
Active Lane **Keep** Centering System

Authors:

Anshuman Singh
Davide Occello
Raymond Wouters
Sharad Bhadgaonkar

Automotive Systems Design
Stan Ackermans Institute
Eindhoven University of Technology

January 13, 2017

Active Lane **Keep** Centering System

MODULE I: TECHNICAL REPORT

Eindhoven University of Technology
Stan Ackermans Institute / Automotive Systems Design


The design that is described in this report has been carried out in accordance with the
TU/e code of scientific conduct

Partners:







Steering Group
Gijs Dubbelman
Rameez Ismail
Peter Heuberger

Abstract

Automotive System Design
Department of Mathematics and Computer Science 

Active Lane Keep Centering System

by

The technical report  presents the functional safety concept of an Active Lane  Keep Centering Systems (ALC). The project mainly focused on studying the Euro NCAP requirements, performing Hazard Analysis and Risk Assessment (HARA) and delivering functional and safety requirements along with system architecture. Having set a time line of one and half months, ALC was initially analyzed to attain a good understanding  the major constituents of such a system and the issues the system deals with. **Benchmark study conducted to understand** the ASIL level requirement for such a system and to know the current state of implementation by different vehicle manufacturers. A project plan was then proposed to complete the project in a given period after clearly defining the scope and limitations of the project. Milestones are prepared such as extracting Euro NCAP and associated functional requirements, deciding the use cases and scenarios, performing HARA Analysis and finding safety goals, evaluating functional safety requirements and functional safety concept in compliant to ISO 26262. Major deliverables of the project are to submit the safety requirement document containing functional safety requirements and technical safety requirements and enhanced architecture to meet the necessary system ASIL level. Additionally, below appendices are mainly provided at the end of report containing requirements/data sheets related to ALC functional safety work.

Appendix A: Euro NCAP requirements

Appendix B: Scenarios

Appendix C: HARA

Appendix D: Functional Safety Requirements

Appendix E: Decomposed Functional Safety Requirements

Appendix F: Benchmarking

Contents



1	Introduction	1
1.1	Project Objective	1
1.2	Project Planning	2
1.3	Benchmark/History of Lane Departure systems	2
2	Functional Requirements and Architecture	3
2.1	Euro NCAP requirements	3
2.2	Basic architecture of system	4
3	Functional Safety Concept	5
3.1	Item Definition	5
3.2	Scenario generation	5
3.3	Hazard Analysis and Risk Assessment (HARA)	6
3.4	Formulation of Safety Goals	8
3.5	Functional Safety Concept	8
4	Functional Architecture with Safety Measures	11
4.1	Decomposition of FSR's for ALC	12
5	Conclusion and Way Forward	13
	Bibliography	15
A	Appendix A: Euro NCAP Requirements	17
B	Scenarios	21
B.1	Scenario 1	21
B.2	Scenario 2	22
B.3	Scenario 3	22
B.4	Scenario 4	22
B.5	Scenario 5	24
B.6	Scenario 6	24
B.7	Scenario 7	25
B.8	Scenario 8	25
B.9	Scenario 9	25
B.10	Scenario 10	26
B.11	Scenario 11	26
B.12	Scenario 12	27
C	Appendix C: HARA and Safety Goals	31
C.1	Safety Goals	31
D	Appendix D: Functional Safety Requirements	33

E	Appendix E: Decomposed Functional Safety Requirements	35
F	Appendix F: Benchmarking	39
G	Appendix G: Controllability justification	41
H	Appendix H: Glossary	43

Chapter 1

Introduction

Advanced driver assistance systems are one of the fastest-growing segments in automotive electronics [Ric14]. These are systems developed to automate/adapt/enhance the vehicle systems for safety and better driving. Safety features are designed to avoid collisions and accidents by offering technologies that alert the driver to potential problems, or to avoid collisions by implementing safeguards and taking over control of the vehicle. Typical accidents are normally occurring due to unintentional lane change [NCave]. Active Lane Keep Centering System (ALC) is a system designed to avoid such accidents or collisions by actively maintaining the vehicle in the lane if unwanted drift away from lane detected. Hence broad level goals for ALC system are to detect lanes, estimate position of the vehicle with respect to lanes and actively steer it to the center of the lane when unintentional drift detected.

1.1 Project Objective

The project mainly focused on establishing a functional safety concept for ALC. Literature study must be conducted in order to extract functional requirements mainly from Euro NCAP requirement document [NCave]. After defining the Item; Hazard Analysis and Risk Assessment (HARA) must be performed in order to derive the necessary ASIL levels and safety goals. Functional safety requirements must be established and if needed further decomposition must be done to lower the ASIL level. Enhanced software and hardware architecture must be delivered meeting necessary safety criteria. The major project objectives for Module-I are summarized as follow:

- Item definition for the ALC system
- Extract the Euro NCAP requirements (and from other documents like ISO, UNEC) for ALC system
- Define Basic Functional Architecture
- Perform HARA and find the functional safety goals with respective ASIL levels
- Establish functional safety requirements (FSR) associated with safety goals
- Decompose FSR's to achieve necessary safety integrity level.
- Establish Enhanced Architecture in compliant to safety concept

1.2 Project Planning

The Figure 1.1 depicts the major milestones planned for first module.

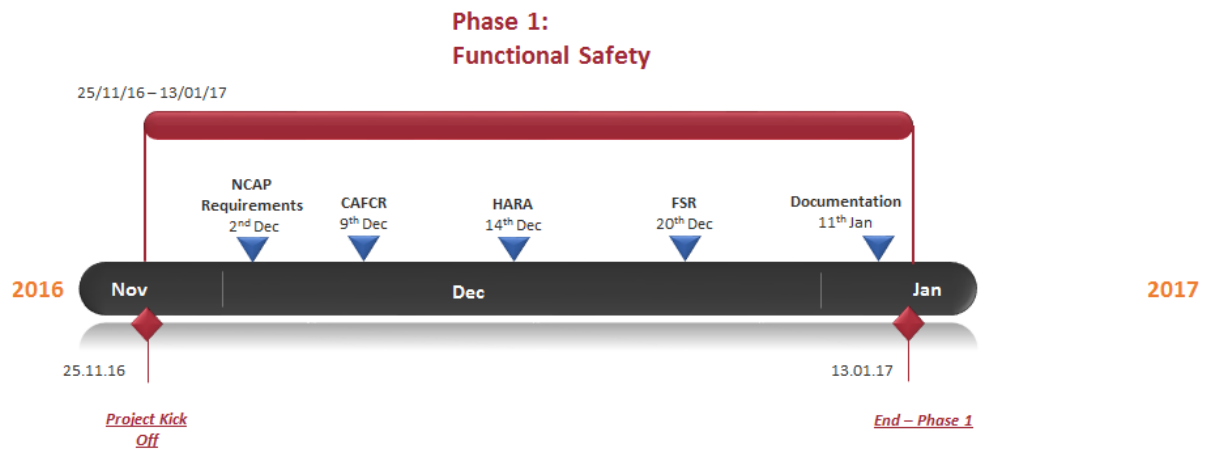


FIGURE 1.1: Project Planning

1.3 Benchmark/History of Lane Departure systems

Although the information on exact ASIL levels of available lane keep systems is unavailable; Figure 1.2 shows the current range of ASIL's seen from customer requirements, to which ADAS have to comply [BFN 0].

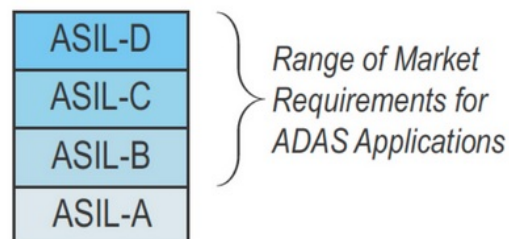


FIGURE 1.2: Market requirement for ADAS

Additionally Table F.1 in Appendix F provides the information regarding year wise development of Lane departure systems by different vehicle manufacturers.

Chapter 2

Functional Requirements and Architecture

2.1 Euro NCAP requirements

The European New Car Assessment Programme (EURO NCAP) provides a protocol that specifies the lateral support system test procedure, which are part of safety assessment [NCave]. The document mainly focuses on enlisting test conditions, test procedure and preparation for vehicle under test (VUT). It provides the minimum criteria that shall be fulfilled by the lateral support system (LSS). To be eligible to score points for lateral support system, the VUT must be equipped with ESC system meeting regulatory requirements [NCave]. Minimum functional requirements are extracted from the NCAP document, some of which are listed below as an example. It must be noted that, Euro NCAP provides the test procedure for Lane Keep Assist (LKA) and Lane Departure Warning (LDW). The requirements are adapted to LCA for the project. However, the requirements when mentioned are kept in their original form as possible.

Sample requirement from Euro NCAP:

LKA and LDWS: LKA and LDWS shall be operational at least under below conditions while performing unintended lane change:

1. Lane width between 3.5 to 3.7 m
2. Dashed line on one side having width of 0.1 to 0.25
3. Solid line on other side with 0.1 to 0.25
4. Dry weather conditions
5. No precipitation
6. Horizontal visibility till 1 km
7. Ambient temperature between 5 to 40 deg
8. Natural ambient illumination excess of 2000 lux for day light with no strong shadow
9. Uniform solid paved surface with consistent slope and no irregularity within a lateral distance of 3.0 m to either side. The minimum peak braking coefficient shall be 0.9
10. Wind speed less than 10 m/s

11. Slope of the surface between 0 and 1 deg
12. Original fitment of tires according to make, model, size, speed and load rating specified by the manufacturer with correct pressure.
13. Default wheel alignment measure set by the OEM

Additionally, documents related to the lane departure system like ISO 11270 [ISO14], UNECE 130 regulation [NAT13], COMPANION D2.2 [AF 0] also referred to derive requirements.

Complete list of extracted requirements can be found in Appendix A.

2.2 Basic architecture of system

Chapter 3

Functional Safety Concept

3.1 Item Definition

The main system function of an 'Active Lane Keeping Centering System (ALC)' is to detect the unintentional drift outside the lane on which it is traveling and to actively steer the vehicle to the center of the current lanes. The system can be activated and deactivated by a HMI button. The system primarily uses camera sensor(s) to detect lane markings. Using information like yaw, acceleration, global positioning, vehicle speed; the system estimates the lateral position of the subject vehicle with respect to lanes and when required, sends command(s) to the actuator(s) to influence the lateral movement of the vehicle. The intention of driver to leave a lane is detected by the toggling of the indicator/turn signal switch or by even measuring the torque applied on the steering wheel of the vehicle. The status information of ALC can be provided to the driver by means of audio, visual or even haptic elements. ALC can autonomously control the vehicle by controlling lateral movement of the vehicle but the responsibility for the safe operation of the vehicle always remains with the driver. Hence, driver needs to intervene in certain time once ALC takes over. To limit the scope of the project, ALC is intended here to be operated only on highways with forward driving speed more than 50 Kph but less than 130 Kph. Temperatures outside -20 to 40 deg Celsius band are considered out of scope for ALC [ISO14]. Roads and lane markings outside Europe are considered out of scope here. Also the actuator for ALC is considered to be an electrical power steering system. The ALC here, can use available softwares like MobilEye to get the data related lane markings.

3.2 Scenario generation

In this section, the operating scenarios where the system will function are described. The Hazard and Risk Analysis for the system has been carried out for these identified scenarios. The work by [HAJ15] provides a good classification of operating scenarios for an automotive system. The different parameters which vary across scenarios are listed in picture 3.1 below.

Some of these parameters are constant for the scenarios in which the ALC system will be operating. The remaining parameters which vary are listed in picture 3.2 below which summarizes the different scenarios considered during the HARA. The diagrams for all the considered scenarios are attached in appendix B.

Operational Situation			
Factor	Sub- factor	Element	State
Vehicle	Driving Speed		Very Slow, Slow, Normal, Fast, and Very Fast
	External Attachment		No external attachment, External attachment
	Operational Mode		Driving, Parking, Fuelling, Repairing
	Maneuver	Engine	On, Off
		Velocity	Accelerating, Constant, Decelerating
		Direction	Lane Keeping, Lane Changing, Turning
		Movement	Stop, Forward, Backward
Road	Linearity		Straight, Curved
	Slope		Plain, Sloped
	Layout		Invisible (blocked) , Visible (unblocked)
	Coarseness		Paved, Unpaved, Troublesome
	Nearby Elements	Obstacle	Clean, Obstacle (e.g. lost cargo dropped in lane of travel)
		Traffic	Smooth flow, Congestion
		Pedestrians	No, A Few, Many
Environment	Surface		Clear, Water (by rain etc), Snow/Ice
	Visibility		Dark, Bright, Foggy
	Temperature		Low, Medium, High
	Momentum		Windy, Calm

FIGURE 3.1: Scenario Parameters

S.No.	Driving and Operating Situation								Exposure
	Vehicle			Road			Weather		
	Driving Speed	Maneuver		Linearity	Coarseness		Surface	Visibility	
		Engine	Direction			Traffic			
1	>50	on	Lane Keeping	Straight	Paved	Smooth	Clear	Bright	E4
2	>50	on	Lane Keeping	Curved	Paved	Smooth	Clear	Bright	E4
3	>50	on	Lane Keeping	Straight	Paved	Smooth	Wet	Bright	E3
4	>50	on	Lane Keeping	Curved	Paved	Smooth	Wet	Bright	E3
5	>50	on	Lane Changing	Straight/Curved	Paved	Smooth	Clear	Bright	E4
6	>50	on	Lane Changing	Straight/Curved	Paved	Smooth	Wet	Bright	E3
7	>50	on	Lane Keeping	Straight/Curved	Paved	Congestion	Clear/Wet	Bright	E4
8	>50	off	Lane Keeping	Straight/Curved	Paved	Smooth	Clear/Wet	Bright	E1
9	>50	on	Lane Keeping	Straight/Curved	Troublesome	Smooth	Clear/Wet	Bright	E3
10	>50	on	Lane Keeping	Straight/Curved	Paved	Smooth	Clear	Dark/Foggy	E3
11	<50	on	Lane Keeping	Straight/Curved	Paved	Congestion	Clear	Bright	E3

FIGURE 3.2: List of all scenarios

3.3 Hazard Analysis and Risk Assessment (HARA)

In this section, the methodology of HARA for the ALC system is explained. An example function from the HARA has been explained explicitly while the remaining functions are attached in appendix C for reference.

The methodology of conducting is derived from the ISO 26262 standard [ISO11]. First we identify the functions that the system as a black box must accomplish. Then

the hazards which are related to these functions are identified. These hazards will lead to different kind of hazardous events in different scenarios. The important point to be noted here is that all the functions, hazards and hazardous events identified at this point in HARA are vehicle level. Each hazardous event is rated for severity, exposure and controllability. Based on these ratings and the table 3.3 from ISO 26262 standard, an Automotive Safety Integrity Level (ASIL) is assigned to each hazardous event which can occur.

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

FIGURE 3.3: ASIL table

For example, consider the function of steering shown in Figure 3.4, which is a vehicle level function of the ALC system, to identify the hazards related to this function. One of the identified hazard is excessive steering where ALC system provides excess steer torque to vehicle than required. For this hazard in all scenarios we have the hazardous event of lateral collision. The severity in all the cases is S3 since the velocity of the vehicle is greater than 50 and therefore the lateral collision can result in fatality. The exposure depends on the scenario since all the scenarios are based on highways they have high exposure. The dry weather condition scenarios have E4 and rainy condition scenarios have exposure E3. The controllability of these hazardous events varies depending upon the weather conditions and kind of maneuver the vehicle is making. The wet conditions and curved road conditions make the vehicle most difficult to control and they are assigned C3. After this the ASIL is assigned to each hazardous event. For scenarios 2 and 7, we have ASIL D.

Hazard Analysis and Risk Assessment																						
Sr.No	Function	Hazard	HazardId	Driving and Operating Situation (Ref. Item Def)	Effect of failure	Severity G-3	Justification - C C-3	Probability P-4	Justification - E E-4	Control ability D-3	Justification - C C-3	Resulting ASIL	Safety Goal	Safety Goal ID	SG ASIL	Safety state						
	Active steering	excessive steering	H4	Scenario 1	Lateral collision (spinning)	3	V > 50 kph	4	Higher exposure, no wet required	2	Straight line driving, car has enough grip	C	The system shall prevent excessive steering in all cases when ALKA is in operation.	SG4	D	Fail Safe						
				Scenario 2	Lateral collision (spinning)	3	V > 50 kph	4	Already cornering and vehicle can spin, a bit harder than the previous	3	Already cornering and vehicle can spin, a bit harder than the previous	D					Fail Safe					
				Scenario 3	Lateral collision (spinning)	3	V > 50 kph	3	Decreased exposure, since rainy conditions	3	Straight line driving, car has decreased grip	C					Fail Safe					
				Scenario 4	Lateral collision (spinning)	3	V > 50 kph	3	Decreased exposure, since rainy conditions	3	Vehicle starts sliding, hard to get grip again	C					Fail Safe					
				Scenario 7	Lateral collision (spinning)	3	V > 50 kph	4	For home-work traffic during rush hours	3	Driver can react too late and has limited space available	D					Fail Safe					

FIGURE 3.4: Example of HARA

3.4 Formulation of Safety Goals

In this section, the Safety Goals of the ALC system are described. Once the ASIL is assigned to every hazardous event, a safety goal is formulated for every hazard. The safety goal is negation of hazard. So for the example in the last section, one safety goal is formulated for the hazard of excessive steering. Every safety goal is also assigned an ASIL. The ASIL of the safety goal is the highest ASIL from its corresponding hazardous events. So in the case of excessive steering the safety goal is that the system must prevent excessive steering in all cases when the ALC system is in operation. The ASIL of this safety goal is ASIL D which is the ASIL for scenarios 2 and 7. The remaining safety goals for the identified hazards are listed in appendix C. In the next section, the functional elements of the system which are impacted by each safety goals are identified and FMEA is performed for these functional components of the system and Functional Safety Requirements are defined.

3.5 Functional Safety Concept

After the HARA according to ISO26262, the next step is the Functional Safety Concept, or FSC. FSC is a list of Functional Safety Requirements (FSR) with an ASIL level, which are allocated to certain components of the Functional Architecture (Chapter 2). In this phase each Safety Goal (SG) which was derived in the previous phase, will be broken down into Functional safety requirements and allocated to the architectural components in order to build the FSC (ref. Annex D). The thought process that we followed is described hereafter, you will find an example in figure 3.5. Every element that leads to the violation of a SG is called “impacted element” of that particular SG, and will receive at least one FSR as a consequence. Every impacted element is then analysed separately and its failure modes are identified. One FSR is derived for each failure mode with the aim to transition to the safe state.

We define two safe states:

1. One in which the system is operational (Fail Operational Approach)
2. One in which the system is deactivate and the user is warned (Fail Safe Approach)

This view (Figure 3.5 tends to be very big and time consuming to write, since the impacted elements tend to repeat themselves and their failure modes tend to do so as well (in particular for the elements to the left of the architecture), we propose an alternative view, which is shown in figure 3.6.

Function	Safety Goal	Safety Goal ID	ASIL(SG)	Elements Impacted	Failure Modes	FSR	ASIL(FSR)
Active Steering	The system shall prevent excessive steering in all cases when ALKA is in operation.	SG4	D	Lateral controller	Lateral controller calculated a too large required torque	The system shall only apply a limited additional steer torque to prevent excessive steering when ALKA is active	D
					Controll settings wrong	The system control parameters shall be adequately tuned in order to prevent large overshoot and ss error	D
					High level supervisor activation message not received	Lateral controller shall receive the High level supervisor activation/deactivation message at all times when ALKA is active	D
					Activation/deactivation signal not received	Lateral controller shall receive the activation/deactivation message at all times when ALKA is active	D
					Vehicle position w.r.t. lane not received	Lateral controller shall receive the vehicle position w.r.t the lane message at all times when ALKA is active	D
				Steer actuator	Steer actuator is incorrectly calibrated	The steer actuator shall be calibrated correctly when the ALKA system is implemented on the car	D

FIGURE 3.5: Derivation of FRSs

Lane Detection Algorithm	No image received	The updated image should be received before calculating the ego state when ALC is active	SG1-3, SG4-6, SG9-11	D
	No image received	If the updated image is not available the system should trigger a warning and deactivate		
	Wrong lane detection	The lane detection should be accurate if ALC is active		
	Wrong lane detection	If the function is not able to detect the correct lanes the system shall trigger a warning and deactivate		
	Wrong/corrupt image received	If the system receives corrupt images it should be able to detect it, deactivate the system and warn the user		
	Wrong/corrupt image received	The system should receive correct images		
	Detected lanes not sent	If the function is not able to send the detected lanes the system shall trigger a warning and deactivate		
	Detected lanes not sent	The labelled image should be sent once available when the ALC is active		

FIGURE 3.6: Failure Modes Analysis

In this view every component of the architecture was analyzed separately, possible failure modes were identified and functional safety requirements were formulated according to the following thought process. The basic idea is that each component can fail due to 3 things:

1. Wrong/Missing input
2. Wrong process
3. Missing output

This way we can assign an FSR to each failure mode, formulating the FSR in a way that will lead to a Safe State, and allocate them to functional components of the architecture. Once we completed the Failure Mode analysis, the impacted Safety Goals were connected to the FSRs and highest ASIL level among the impacted Safety Goals was attributed to the FSRs.

We have two types of functional safety requirements, an FSR related to the Fail Operational approach (in white), and an FSR related to the Fail Safe approach (in green), which acts as a fallback option in case of fault. An example of this can be seen in 3.6.



Chapter 4

Functional Architecture with Safety Measures



From Chapter ?? it follows that the ALC system reaches an ASIL D level, which leads to a safety critical system. During the functional safety assessment of an automotive system design it can be chosen to reduce the ASIL levels via ASIL decomposition. ASIL decomposition is a method to assign ASILs to redundant requirements. The redundant requirements can be used to improve the integrity of the system. In this case the FSRs originating from the safety goals are decomposed into redundant and sub requirements that ensure the achievement of the 'parent' FSR. The decomposed FSRs are tested afterwards to ensure that the system is working correctly.

The main rule for this decomposition is that the redundant requirements are allocated to different components of the system. If one component fails to satisfy a particular FSR, the other component can still do so, which improves the system integrity. Important to mention is that the ASIL decomposition can be applied to any requirement at any stage in the design process. The ASIL decomposition can be used to reduce the ASIL level of a safety goal via the rules shown in Table. 4.1. According to [JGDGMC13], the highest decomposed ASIL are assigned to the sub requirements based safety mechanism. Adding redundant safety mechanisms to the system will lead to an equal ASIL assignment to the decomposed FSRs.

TABLE 4.1: ASIL Decomposition [JGDGMC13]

ASIL before Decomposition	ASIL after Decomposition
ASIL D Requirement	ASIL C(D) Requirement + Asil A(D) Requirement or ASIL B(D) Requirement + Asil B(D) Requirement or ASIL D(D) Requirement + Asil QM(D) Requirement
ASIL C Requirement	ASIL B(C) Requirement + Asil A(C) Requirement or ASIL C(C) Requirement + Asil QM(C) Requirement
ASIL B Requirement	ASIL A(B) Requirement + Asil A(B) Requirement or ASIL B(B) Requirement + Asil A(B) Requirement
ASIL A Requirement	ASIL A(A) Requirement + Asil QM(A)

4.1 Decomposition of FSR's for ALC

The first step in the ASIL decomposition is to determine the safety measures. It can be concluded from Chapter ?? that the safety goals are related to: wrong/missing input, wrong process or missing output. Therefore, the corresponding safety measures that are required for the decomposition are functions/mechanisms that check the:

- arrival and sending of the data at specific components/functions
- correctness of the received/calculated data by means of redundancy or predictions
- correctness of the decisions made by the supervisors

The updated functional architecture with safety mechanism is provided in Appendix E. Each safety mechanism adds new FSRs to the system. Most of the Decomposed Functional Safety Requirements (DFSRs) are safety measure related requirements that are added to the system to check incorrect operation and reach the corresponding safe states. Therefore, most FSR are decomposed into ASIL C(D) + ASIL A(D) requirements. To decompose the ASIL D FSR into two ASIL B (D) DFSRs, redundant safety mechanism should be added. One example of such a redundant safety measure is to use both the Mobileye lane detection system and the own designed lane detection algorithm.

The ASIL decomposition will now be explained for the excessive steering scenario, previously explained in Chapter ?. The ASIL decomposition of this FSR is shown in Fig. 4.1. According to FSR 24 in Fig. 4.1, "the system shall only apply a limited additional steer torque to prevent excessive steering when ALC is active". The according safety mechanism is a filter that limits the output steer torque to a certain value". This comes with the functional safety requirement: "the lateral controller output should be limited to avoid excessive steering torques. Since this safety mechanism is sub requirement based an ASIL C(D) is assigned to the safety mechanism related FSR, whereas an ASIL A(D) is assigned to the original FSR.

8	Lateral controller	Lateral controller calculated a too large required torque	The system shall only apply a limited additional steer torque to prevent excessive steering when ALC is active	SG4-6	D	24	A	limum ste	c	The lateral controller output should be limited to avoid excessive steering torques	11
		Lateral controller calculated the torque incorrectly	If the lateral controller calculates the required torque incorrectly the system shall trigger a warning and deactivate			24.1					
		Lateral controller calculated the torque incorrectly	The system shall calculate the correct steer torque at all times when ALC is active			25	A	psition w.r	C	The next vehicle positions w.r.t. lane markings should be predicted by the system to validate the correctness of the lateral controller and vehicle position determination	6
		Control settings wrong	The system control parameters shall be adequately tuned in order to prevent large overshoot and ss error			26	A	psition w.r	C	The next vehicle positions w.r.t. lane markings should be predicted by the system to validate the correctness of the lateral controller and vehicle position determination	6
		High level supervisor activation/deactivation signal not received	Lateral controller shall receive the High level supervisor activation/deactivation signal at all times when ALC is active			27	A	if of later	C	It should be checked if an updated High level Supervisor signal is arrived before the times of the lateral controller runs	10

FIGURE 4.1: Decomposed FSR for excessive steering

It can be concluded from Appendix ?? that the final ASIL level of the system is ASIL C. For future work it may be possible to reduce the ASIL levels further by using decomposition methods like software redundancy or hardware redundancy. Compared to hardware redundancy, the relative costs of software redundancy is much smaller.

Chapter 5

Conclusion and Way Forward

In this report, the Euro NCAP requirements and the Functional Safety concept for the ALC system is summarized. The requirements for the LC system coming from Euro NCAP are identified and listed. For the purpose of Automotive Functional Safety of ALC system, HARA was conducted and safety goals were formulated. FMEA was done for the functional elements of the system and functional safety requirements were formulated for the ALC system. These requirements were assigned ASIL depending upon their influencing safety goals. Safety measures have been identified for components with higher ASIL and their corresponding safety requirements were decomposed.

In the next phase of the project, the system architecture model of the ALC system will be delivered. The CAFCR views of the system will be discussed in detail and the technical safety concept of the system will be presented with requirements for both hardware and software components of the ALC system.

Bibliography

- [AF 0] Alvaro Arrue (IDIADA) Alba Fornells. "Cooperative dynamic formation of platoons for safe AND energy-optimized goods transportation". In: *Companion : Current State Of EU Legislation*. 28-05-2014.
- [BFN 0] Altera By Frank Noha. "<http://www.automotive-eetimes.com/content/functional-safety-considerations-ad-as-designs-using-fpgas>". In: *Functional safety considerations for ADAS designs using FPGAs*. 15-07-2014.
- [HAJ15] Sung-Hoon Hong Min Koo Lee Hyeon Ae Jang Hyuck Moo Kwon. "A Study on Situation Analysis for ASIL Determination". In: *Journal of Industrial and Intelligent Information Vol. 3, No. 2*. Engineering and Technology Publishing, 2015.
- [ISO11] ISO. "Road vehicles Functional safety Part 3: Concept phase". In: *INTERNATIONAL STANDARD ISO 26262-3*. 2011.
- [ISO14] ISO. "Intelligent transport systems — Lane keeping assistance systems (LKAS) — Performance requirements and test procedures". In: *ISO 11270:2014(en)*. 2014.
- [JGDGMC13] Rami Debouk General Motors Company Joseph G. D'Ambrosio General Motors Company. "ASIL Decomposition: The Good, the Bad, and the Ugly". In: *SAE Technical Paper 2013-01-0195*. 2013.
- [NAT13] UNITED NATIONS. "Uniform provisions concerning the approval of motor vehicles with regard to the Lane Departure Warning System (LDWS)". In: *UNECE 130: 2013*. 2013.
- [NCave] Euro NCAP. "TEST PROTOCOL – Lane Support Systems. Version 1.0". In: *EUROPEAN NEW CAR ASSESSMENT PROGRAMME*. November 2015.
- [Ric14] Ian Riches. "Strategy Analytics: Automotive Ethernet: Market Growth Outlook." In: *Keynote Speech 2014 IEEE SA - Ethernet and IP at Automotive Technology Day*. 2014.

Appendix A

Appendix A: Euro NCAP Requirements

Important functional requirements:

1. LKA: LKA should detect unintentional lane change at latest, when outside of the tire closest to the outside of the lane markings crosses 0.3 m.
(Source: Partially from EURO NCAP: Section1 and UNECE)
2. LKA: LKA shall use the lateral support system to restore control of the vehicle while countering the unintentional lane change.
(Source: EURO NCAP: Section1)
3. LKA: LKA system shall be available only if vehicle possess Electronic Stability Control system in compliance with regulatory requirements.
(Source: EURO NCAP: Section1)
4. LDW: LDW shall automatically warn the driver (e.g. audible signal, vibrating steering wheel etc.) at least when, outside of the tire closest to the outside of the lane markings crosses 0.3 m or beyond.
(Source: Partially EURO NCAP: Section1 and definition of LDW and UNECE)
5. LKA: LKA shall determine the lateral deviation from path which is distance between current center of vehicle and center of intended path.
(Source: 1st sentence from Euro NCAP: Section 3.2)
6. LDW and LKA: Both LKA and LDW shall be operational at least when driving on straight road with radius more than 1000 m and 250 m on curved road, unless manually deactivated.
(Source: Regulation: 130 UNECE)
7. LDW: The LDW should be active at least if vehicle speeds exceeds 60 km/h, unless manually deactivated.
(Source: Regulation: 130 UNECE)
8. LDW: If a vehicle is equipped with a means to deactivate the LDW function, the following condition shall apply as appropriate: The LDW function shall be automatically reinstated at the initiation of each new ignition on (run) cycle.
(Source: EURO NCAP and Regulation: 130 UNECE)
9. LKA and LDW: LKA and LDW shall be operational at least under below conditions while performing unintended lane change.
 - Lane width between 3.5 to 3.7 m

- Dashed line on one side having width of 0.1 to 0.25
- Solid line on other side with 0.1 to 0.25
- Dry weather conditions
- No precipitation
- Horizontal visibility till 1 km
- Ambient temperature between 5 to 40 deg
- Natural ambient illumination excess of 2000 lux for day light with no strong shadow
- Uniform solid paved surface with consistent slope and no irregularity within a lateral distance of 3.0 m to either side. The minimum peak braking coefficient shall be 0.9
- Wind speed less than 10 m/s
- Slope of the surface between 0 and 1 deg
- Original fitment of tires according to make, model, size, speed and load rating specified by the manufacturer with correct pressure.
- Slope of the surface between 0 and 1 deg
- Default wheel alignment measure set by the OEM

(Source: EURO NCAP: Section 5)

10. LKA: The steering to counter lateral deviation, shall be smooth controlled manner and with minimal overshoot.
 - Lateral acceleration $< 2 \text{ m/s}^2$ while cornering,
 - Lateral acceleration $< 0.5 \text{ m/s}^2$ while driving straight
 - Lateral jerk $< 5 \text{ m/s}^3$ overall,
 - Longitudinal deceleration $< 3 \text{ m/s}^2$
 - If Longitudinal deceleration $> 1 \text{ m/s}^2$ then, longitudinal speed reduction $< 18 \text{ km/h}$

(Source: Partially from EURO NCAP: Section 6.4 and ISO 11270)

11. LKA and LDW [Input Requirement]: The system must have an accuracy of
 - 0.1 km/h in longitudinal speed
 - 0.03 m in longitudinal and lateral position
 - 0.1 degrees in heading angle
 - 0.1 deg/sec in yaw rate
 - 0.1 m/sec² in longitudinal acceleration
 - 1 deg/sec in steering wheel velocity

(Source: EURO NCAP: Section4.3)

12. LKA: LKA shall make sure the driver remains in control at all times (as long as LKA active).

(Source: EURO NCAP: Section1)

13. LKA and LDW [Country specific]: The system must be able to identify lane markings and lane width according to the country of operation.

Less important functional requirements

1. LKA: LKA may function while only one distinct marking on either side (no/ non distinct marking on other).
(Source: EURO NCAP: Section1)
2. LKA: LKA may function while only one distinct marking on either side (no/ non distinct marking on other).
(Source: EURO NCAP: Section1)
3. LDW: The effectiveness of the LDW shall not be adversely affected by magnetic or electrical fields.
(Source: Regulation: 130 UNECE)

HMI related requirements:

1. LDW [HMI]: The warning above shall be noticeable by the driver and be provided by:
 - At least two warning means out of optical, acoustic and haptic, or
 - One warning means out of haptic and acoustic, with spatial indication about the direction of unintended drift of the vehicle.
(Source: Regulation: 130 UNECE)
2. LDW [HMI]: The warning mentioned above may be suppressed when there is a driver action which indicates an intention to depart from the lane.
(Source: Regulation: 130 UNECE)
3. LDW [HMI]: LDW shall also provide the driver a warning as a yellow optical warning signal to detect failure. Failure must be detected when: the power source to any LDW component or any electrical connection between LDW components disconnected.
(Source: Regulation: 130 UNECE)
4. LDW [HMI]: The failure warning signal shall be activated and remain activated while the vehicle is being driven and be reactivated after a subsequent ignition off – ignition on cycle as long as the failure exists.
(Source: Regulation: 130 UNECE)
5. LDW [HMI]: Where an optical signal is used for the lane departure warning, it may use the failure warning signal. (Source: Regulation: 130 UNECE)
6. LDW [HMI]: The LDW optical warning signals shall be activated either when the ignition (start) switch is turned to the on (run) position or when the ignition (start) switch is in a position between the on (run) and start that is designated by the manufacturer as a check position (initial system (power-on)). This requirement does not apply to warning signals shown in a common spaces.
(Source: Regulation: 130 UNECE)

7. LDW [HMI]: The optical warning signals shall be visible even by daylight; the satisfactory condition of the signals must be easily verifiable by the driver from the driver's seat.
(Source: Regulation: 130 UNECE)
8. LDW [HMI]: When the driver is provided with an optical warning signal to indicate that the LDW is temporarily not available, for example due to inclement weather conditions, the signal shall be constant. It may use failure warning signal for the same.
(Source: Regulation: 130 UNECE)
9. LDW [HMI]: At a periodic technical inspection it shall be possible to confirm the correct operational status of the LDW by a visible observation of the failure warning signal status, following a power ON (off system OK, on system fault present).
(Source: Regulation: 130 UNECE)
10. LDW [HMI]: If a vehicle is equipped with a means to deactivate the LDW function, when LDW deactivated, a constant optical warning signal shall inform the driver that the LDW function has been deactivated. The same yellow warning failure signal can be used.
(Source: Regulation: 130 UNECE).
11. LKA and LDW [HMI]: Care shall be taken that the Driver shall not get distracted by LKA warning.
(Source: EURO NCAP: Section1)

Additional requirements (Originated from group discussion):

1. LKA: LKA must be deactivated when
 - Manually deactivated by the user
 - LKA is active currently and driver does the counter steering (opposite to assist torque)
 - LKA is active and driver doesn't intervene to the steering wheel within 5 seconds.
 - Turn signal is activated
2. LKA: The LKA should be active at least when vehicle speed exceeds 50 km/h, unless manually deactivated. [Source: Japanese guidelines] [ISO 11270 states: LKAS shall be operational between 72km/h and the maximum speed which is 108km/h or the maximum possible vehicle speed, whichever is less.]
3. LKA: The absolute deviation shall not exceed 0.15 m. (refer 5th req)
4. LDW: The LDW should be active at least if vehicle speeds exceeds 50 km/h, unless manually deactivated. (Requirement 7 is adapted to take care of conflicting requirements for LDW and LKA activation.)

Appendix B

Scenarios

The scenarios considered while performing HARA are described here with help of diagrams.

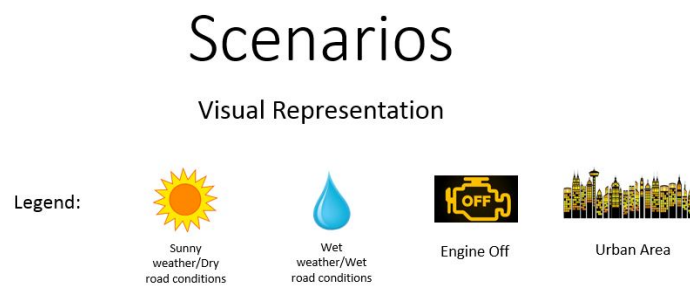


FIGURE B.1: Scenario Legends

B.1 Scenario 1

- Driving on a highway
- Vehicle speed >50 kph
- On a straight road ($R > 1000$ m)
- Sunny weather
- Dry road conditions

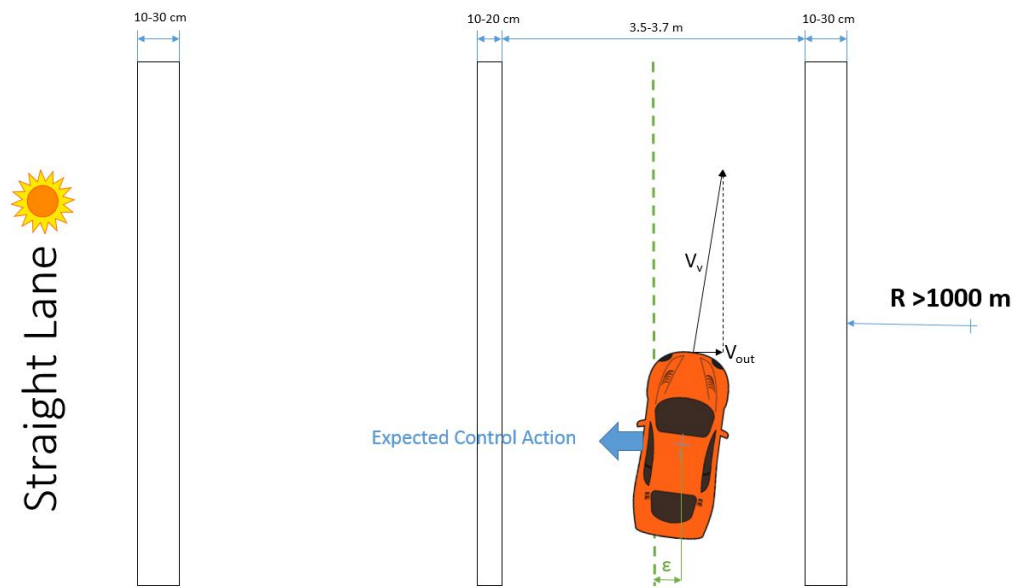


FIGURE B.2: Scenario 1

B.2 Scenario 2

- Driving on a highway
- Vehicle speed $>50 \text{ kph}$
- Approaching a curved road ($1000 \text{ m} > R > 250 \text{ m}$)
- Sunny weather
- Dry road conditions

B.3 Scenario 3

- Driving on a highway
- Vehicle speed $>50 \text{ kph}$
- On a straight road ($R > 1000 \text{ m}$)
- Rainy/snowy weather
- Wet/slippery road conditions

B.4 Scenario 4

- Driving on a highway
- Vehicle speed $>50 \text{ kph}$

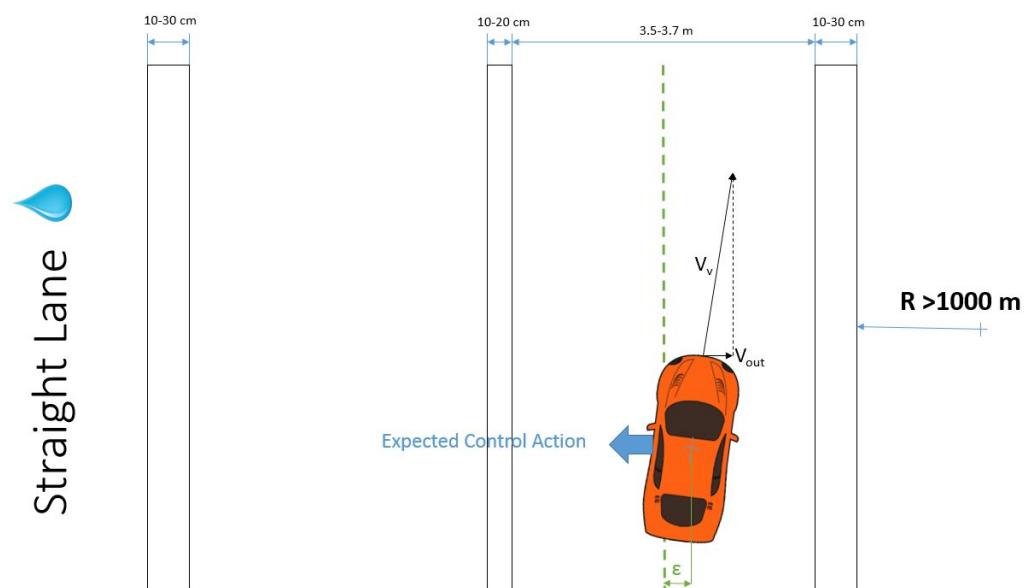


FIGURE B.3: Scenario 2

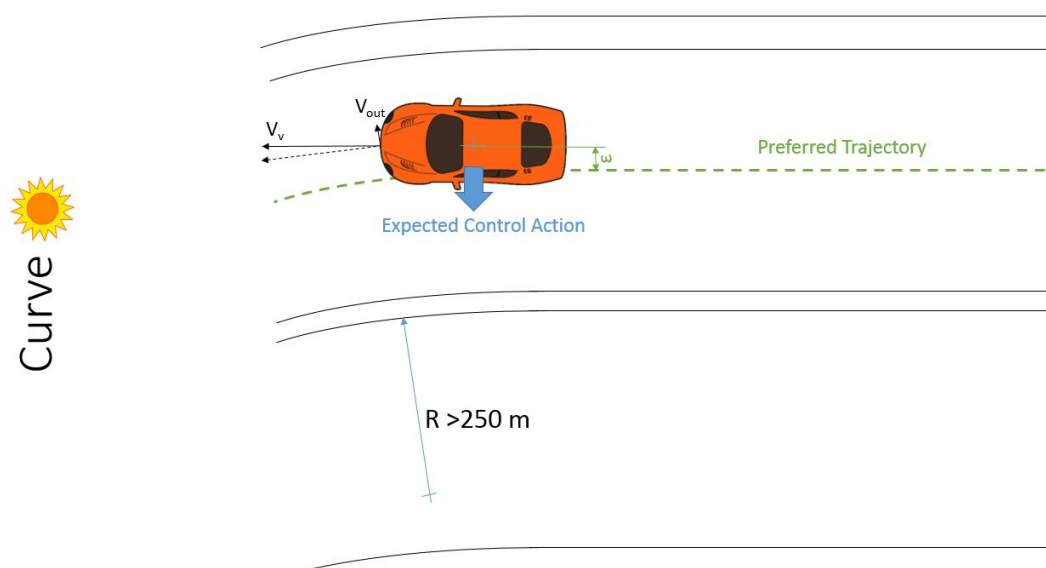


FIGURE B.4: Scenario 3

- Approaching a curved road ($1000\text{ m} > R > 250\text{ m}$)
- Rainy/snowy weather
- Wet/slippy road conditions

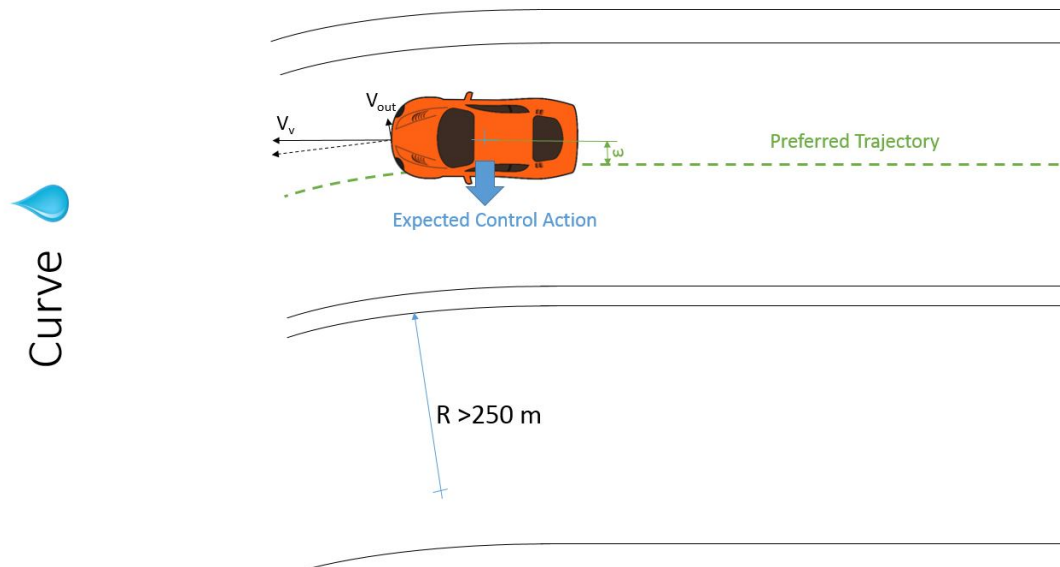


FIGURE B.5: Scenario 4

B.5 Scenario 5

- Driving on a highway and overtaking
- Vehicle speed $> 50\text{ kph}$
- On a straight road ($R > 1000\text{ m}$)
- Sunny weather
- Dry road conditions

B.6 Scenario 6

- Driving on a highway and overtaking
- Vehicle speed $> 50\text{ kph}$
- On a straight road ($R > 1000\text{ m}$)
- Rainy/snowy weather
- Wet/slippy road conditions

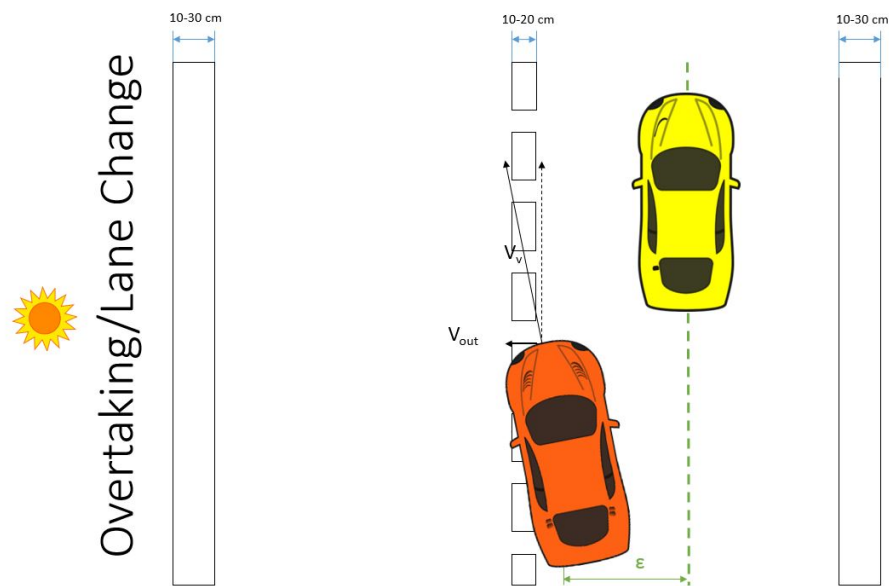


FIGURE B.6: Scenario 5

B.7 Scenario 7

- Driving on a highway in traffic
- Vehicle speed >50 kph
- On a straight road ($R > 1000$ m)
- All weather conditions
- Dry road conditions

B.8 Scenario 8

- Driving on a highway and engine off
- Vehicle speed >50 kph
- On a straight road ($R > 1000$ m)
- All weather conditions
- All road conditions

B.9 Scenario 9

- Driving on a highway
- Vehicle speed >50 kph

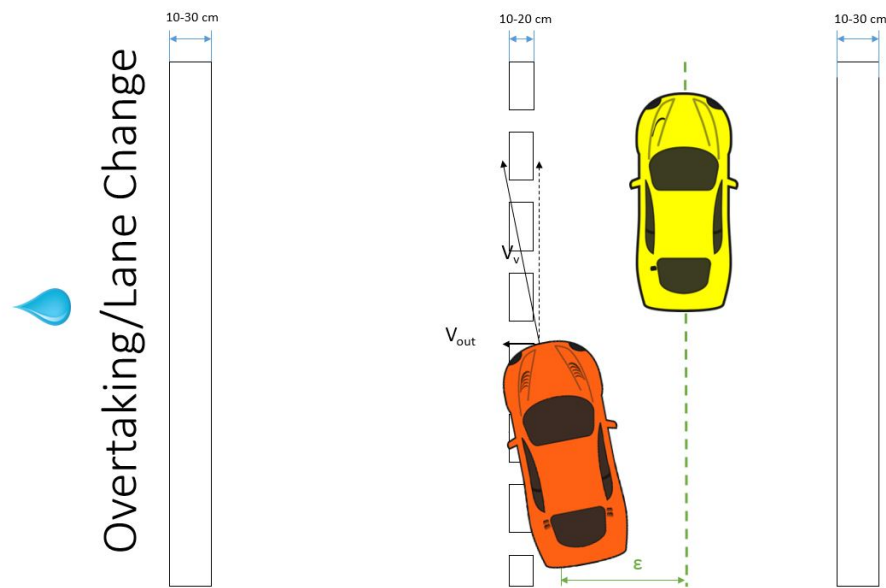


FIGURE B.7: Scenario 6

- On a straight road ($R > 1000$ m)
- All weather conditions
- Poor road conditions

B.10 Scenario 10

- Driving on a highway
- Vehicle speed > 50 kph
- On a straight road ($R > 1000$ m)
- Low visibility / View obstruction by an object
- All weather conditions
- All road conditions

B.11 Scenario 11

- Driving on a highway and traffic
- Vehicle speed < 50 kph
- On a straight road ($R > 1000$ m)
- All weather conditions
- All road conditions

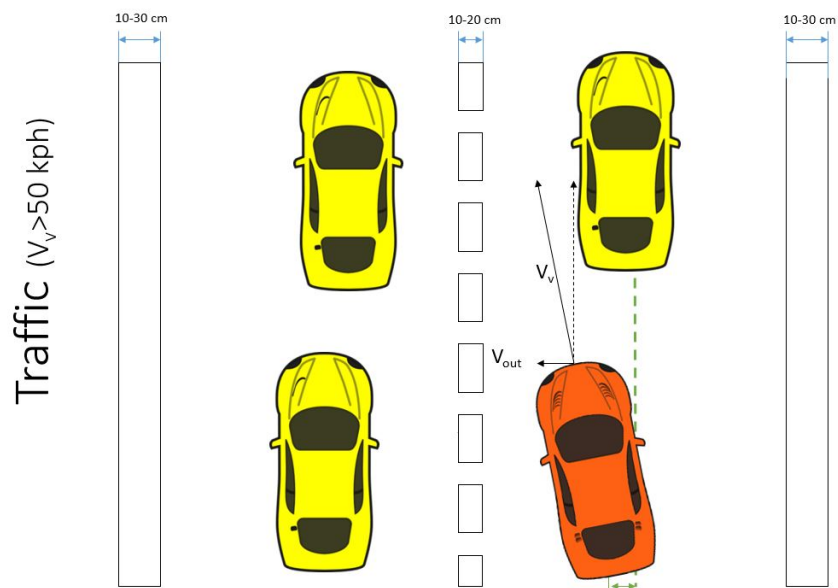


FIGURE B.8: Scenario 7

B.12 Scenario 12

- Driving in urban area
- Vehicle speed < 50 kph
- On a straight road ($R > 1000$ m)
- Pedestrian and obstacles present
- All weather conditions
- All road conditions

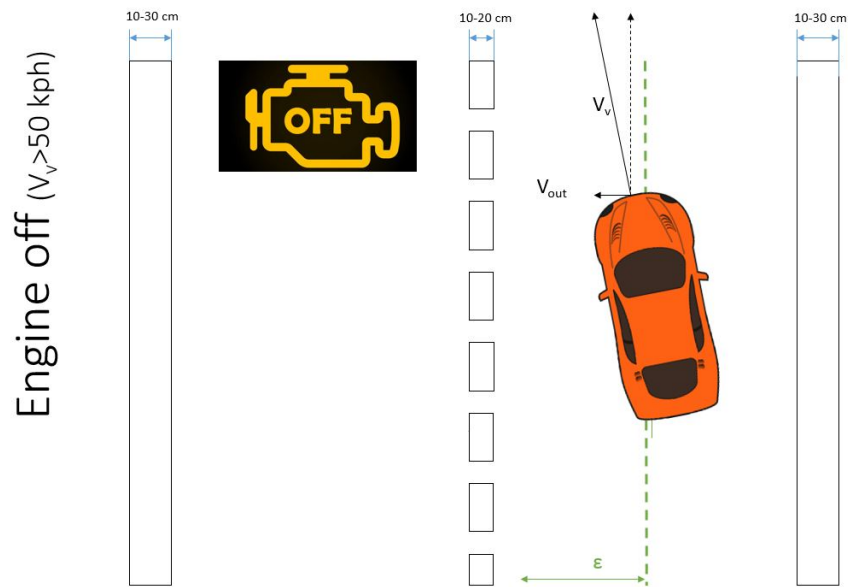


FIGURE B.9: Scenario 8

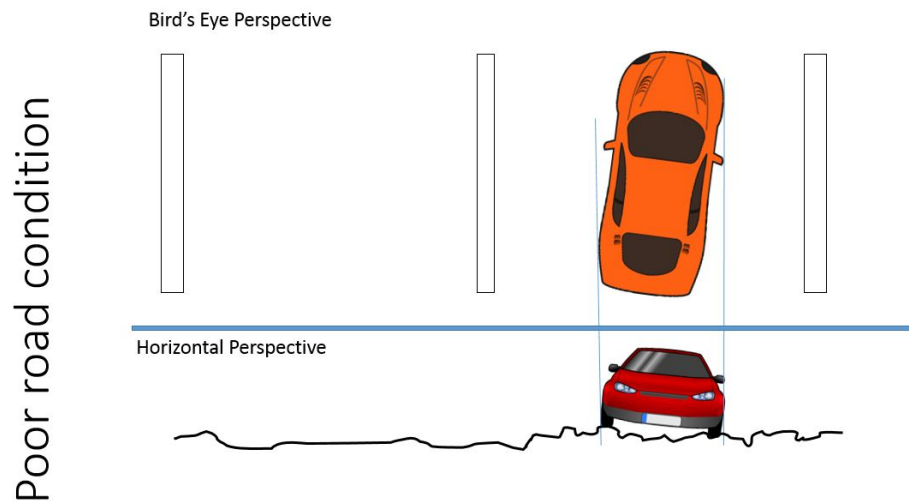


FIGURE B.10: Scenario 9

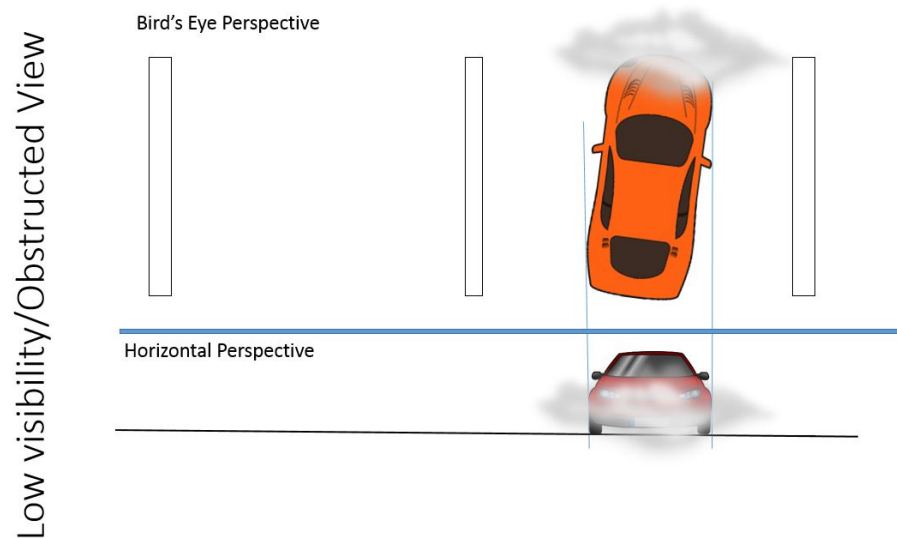


FIGURE B.11: Scenario 10

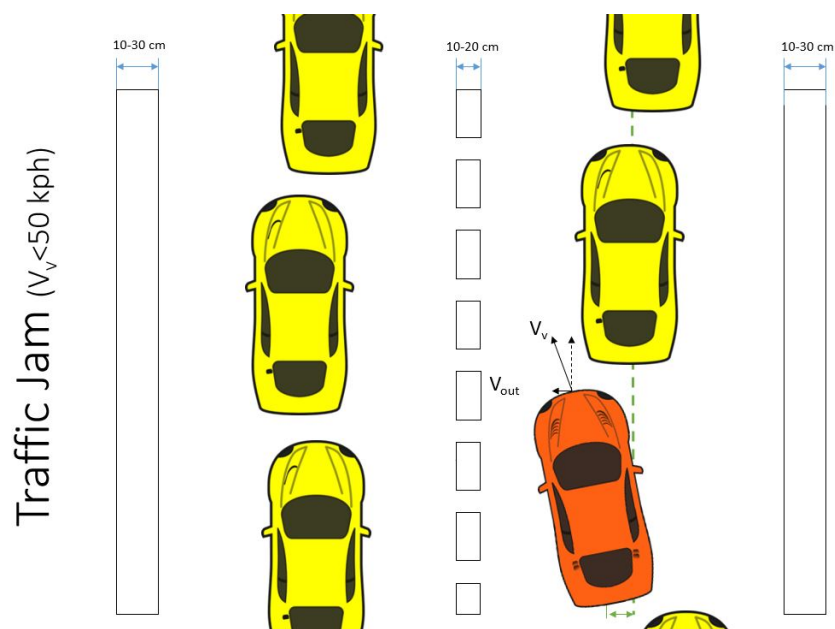


FIGURE B.12: Scenario 11

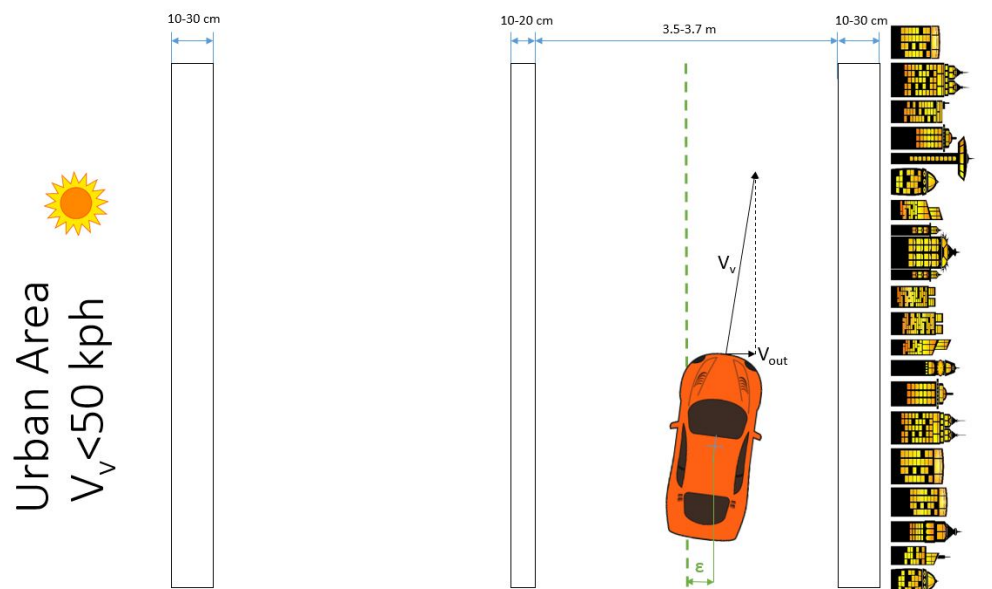


FIGURE B.13: Scenario 12

Appendix C

Appendix C: HARA and Safety Goals

C.1 Safety Goals

S. No.	Safety Goal	Safety Goal ID	SG ASIL
1	The system shall ensure the activation of the ALC when all the conditions for activation are satisfied	SG1	C
2	The system shall prevent the unwanted activation of the ALC when driving	SG2	C
3	The system shall ensure that the lag after the activation command is smaller than 0.5s	SG3	C
4	The system shall prevent excessive steering in all cases when ALC is in operation.	SG4	D
5	The ALC system shall steer the vehicle such that it follows the correct setpoint	SG5	D
6	The system shall prevent too small steering torques in all cases when ALC is in operation.	SG6	C
7	The system must deactivate when all the deactivation conditions are met.	SG7	C
8	The system should not deactivate when it is not desired.	SG8	C
9	The system shall deactivate within 0.5sec when the deactivation button is pressed.	SG9	C
10	The system shall flash warning signal when vehicle crosses lane unintentionally.	SG10	QM
11	The system shall flash warning signal immediately when vehicle crosses lane unintentionally.	SG11	QM
12	The system shall flash correct warning signal when vehicle crosses lane unintentionally.	SG12	QM
13	The system shall flash activation signal when system is activated.	SG13	QM
14	The system shall flash activation signal immediately when system is activated.	SG14	QM
15	The system shall flash correct activation signal when system is activated.	SG15	QM
16	The system shall flash deactivation signal when system is deactivated.	SG16	QM
17	The system shall flash deactivation signal immediately when system is deactivated.	SG17	QM
18	The system shall flash correct deactivation signal when system is deactivated.	SG18	QM
19	The system shall flash correct lane detection signal when it detects lane markings.	SG19	QM

FIGURE C.1: Safety Goals

Appendix D

Appendix D: Functional Safety Requirements

Appendix E

Appendix E: Decomposed Functional Safety Requirements

- **FSR 1 → DFSR 1:** The correctness of the Activation/Deactivation Signal should be checked before the computation of the system on/off supervisor starts. ASIL B (C)
- **FSR 2,5 → DFSR 2:** It should be checked if an updated Activation/Deactivation Signal is arrived before the timer of the system on/off supervisor runs out. ASIL B (C)
- **FSR 3 → DFSR 3:** The correctness of the Ignition Key signal should be checked before the computation of the system on/off supervisor starts. ASIL B (C)
- **FSR 4,6 → DFSR 4:** It should be checked if an updated Ignition Key signal is arrived before the timer of the system on/off supervisor runs out. ASIL B (C)
- **FSR 7 → DFSR 5:** It should be checked if an updated supervisor On/Off signal is arrived before the timer of the actuation switch runs out. ASIL B (C)
- **FSR 7,9 → DFSR 6:** It should be checked if an updated supervisor On/Off signal is arrived before the timer of the High level supervisor runs out. ASIL B (C)
- **FSR 8 → DFSR 7:** The formal verification of the On/Off supervisor should check the correctness of the decision made by the supervisor. ASIL B (C)
- **FSR 10 → DFSR 8:** It should be checked if an updated indicator signal is arrived before the timer of the High Level Supervisor runs out. ASIL B (C)
- **FSR 11 → DFSR 9:** It should be checked if an updated vehicle position w.r.t lane markings signal is arrived before the timer of the High Level Supervisor runs out. ASIL B (C)
- **FSR 12, 27 → DFSR 10:** It should be checked if an updated High Level Supervisor signal is arrived before the timer of the lateral controller runs out. ASIL B (C)
- **FSR 12,14 → DFSR 11:** It should be checked if an updated High Level Supervisor signal is arrived before the timer of the warning signal generator runs out. ASIL B (C)
- **FSR 13 → DFSR 12:** The formal verification of the High Level supervisor should check the correctness of the decision made by the supervisor ASIL B (C)

- **FSR 24 → DFSR 13:** The lateral controller output should be limited to avoid excessive steering torques. ASIL C (D)
- **FSR 25,26,29 → DFSR 14:** The next vehicle positions w.r.t. lane markings should be predicted by the system to validate the correctness of the lateral controller and vehicle position determination. ASIL C (D)
- **FSR 28 → DFSR 15:** It should be checked if an updated Vehicle Position w.r.t. Lane Markings signal is arrived before the timer of the lateral controller runs out. ASIL C (D)
- **FSR 30 → DFSR 16:** It should be checked if an updated steer torque signal is arrived before the timer of the actuation switch runs out. ASIL B (C)
- **FSR 31 → DFSR 17:** It should be checked if an activation/deactivation signal is arrived before the timer of the actuation switch runs out. ASIL B (C)
- **FSR 32 → DFSR 18:** The sending of the steer torque signal to the steer actuator should be checked. ASIL B (C)
- **FSR 33,44 → DFSR 19:** It should be checked if an gyro signal is arrived before the timer of the Determine Vehicle Ego State runs out. ASIL C (D)
- **FSR 34 → DFSR 20:** The correctness of the gyro sensor signal should be checked before the computation of the Determine Vehicle Ego State starts. ASIL C (D)
- **FSR 35,46 → DFSR 21:** It should be checked if an steering angular speed signal is arrived before the timer of the Determine Vehicle Ego State runs out. ASIL C (D)
- **FSR 36 → DFSR 22:** The correctness of the steering angular speed sensor signal should be checked before the computation of the Determine Vehicle Ego State starts. ASIL C (D)
- **FSR 37,43 → DFSR 23:** It should be checked if an updated GPS signal is arrived before the timer of the Determine Vehicle Ego State runs out. ASIL B (C)
- **FSR 38 → DFSR 24:** The correctness of the GPS signal should be checked before the computation of the Determine Vehicle Ego State starts. ASIL B (C)
- **FSR 39,45 → DFSR 25:** It should be checked if an VSS signal is arrived before the timer of the Determine Vehicle Ego State runs out. ASIL B (C)
- **FSR 40 → DFSR 26:** The correctness of the VSS sensor signal should be checked before the computation of the Determine Vehicle Ego State starts. ASIL C (D)
- **FSR 41 → DFSR 27:** It should be checked if an acquired image is arrived before the timer of the lane detection algorithm runs out. ASIL C (D)
- **FSR 42 → DFSR 28: The correctness of the Acquired image should be checked before the computation of the lane detection algorithm starts.**

It should be checked if an updated Vehicle Ego state signal is arrived before the timer of the Determine Vehicle Positions w.r.t Lane markings runs out. ASIL C (D)

- **FSR → DFSR 27:** It should be checked if a pre-processed image is arrived before the timer of the Determine Vehicle Position w.r.t. Lane Markings runs out. ASIL C (D)
- **FSR → DFSR 28:** It should be checked if a pre-processed Mobileye image is arrived before the timer of the Determine Vehicle Position w.r.t. Lane Markings runs out. ASIL C (D)

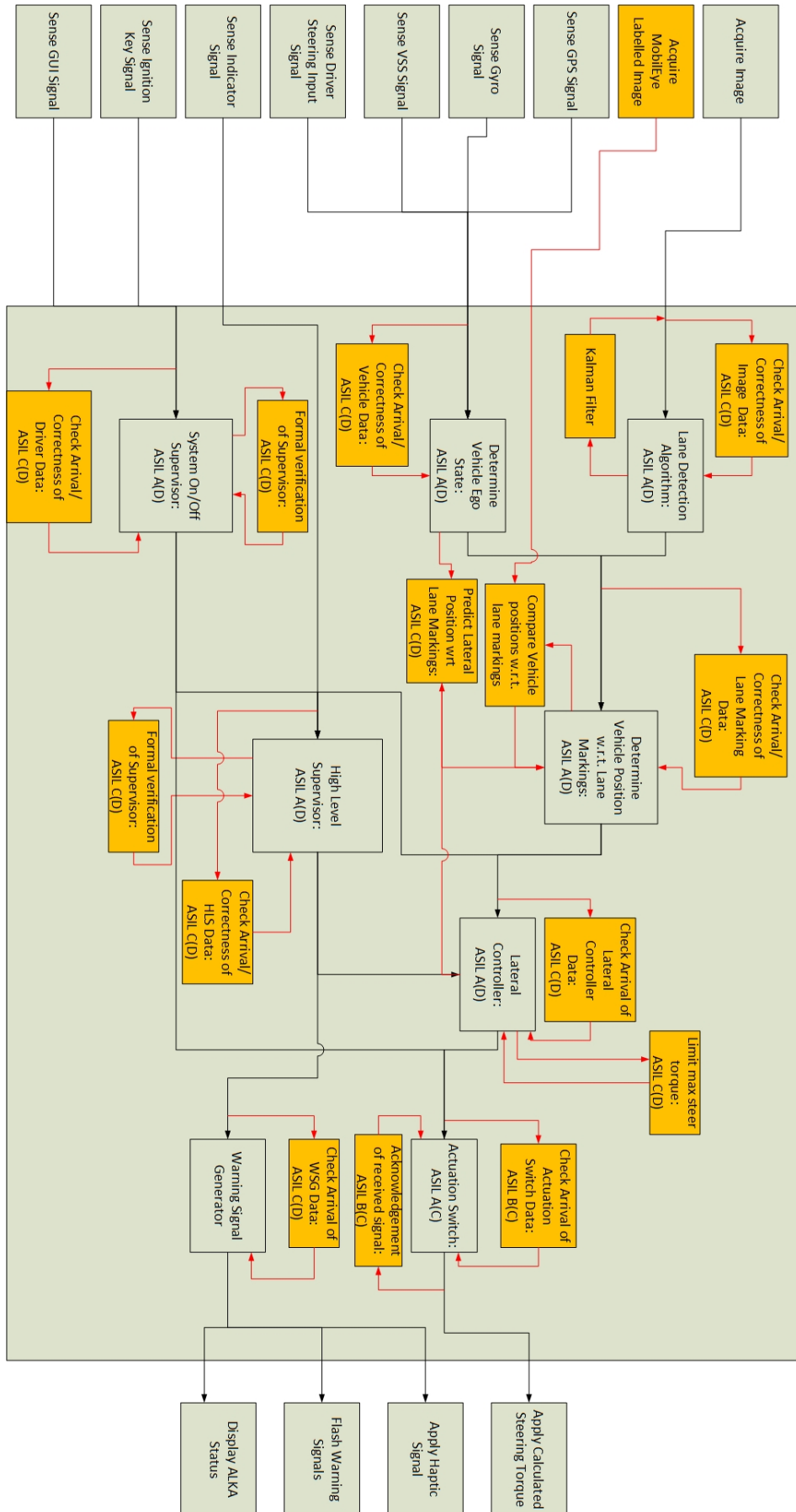


FIGURE E.1: Decomposed Functional Architecture

Appendix F

Appendix F: Benchmarking

TABLE F.1: History of developments in Lane Departure systems

Company	Year	Remarks: Lane Departure Systems
Mitsubishi	1992	Began offering a camera-assisted lane-keeping support system.
Nissan	2001	Began offering a camera-assisted lane-keeping support system.
	2004	Toyota added Lane Keeping Assist feature to the Crown Majesta which can apply a small counter-steering force to aid in keeping the vehicle in its lane.
Honda	2003	Launched its Lane Keep Assist System. Provides up to 80% of steering torque to keep the car in its lane on the highway.
	2015	Lane Keeping Assist System (LKAS)* works proactively at speeds over 45 MPH to help keep the vehicle centered inside a detected lane by providing steering torque so long as there is no turn signal activated. As the vehicle moves from the center of the lane, the EPS applies torque to return the vehicle to the middle of the lane. The farther it gets from the center, the more torque is applied. The Lane Keeping Assist System is not a substitute for steering the vehicle. The driver must keep their hands on the wheel for the system to operate.
Infiniti FX	2004	A warning tone is triggered to alert the driver when the vehicle begins to drift over the markings.
	2007	Introduced Lane Departure Prevention (LDP) system. This feature utilizes the vehicle stability control system to help assist the driver maintain lane position by applying gentle brake pressure on the appropriate wheels.
	2014-17	Available fly-by-wire (Direct Adaptive Steering) autonomous steering, lane keeping (Lane Assist), (Intelligent Cruise control)adaptive cruise control, and Predictive Forward Collision Warning system.
Citroën	2005	First in Europe to offer LDWS. A vibration mechanism in the seat alerts the driver of deviation.
Lexus	2006	Introduced a multi-mode Lane Keeping Assist system on the LS 460. This system can issue an audiovisual warning and also using EPS, steer the vehicle to hold its lane. It also applies counter-steering torque to help ensure the driver does not over-correct or "saw" the steering wheel while attempting to return the vehicle to its proper lane. If the radar cruise control system is engaged, the Lane Keep function works to help reduce the driver's steering-input burden by providing steering torque; however, the driver must remain active or the system will deactivate.

Audi	2007	Began offering its Audi Lane Assist feature in Q7. Will not intervene in actual driving; rather, it will vibrate the steering wheel if the vehicle appears to be exiting its lane.
	2016	Semi-autonomous traffic assistant marketed as "Traffic Jam Assist" offered as an option.
GM	2008	Introduced Lane Departure Warning on its 2008 model-year Cadillac STS, DTS and Buick Lucerne models. Warns the driver with an audible tone and a warning indicator on the dashboard. (core technology from Mobileye).
BMW	2008	Introduced Lane Departure Warning on the 5 series and 6 series, using a vibrating steering wheel to warn the driver of unintended departures. (core technology from Mobileye).
	2013	Updated the system with Traffic Jam Assistant appearing first on the redesigned X5, this system works below 25 mph.
Volvo	2008	Introduced the Lane Departure Warning system and the Driver Alert Control on its 2008 model-year S80, the V70 and XC70 executive cars. (core technology from Mobileye).
	2015	Part of the Pilot Assist II system. The system is active up to 81mph and steers, brakes and accelerates the car on its own without needing a car which to follow. The driver is required to confirm his presence in regular intervals for the system to stay active.
M.Benz	2009	Began offering a Lane Keeping Assist function on the new E-class. System warns the driver (with a steering-wheel vibration) if it appears the vehicle is beginning to leave its lane.
	2013	Mercedes began DISTRONIC Plus with Steering Assist and Stop and Go Pilot on the redesigned S-class in 2013.
	2015	Autonomous steering, lane keeping, adaptive cruise control, parking, and accident avoidance. Semi-autonomous traffic assistant for speeds up to 37 miles per hour.
Kia Motors	2010	Offered the 2011 Cadenza premium sedan with an optional Lane Departure Warning System (LDWS) in limited markets.
Tesla	2014	Combines automatic lane change (after signal is applied), adaptive cruise control, and sign recognition to regulate speed and location.
	2015	Part of the autopilot system released in 2015. This combines automatic lane change (after signal is applied), adaptive cruise control, and sign recognition to regulate speed and location.
VW	2015	Part of the driver assistance pack plus in the new VW Passat B8. It contains a traffic jam assist which is active up to 37 miles per hour. This system steers, brakes and accelerates. Another part is the emergency assist which takes complete control over the vehicle when the driver does not react anymore. The vehicle is brought autonomously to a complete stop without any driver intervention.
Ford	2013	Minimum speed requirement : 40 mph (64 km/h). Works as long as it detects one lane marking. When aid mode on, system detects no steering activity for a short period of time and alerts. In aid mode, system provides assistance steering torque input towards the lane center.

Appendix G

Appendix G: Controllability justification

In this appendix the controllability assignment of the HARA will be justified by means of calculations. The main aim is to calculate the available reaction time and compare it with the reaction time of an average driver. A lower controllability level can be assigned to a HARA when there is enough time for the driver to react to insufficient steering of the system. A cornering vehicle and the corresponding malfunctioning trajectory is shown in Fig. G.1. For this trajectory it is assumed that system does not work correctly and the system fails to control the vehicle such that it continues in a straight line. It is assumed that the vehicle is located at the center between the lines when entering the corner. Applying Pythagoras theorem to Fig. G.1 yields:

$$x = \sqrt{(R_{min} + \frac{1}{2}w_{lane})^2 - R_{min}^2} \quad (G.1)$$

In this equation, R_{min} equals the minimum radius for which it is assumed that the system needs to work. This value equals 250 m according to [companion]. The parameter w_{lane} is the minimum lane width for which it is assumed that the system needs to work and equals 3.0 m [UNECE]. The resulting parameter x is the longitudinal distance to the point where the vehicle exits the lane. The available time to react t can then be calculated with:

$$t = x/v_x \quad (G.2)$$

The longitudinal velocity of the ego vehicle is represented by the parameter v_x . For a maximum longitudinal velocity of 36.1 m/s (130 k/h), it can be found that the available time to react equals 0.8 s. The reaction time of an average driver equals 0.3 m [], so it can be assumed that an operating velocity of 130 k/h the driver is capable to react before the vehicle exits the lane marking.

The above scenario represents the worst case scenarios in which the vehicle can be operated. The UNECE (United Nations Economic Commission for Europe) agreed on some strict rules regarding the international road network in [UNECE]. In this directive the UNECE sets minimum limits on the corner radii for roads with different design speeds. The corresponding available time to react for these roads have been calculated and are shown in Table G.1. It can be concluded from Table G.1 that for normal operating conditions, the driver has enough time available to react to a malfunctioning of the system.

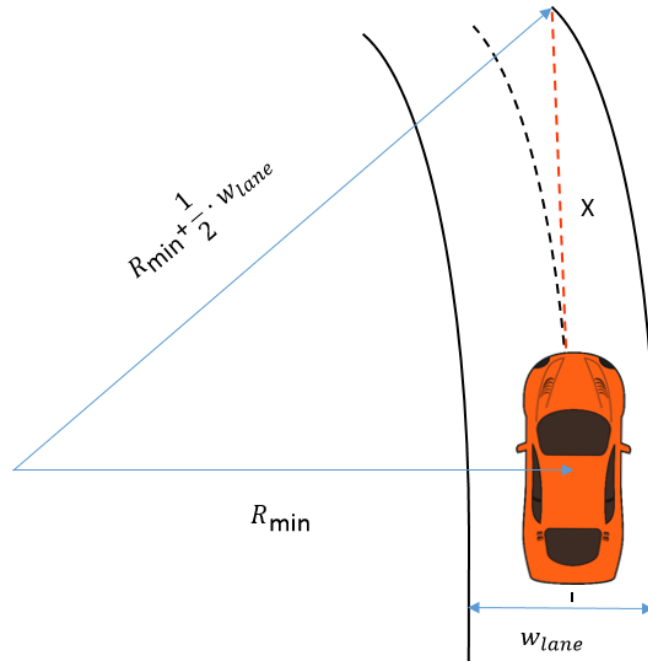


FIGURE G.1: Vehicle trajectory during malfunctioning ALC

TABLE G.1: Time to react to insufficient steering for UNECE approved international roads with different design speeds

	$R_{min} = 120 \text{ m}$ $v_x = 60 \text{ k/h}$	$R_{min} = 240 \text{ m}$ $v_x = 80 \text{ k/h}$	$R_{min} = 450 \text{ m}$ $v_x = 100 \text{ k/h}$	$R_{min} = 650 \text{ m}$ $v_x = 120 \text{ k/h}$	$R_{min} = 1000 \text{ m}$ $v_x = 140 \text{ k/h}$
$t \text{ [s]}$	1.14	1.21	1.32	1.33	1.41

For the straight line driving scenario, the maximum lateral velocity of the vehicle needs to be used. According to [], the maximum lateral drifting velocity of the system equals 0.8 m/s. It is again assumed that the minimum lane width equals 1.5 m []. Based on these values, the driver has 1.9 s to react before the vehicle exceeds the lane markings for driving on a straight road.

Appendix H

Appendix H: Glossary

1	ALC	: Active Lane Centering
3	LKA	: Lane Keep Assist
	ALKA	: Active Lane Keep Assist
5	LDW	: Lane Departure Warning
	Euro NCAP	: European New Car Assessment Programme
7	ASIL	: Automotive Safety Integrity Level
	FSG	: Functional Safety Goal
9	FSR	: Functional Safety Requirement
	TSR	: Technical Safety Requirement
11	DFSR	: Decomposed Functional Safety Requirement
	HARA	: Hazard Analysis and Risk Assessment
13	FMEA	: Failure Mode Element Analysis
	LSS	: Lateral Support System
15	VUT	: Vehicle Under Test
	HMI	: Human Machine Interaction