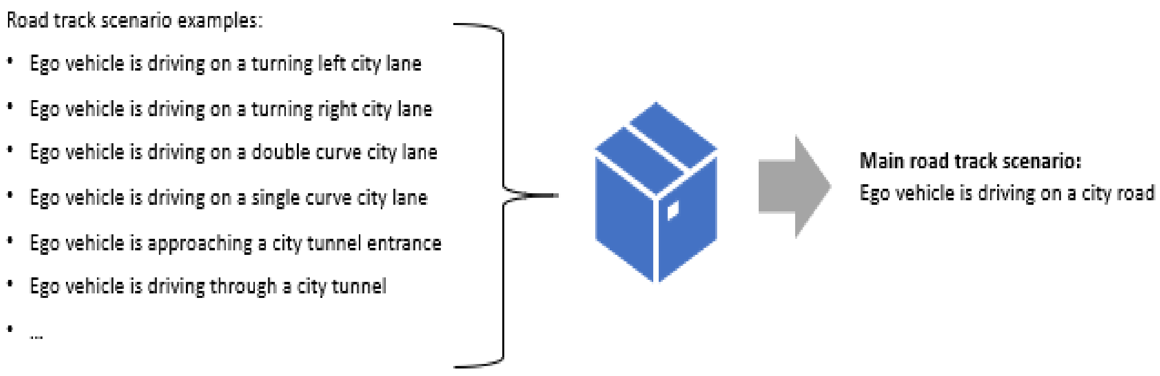

Figure 3.5 Main Road Track Scenario

An example shown in Figure 3.6 how operational driving scenarios for city driving are developed.

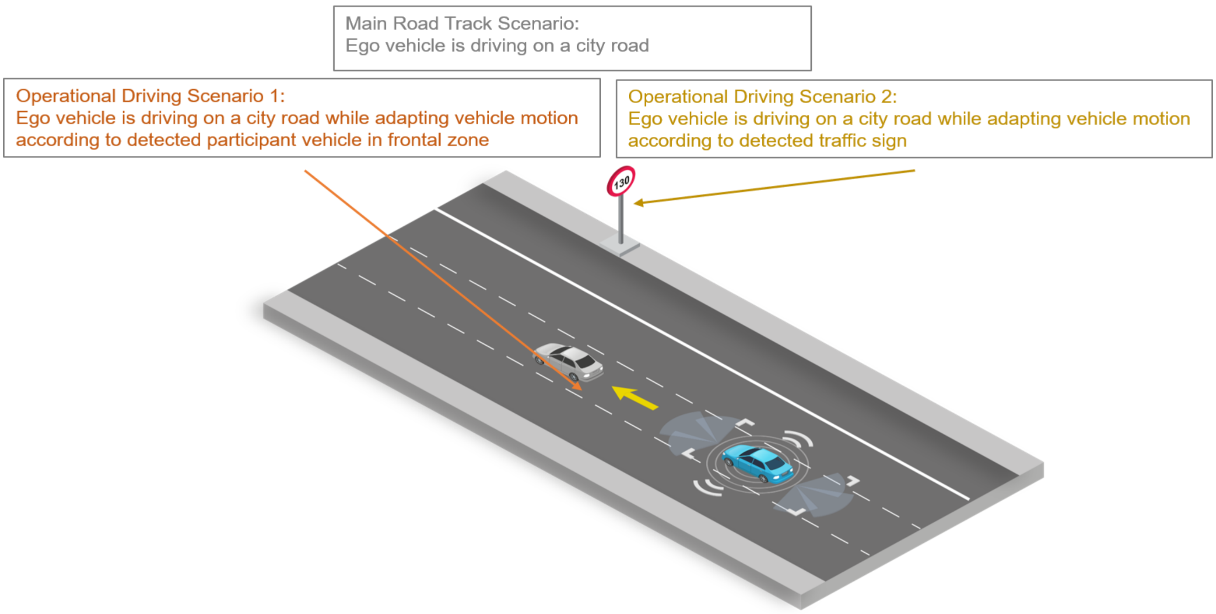

Figure 3.6 Example of Operational Driving Scenarios

- **Environmental Driving Scenarios**

Environmental conditions play a vital role in the safe operation of a variety of AD applications and pose one of the greatest challenges to implementation, particularly in early implementation. The environment can affect visibility, sensor fidelity, vehicle operations and communications systems.

On average, there are more than 5.7 million vehicle accidents each year. Approximately 22 percent of these accidents, almost 1.3 million, are related to the climate (Erdman, 2015) [8].

City Pilot environmental driving scenarios consider almost all possible environmental conditions and elements in order to provide a good solution to resolve climate related problems in the development of automated driving vehicles. Environmental driving scenarios will be derived from Road Track Scenarios with the support of adding environmental conditions elements to the track. An example shows in figure 3.7 below;

Figure 3.7 Example of Environmental Driving Scenarios

- **Functional Driving Scenarios**

After having a clear definition of the Road Track, the “Functional Driving Scenarios” can be allocated anywhere on the road track, that describes a specific situation and response. Functional driving scenarios based on “Road Track Scenarios” describe our road and “Operational driving scenarios” describe the operational situations. The “Functional Driving Scenarios describe” the vehicle behaviour at each moment and situation of the road track. Also, functional scenarios are a way to explain Object, Event detection and Response Analyses (section 3.3.1.3) in words. An example shows in figure 3.8 explains functional driving scenarios.

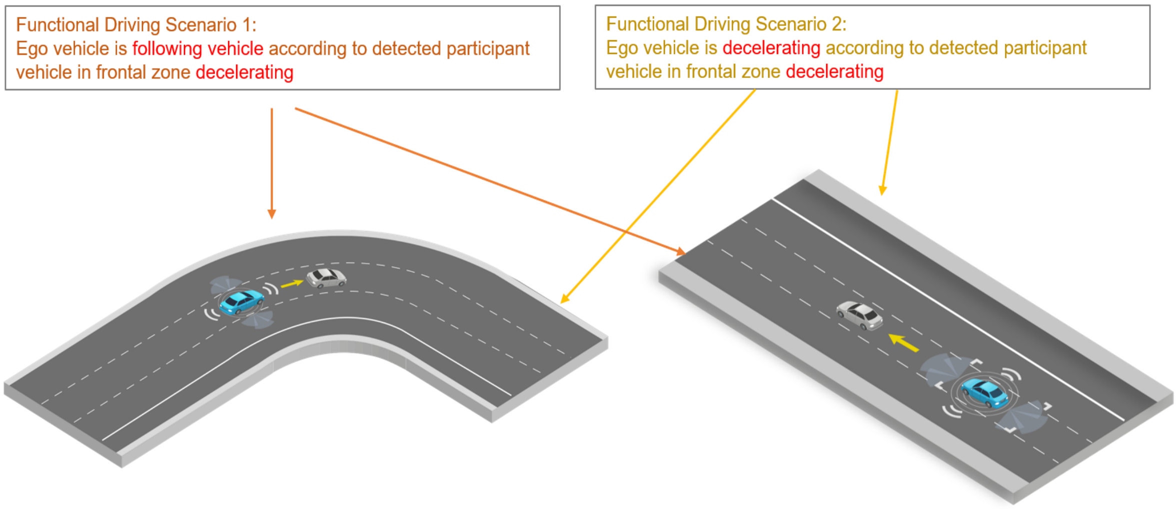

Figure 3.8 Example One of Functional Driving Scenarios

Functional driving scenarios have also been derived from the “Environmental Driving Scenarios”, which describe, e.g. the vehicle behavior when is raining, (figure 3.9).

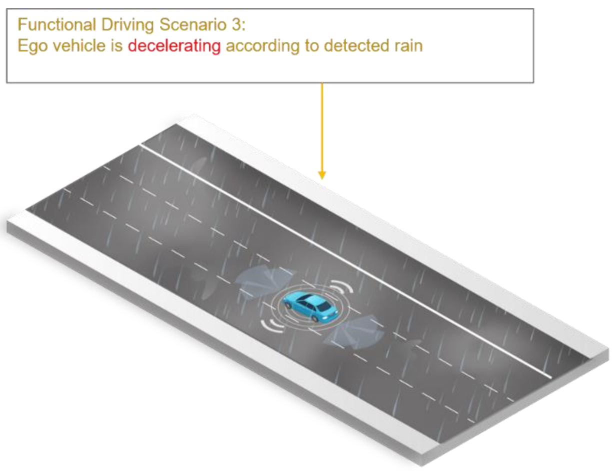

Figure 3.9 Example Two of Functional Driving Scenario

3.3.1.3 Explanation of OEDR Analysis

Object, Event detection and Response represents the ability of the HAD features to detect any circumstance that is immediately relevant to the driving task and implement an appropriate response. The main inputs for OEDR analyses are tactical operations behaviour from feature description and Operational Design Domain. In Highly Automated Driving such as Level 4 City Pilot, system of the feature is responsible to detect, recognize and classify objects and events, prepare to respond as needed and execute an appropriate response to such objects and events. The OEDR analyses capabilities provide support to sample tests of High Automated Driving (HAD) features. In section 2.2.2 determined important steps for OEDR and figure 3.10 shows an example of OEDR analyses made for city driving.

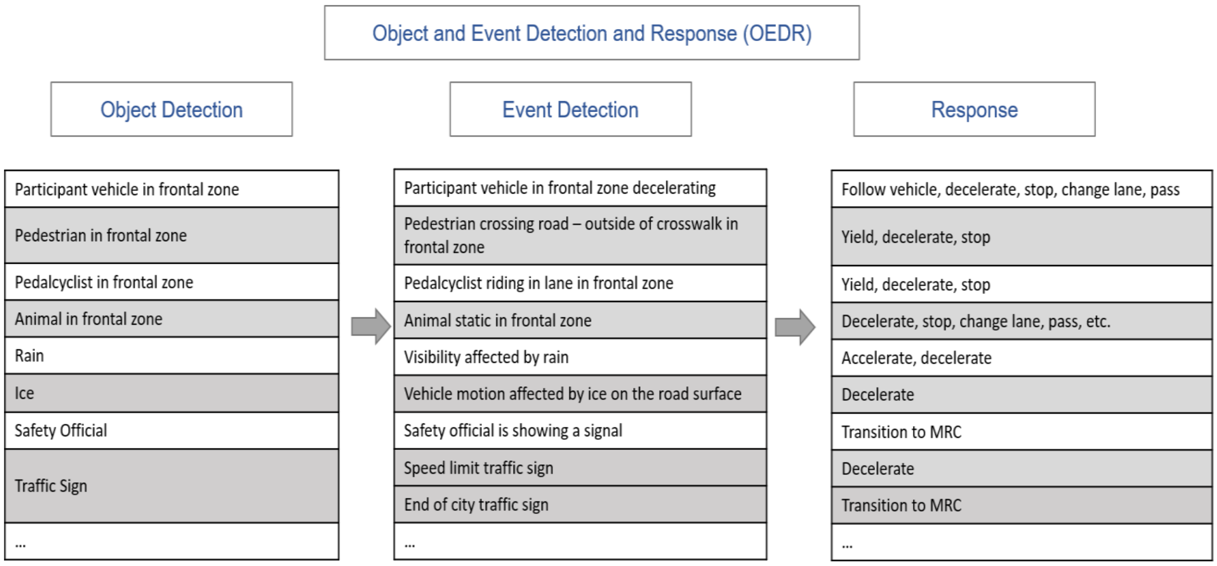

Figure 3.10 Example of OEDR Analysis

3.3.1.4 Development of Operational Design Domain

The Operational Design Domain for City Pilot is created according to the requirements of the NHTSA explained in section 2.2.2 and structure shown in figure 2.4 “ODD Levels Framework” in chapter 2. According to technical paper NHTSA the definition of ODD described as “The specific operating domains in which an automated driving system feature is designed to function with respect to roadway types, speed range, lighting conditions (day and/or night), weather conditions, and other operations constraints”.

Operational Design Domain takes input from feature description, road track scenarios e.g. roadway types, roadway geometry, etc., operational and environmental driving scenarios e.g. roadway users, signage’s and weather conditions etc. Furthermore, City

Pilot ODD also considers SAE standard and according to J3016 “The specific conditions under which a given feature thereof is designed to function, including, but not limited to, driving modes.” J3016 also provides ODD example relative to levels show in figure 3.11. An ODD may include one or more driving modes. For example, a given feature may be designed to operate a vehicle only on highways with full access and in low speed traffic, high speed traffic or in both driving modes [2].

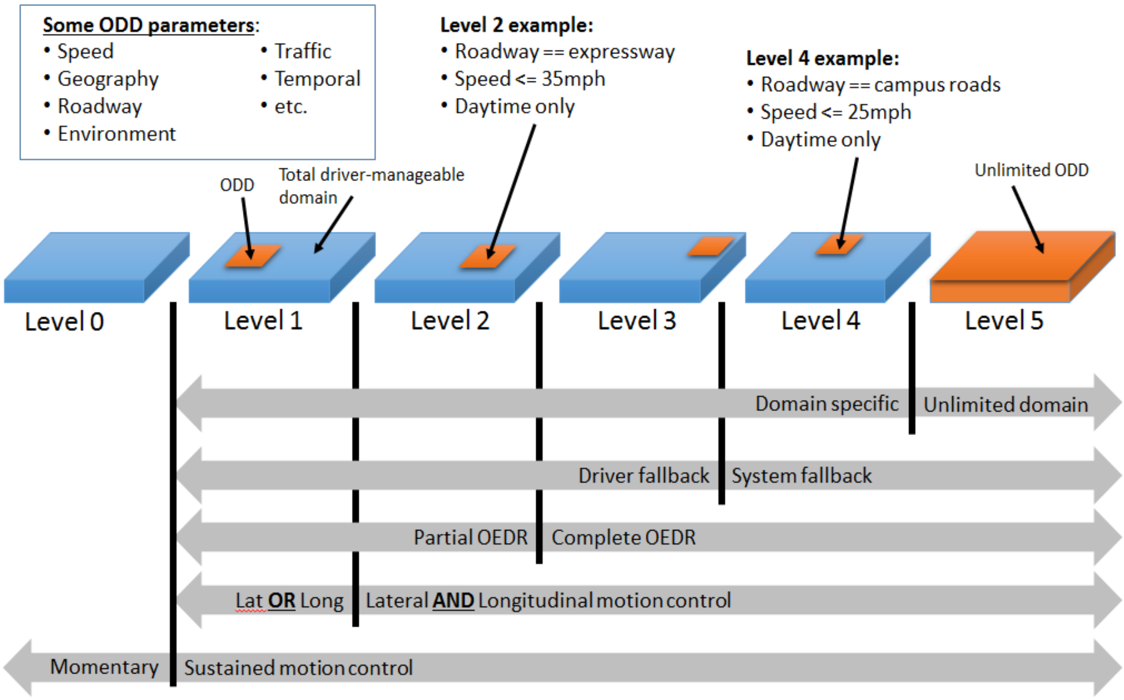

Figure 3.11 ODD Relative to Levels (SAE International, 2016) [2]

3.3.2 Concept Phase

In concept phase, item level definition for SAE level 4 city driving is obtained with the help and assumptions of feature definition approach which is explained in the previous section 3.3.1. Further with the help of SysML modelling language, modelled City Pilot use cases, activity diagrams and functional architecture. Hazard Analysis and Risk Assessment is also a part of concept phase.

3.3.2.1 Definition of Use Cases

The use case diagrams are intended to describe basic high-level functionality by specifying the usage of the system by its actors to achieve a goal. In order to give an overview of the structure of City Pilot, an overall use case diagram was needed to be described and for creating the overall use case diagram as well as sub use cases diagrams of the system, SysML modelling language is used.

For overall use case diagram of City Pilot, six aspects of city driving were considered, and these six aspects fulfill the requirements of high automated drive in city. Approach for overall use case consists of;

- Driver Monitoring/Interaction explains driver presence and driver setting inputs e.g. speed, distance and route set by driver etc.
- Ego Vehicle Monitoring/Internal Monitoring contains information regarding to ego vehicle e.g. actual speed, actual steering angle etc., navigation and failures related to Dynamic Driving Task fallback.
- Environment Monitoring/External Monitoring detects all surroundings aspects like objects, traffic signs and lights, road elements as well as environmental conditions.
- Event Understanding understands the events that happen when a certain object or element influences the vehicle behavior and sends specific outputs to Decision Making
- Decision Making makes required arrangements for adapt control e.g. steering or accelerating etc. according to event understanding and prioritize the control adaptation (e.g. steering, accelerating) according to the situation.
- Vehicle Controlling controls vehicle according to received signal from decision making.

These all use cases of city driving work together and send/receive signals between each other to communicate and share information. Overall use case diagram are provided in results of concept phase in chapter 5 section 5.1.

3.3.2.2 Definition of Activity Diagrams

An activity diagram describes the process of creating an item functional principle with the help of SysML modelling language. City Pilot does not have overall activity diagram, but it has individual’s activity diagrams for each use case in City Pilot model. The use case diagrams give a first overview of the structure and involved actors within the system but provides no insight view into the functions and processes behavior of use cases. Therefore, an activity diagram was sketched through system modelling language (SysML 1.4). The role of the activity diagram is to represent the flow of inputs and outputs and the flow of control between actions. The results in chapter 5 described and shown modelled activity diagrams of some use cases of city driving.

3.3.2.3 Explained Functional Architecture and Requirements

As described above in section 3.2.2, functional architecture is a model that identifies system functions and their interactions. It defines how the functions will operate together to perform the system complete operations. A functional view also allows a deeper insight into the whole system. Functional requirements are needed for developing a functional architecture. The functional requirements of the system were worked out with the definition of the use cases as explained in above section 3.3.2.1 and later with the help of these use cases creating activity diagrams. Now system functional architecture results from grouping the activities of the use cases into functional elements.

As described in above section 3.3.2.2, now the control flow between actions of activities is irrelevant for the functional architecture. Most important here are the actions themselves and the object flow, which describes input and outputs of the actions. As explained in chapter 2 section 2.6.3 block definition diagram is used to represent functional structure. Each block contains information and communicate through input and output ports which shows the connection between them. A complete functional architecture of city pilot can be found in chapter 5.

3.3.2.4 Approach for HARA

In order to identify the malfunctions of the item and the resulting hazardous events, it is important to define all the system functions/use cases of City Pilot. This was made with the definition of use cases in section 3.3.2.1 and the main input for these use cases is feature definition approach explained in section 3.3.1. That’s why it is important to define in idea phase a complete feature approach to get an overview of all the functions.

The definition of malfunctioning behavior that leads to a hazardous event is a key task of the HARA. The some of main system functions of City Pilot shown in Table 6 serve as the basis for the malfunction identification of the feature. A complete use case diagram of City Pilot system functions can be found be Appendix B.1 named as "Decision Making Diagram".

Table 6 System Functions/Use Cases Example of City Pilot

System Functions/Use Cases
Minimal risk condition transitioning
Adapting vehicle control according to speed limit changes
Navigation of work zones
Performing car following
Navigating roundabouts
Navigating intersections
Performing car following
Adapting vehicle control according to stopped vehicles
Adapting vehicle control according to Cut-Outs / Cut-Ins
Performing static objects avoidance
Performing dynamic objects avoidance
Adapting vehicle control according to emergency vehicles
Enhancing conspicuity
Performing Lane Switching/Overtaking
Navigating crosswalks
Performing Lane Centering
Adapting vehicle control according to traffic signs & lights

- ### Malfunctions and hazards Examples:

No longitudinal deceleration when requested leading to no car following performance

HAZARD=decreasing distance to participant vehicle in frontal zone

No participant vehicle detection leading to no car following performance

HAZARD=decreasing distance to participant vehicle in frontal zone

More than intended longitudinal acceleration leading to wrong car following performance

HAZARD=decreasing distance to participant vehicle in frontal zone

No longitudinal deceleration when requested leading to no vehicle control adaptation acc. to stop vehicles

HAZARD=decreasing distance to participant vehicle in frontal zone

After the determination of the malfunctions, the risk assessment can be implemented. In this part of the HARA, all malfunctions are examined for their possible consequences (hazardous events), with regards to different driving situations.

- **Identification of situations:**

Medini software is used to provide already pre-filled situations that can be selected. Medini creates automatically all possible combinations. The Medini catalogue needs to be matched with the ODD of the feature e.g. City Pilot, all ODD elements shall be in the Hazard Analysis Catalogue within Medini.

And classified afterwards, according to the ASIL determination in chapter 2 section 2.5.2 in classification of hazards event and ASIL. With the results of the risk assessment, the safety goals of the feature can now be formulated. Each malfunction with its resulting hazardous event shall apply to one safety goal. The ASIL for each safety goal is transferred from the hazardous event with the highest determination. The determination of the safety goals may vary depending on the view and interpretation of the analyzer.

3.4 Driving Routines and Boundaries

Boundaries for High Automated Driving feature routine like City pilot are some general and some of city driving approach related. General routine limitations such as L3 to L5 vehicles cannot be driven in city at high speed as compared to L0 vehicles which are manual because in city there are many objects and situations which need to be detected. For this purpose, high technology with very good precision and accuracy is required. At the moment is not possible for high-tech sensors to provide accurate results and communicate on high speed. That's why all highly automated vehicles drive in a city on low speed not more than 60 km/h and also the lack of reliable communication between vehicles to infrastructure (V2I**)** and vehicles to other vehicles (V2V**)** represents one of the largest barriers to a completely driverless ecosystem.

City Pilot driving routine related boundaries, due to the complexity and number of possible driving scenarios in a city would be more and beyond the thesis scope because it is not possible to consider all driving situations in a limited period of time. For that reason, the driving scenarios for City Pilot had to be delimited. A fictional city environment shown in figure 3.12 was created, where the ego vehicle drives through this fictional city on a set and fixed route. This route covers a great number of all possible driving scenarios, which would occur in a city. The bold yellow line shows the route of the ego vehicle in a city. Out of this environment, the road track driving scenarios were formulated as explained in section 3.3.1.2. All the later work based on these driving scenarios. ODD of City Pilot also consider as a boundary line by defining inside and outside elements for City Pilot operating domain.

Figure 3.12 Overview of the Driving Route in the Fictional City

4 Results on Idea Phase

This chapter contains results of feature definition approach developed in idea phase in section 3.3.1. The results explain feature description of level 4 City Pilot, all considered driving scenarios, Object, Event Detection and Response Analysis as well as Operational Design Domain of SAE L4 city driving.

4.1 Feature Description of Level 4 City Pilot

Feature description of level 4 City Pilot is developed under consideration of NHTSA and SAE J3016 standards. Feature description structure as follows;

Feature Name: City Pilot (CP)

Country of Operation: All the Europe except England (e.g. left side driving) and for different driving conditions we must instigate and make different analysis.

Level of Driving Automation: SAE Level 4 - High Driving Automation.

Purpose of Feature:

City Pilot (CP) is SAE Level 4 feature for autonomous driving on city driving allowing not only “hands-off” and “eye off” but also “mind-off” within the operational driving range. CP takes over the driving task from the driver when driving on city roads. CP keeps the speed or distance to the vehicle in front and keeps the vehicle near the center of the current lane (according to the driver settings before activation) and able to detect more objects and obstacles to avoid collision.

In total the engaged automated driving system keeps the speed or distance to the vehicle in front via acceleration or braking and keeps the vehicle in the center of the current lane via steering. The vehicle does not need to stay within the ego lane. It has the possibility in case of a two-lane road or in case of a single-lane taking the opposite lane that is used by oncoming traffic to execute a lane change for overtaking a slower vehicle ahead, avoiding a collision with an obstacle in the ego lane or because of infrastructural reasons.

CP will not allow exceeding the maximum permitted speed of 60 km/h. No transition to the SAE Level 3 mode (or SAE Level 2 mode) is required.

Tactical and Operational Maneuvers of Feature:

Table 7 explains the some of behavioral competencies, description according to NHTSA as well as relevancy for City Pilot feature. Complete table attached in Appendix A.1.

Table 7 Tactical and Operational Maneuvers of Feature

Behavioral Competencies	Description according to NHTSA	Relevant for City Pilot
Navigating Parking Lots & Locating Open Spaces	ADS comes to a complete stop within a vacant parking spot; may be further qualified by parallel or perpendicular orientations, lot type (closed/open), initiation conditions, etc.	No
Maintaining Speed	ADS maintains a safe speed set through longitudinal control with acceptable following distances.	Yes
Performing Car Following	ADS identifies and follows a target vehicle at acceptable following distance through longitudinal control including Stop&Go and Emergency Braking.	Yes
Performing Lane Centering	ADS stays within a lane through lateral control while free driving or car following.	Yes
Performing Lane Switching/Overtaking	ADS crosses lanes or overtakes an upcoming vehicle based on a projected path or hazard.	Yes
Enhancing Conspicuity	ADS controls vehicle blinkers, headlights, horn, or other methods used to communicate with other drivers.	Yes

<u>Characteristics of City Pilot and role of human driver acc. To SAE J3016:</u>

- The City Pilot permits engagement only within its operational design domain (ODD)

Role of driver while the City Pilot is not engaged

- The driver verifies operational readiness of the City Pilot-equipped vehicle. The driver determines whether to engage the City Pilot
- The driver becomes a dispatcher/passenger when the City Pilot is not engaged only if physically present in the driver's seat in the vehicle

Role of dispatcher while the City Pilot is engaged

- The dispatcher needs not to perform the DDT or DDT fallback
- The dispatcher needs not to determine whether and how to achieve a minimal risk condition
- The dispatcher may perform the DDT fallback following a request to intervene
- The dispatcher may request that the City Pilot disengage and may achieve a minimal risk condition after it is disengaged
- The dispatcher may become the driver after a requested disengagement

Role of City Pilot while engaged

- The City Pilot performs the entire DDT within its ODD
- The City Pilot may issue a timely request to intervene
- The City Pilot performs DDT fallback and transitions automatically to a minimal risk condition when
    - A DDT performance-relevant system failure occurs or
    - A user does not respond to a request to intervene or
    - A user requests that it achieves a minimal risk condition
- The City Pilot disengages, if appropriate, only after
    - It achieves a minimal risk condition or
    - A driver is performing the DDT

The City Pilot may delay user-requested disengagement

4.2 Driving Scenarios of City Pilot

As discussed in section 3.3.1.2 City Pilot is considered different driving scenarios and attempted to cover almost each aspects of driving situations. Now results for each driving scenarios are listed in this section below;

4.2.1 Road Track Driving Scenarios

As described in chapter 3 road track driving scenarios are related to road track e.g. physical infrastructure which is made for city driving according to SAE level 4 and covers almost 42 driving scenarios some of which are listed below in Table 8 and further complete scenarios Appendix A.2

Table 8 Results of Road Track Scenarios

Nr.	Road track
1	Ego vehicle is approaching a city entrance with continuous road lane markings
2	Ego vehicle is approaching a city entrance with discontinuous road lane markings
3	Ego vehicle is driving on a city road lane with temporary discontinuous road lane markings
4	Ego vehicle is driving on a city road lane with temporary continuous road lane markings
5	Ego vehicle is driving on a straight city lane with continuous road lane markings
6	Ego vehicle is driving on a straight city lane with discontinuous road lane markings
7	Ego vehicle is driving on a curved city lane turning left with continuous road lane markings
8	Ego vehicle is driving on a curved city lane turning left with discontinuous road lane markings
9	Ego vehicle is driving on a curved city lane turning right with continuous road lane markings
10	Ego vehicle is driving on a curved city lane turning right with discontinuous road lane markings
11	Ego vehicle is approaching a city double curve, first to the left with continuous road lane markings

4.2.2 Operational Driving Scenarios

Operational scenarios based on operational constraints and objects. Some scenarios listed below in Table 9 and further scenarios attached in Appendix A.3. For manage the numbers of operational driving scenarios considered main road track as explained in chapter 3.

Table 9 Results of Operational Driving Scenarios

Nr.	**Main Road Track Scenario**		**Operational Driving Scenarios**
1	Ego vehicle is driving on a city road		Ego vehicle is driving on a city road while adapting vehicle motion according to detected **non-emergency participant vehicle i**n **frontal zone**
2			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **non-emergency participant vehicle** in **left side zone**
3			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **non-emergency participant vehicle** in **right side zone**
4			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **non-emergency participant vehicle** in **rear zone**
5			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **non-emergency participant vehicles in the left and right-side zones**
6			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **non-**

			emergency participant vehicles in the frontal and left side zones
7			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **non-emergency participant vehicles in the frontal and right-side zones**
8			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **non-emergency participant vehicles in the frontal and rear side zones**
9			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **non-emergency participant vehicles in the rear and left side zones**
10			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **non-emergency participant vehicles in the rear and right-side zones**
11			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **non-emergency participant vehicles in frontal, rear and left side zones**

Information
Non-emergency participant vehicles: cars, light truck, bus, motorcycle
Emergency vehicles: police, ambulance, firefighter, emergency trailer
Oncoming traffic on left side zone

4.2.3 Environmental Driving Scenarios

Environmental driving scenarios are considered according to environmental conditions. Table 10 shown environmental scenarios for city driving.

Table 10 Results of Environmental Driving Scenarios

Nr.	Environmental Driving Scenarios - high level		Environmental Driving Scenarios
1	Ego vehicle is driving on a city road with a specific **weather/visibility condition**		Ego vehicle is driving on a city road while adapting vehicle motion according to detected **rain**
2			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **fog/smog/smoke**
3			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **snow**
4			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **sleet**
5			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **hail**
			Ego vehicle is driving on a city road while adapting vehicle motion control according to detected **wind**
6			Ego vehicle is driving on a city road while adapting vehicle motion control according to detected **extreme weather condition**

7	Ego vehicle is driving on a city road with a specific **weather-induced roadway condition**		Ego vehicle is driving on a city road while adapting vehicle motion according to detected **icy road**
8			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **wet road detection**
9			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **road surface damages**
10			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **standing water**
11			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **dirt**
12			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **snow on the road**
13	Ego vehicle is driving on a city road with a specific **light condition**		Ego vehicle is driving on a city road according to detected **daytime**
14			Ego vehicle is driving on a city road according to detected **night-time**
15			Ego vehicle is driving on a city road according to detected **dusk**
16			Ego vehicle is driving on a city road according to detected **dawn**

17			Ego vehicle is driving on a city road according to detected **streetlights**

4.2.4 Functional Driving Scenarios

City Pilot development approach considered more than three hundred functional driving scenarios according to the definition which is explained in section 3.3.1.2. Some results of functional scenarios for city driving are listed in different tables below according to different cases of operational driving scenarios.

CASE ONE: *Ego vehicle is driving on a city road while adapting vehicle motion according to detected non-emergency participant vehicle in frontal zone*

Table 11 Case One: Results of Functional Driving Scenarios

Nr.	**Operational Driving Scenarios**		**Functional Driving Scenarios**
1	Ego vehicle is driving on a city road while adapting vehicle motion according to detected non-emergency participant vehicle in frontal zone		Ego vehicle is **following vehicle** according to detected non-emergency participant vehicle in frontal zone **decelerating**
2			Ego vehicle is **decelerating** according to detected non-emergency participant vehicle in frontal zone **decelerating**
3			Ego vehicle is **stopping** according to detected non-emergency participant vehicle in frontal zone **decelerating**
4			Ego vehicle is **changing lane** according to detected non-emergency participant vehicle in frontal zone **decelerating**
5			Ego vehicle is **passing (overtaking)** according to detected non-emergency participant vehicle in frontal zone **decelerating**

6			Ego vehicle is **decelerating** according to detected non-emergency participant vehicle in frontal zone **stopping**
7			Ego vehicle is **stopping** according to detected non-emergency participant vehicle in frontal zone **stopping**
8			Ego vehicle is **changing lane** according to detected non-emergency participant vehicle in frontal zone **stopping**
9			Ego vehicle is **passing (overtaking)** according to detected non-emergency participant vehicle in frontal zone **stopping**
10			Ego vehicle is **following vehicle** according to detected non-emergency participant vehicle in frontal zone **accelerating**
11			Ego vehicle is **accelerating** according to detected non-emergency participant vehicle in frontal zone **accelerating**
12			Ego vehicle is **yielding** according to detected non-emergency participant vehicle in frontal zone **changing lane**
13			Ego vehicle is **decelerating** according to detected non-emergency participant vehicle in frontal zone **changing lane**
14			Ego vehicle is **accelerating** according to detected non-emergency participant vehicle in frontal zone **cutting out**
15			Ego vehicle is **stopping** according to detected non-emergency participant vehicle in frontal zone **cutting out**
16			Ego vehicle is **decelerating** according to detected non-emergency participant vehicle in frontal zone **cutting out**

CASE TWO: *Ego vehicle is driving on a city road while adapting vehicle motion according to detected traffic signs*

Table 12 Case Two: Results of Functional Driving Scenarios

1	Ego vehicle is driving on a city road while adapting vehicle motion according to detected traffic signs		Ego vehicle is **accelerating** according to detected **speed limit traffic sign**
2			Ego vehicle is **decelerating** according to detected **speed limit traffic sign**
3			Ego vehicle is **aborting lane change** according to detected **no passing traffic sign**
4			Ego vehicle is **aborting passing** according to detected **no passing traffic sign**
5			Ego vehicle is **decelerating** according to detected **no passing traffic sign**
6			Ego vehicle is **changing lane** (when changing lane needed) according to detected **end of no passing traffic sign**
7			Ego vehicle is **accelerating** according to detected **wet weather/daytime speed limit traffic sign**
8			Ego vehicle is **decelerating** according to detected **wet weather/daytime speed limit traffic sign**
9			Ego vehicle is **accelerating** according to detected **end of speed limit traffic sign**

10			Ego vehicle is **steering** according to detected **curve turning left traffic sign**
11			Ego vehicle is **decelerating** according to detected **curve turning left traffic sign**

4.3 Object, Event Detection and Response Analysis

Functional driving scenarios explains OEDR Analysis in words or sentences in order to provide more clarity and understanding. More than 300 OEDR Analysis were created for systematic development approach of city driving in tabular form method. Each object, event and response individually analysis in tabular method for better understanding and described each response description. As mentioned above in this section OEDR Analysis results are more than hundred, so here only for some operational driving scenarios OEDR result in different tables along with response description are given below.

Object One: Non-emergency participant vehicle

Object Type: Roadway users

Table 13 Frontal Zone Roadway Users OEDR Analysis

Operational Driving Scenarios		**Objects**		**Event**		**Response**
1 Objects						
1.1 Roadway users						
Ego vehicle is driving on a city road while adapting vehicle motion according to		Non-emergency participant vehicle in		Non-emergency participant vehicle in		Follow vehicle
						Decelerate
						Stop
						Change lane

detected non-emergency participant vehicle in frontal zone		frontal zone		frontal zone decelerating		Pass
				Non-emergency participant vehicle in frontal zone stopping		Decelerate
						Stop
						Change lane
						Pass
				Non-emergency participant vehicle in frontal zone accelerating		Follow vehicle
						Accelerate
				Non-emergency participant vehicle in frontal zone changing lane		Yield
						Decelerate
				Non-emergency participant vehicle in frontal zone cutting out		Accelerate
						Decelerate
						Stop

Table 14 Left Side Zone Roadway Users OEDR Analysis

						Yield

Ego vehicle is driving on a city road while adapting vehicle motion according to detected non-emergency participant vehicle in left side zone		Non-emergency participant vehicle in left side zone		Non-emergency participant vehicle in the left side zone cutting in		Decelerate
						Stop
						Follow vehicle
						Change lane
				Non-emergency participant vehicle in the left side zone encroaching		Decelerate
						Stop
						Shift within the lane
						Shift outside of the lane
						Change lane

Table 15 Right Side Zone Roadway Users OEDR Analysis

Ego vehicle is driving on a city road while adapting vehicle motion according to detected non-emergency participant vehicle in right side zone		Non-emergency participant vehicle in right side zone		Non-emergency participant vehicle in the right-side zone cutting in		Yield
						Decelerate
						Stop
						Follow vehicle
						Change lane
				Non-emergency participant vehicle in the right-side zone encroaching		Decelerate
						Stop
						Shift within the lane
						Shift outside of the lane
						Change lane

Object Two: Animal

Object Type: Non-roadway users

Table 16 Frontal Zone Non-Roadway Users OEDR Analysis

1.2 Non-roadway users							
Ego vehicle is driving on a city road while adapting vehicle motion according to detected animal in frontal zone		Animal in frontal zone		Animal static in frontal zone		Decelerate
						Stop
						Change lane
						Pass
						Shift within the lane
						Shift outside of the lane
				Animal moving into/out of frontal zone		Decelerate
						Stop
						Change lane
						Pass
						Shift within the lane
						Shift outside of the lane

Table 17 Frontal Zone Non-Roadway Users OEDR Analysis

Ego vehicle is driving on a city road while adapting		Animal in left side zone		Animal moving from the left		Decelerate
						Stop
						Change lane
						Pass

vehicle motion according to detected animal in left side zone				side zone		Shift within the lane
						Shift outside of the lane

Table 18 Right Side Zone Non-Roadway Users OEDR Analysis

Ego vehicle is driving on a city road while adapting vehicle motion according to detected animal in right side zone		Animal in right side zone		Animal moving from the right-side zone		Decelerate
						Stop
						Change lane
						Pass
						Shift within the lane
						Shift outside of the lane

Table 19 Response Description of OEDR Analysis

Response Description
Follow vehicle: Implement lateral and/or longitudinal control actions to maintain a safe following distance from an immediate lead vehicle, while continuing to follow the current lane of travel.
Accelerate: Implement longitudinal control actions to increase speed, as appropriate and lawful.

Decelerate: Implement longitudinal control actions to decrease speed, as appropriate.
Stop: Implement longitudinal control actions to decelerate in a safe and stable manner to a complete stop.
Yield: Relinquish right-of-way to another road user.
Change lane: Implement longitudinal and/or lateral control actions to shift into an adjacent lane.
Abort lane change: Cancel the manoeuvre to shift into an adjacent lane (remain in or return to original lane).
Pass (overtaking): Implement longitudinal and/or lateral control actions to shift into an adjacent lane to accelerate to desired speed.
Abort Pass: Cancel manoeuvre to shift into an adjacent lane (remain in or return to original lane).
Shift within lane: Implement lateral and/or longitudinal control actions such that the ADS does not follow the centre (or near centre) of the current lane but remains fully within the current lane.
Shift outside of the lane: Implement lateral and/or longitudinal control actions such that the ADS partially or fully move outside of the current lane of travel (i.e., one or more wheels cross the lane boundary)
Move out of travel lane/park: Implement lateral and longitudinal control actions such that the ADS fully exit the current active lane of travel onto a shoulder or parking lane and stops.

Transition to Minimal Risk Condition	**Return Control to Fallback-ready User:** Return longitudinal and lateral control to human occupant/driver (while providing enough warning).
	ADS Implements Minimal Risk Manoeuvre: Implement lateral and/or longitudinal control actions to achieve a minimal risk condition.
***Steering:** Implement lateral control actions, as appropriate and lawful.	
Choose new lane to follow: Implement lateral and/or longitudinal control actions to shift into a new lane, when lanes are splitting.	
Follow temporary lanes: Implement lateral and/or longitudinal control actions to shift into a new temporary lane, in a construction zone.	
Calibrate headlights: Switch between low-beams and high-beams, to adjust visibility to environment conditions, without blinding the other participants at traffic.	

4.4 Operational Design Domain of City Pilot

The ODD describes the specific operating domains in which the system is designed to function as described in chapter 2. Six categories are identified in accordance to NHTSA to integrate all the conditions inside and outside ODD. The categories are:

- Physical Infrastructure
- Operational Constraints
- Objects
- Connectivity
- Environmental Conditions
- Zones

4.4.1 Inside ODD of City Pilot

Countries of operation: All country of Europe except **England.**

- **Physical infrastructure**

Physical infrastructure refers to facilities and systems that serve a country, city, or area and enable its economy to function.

Table 20 Physical Infrastructure inside ODD

PHYSICAL INFRASTRUCTURE
Roadway Types
Urban (city), multi-lane, single lane, one-way, turn-only lanes, intersections (signals, 3-way/2-way stop, roundabout, split lanes, merge lanes, crosswalk, tram track crossing), oncoming lanes.
Roadway Surfaces
Friction coefficient boundary: asphalt, concrete, mixed, grating, brick, dirt, gravel, scraped road, partially occluded, bumps, potholes, grass
Roadway Boundaries & Markings
Lane markers continuous & discontinuous, temporary lane markers continuous & discontinuous, shoulder paved or gravel, shoulder grass, lane barriers, gratings, cones, walls, concrete barriers, separators, tram track
Roadway Geometry
Straightaways, curves, double curves, lateral crests, corners/turns, EGO lane width.

- **Operational Constrains**

It refers to the functional boundaries that need to be considered when designing and testing ADS applications.

Table 21 Operational Constrains Inside ODD

OPERATION CONSTRAINTS
Speed Limits
0 Km/h to 60 Km/h
Operation in right road traffic
Traffic Conditions

Traffic density minimal, normal and heavy. Altered due to accident, emergency vehicle, construction, closed road, special event, etc.
Temperature
Ambient temperature: 52°C to -62.2°C
Lifecycle
Operational lifecycle: 15 years

- **Objects**

It refers to identified objects that can likely be expected to exist within the ODD.

Table 22 Objects Inside ODD

OBJECTS
Signage
Bumpy road traffic sign Closure/ending ego lane traffic sign Construction/school zone traffic sign Curve turning left traffic sign Curve turning right traffic sign Double curve, first to the left traffic sign Double curve, first to the right traffic sign End of city traffic sign End of speed limit traffic sign City entrance traffic sign City exit traffic sign City lane split traffic sign City lane merge traffic sign City tunnel ahead traffic sign City tunnel exit traffic sign Roundabout traffic sign Road narrows traffic sign Crosswalks Tram track crossing Mandatory turn right traffic sign Mandatory turn left traffic sign Mandatory turn right or ahead traffic sign Mandatory turn left or ahead traffic sign Mandatory straight traffic sign No passing traffic sign End of no passing traffic sign Stopped buses sign Speed limit traffic sign Stop traffic sign

Traffic light or Arrow traffic sign is green Traffic light or Arrow traffic is red Traffic light is yellow Yellow traffic light is flashing - Construction zone Yield traffic sign Wet road/daytime speed limit traffic sign Safety officials (Hand signals) First responder signals
Roadway Users
Vehicles, pedestrians and cyclists Cars, light trucks, buses, two-wheelers, emergency vehicles, construction vehicles, stopped vehicle, other automated vehicles, pedestrians, pedal cyclists
Non-Roadway Users Obstacles
Animals (e.g., dogs, cats, etc.), shopping carts, debris (e.g., pieces of tire, trash, ladders), construction equipment's

- **Connectivity**

Connectivity constitutes a communications link between other vehicles, road users, remote fleet management operators, and physical and digital infrastructure elements. Just the elements related to navigation are considered relevant in this approach.

Table 23 Connectivity Characteristics inside ODD

CONNECTIVITY
GPS, 3D maps, V2I, Broadcast traffic information

Table 24 Maintenance, Updates and Data providing

MAINTENANCE, UPDATES & DATA PROVIDING	
Offline & online SW-update	Avaliable
Offline & online diagnostics	Avaliable
Online providing of vehicle data	Avaliable
Data logging	Avaliable
Other	Not Avaliable

- **Environmental conditions**

The environment can affect visibility, sensor fidelity, vehicle manoeuvrability, and communications systems.

Table 25 Environmental Conditions inside ODD

ENVIRONMENTAL CONDITIONS
Weather
Wind Calm, light air, light, gentle, moderate
Rain Light rain, moderate rain
Snow Light snow, moderate snow
Hail hard Hail
Sleet Light and moderate intensity
Weather-Induced Roadway Conditions
Standing water, Icy road, snow on the road, dirt
Particulate Matter
Fog, smog & smoke Pure air, exceptionally clear, very clear, clear, light haze, haze, thin fog, light fog
Illumination
Day, dawn, dusk, night, streetlights, headlights (regular, high beam), oncoming vehicles lights

- **Zones**

ADS features may be limited spatially by zones. The boundaries of these zones may be fixed or dynamic, and conditions that define a boundary may be based on complexity, operating procedures, or other factors. Zones help to refine the feature description.

Table 26 Zones inside ODD

ZONES
Geo-fencing
Fixed Route
School/Construction Zone
School/Construction Zone
Interference Zones
Tunnels

Additional Information Note:

- Fixed route refers to the driver possibility of setting prior to initiate the trip the starting and destination point.
- Construction zone is included in Objects and Zones because in the first category it is considered as a traffic sign / detection feature while in Zones it will help to refine the operational boundaries of the system.
- Tunnel is included in Physical Infrastructure and Zones because of its nature as an element of the road track and its likelihood to affect navigation as an inference zone. It is important to consider both categories given that this can affect the responses to a single event e.g. driving through a tunnel.

4.4.2 Outside ODD of City Pilot

Countries of operation: England and other not specified in ODD

- **Physical infrastructure**

Table 27 Physical Infrastructure outside ODD

PHYSICAL INFRASTRUCTURE
Roadway Types
Arterial, highway, rural, parking, emergency evacuation routes, private roads, reversible lanes, any other not specified in ODD
Roadway Surfaces
Friction coefficient boundary

Roadway Boundaries & Markings
Rails, any other not specified in ODD
Roadway Geometry
Any other not specify in ODD

- **Operational Constraints**

Table 28 Operational Constrains outside ODD

OPERATION CONSTRAINTS
Speed Limits
Greater than 60 km/h
Any other not specified in ODD
Traffic Conditions
Any other not specified in ODD
Temperature
Bellow -62.2°C and greater than 52°C

- **Objects**

Table 29 Objects outside ODD

OBJECTS
Signage
Distress signals, roadway user signals, any other not specified in ODD
Roadway Users
Farming equipment, horse-drawn, carriages/buggies, caravans, campervans any other not specified in ODD

Non-Roadway Users Obstacles
Any other not specify in ODD

- **Connectivity**

V2V-Communication is not considered due to mixed traffic in the near future (only few vehicles will have V2V), reducing the assumptions-based development effort and higher prioritization of V2I for having divers' solutions in place.

Table 30 Connectivity Characteristics outside ODD

CONNECTIVITY
Any other not specify in ODD

- **Environmental conditions**

Table 31 Environmental conditions outside ODD

ENVIRONMENTAL CONDITIONS
Weather
Wind Greater than moderate (fresh/strong)
Rain Greater than moderate (heavy/violent rain)
Snow Greater than moderate (heavy snow)
Hail Greater than hard hail
Sleet Heavy intensity
Weather-Induced Roadway Conditions
Flooded roadways, any other not specify in ODD

Particulate Matter
Fog, smog & smoke Greater than light fog (moderate/thick/dense fog)
Illumination
Any other not specify in ODD

- **Zones**

Table 32 Zones outside ODD

ZONES
Any other not specify in ODD

5 Results on Concept Phase

This chapter contains results of item definition approach developed in concept phase of V Model in section 3.3.2. The results of use cases diagrams and activity diagrams of level 4 City Pilot model, functional architecture as well as Hazards Analysis and Risk Assessment for city driving can be found in this chapter, which were created with the support of SysML modelling language.

5.1 Description and Overall Use Case Diagram of City Pilot

Overall use case diagram represents all functions of system for HAD of City Pilot feature. City Pilot feature is able to perform driver monitoring e.g. detect driver presence, setting inputs such as speed, distance and route etc., ego vehicle monitoring e.g. detect vehicle information like actual speed, steering angle etc., environment monitoring e.g. detect surroundings like objects, traffic signs, traffic lights etc., after monitoring all above described aspects of city driving now understand the events and make decision according to predicted events and afterward sends signals to vehicle controlling. Figure 5.1 shown below represents overall use case diagram of City Pilot.

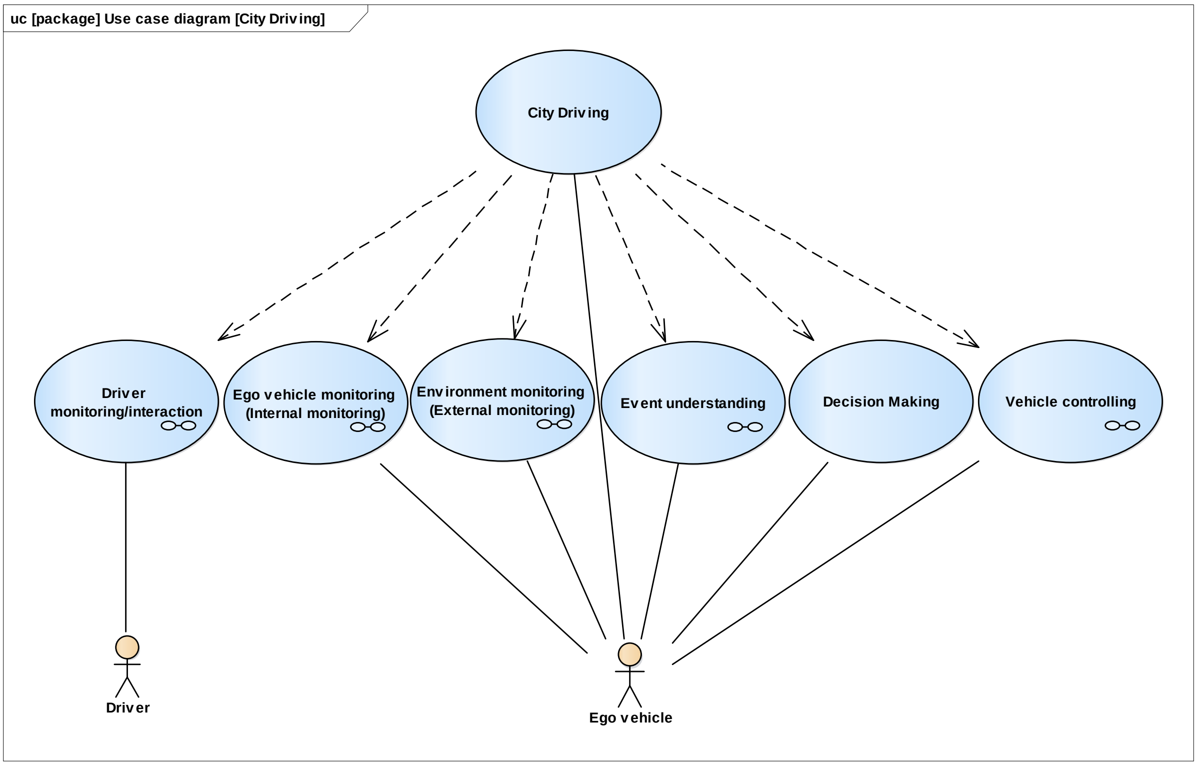

Figure 5.1 Overall Use Case Diagram of City pilot

5.2 Example of Ego Vehicle Monitoring Use Case Diagram

City driving is the main use case which includes further sub use cases diagrams for city driving system functions. Ego vehicle monitoring use case diagram is an example from one of them. In this thesis work created more than 100 use case diagrams which illustrated in detail each aspect and function of city driving. As shown Figure 25 below explains ego vehicle monitoring use case diagram and functionality of diagram as described in section 3.3.2.1.

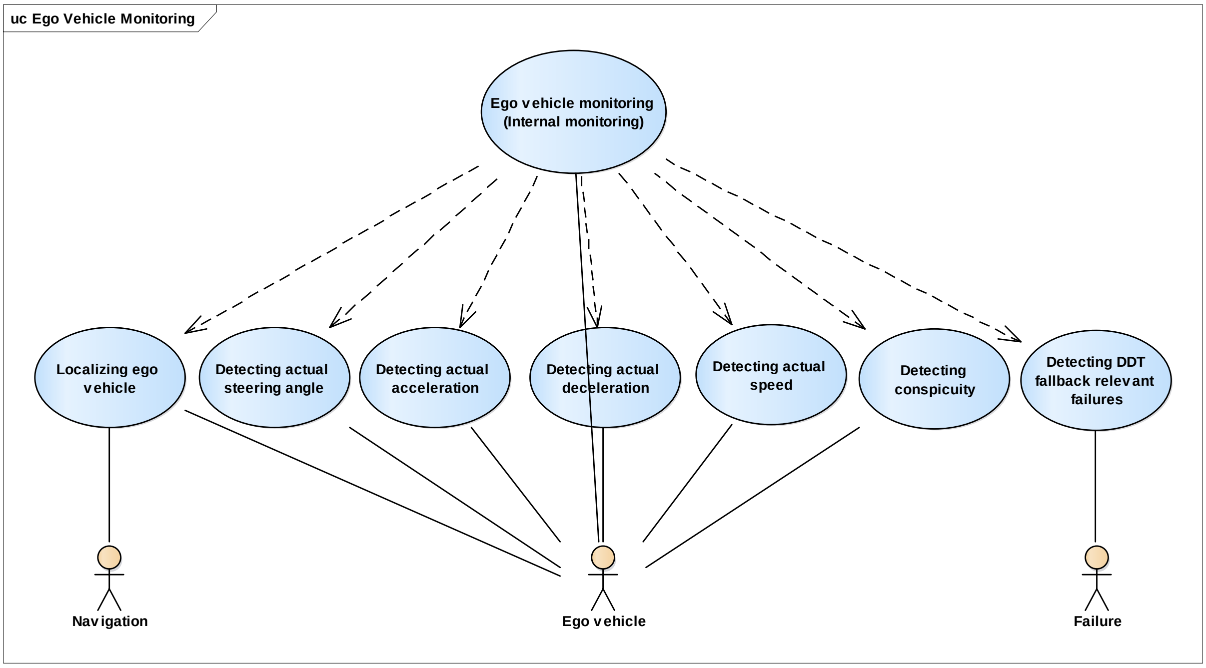

Figure 5.2 Ego Vehicle Monitoring Use Case Diagram

Furthermore, ego vehicle monitoring use case of city driving has functions to localizing ego vehicle (e.g. position on the map, position on the road, position between lanes) by navigation, sensing ego vehicle actual steering angle, actual acceleration and deceleration, actual speed, actual distance, detecting conspicuity along with detecting dynamic driving task (DDT) fallback relevant failures in order to be able to transition to MRC and sends signals to decision making.

5.3 Internal and External Monitoring Activity Diagrams of City Pilot

As described in chapter 2, the activity diagrams explain functional principle. In this section some examples of resulted internal and external monitoring activity diagrams of City Pilot are provided for better understanding of use cases.

5.3.1 Ego Vehicle Monitoring (Internal Monitoring)

- **Localizing Ego Vehicle Activity Diagram**

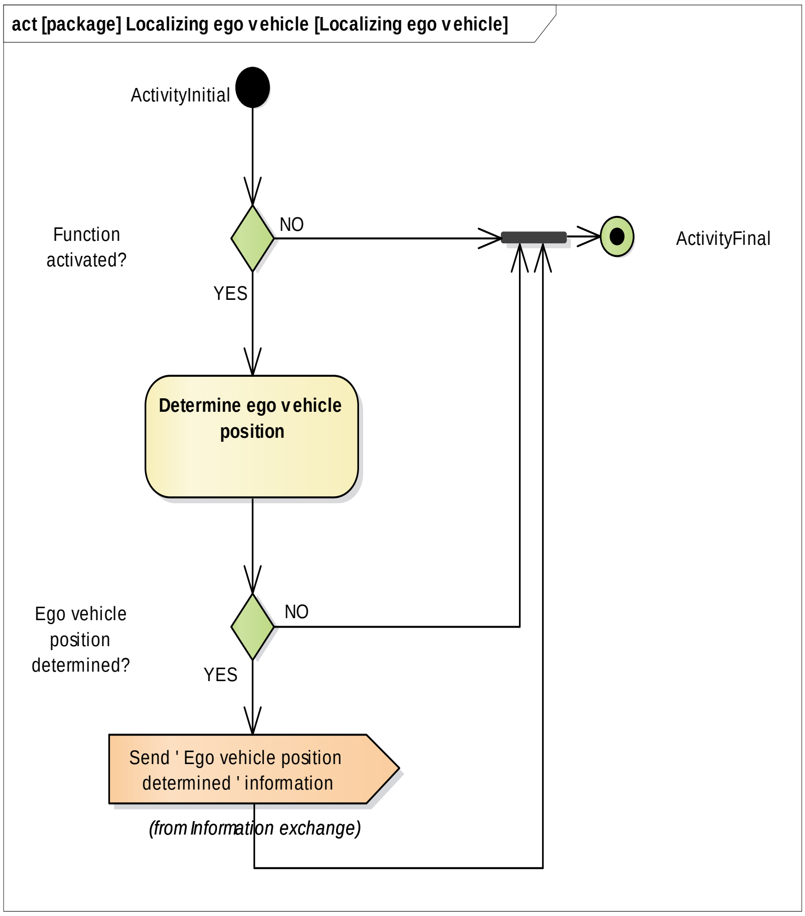

Figure 5.3 Localizing Ego Vehicle Activity Diagram

- **Detecting Actual Steering Angle**

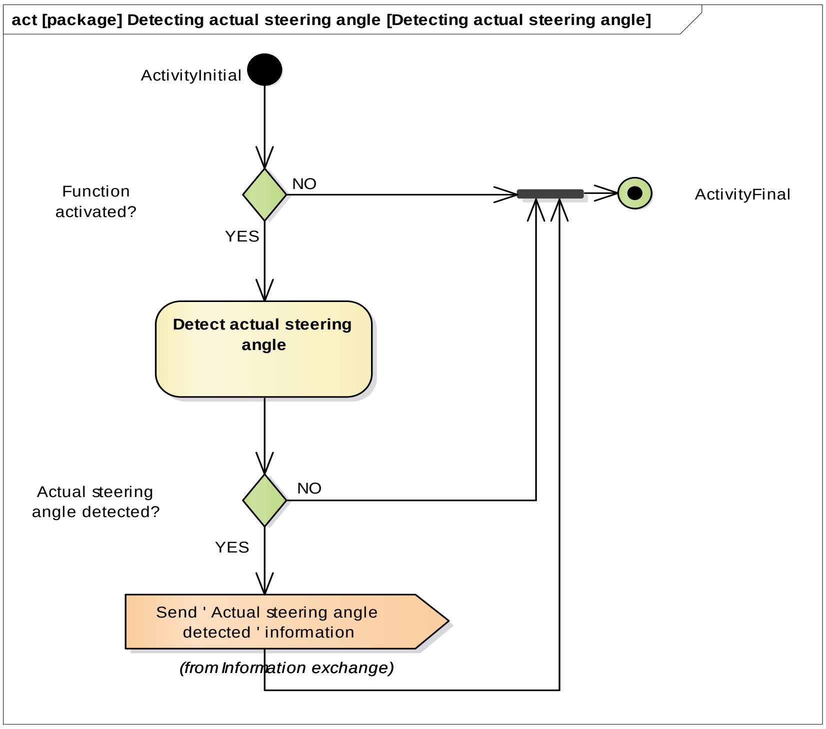

Figure 5.4 Detecting Actual Steering Angle Activity Diagram

- ## Detecting Actual Speed Activity Diagram

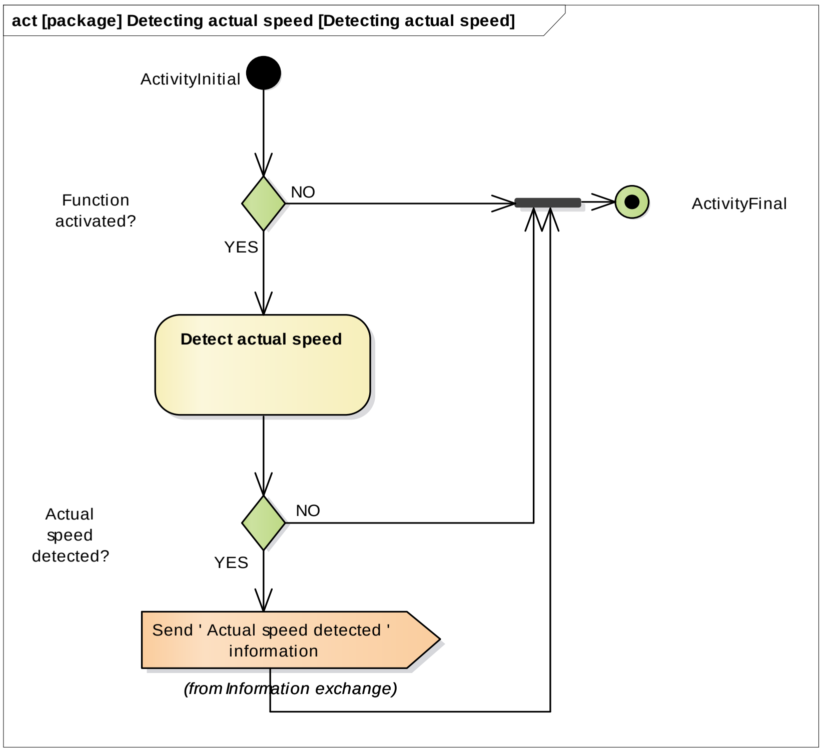

Figure 5.5 Detecting Actual Speed Activity Diagram

5.3.2 Environment Monitoring (External Monitoring)

- **Detecting Dynamic Objects Activity Diagram**

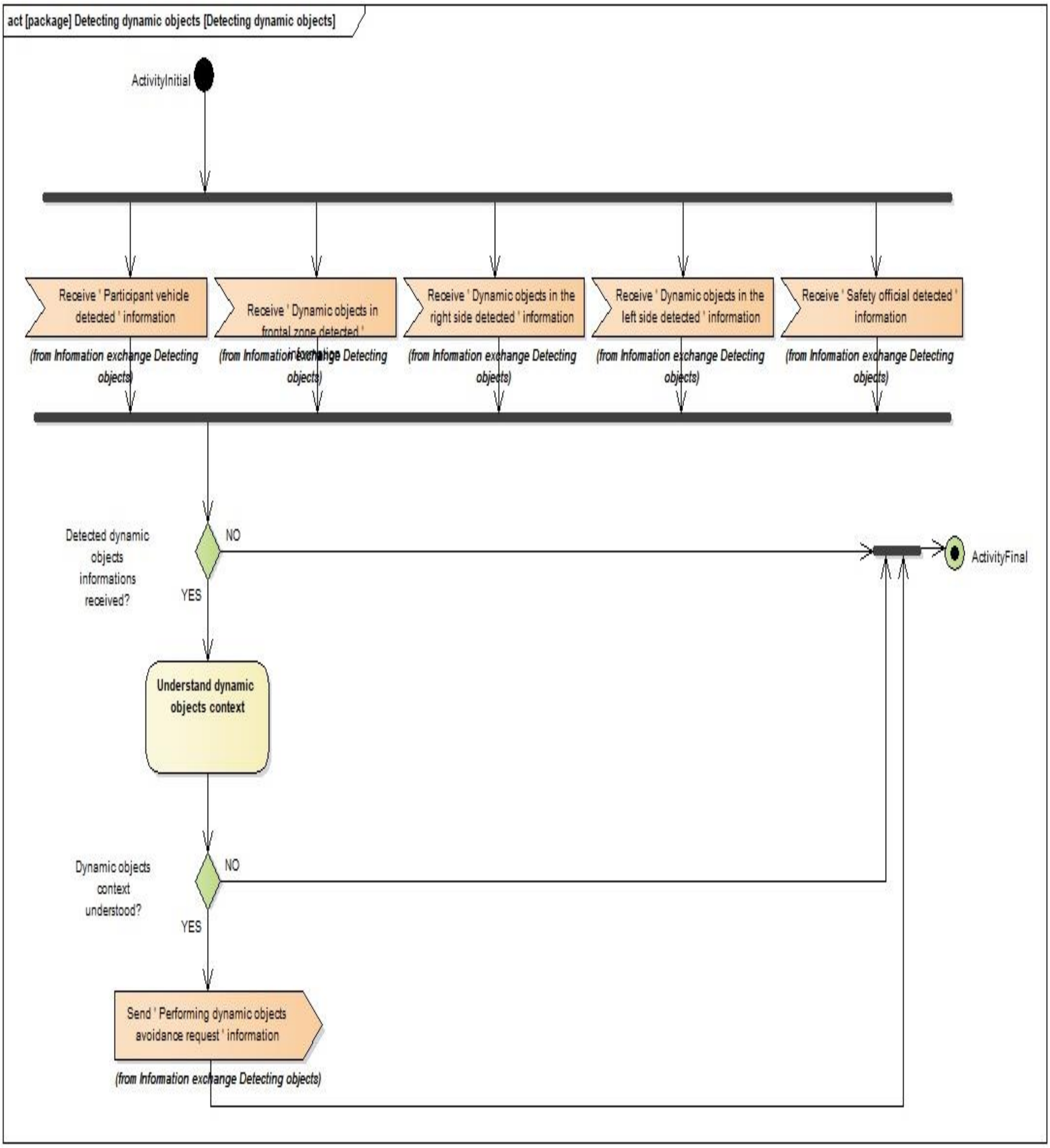

Figure 5.6 Detecting Dynamic Objects Activity Diagram

- **Localizing Dynamic Objects**

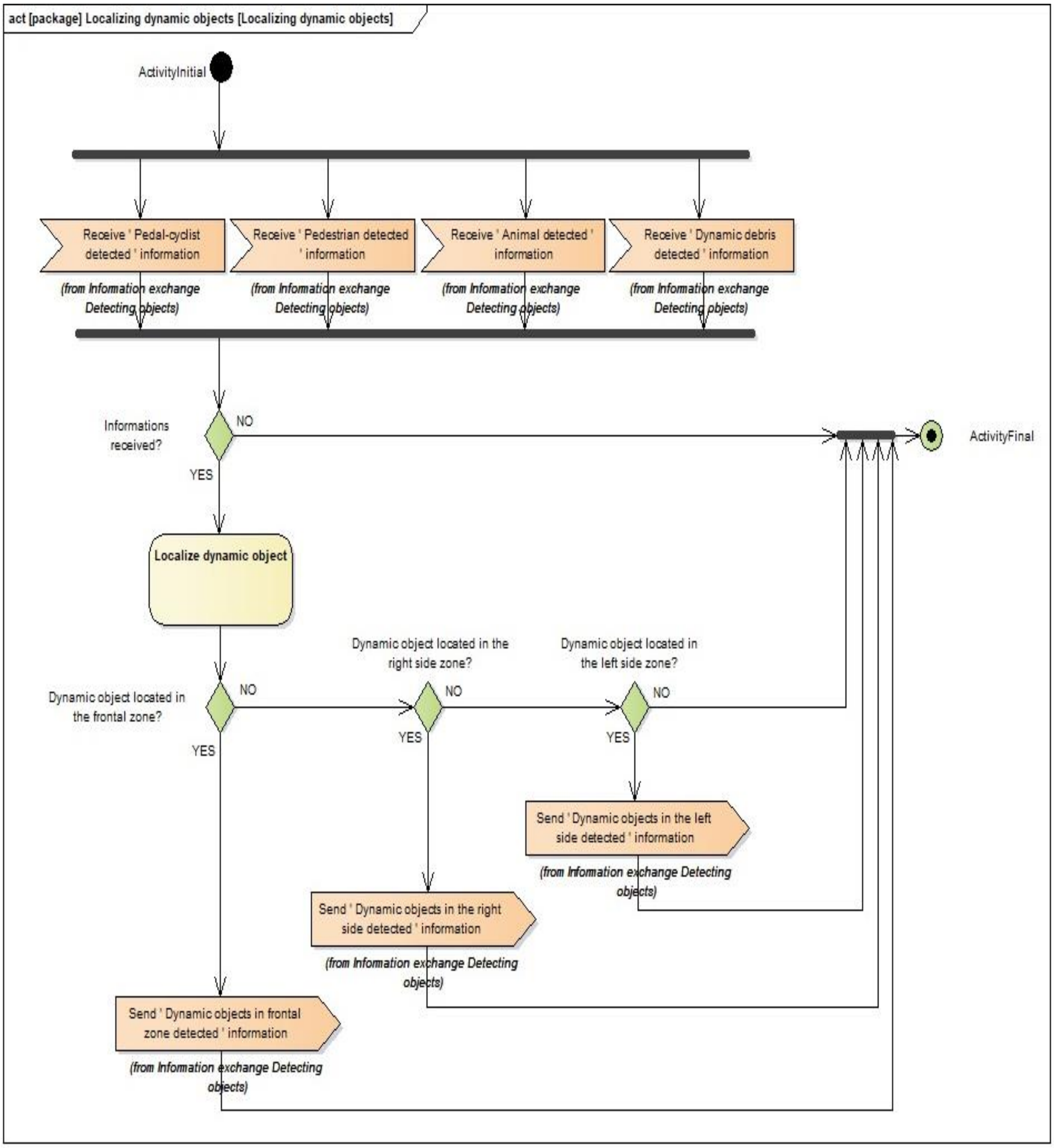

Figure 5.7 Localizing Dynamic Object

5.4 Event Understanding and Decision-Making Activity Diagrams

In this section events understanding, and decision-making activity diagram are provided which explain the functional principle of system functions of city driving.

5.4.1 Dynamic Object in Frontal/left/right Side Zone Event Understanding Activity Diagram

Dynamic Object in Frontal/left/right Side Zone is one of activity diagram from event understanding which explains how dynamic objects are predicted from environment of city before decision making.

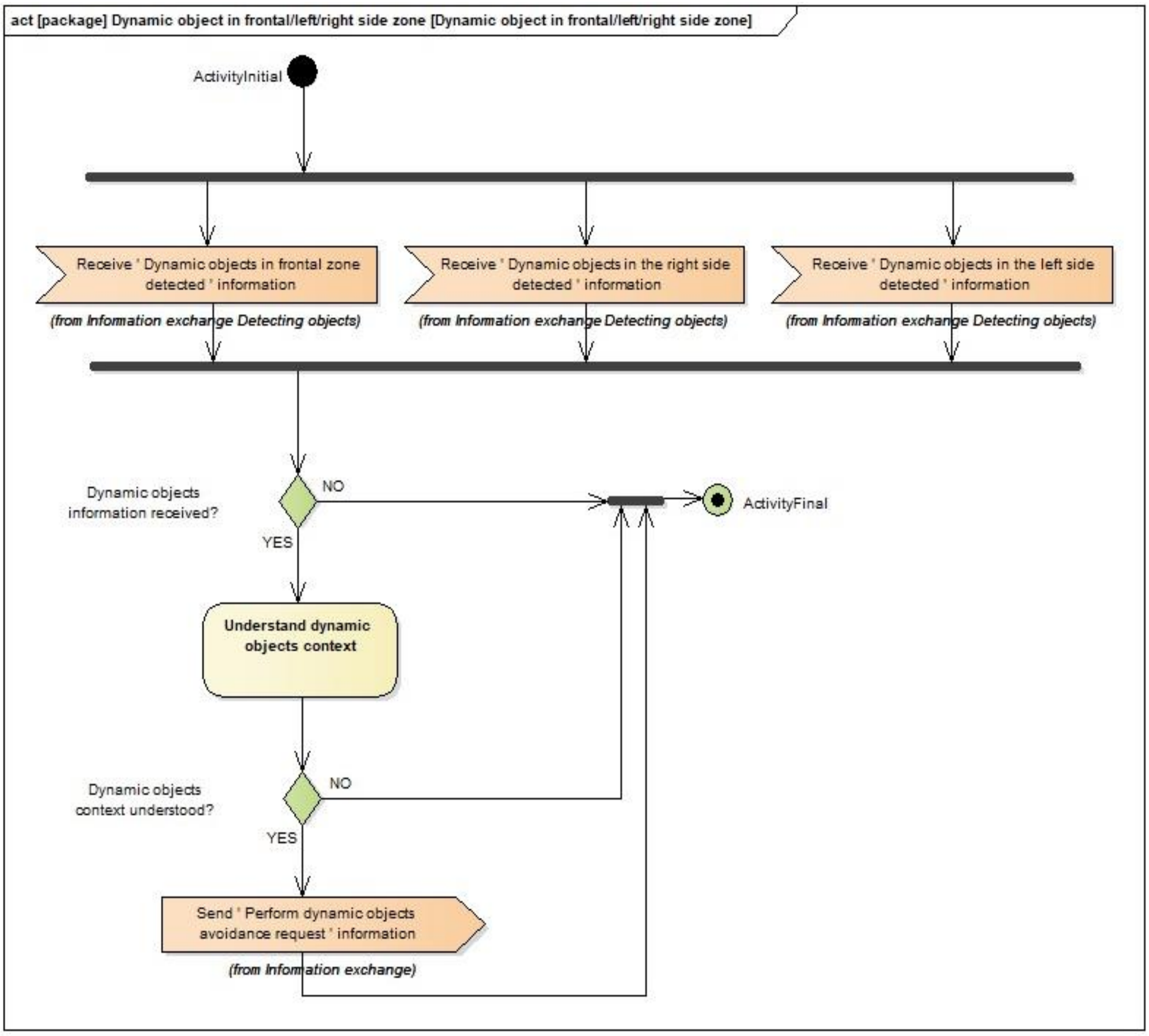

Figure 5.8 Dynamic Object in Frontal/left/right Side Zone

5.4.2 Performing Dynamic Object Avoidance Decision Making Activity Diagram

Performing Dynamic Object Avoidance activity diagram shown in figure 5.9, it is one of activity from different activity diagrams of decision making.

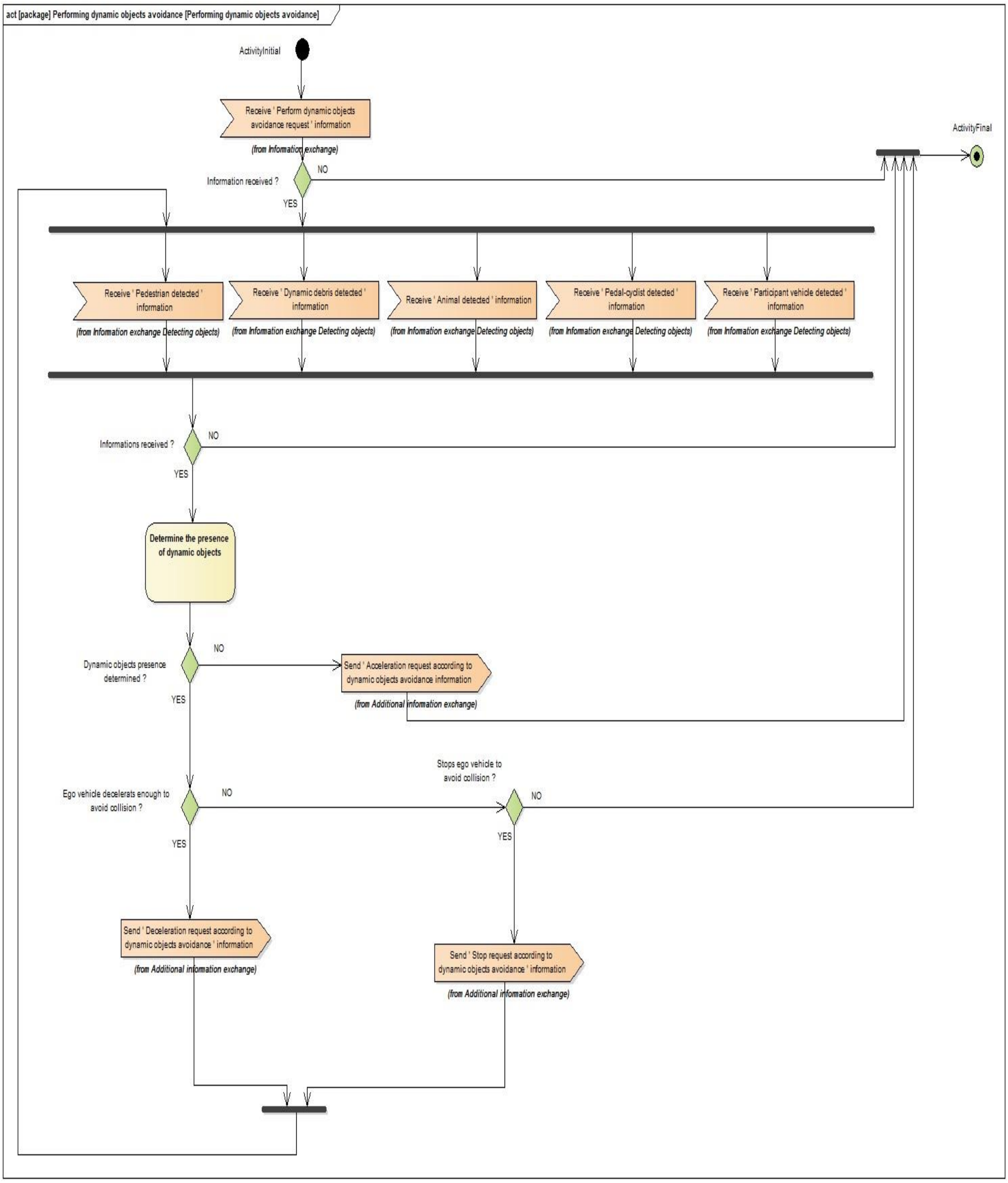

Figure 5.9 Performing Dynamic Object Avoidance

5.5 Functional Architecture of City Pilot Feature Functions

In Figure 5.10 is illustrate functional architecture of City Pilot feature function. Further one more example of functional architecture provided in Appendix B.3.

Performing dynamic object avoidance.

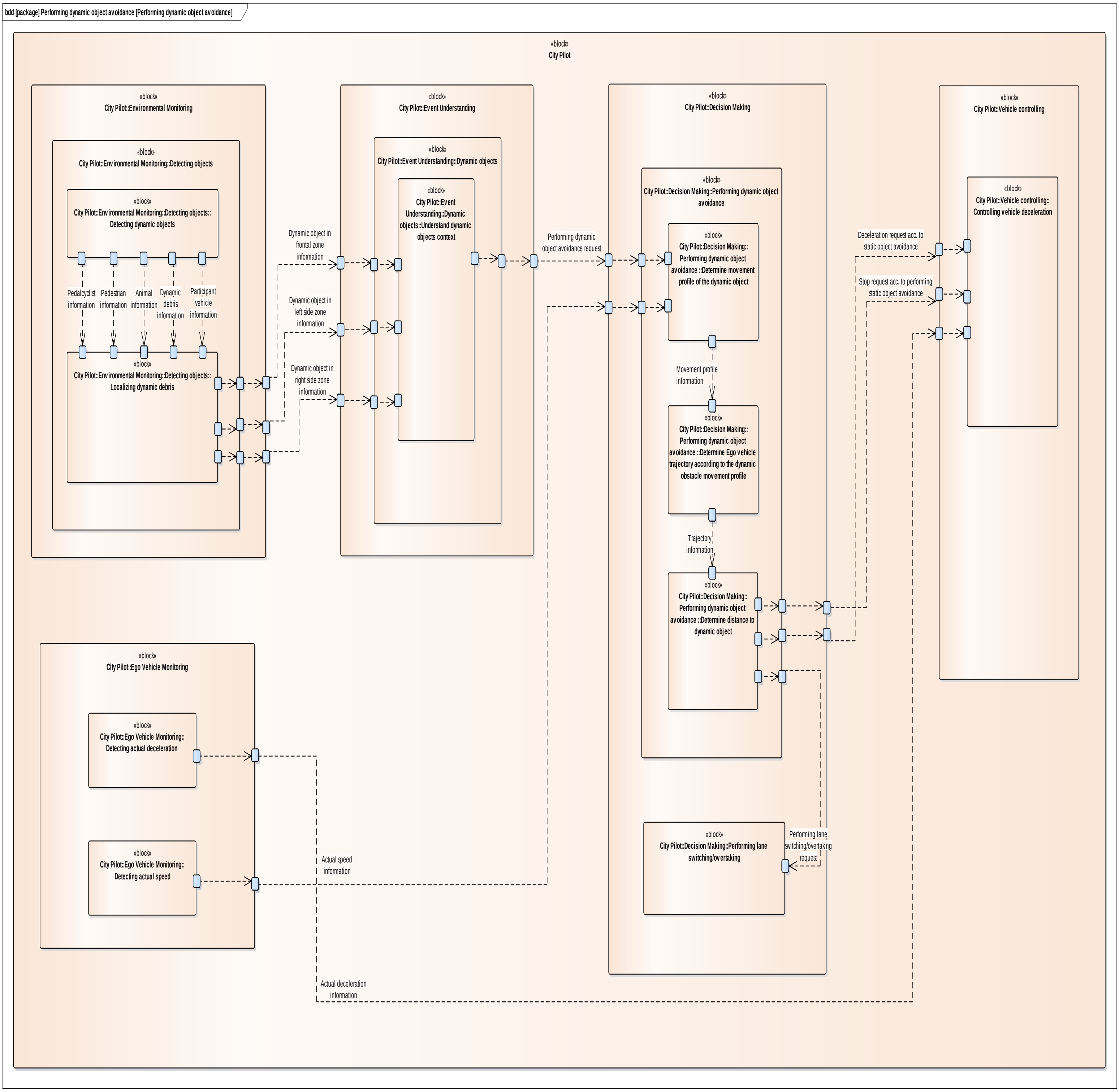

Figure 5.10 Functional Architecture of Performing dynamic object avoidance

5.6 Hazards Analysis and Risk Assessment

The HARA (Hazard Analysis and Risk Assessment) is an important part of functional safety and a specification in the ISO 26262 standard. This section explains HARA and safety goals for City Pilot according to approach which described in chapter 3.

5.6.1 Situation Catalogue of City Pilot

The ISO 26262 standard requires that "the operational situations and operating modes in which an item's malfunctioning behavior will result in a hazardous event shall be described". For this reason, the situation catalogue shown in table 33 was made. It specifies all situations in which the behavior of vehicle in presence of a system feature malfunction is assessed.

Table 33 Situation Catalogue of City Pilot

Relevant Situations Considered for City Pilot			
Driving	**City**	**Specifics**	**Involved Persons**
Forward Driving	In the city until 60km/h	Free drive	Driver
Curve Driving	30km/h zone	Follow drive	Pedestrian
Accelerating from standstill	Crosswalks	Traffic jam	Persons in another vehicle
Accelerating	Traffic light	Oncoming traffic	Cyclist
Turning	Intersection	Straight	
Deceleration	Sidewalk	Curve	
Full braking	Cycle track	Construction zone	
Stopping	Tunnel	Night	
Lane change	Roundabouts	Fog	
Overtaking	Tram track	Rain	

Standstill		**Snow**	
		Road wetness	
		Ice	

5.6.2 Functions of City Pilot

In order to identify the malfunctions of the item and the resulting hazardous events, it is important to define all the functions, City Pilot covers up. This was made with the definition of the use cases in chapter 3. The main input for these use cases are the driving scenarios. That's why it is useful to describe these scenarios, to get an overview of all the functions.

As an example, the driving scenario of City Pilot "Ego vehicle turns far side in an intersection with bicycle and pedestrian crossing" is taken in consideration. For this driving scenario the description would be:

"Ego vehicle checks if turning left in the intersection is permitted. Ego vehicle detects other participant vehicles, bicycles or pedestrians in intersection and gives priority if it has to, according to traffic signs and road lanes. If no traffic sign is present, ego vehicle gives priority to the participants coming from the right side. Ego vehicle detects the crossing pedestrian and bicycle and adapts speed. Ego vehicle checks if ego lane is free ahead. If yes, ego vehicle turns left. If no, ego vehicle adapts speed."

Out of this description, the malfunctions can be worked out, which is part of the next section.

5.6.3 Malfunctions of City Pilot functions

The definition of malfunctioning behavior that leads to a hazardous event is a key task of the HARA.The main functions (use cases) of City Pilot (shown in Table 6) serve as the basis for the malfunction identification of the feature. Each main function was taken in consideration separately. With the help of the detailed driving scenario descriptions in the section above, all functions within the main functions were worked out. These "sub functions" were than examined for possible malfunction behavior.

As an example, the driving scenario “Ego vehicle turns far side in an intersection with bicycle and pedestrian crossing” will be analyzed again. Functions that can be derived from the description are:

- Road lane detection
- Participant vehicle detection
- Pedestrian detection
- Bicycle detection
- Lateral steering
- Longitudinal acceleration
- Longitudinal deceleration

The determination of the malfunctions is done according to the interpretation of the SAE J2980, which divides the function up to five different possible behaviors which are:

- Function not provided when intended - loss of function
- Function provided incorrectly when intended - more than intended
- Function provided incorrectly when intended - less than intended
- Function provided incorrectly when intended - wrong direction
- Function provided when not intended - unintended activation of function

Every function is now combined with a malfunctioning behavior. For “Lateral steering” the malfunctions would be:

- No lateral steering support when requested
- More than intended lateral steering support
- Less than intended lateral steering support
- Steering support in wrong direction
- Unintended lateral steering support

This leads to a detailed and complete list of all possible malfunctions of City Pilot.

But not all combinations are safety relevant. A good example for this statement is the function “Give way sign detection”. The malfunctions would be:

- No give way sign detection
- More than intended give way sign detection
- Less than intended give way sign detection

- Wrong give way sign detection
- Unintended give way sign detection

The first malfunction “No give way sign detection” is safety relevant, because no detection could lead to a collision of the ego vehicle with a possible existing participant vehicle.

The malfunction “Unintended give way sign detection” must also be considered as safety relevant because an unintended detection (the system detects a not existing give way sign) leads to a reaction of the ego vehicle, in form of braking. This unfounded reaction could result in an unexpected situation for other participants and a collision with the ego vehicle.

In contrast, the malfunction “More than intended give way sign detection” is not relevant for safety. In this case the system detects e.g. two signs instead of one. But this does not lead to a collision with the ego vehicle because the reaction to one or two detected signs is the same.

“Less than intended give way sign detection” is also not applicable. As there is only one kind of traffic sign for each for every infrastructural area (only one give-way sign for one intersection), the system cannot detect less than this one.

The malfunction “Wrong give way sign detection” is also not safety relevant because there is only one type of give way sings. These “Wrong detection” malfunctions are only applicable for functions, where the type of the detected object is important e.g. speed limit signs, traffic lights, road lanes, etc.

5.6.4 Risk Assessment of City Pilot

After the determination of the malfunctions, the risk assessment can be implemented. In this part of the HARA all malfunctions are examined for their possible consequences (hazardous events), with regard of different driving situations, and afterwards classified according to the ASIL determination in chapter 2.

The malfunction “No lateral steering support when requested”, from the main function “Turning in an intersection”, will now be analyzed.

First step is to set a safety relevant driving situation, regarding the situation catalogue in section 5.6.1. One possible option could be:

- Driving mode: Turning
- Location: City
- Road conditions: Paved dry road
- Environment: Daytime
- Infrastructure and involved persons: Driver, participant vehicle, persons in participant vehicle

The parameters Driving mode and location are not changeable for this malfunction, as the main function is “Turning in an intersection” and the location is always in the city. The others can be changed and combined according to the situation catalogue. Each combination leads to another ASIL determination.

The next step is to identify the state change and its consequence, due to the malfunction. In this case they are:

- State change: No vehicle lateral control
- Consequence: Leaving of track, front-end collision with oncoming traffic

With this Information, the ASIL determination can be implemented.

The probability of exposure would be E4 in this case, because the driving mode on daytime with paved dry road occurs during almost every drive on average.

The severity would be S3. A front-end collision with an oncoming participant vehicle with a possible speed difference of over 60 km/h can lead to life-threatening injuries.

The controllability is always C3 for City Pilot, because it is a Level 4 feature where the driver is not part of the DDT.

With these parameters, the hazardous event would be assessed as ASIL D. But with the change of just some parts of the driving situation, the ASIL determination could change:

- Road conditions: Iced road
- Environment: Snow

These will result to a lower probability of exposure (E2 instead of E4) because this scenario occurs just a few times a year for the great majority of drivers. The lower probability of exposure will lead to an ASIL B.

For the risk assessment in this thesis, all malfunctions were considered. The driving situations were set in order to reach a rather higher ASIL determination, and thereby achieving a worst-case examination.

5.7 Safety Goals of City Pilot

With the results of the risk assessment, the safety goals of the feature can now be formulated. Each malfunction with its resulting hazardous event shall apply to one safety goal. The ASIL for each safety goal is transferred from the hazardous event with the highest determination. For City Pilot, 10 safety goals were set, which can be seen in table 34.

Table 34 Safety Goals of City Pilot

Safety Goal	**Safe State**	**ASIL**
[SG01] The City Pilot System Shall provide requested steering support	Fail operational 10 sec. Initiation of request dispatcher to intervene	ASIL D
[SG02] The City Pilot System Shall avoid unintended steering support	Fail operational 10 sec. Initiation of request dispatcher to intervene	ASIL D
[SG03] The City Pilot System Shall provide requested acceleration	Fail operational 10 sec. Initiation of request dispatcher to intervene	ASIL D
[SG04] The City Pilot System Shall avoid unintended acceleration	Fail operational 10 sec. Initiation of request dispatcher to intervene	ASIL D
[SG05] The City Pilot System Shall provide requested deceleration	Fail operational 10 sec. Initiation of request dispatcher to intervene	ASIL D

[SG06] The City Pilot System Shall avoid unintended deceleration	Fail operational 10 sec. Initiation of request dispatcher to intervene	ASIL D
[SG07] The City Pilot System Shall provide object and event detection and respond to it	Fail operational 10 sec. Initiation of request dispatcher to intervene	ASIL D
[SG08] The City Pilot System Shall avoid unintended object and event detection and respond	Fail operational 10 sec. Initiation of request dispatcher to intervene	ASIL C
[SG09] The City Pilot System Shall be overrule at any time	Fail operational 10 sec. Initiation of request dispatcher to intervene	ASIL D
[SG10] The City Pilot System Shall avoid unintended overruling request	Fail operational 10 sec. Initiation of request dispatcher to intervene	ASIL D

The determination of the safety goals may vary depending on the view and interpretation of the editor. However, some safety goals emerge relatively clearly from the malfunctions. Examples are:

- Safety Goal 01 [SG01] "The City Pilot system shall provide requested steering support" for Malfunction 001 [MF001] "No lateral steering support when requested"
- Safety Goal 05 [SG05] "The City Pilot System shall provide requested deceleration" for Malfunction 007 [MF007] "No longitudinal deceleration when requested"

Other safety goals are formulated in a more general way, in order to be applicable to a larger number of malfunctions. Examples are:

- Safety Goal 07 [SG07] “The City Pilot system shall provide object and event detection and respond to it” for Malfunction 016 [MF016] “No participant vehicle detection”
- Safety Goal 07 [SG07] “The City Pilot system shall provide object and event detection and respond to it” for Malfunction 029 [MF029] “No red traffic light detection”

Here two rather different malfunctions have the same safety goal, which is allowed in the ISO 26262. A benefit of this more general formulation is a much reduced number of safety goals.

There could be of course other possible formulations for these malfunctions, like “The City Pilot system shall provide participant vehicle detection and respond to it” or “The City Pilot system shall provide red traffic light detection and respond to it. Due to the large number of different malfunctions in the feature, this would lead to an almost similar number of safety goals, which is not intended to be the case.

The safe state is an “operating mode of an item without an unreasonable level of risk”, like the intended operating mode or the switched off mode. The formulation, how a safe state could be reached, is part of the functional safety concept in the ISO 26262. A safe state for City Pilot (deactivation/switched off mode) can be achieved with an intervention of the dispatcher. If the dispatcher does not react to the request within a specified Fault Tolerant Time Interval (FTTI), the system will put the vehicle into a safe position. For City Pilot, the FTTI was set to 10 seconds for all safety goals [28][29][30].

6 Conclusion and Future Development

6.1 Concluding summary

The concept of autonomous cars and self-driving vehicles introduce several new opportunities including enough time to do some extra work or relax or even sleep inside a car. Apart from comfort another major aspect of autonomous cars is improved safety and much lower error probability, machines are not prone to commit errors like humans do, therefore it is expected that autonomous cars will significantly reduce the accidents and causality ratio in near future.

Considering these emerging trends, this research work is carried out to propose systematic development approach for level 4 autonomous vehicles. Since Society of Automotive Engineers have classified autonomous driving in to 6 levels ranging from 0 to 5 where 0 shows no automation and 5 represents completely driverless robotic cars. The vehicles belong to level 5 will not appear too soon owing to technology limitations but the level 4 autonomous vehicles are expected to appear in market in the next 5 to 6 years. Therefore, it is the right time to investigate and to develop systematic approach for such cars.

This thesis has presented in detail about V model and adopted its left side for feature idea and conception all the way to item level definition and modelling for various potential scenarios that come up for level 4 autonomous cars. Since level 4 represents high automation, where system takes responsibility of all aspects of dynamic driving routines, thus it is not possible to cover them all, even though the scope of this work is cover more than 500 city driving situations for the City Pilot (CP) feature of level 4 autonomous cars. This thesis has shown how the development of a high automated driving feature, according to SAE Level 4, could be approached with methods of system engineering.

One result of this thesis is the assumption of the City Pilot feature definition approach in idea phase of V Model, which is capable to handle different driving situations in the city. This definition contains:

- A high-level feature description, which shows general requirements for the City Pilot and it gives a first overview of what City Pilot is and what it should be able to do.
- The definition of driving scenarios, City Pilot can perform. They are based on city driving route and cover frequently occurring situations when driving in a city.
- Object, event detection and response analysis for City Pilot feature according to driving situations.
- The definition of an operational design domain, to which the usage of City Pilot is bounded.

Second result of this thesis is the assumption of the City Pilot item definition approach in concept phase of V Model. This definition contains:

- The definition of use case diagrams for City Pilot with SysML. Out of driving scenarios formed the main use cases of the feature. As a result, the high-level functionality of the whole feature and the main functions became visible.
- A description of the functional principle behind these use cases with SysML activity diagrams. Each of the main use cases was analyzed.

Another result of the thesis is the assumption of safety goals for the feature City Pilot. This was achieved with executing a Hazard Analysis and Risk Assessment according to the ISO 26262. As a result of this HARA, every hazardous event was given an ASIL safety integrity level. The safety goals were determined for these hazardous events and later combined in case of a similarity, which lead to 10 safety goals for City Pilot.

In order to represent the whole system's functions and their interaction, a functional architecture of the feature functions of City Pilot were created using the block definition diagram in SysML. This enables an insight on how the functions operate together and what their input and output objects are. These functional architectures serve as a basis for further developing processes on a technical level.

6.2 Future Development for SAE Level 4 City Pilot

Since it has been concluded that a massive research and development potential is available as far as level 4 autonomous vehicles are concerned here are few of the possible potential extensions of this research work.

The thesis work can be extended to include all driving systems for level 4 autonomous cars that include driving in traffic jam, highway automated driving and rural driving. This will allow further exploration of scenarios that could come up for autonomous vehicles.

Further future potential development on this master thesis can be in two ways. The concepts can be expanded and designed for a larger ODD. Furthermore, the Top-Down approach can be continued and detailed further.

For the continuation of the Top-Down approach, the V-Model explained in chapter 2 must be taken in consideration. Generally said, for further progression of the Top-Down approach, the architecture will be refined more and more until the system is ready for the implementation and testing.

References:

[1] Autonomous Driving – Five Steps to the Self-Driving Car. [Online, last visited 16-06-2019]. url: https://Www.Bmw.Com/En/Automotive-Life/Autonomous-Driving.Html

[2] Society Of Automotive Engineers (SAE), "J3016 - Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems," Society of Automotive Engineers (SAE), 2016.

[3] Top 3 Challenges to Produce Level 5 Autonomous Vehicles. [Online, last visited 16-06-2019]. url: https://Www.Ansys.Com/Blog/Challenges-Level-5-Autonomous-Vehicles

[4] European Road Safety Observatory. Annual Accident Report 2018. [Online, last visited 17-06-2019]. url:https://Ec.Europa.Eu/Transport/Road_Safety/Sites/Roadsafety/Files/Pdf/Statistics/Dacota/Asr2018.Pdf

[5] Ertrac Working Group, "Connectivity and Automated Driving Roadmap" Version 8, 08 March 2019.

[6] Ertrac - All Documents & Publications. [Online, last visited 21-06-2019]. url: https://Www.Ertrac.Org/Index.Php?Page=Ertrac-Publications

[7] Donna E. Gilmore, ESV Technical Coordinator, DOT/NHTSA, 23rd International Technical Conference on the Enhanced Safety of Vehicles, Seoul, Korea, May 2013.

[8] Staplin, L., Mastromatto, T., Lococo, K. H., Kenneth W. Gish, K. W., And Brooks, J. O., The Effects of Medical Conditions on Driving Performance (Report No. Dot Hs 812 623), Washington, Dc: National Highway Traffic Safety Administration, September 2018.

[9] Reese, H. (N.D.). Updated: Autonomous Driving Levels 0 To 5: Understanding the Differences. [Online, last visited 21-06-2019]. url: https:// Www .Techrepublic .Com /Article / Autonomous-Driving -Levels-0-To-5- Understanding -The- Differences

[10] Bloomberg - Are you a Robot. [Online, last visited 20-06-2019]. url: https://www.bloomberg.com/news/features/2018-05-07/who-s-winning-the-self-driving-car-race

[11] ISO, 26262 – Road Vehicles – Functional Safety, 2016.

[12] Dov Dori. Model-Based Systems Engineering with Opm and Sysml. Springer, 2016.

[13] "01_Introduction_14082018", Internal Company Document Of 1acue.

[14] "What Is Systems Engineering", Webpage Of The INCOSE Organization. [Online, last visited 22-06-2019]. url: https://Www.Incose.Org/Systems-Engineering

[15] Sumner Sara, "The Three Systems Engineering Approaches: Top-Down, Middle-Out and BottomUp",WebpageofVitech. [Online, last visited 23-06-2019]. url: http://Community.Vitechcorp.Com/Index.Php/The-Three-Systems-Engineering-Approaches-Top-Down-Middle-Out-And-Bottom-Up.Aspx

[16] O.Alt.Modell-Basierte System Entwicklung Mit Sysml.Carl Hanser Verlag Gmbh Co. Kg, 2012.

[17] Omg Systems Modeling Language (Omg sysml) Version1.3, June 2012.

[18] Sysml Forum. [Online, last visited 28-06-2019]. url: https://Sysmlforum.Com/Sysml-Overview/

[19] Fabrice Kordon. Embedded Systems: Analysis And Modeling With Sysml, Uml And Aadl. John Wiley Sons Incorporated, 2013.

[20] Andreas Miosga, Bachelor Thesis "High Automation Rural Driving", Mechanical Engineering Department Of Augsburg University Of Applied Sciences, 13 March 2019.

[21] The Difference between "Document-Based" And "Model-Based" – Ostrogothia. [Online, last visited 06-07-2019]. url: http://Www.Ostrogothia.Com/Blog/?P=1858

[22] Rahul Kumar Richa. Autonomous vehicle market expected to reach 54.23$ billion, globally, by 2026. [Online, last visited 10-07-2019]. url: https://www.alliedmarketresearch.com/ autonomous-vehicle-market, 2018

[23] Anju Manjooran, Anphy Varghese, Annmariya Seby and Krishnadas J,"Traffic Sign Board Detection and Voice Alert System Along with Speed Control", India, 30 March 2018.

[24] L. Estevez and N. Kehtarnavaz, "A Real-Time Histographic Approach to Road Sign Recognition," Image Analysis and Interpretation, 1996, Proceedings of the IEEE Southwest Symposium on, pp. 95–100, Apr 1996.

[25] R. Timofte, K. Zimmermann, and L. Van Gool, “Multi-view Traffic Sign Detection, Recognition, and 3d Localisation,” Snowbird, Utah, 2009, pp. 69–76.

[26] M. A. Hannan,S.B.Wali, T. J. Pin, A. Hussain, and S.A.Samad, “Traffic Sign Recognition Based on Neural Network for Advance Driver Assistance System,” Przegląd Elektrotechniczny,vol.1,no. 12, pp. 169–172, 2014.

[27] Hervé Jégou, Matthijs Douze, Cordelia Schmid, and Patrick Pérez. Aggregating Local Descriptors into a Compact Image Representation. In Computer Vision and Pattern Recognition (CVPR), 2010 IEEE Conference on, pages 3304–3311. IEEE, 2010.

[28] L. Chen,Q.Li, M. Li,L.Zhang,and Q. Mao, “Designofamulti- sensor cooperation travel 75 environment perception system for autonomous vehicle,” Sensors,vol.12, no.9,pp. 12386–12404, 2012.

[29] G. Loy, “Fast Shape-Based Road Sign Detection for a Driver Assistance Aystem,” in IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS, 2004, pp. 70–75).

[30] Umar.Z.A.Hamid, “A Review on Threat Assessment, Path Planning and Path Tracking Strategies for Collision Avoidance Systems of Autonomous Vehicles, International Journal of Vehicle Autonomous Systems, 2018.

From Technische Universität Chemnitz

[31] M. Umer Shafique, Prof. Dr. W. Hardt and Andreas Schuhmann, “Multi Sensor Setup for Highly Automated Driving Vehicles “, Dept. of Computer Science, Technical University Chemnitz,15 May 2019.

[32] Wolfram Hardt and Stefan Ihmor and Johannes Lessmann “Analyzing non-functional requirements of embedded systems”, IN Proceedings of the IASTED International Conference Modelling, Identification and Control (MIC 2002), ISBN: 0-88986-319-9, page 60 - 65, February 2002

[33] Mike Heuchling and Wolfgang Ecker and Michael Mrva, “Automating System Construction by Domain Based Approaches”, IN Proc. EUROMICRO97, IEEE Computer Society, ISBN: 08186-8129-2, page 336 - 342 September 1997.

[34] Dieter Monjau, “A new model-based approach to the CoDesign of heterogeneous systems”, IN Proceedings of the EUROCAST'93, Springer Verlag, February 1993.

Appendix A

A.1 Tactical and Operational Maneuvers of Feature (CP)

Table A.1 Tactical and Operational Maneuvers of Feature (CP)

Behavioral Competencies	Description according to NHTSA	Relevant for City Pilot
Navigating Parking Lots & Locating Open Spaces	ADS comes to a complete stop within a vacant parking spot; may be further qualified by parallel or perpendicular orientations, lot type (closed/open), initiation conditions, etc.	No
Maintaining Speed	ADS maintains a safe speed set through longitudinal control with acceptable following distances.	Yes
Performing Car Following	ADS identifies and follows a target vehicle at acceptable following distance through longitudinal control including Stop&Go and Emergency Braking.	Yes
Performing Lane Centering	ADS stays within a lane through lateral control while free driving or car following.	Yes
Performing Lane Switching/Overtaking	ADS crosses lanes or overtakes an upcoming vehicle based on a projected path or hazard.	Yes
Enhancing Conspicuity	ADS controls vehicle blinkers, headlights, horn, or other methods used to communicate with other drivers.	Yes

Performing Low-Speed Merge	ADS merges into a lane below about 45 mph, for example from an exit ramp, by identifying a vacant lane position and matching speed.	No
Performing High-Speed Merge	ADS merges into a lane above about 45 mph, for example from an exit ramp, by identifying a vacant lane position and matching speed.	No
Adapting vehicle control according to speed limit changes	ADS obeys to speed limit changes through longitudinal control.	Yes
Navigating Entrance/Exit Ramps	ADS drives on on/off-ramps, which are typically oneway, steeply curved, and banked road segments.	No
Adapting vehicle control according to stopped vehicles	ADS avoids collision with stopped vehicles through longitudinal control.	Yes
Navigating Roundabouts	ADS determines right-of-way, enters, navigates, and exits a roundabout, and communicates with other road users as necessary.	Yes
Navigating Intersections	ADS determines right-of-way, enters, navigates, and exits intersections, including signalized, stop signs, 4/3/2-ways, and communicates with other road users as necessary; may include left or right turns across oncoming traffic.	Yes
Navigating Crosswalks	ADS determines right-of-way, enters, navigates, and exits pedestrian	Yes

	crosswalks, and communicates with other road users as necessary.	
Navigating Work Zones	ADS determines right-of-way and traffic patterns, enters, navigates and exits work zone, and communicates with other road users as necessary.	Yes
Performing Turns	ADS makes a heading adjustment that involves alternating between forward and reverse movement and adjusting steering to reposition the vehicle within a tight space. Additional ADS determines right-of-way, initiates, and completes a U-turn, and communicates with other road users as necessary.	No
Adapting vehicle control according to access restrictions	ADS obeys to directional restrictions (for example one-way roads and actively managed lanes) through longitudinal and lateral control.	Yes
Transitioning to Minimal Risk Condition	MRC is defined in SAE J3016 as a condition to which a user or an ADS may bring a vehicle after performing the DDT fallback in order to reduce the risk of a crash when a given trip cannot or should not be completed.	Yes
Adapting vehicle control according to Intended Lane Changes/ Cut-Outs / Cut-Ins	ADS adapts control according to followed participant vehicle in frontal zone that is changing lane or suddenly cuts out into another adjacent lane. ADS adapts control according to participant vehicles in right and/or left side	Yes

	zone cutting into ego lane to the extent that a collision would occur if ego vehicle control is not adaptated according to the situation.	
Performing Static Objects Avoidance	ADS identifies and responds to on-road hazards, such as static debris, work zone objects etc.	Yes
Performing Dynamic Objects Avoidance	ADS identifies and responds to on-road hazards, such as pedestrians, dynamic debris, animals, etc.	Yes
Adapting vehicle control according to emergency vehicles	ADS obeys to emergency vehicles through longitudinal and lateral control.	Yes
Adapting vehicle control according to encroaching vehicles	ADS adapts vehicle control according to participant vehicles in rear, left and/or right side zone encroaching into ego lane to the extent that a collision would occur if the ego vehicle control is not adapted according to the situation.	Yes
Adapting vehicle control according to traffic signs & lights	ADS obeys to traffic signs and lights through longitudinal and lateral control.	Yes

A.2 Road Track Driving Scenarios

Table A.2 Road Track Driving Scenarios

Nr.	Road track
1	Ego vehicle is approaching a city entrance with continuous road lane markings
2	Ego vehicle is approaching a city entrance with discontinuous road lane markings
3	Ego vehicle is driving on a city road lane with temporary discontinuous road lane markings
4	Ego vehicle is driving on a city road lane with temporary continuous road lane markings
5	Ego vehicle is driving on a straight city lane with continuous road lane markings
6	Ego vehicle is driving on a straight city lane with discontinuous road lane markings
7	Ego vehicle is driving on a curved city lane turning left with continuous road lane markings
8	Ego vehicle is driving on a curved city lane turning left with discontinuous road lane markings
9	Ego vehicle is driving on a curved city lane turning right with continuous road lane markings
10	Ego vehicle is driving on a curved city lane turning right with discontinuous road lane markings

11	Ego vehicle is approaching a city double curve, first to the left with continuous road lane markings
12	Ego vehicle is approaching a city double curve, first to the left with discontinuous road lane markings
13	Ego vehicle is driving in a city double curve, first to the right with continuous road lane markings
14	Ego vehicle is driving in a city double curve, first to the right with discontinuous road lane markings
15	Ego vehicle is approaching a city roundabout with continuous/discontinuous road lane markings
16	Ego vehicle is driving in a city roundabout with continuous/discontinuous road lane markings
17	Ego vehicle is driving out of a city roundabout with continuous/discontinuous road lane markings
18	Ego vehicle is approaching a city lane merge with continuous road lane markings
19	Ego vehicle is approaching a city lane merge with discontinuous road lane markings
20	Ego vehicle is approaching a city lane split with continuous road lane markings
21	Ego vehicle is approaching a city lane split with discontinuous road lane markings
22	Ego vehicle is approaching a city tunnel entrance with continuous road lane markings

23	Ego vehicle is approaching a city tunnel entrance with discontinuous road lane marking
24	Ego vehicle is driving through a city tunnel with continuous road lane markings
25	Ego vehicle is driving through a city tunnel with discontinuous road lane markings
26	Ego vehicle is approaching a city tunnel exit with continuous road lane markings
27	Ego vehicle is approaching a city tunnel exit with discontinuous road lane markings
28	Ego vehicle is approaching a city tram track with continuous road lane markings
29	Ego vehicle is approaching a city tram track with discontinuous road lane markings
30	Ego vehicle is driving on a city road lane with side a tram track with continuous road lane markings
31	Ego vehicle is driving on a city road lane with side a tram track with discontinuous road lane markings
32	Ego vehicle is approaching a temporary block road with continuous road lane markings
33	Ego vehicle is approaching a temporary block road with discontinuous road lane markings
34	Ego vehicle is approaching a road with several lane choices with discontinuous road lane markings and after that, the same, but with continuous lane markings

35	Ego vehicle is approaching an intersection with other roads with discontinuous lane markings and after that, the same, but with continuous lane markings
36	Ego vehicle is driving on a road an intersection with other roads with discontinuous road lane markings and after that, the same, but with continuous lane markings
37	Ego vehicle is approaching on a road an intersection with tram track with discontinuous road lane markings and after that, the same, but with continuous lane markings
38	Ego vehicle is driving on a road an intersection with tram track with discontinuous road lane markings and after that, the same, but with continuous lane markings
39	Ego vehicle is approaching on a road an intersection with tram track also with other roads with discontinuous road lane markings and after that, the same, but with continuous lane markings
40	Ego vehicle is driving on a road an intersection with tram track also with other roads with discontinuous road lane markings and after that, the same, but with continuous lane markings
41	Ego vehicle is approaching a city exit with continuous lane markings
42	Ego vehicle is approaching a city exit with discontinuous lane markings

A.3 Operational Driving Scenarios

Table A.3 Operational Driving Scenarios

Nr.	**Main Road Track Scenario**		**Operational Driving Scenarios**

1	Ego vehicle is driving on a city road		Ego vehicle is driving on a city road while adapting vehicle motion according to detected **non-emergency participant vehicle i**n **frontal zone**
2			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **non-emergency participant vehicle** in **left side zone**
3			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **non-emergency participant vehicle** in **right side zone**
4			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **non-emergency participant vehicle** in **rear zone**
5			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **non-emergency participant vehicles in the left and right-side zones**
6			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **non-emergency participant vehicles in the frontal and left side zones**
7			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **non-emergency participant vehicles in the frontal and right-side zones**
8			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **non-emergency participant vehicles in the frontal and rear side zones**

9			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **non-emergency participant vehicles in the rear and left side zones**
10			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **non-emergency participant vehicles in the rear and right-side zones**
11			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **non-emergency participant vehicles in frontal, rear and left side zones**
12			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **non-emergency participant vehicles in frontal, rear and right-side zones**
13			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **non-emergency participant vehicles in frontal, left and right-side zones**
14			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **non-emergency participant vehicles in rear, left and right-side zones**
15			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **non-emergency participant vehicles in frontal, rear, left and right-side zones**

16			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **emergency participant vehicle in frontal zone**
17			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **emergency participant vehicle in the rear zone**
18			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **emergency participant vehicle in the left side zone**
19			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **emergency participant vehicle in the right-side zone**
20			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **pedestrian** in **frontal zone**
21			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **pedestrian** in **left side zone**
22			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **pedestrian** in **right side zone**
23			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **pedal cyclist** in **frontal zone**
24			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **pedal cyclist** in **left side zone**

25			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **pedal cyclist** in **right side zone**
26			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **animal** in **frontal zone**
27			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **animal** in **left side zone**
28			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **animal** in **right side zone**
29			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **dynamic object** in **frontal zone**
30			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **dynamic object** in **left side zone**
31			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **dynamic object** in **right side zone**
32			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **static debris** in **frontal zone**
33			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **static debris** in **left side zone**

34			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **static debris** in **right side zone**
35			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **work zone object** in **frontal zone**
36			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **work zone object** in **left side zone**
37			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **work zone object** in **right side zone**
			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **safety official guidance signals**
38			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **traffic sign**
39			Ego vehicle is driving on a city road while adapting vehicle motion according to detected **traffic light**
40			Ego vehicle is driving **outside operational design domain**

A.4 Functional Driving Scenarios

Case Two: Ego vehicle adapting control according to traffic signs.

Table A.4 Functional Driving Scenarios

1	Ego vehicle is driving on a city road while adapting vehicle motion according to detected traffic signs		Ego vehicle is **accelerating** according to detected **speed limit traffic sign**
2			Ego vehicle is **decelerating** according to detected **speed limit traffic sign**
3			Ego vehicle is **aborting lane change** according to detected **no passing traffic sign**
4			Ego vehicle is **aborting passing** according to detected **no passing traffic sign**
5			Ego vehicle is **decelerating** according to detected **no passing traffic sign**
6			Ego vehicle is **changing lane** (when changing lane needed) according to detected **end of no passing traffic sign**
7			Ego vehicle is **accelerating** according to detected **wet weather/daytime speed limit traffic sign**
8			Ego vehicle is **decelerating** according to detected **wet weather/daytime speed limit traffic sign**
9			Ego vehicle is **accelerating** according to detected **end of speed limit traffic sign**

10			Ego vehicle is **steering** according to detected **curve turning left traffic sign**
11			Ego vehicle is **decelerating** according to detected **curve turning left traffic sign**
12			Ego vehicle is **steering** according to detected **curve turning right traffic sign**
13			Ego vehicle is **decelerating** according to detected **curve turning right traffic sign**
14			Ego vehicle is **steering** according to detected **double curve, first to the left traffic sign**
15			Ego vehicle is **decelerating** according to detected **double curve, first to the left traffic sign**
16			Ego vehicle is **steering** according to detected **double curve, first to the right traffic sign**
17			Ego vehicle is **decelerating** according to detected **double curve, first to the right traffic sign**
18			Ego vehicle is **steering** according to detected **city entrance traffic sign**
19			Ego vehicle is **decelerating** according to detected **city entrance traffic sign**
20			Ego vehicle is **steering** according to detected **city exit traffic sign**

21			Ego vehicle is **accelerating** according to detected **city exit traffic sign**
22			Ego vehicle is steering according to detected **city lane merge traffic sign**
23			Ego vehicle is **steering** according to detected **city lane split traffic sign**
24			Ego vehicle is **choosing new lane to follow** according to detected **city lane split traffic sign**
25			Ego vehicle is **calibrating headlights** according to detected **city tunnel ahead traffic sign**
26			Ego vehicle is **calibrating headlights** according to detected **city tunnel exit traffic sign**
27			Ego vehicle is **decelerating** according to detected **end of city traffic sign**
28			Ego vehicle is **transitioning to minimal risk condition** (fallback ready user or ADS) according to detected **end of city traffic sign**
29			Ego vehicle is **decelerating** according to detected **construction zone traffic sign**
30			Ego vehicle is **following temporary lanes** according to detected **construction zone traffic sign**

31			Ego vehicle is **decelerating** according to detected **temporary lane closure/ending ego lane traffic sign**
32			Ego vehicle is **stopping** according to detected **temporary lane closure/ending ego lane traffic sign**
33			Ego vehicle is **changing lane** according to detected **temporary lane closure/ending ego lane traffic sign**
34			Ego vehicle is **yielding** according to detected **yield traffic sign**
35			Ego vehicle is **stopping** according to detected **yield traffic sign**
36			Ego vehicle is **decelerating** according to detected **yield traffic sign**
37			Ego vehicle is **stopping** according to detected **stop traffic sign**
38			Ego vehicle is **decelerating** according to detected **stop traffic sign**
39			Ego vehicle is **shifting within the lane** according to detected **road narrows traffic sign**
40			Ego vehicle is **decelerating** according to detected **bumpy road traffic sign**
41			Ego vehicle is **decelerating** according to detected **oncoming traffic priority sign**

42			Ego vehicle is **decelerating** according to detected **pedestrians crossing traffic sign**
43			Ego vehicle is **stopping** according to detected **pedestrians crossing traffic sign**
44			Ego vehicle is **decelerating** according to detected **cyclists crossing traffic sign**
45			Ego vehicle is **stopping** according to detected **cyclists crossing traffic sign**
46			Ego vehicle is steering according to detected **mandatory turn left or ahead** traffic sign
47			Ego vehicle is steering according to detected **mandatory turn right or ahead** traffic sign
48			Ego vehicle is **steering** according to detected **mandatory turn left traffic sign**
49			Ego vehicle is **steering** according to detected **mandatory turn right traffic sign**
50			Ego vehicle is **steering** according to detected **mandatory straight traffic sign**
51			Ego vehicle is decelerating according to detected **roundabout** traffic sign
52			Ego vehicle is accelerating according to detected **roundabout** traffic sign
53			Ego vehicle is **stopping** according to detected **roundabout** traffic sign

54			Ego vehicle is **steering** according to detected **roundabout** traffic sign
55			Ego vehicle is **decelerating** according to detected school **zone** traffic sign

Appendix B

B.1 Use Case Diagrams of City Pilot L4

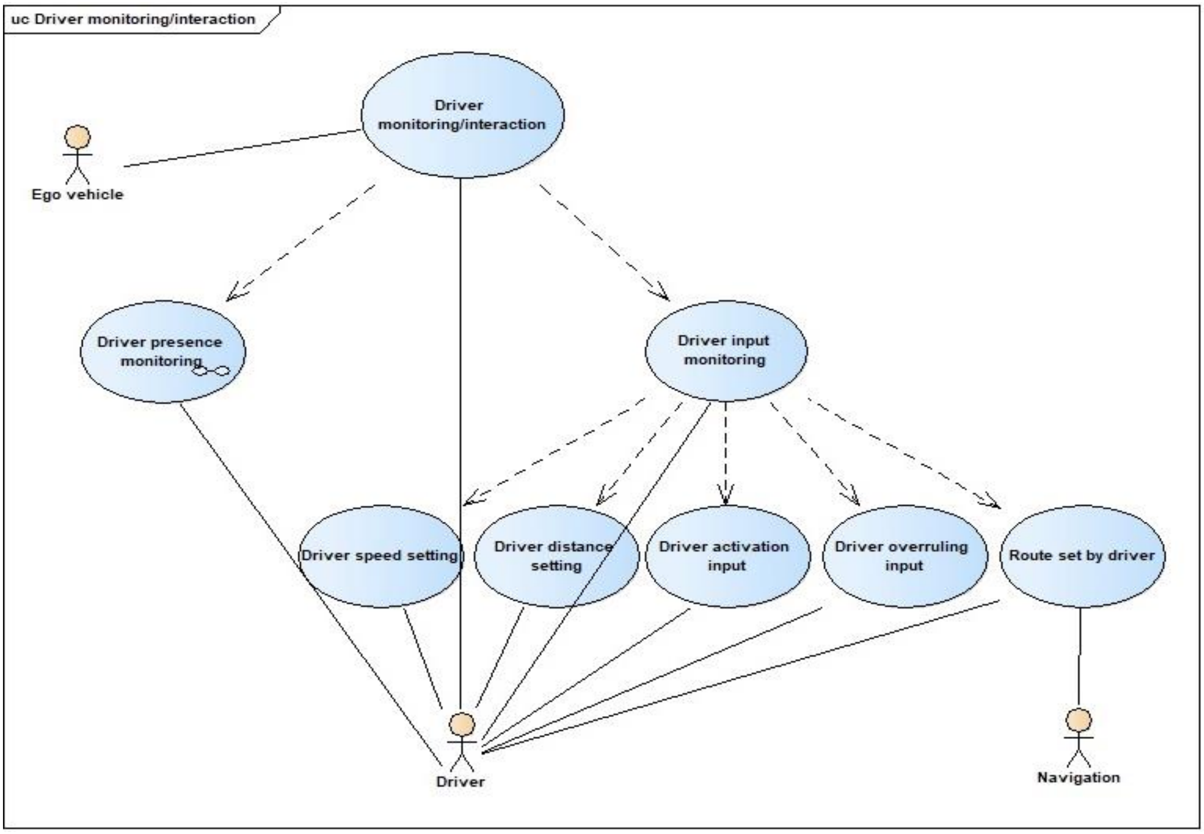

Figure B1.1 Driver Monitoring/Interaction Use Case Diagram

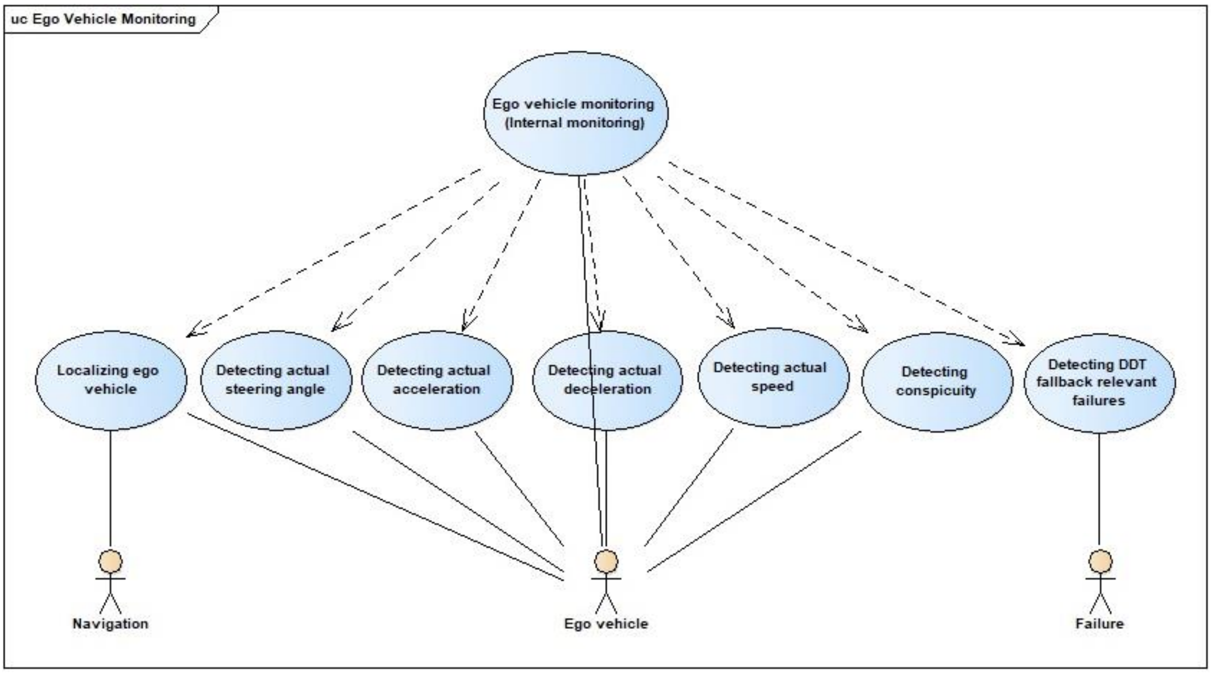

Figure B1.2 Ego Vehicle Monitoring Use Case Diagram

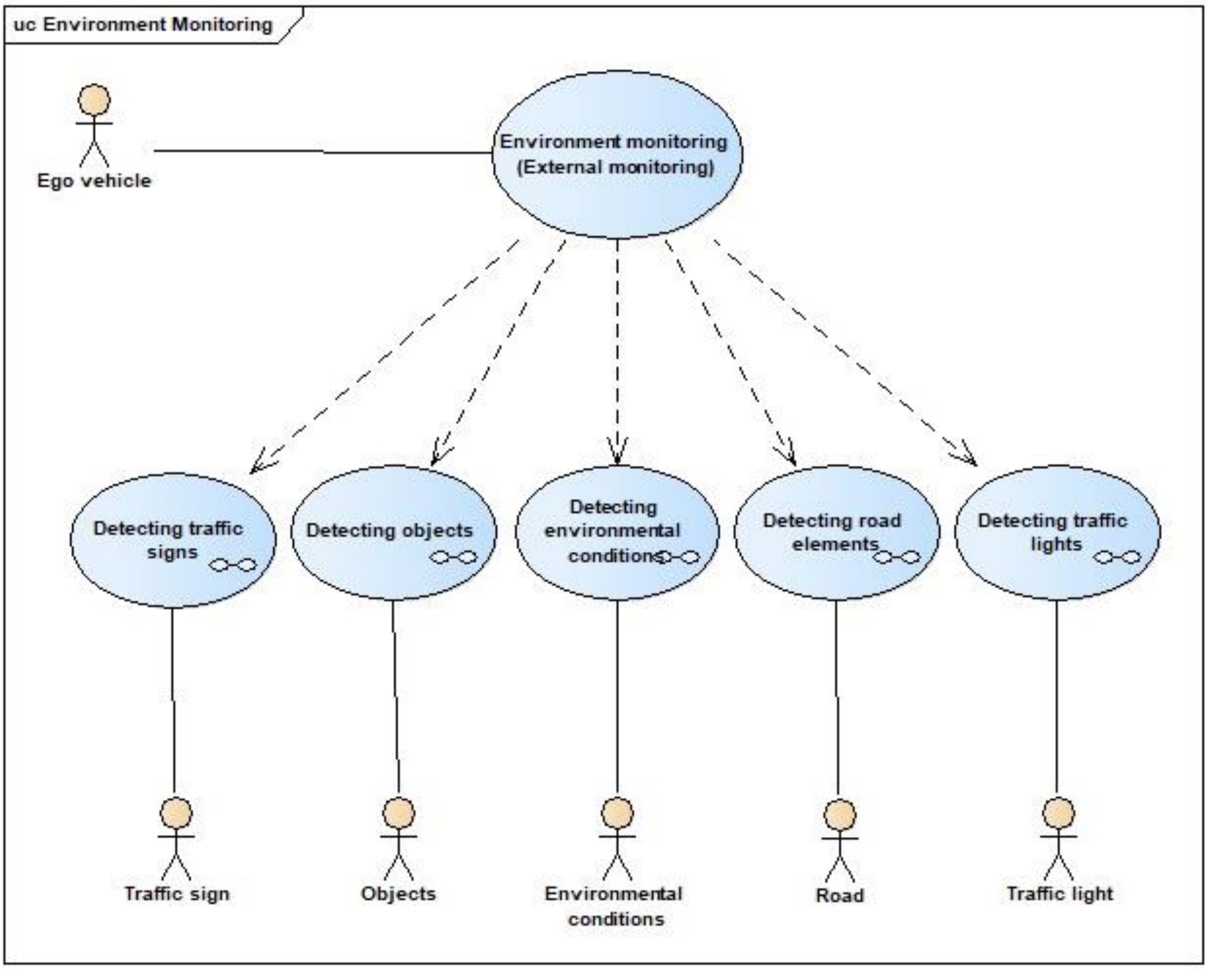

Figure B1.3 Environmental Monitoring Use Case Diagram

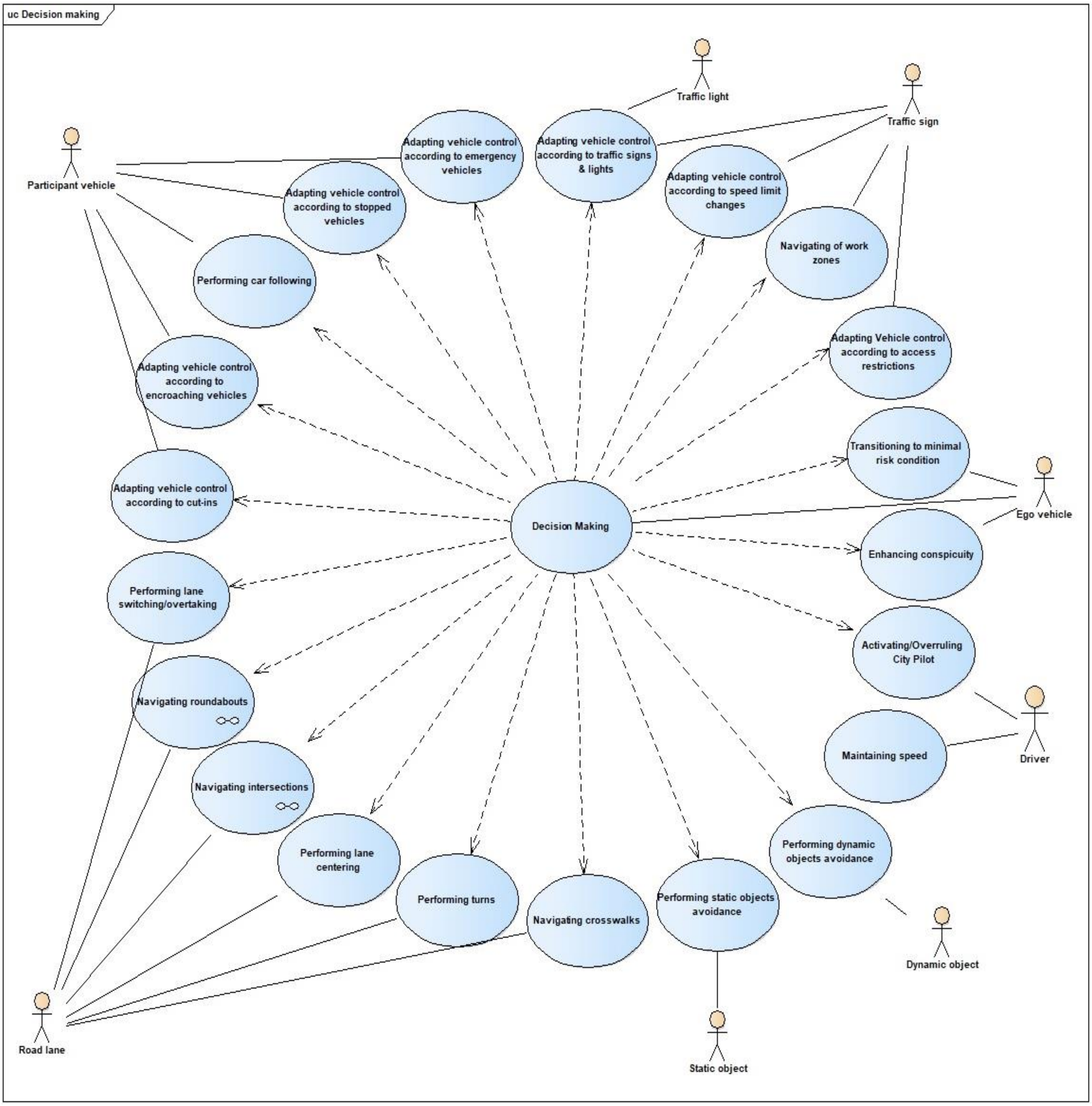

Figure B1.4 Decision Making Use Case Diagram

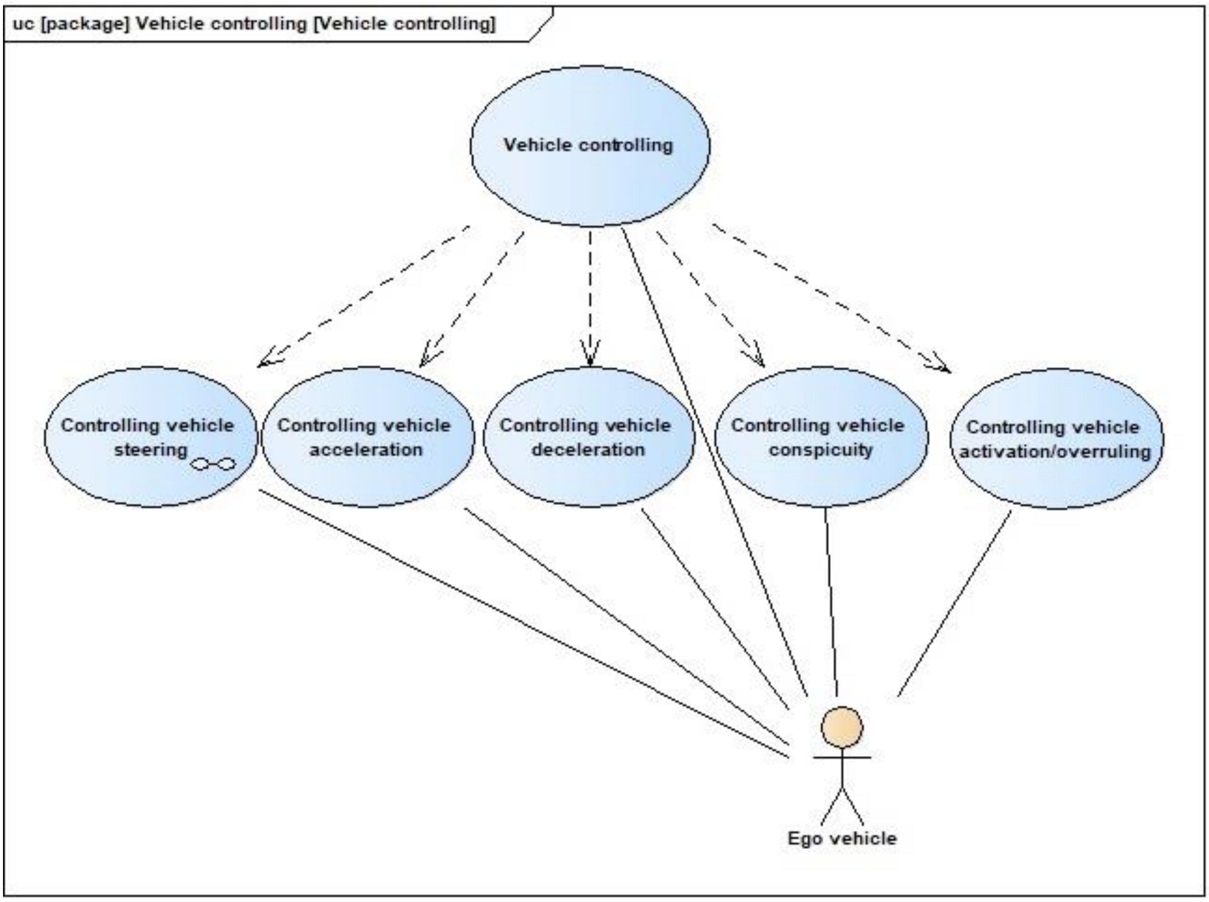

Figure B1.5 Vehicle Controlling Use Case Diagram

B.2 Activity Diagrams of City Pilot L4

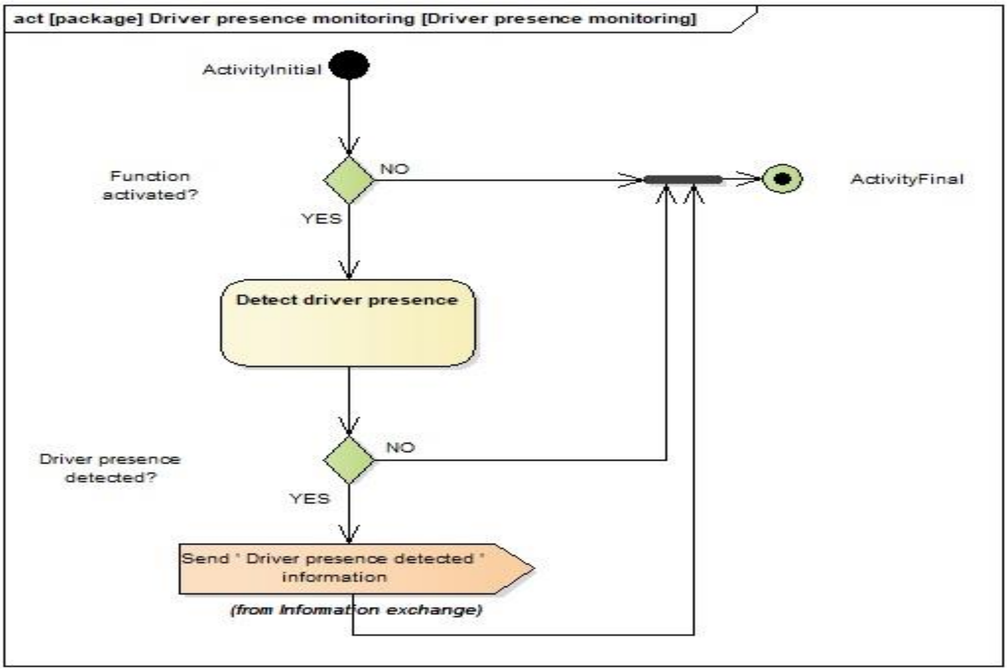

Figure B2.1 Driver Presence Activity Diagram

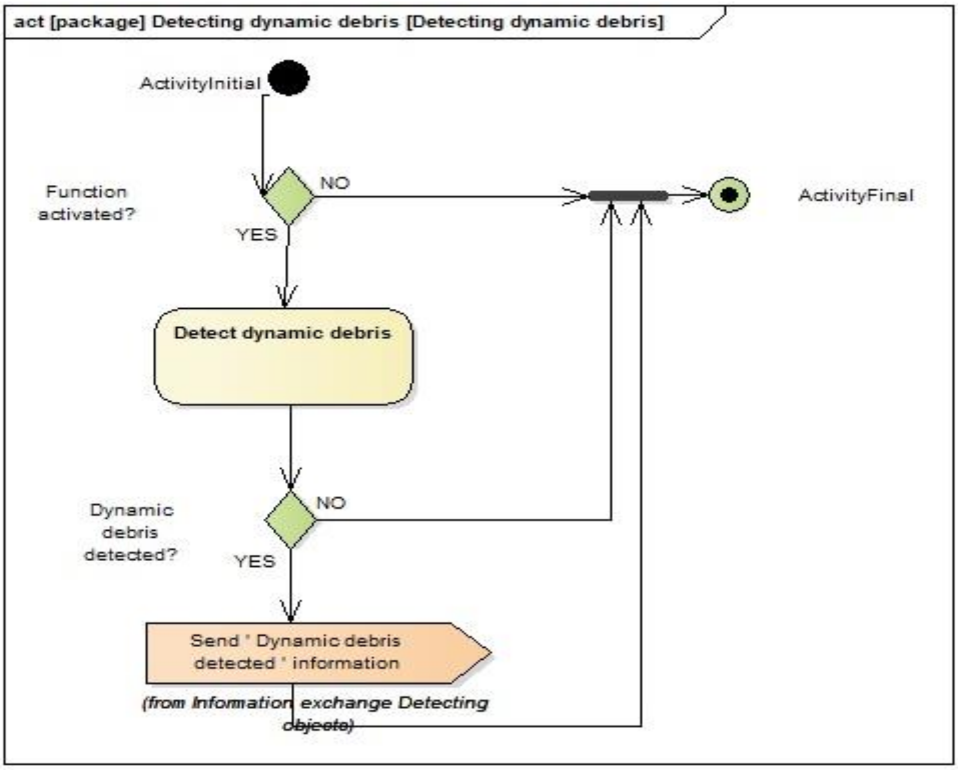

Figure B2.2 Example of External Monitoring (Dynamic Debris) Activity Diagram

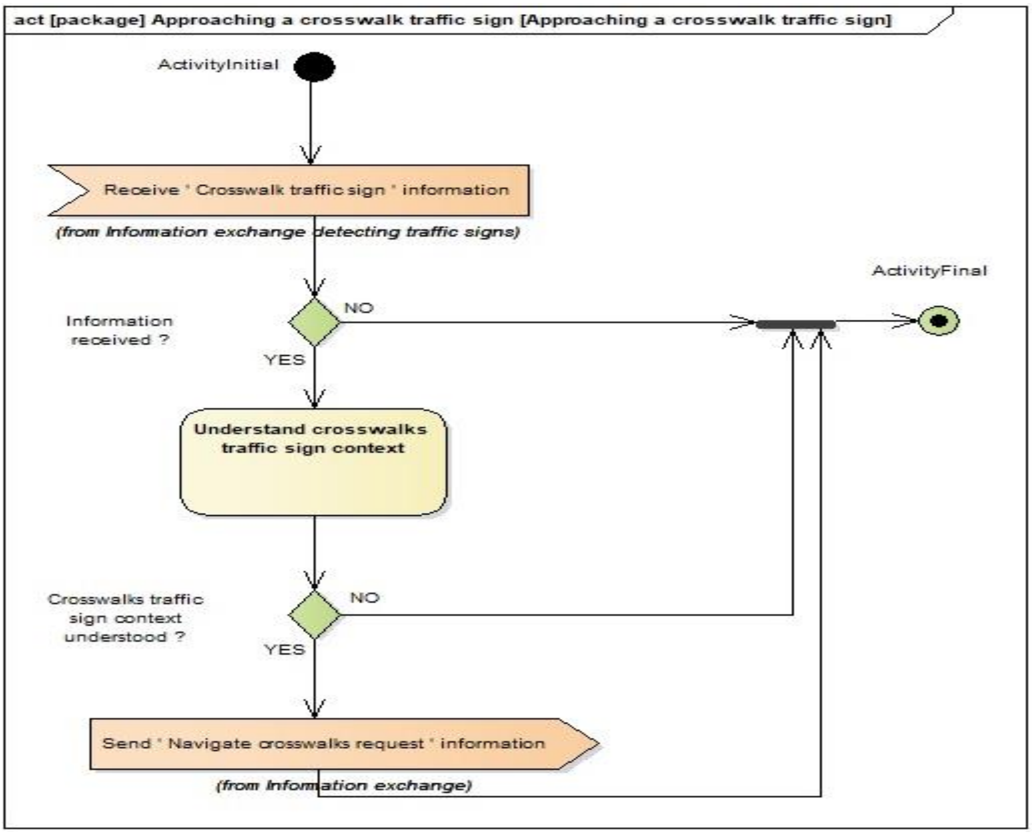

Figure B2.3 Example of External Monitoring (Crosswalk Traffic Sign) Diagram

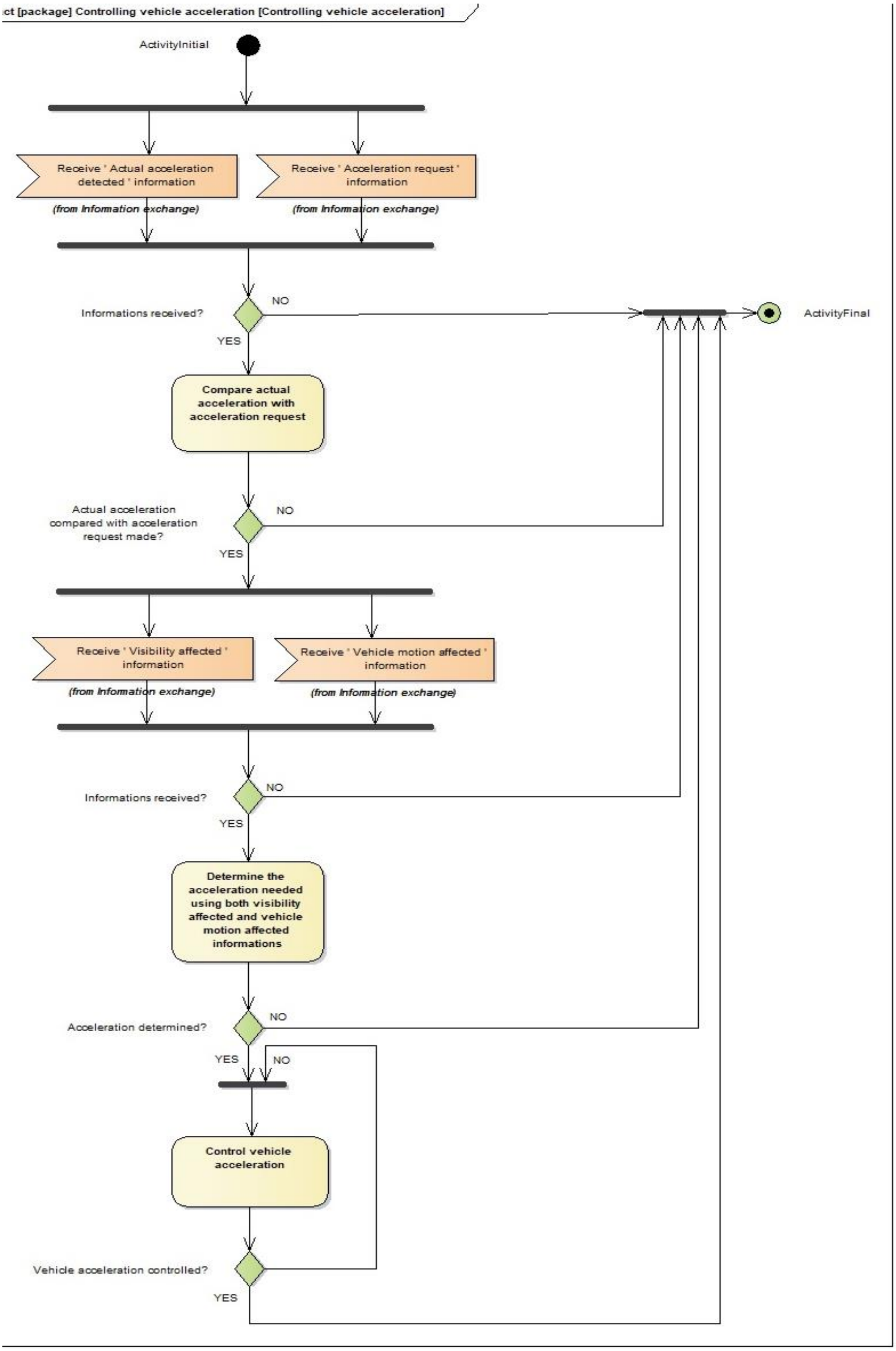

Figure B2.4 Vehicle Controlling (Acceleration) Activity Diagram

B.3 Feature Functional Architecture

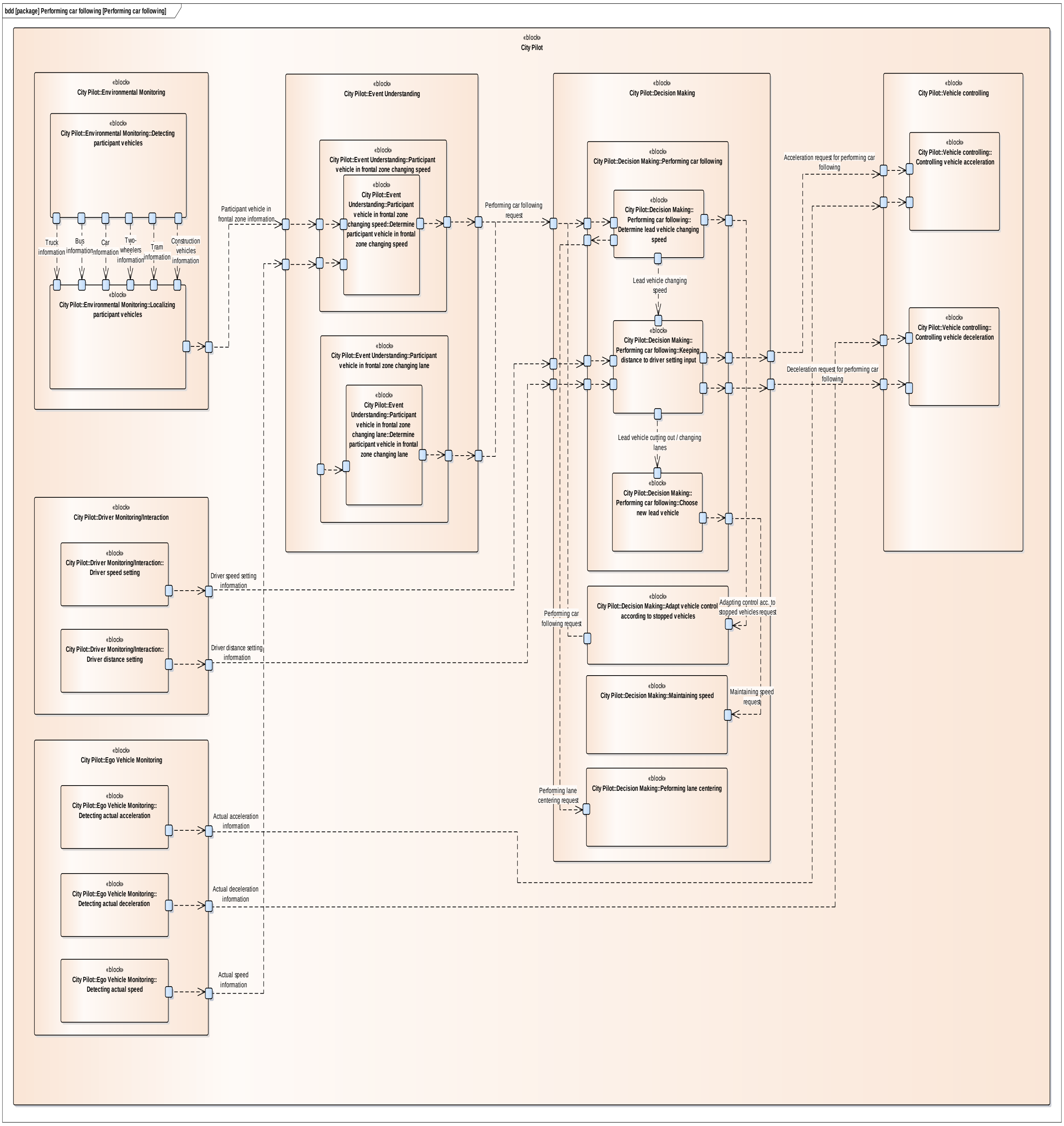

Figure B3.1 Performing Car Following Functional Architecture