POLITECNICO DI TORINO

**Department of Control and Computer Engineering**

**Master's Degree in Mechatronic Engineering**

# Functional Safety Assessment for Advanced Driver Assistance System

**Advisor**
Professor. Massimo Violante

**Candidate**
Rubin Gnaniah

March 2019

# Preface

This master thesis has been carried out at the Department of Control and Computer Engineering (DAUIN)-Politecnico Di Torino, in cooperation with MCA Engineering-Turin.

I want to thank:

Luca and Vincenzo, of MCA Engineering. for providing me this project and for their support and ideas throughout the duration of the thesis.

Professor Massimo Violate, for his support during this master's thesis project as well as his precious guidance and advice.

The City of Turin, its people, climate and its resounding provision and conveniences in my studies, research, work and life.

*"SYSTEM ENGINEERING IS THE ART AND SCIENCE OF CREATING EFFECTIVE SYSTEMS, USING WHOLE SYSTEM, WHOLE LIFE PRINCIPLES."*

*DEREK HITCHINS (1995)*

# Abstract

OEMs of the automobile industry are constantly looking out for ways to incorporate and improve ADAS functionalities into their vehicles. One of the major tasks of OEMs is to derive system and functional safety requirements during the system concept stage of the project, adhering to system engineering concepts and ISO26262.

The purpose of this thesis is to study derivation of system and functional safety requirements for the Advanced Driver Assistance System (ADAS) architecture of the present and future.

***keywords:*** *ISO26262, HARA, functional safety, system engineering, safety analysis, ADAS, concept phase.*

# Contents

# List of Figures

# List of Tables

# 1 Introduction

Vehicle functions are assortment of strategies and requirements adopted by automotive OEMs. These functions are OEMs means to express their unique identity, driving experience and to provide the possibilities for the end users to define their driving experiences.

## 1.1 Automotive Electronics

Automotive electronics controls are the heartbeat of cars since the dawn of this century. They play a key part in designing the vehicle functions and are part of the smooth functioning of the car from the ignition, air-fuel mixture ration, wheel antilock, navigation to complex safety features like crash avoidance alerts and autonomous braking. *Figure 1* shows different *Electronic Control Unit (ECU)* and their network connection.

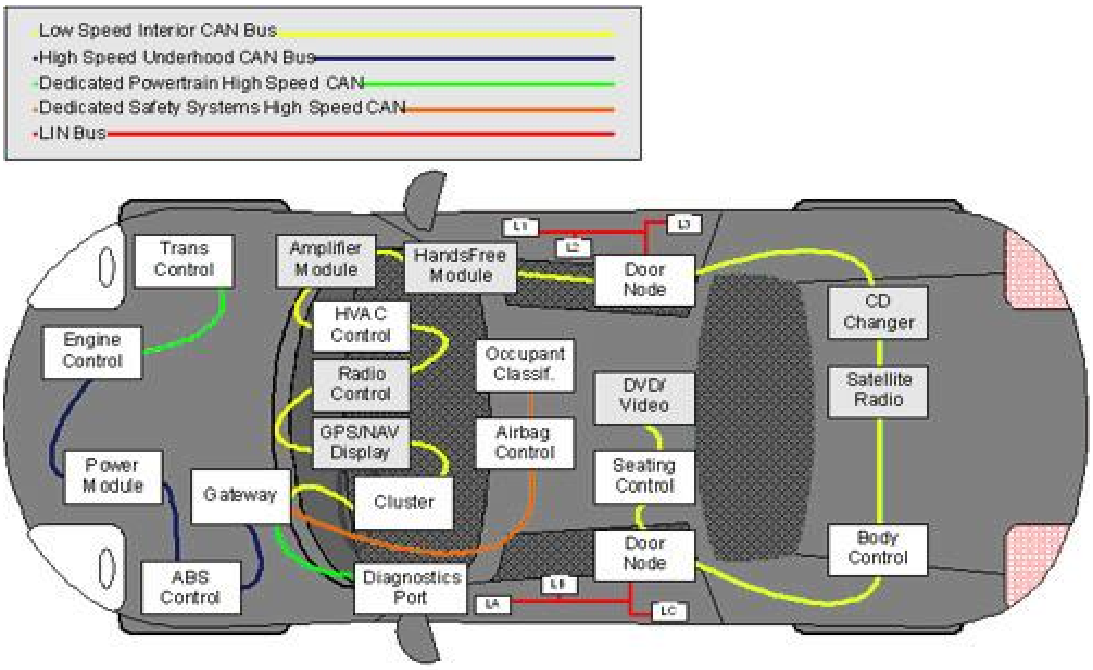


Figure 1 Different ECU's of a modern car, source (FEV 2013)

### 1.1.1 ECU

These complex vehicle functions are realized in ECU. An ECU is embedded system of hardware and software. Cars of recent times have almost up to 80 ECUs, controlling various aspects of the car and assisting the driver. Most of these functionalities need co-operation and information exchange to accomplish their specific task; the need for such information exchange in a structured method is addressed by Multi-Master and Multi-Slave protocol in *CAN*.

The CAN cable runs through the entire vehicle and connects all the ECUs. Some of the ECUs are powered up and run on battery called as *KL30*, while *KL15* which are powered up after the ignition of the engine.

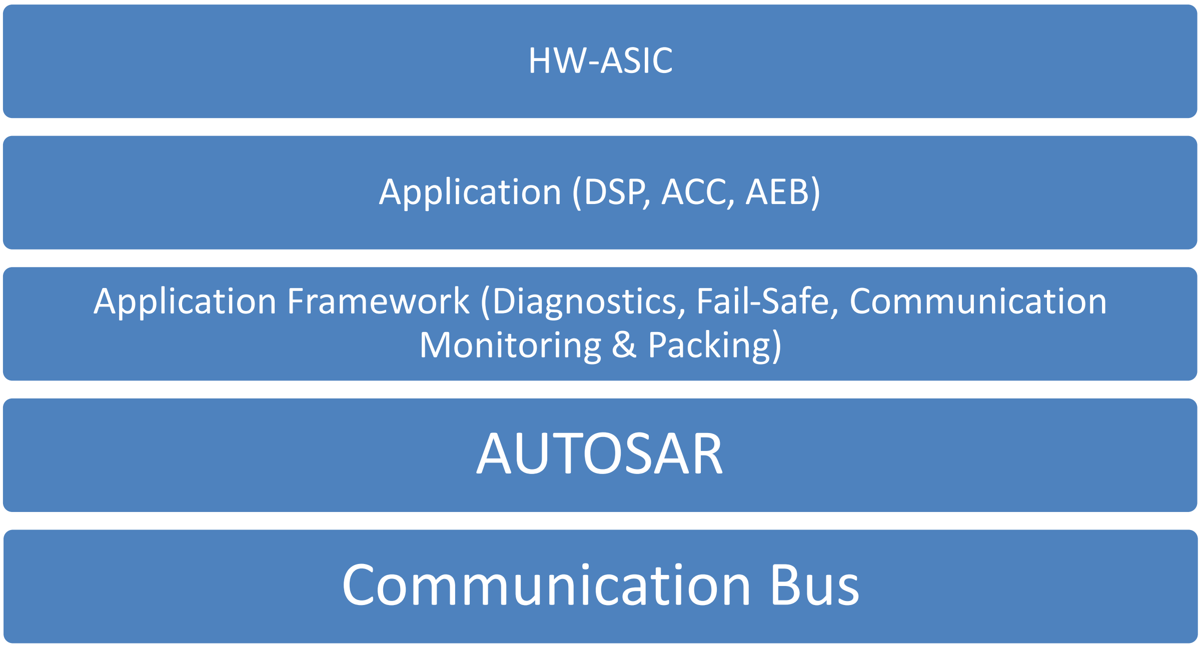

HW-ASIC
Application (DSP, ACC, AEB)
Application Framework (Diagnostics, Fail-Safe, Communication Monitoring & Packing)
AUTOSAR
Communication Bus

**Figure 2 Typical function blocks of an ADAS ECU**

*Figure 2* shows different functional blocks inside an ECU. The flow of information between the blocks is accomplished using *Virtual Data Bus (VDB).* ECU consists of both OEM specific and supplier specific functions.

## 1.2 ADAS Vehicle Functions

Driving is a demanding activity; it needs concentration and swift decision-making with respect to road traffic and environment. Fatigue from other life activities and then driving long hours can lead to decreased road safety. These all began to change with the onset of *Prometheus/Eureka* (PROMETHEUS 1995) funding which began the studies to improve the vehicle safety and reduce the burden on the driver with decision-making. One of these studies is *ARGOS*, which achieved *'Mille Miglia Automatico'* (Broggi, et al. 1999).

The results of *Prometheus* and technological progress in the field of sensing, communication, and information processing has led to the growth of intelligent functions in vehicles (Dr. Azim Eskandarian 2012). These intelligent vehicle functions are part of active safety systems and are categorized as *Advanced Driver Assistance System (ADAS)*. AEBS, ACC, LDW and Blind Spot detection etc. are a few functionalities of ADAS.

A typical ADAS system consists of a sensor or multiple sensors to sense the environment, connected to an ECU that processes the data and communication channels to communicate with other ECUs in the vehicle, thus providing dependable results to assist the driver in the task of driving. The results are presented to the driver as warnings/alerts in audio or visual form through HMI. The HMI also provides the parameters to customize the vehicle behavior based on the desire of the driver.

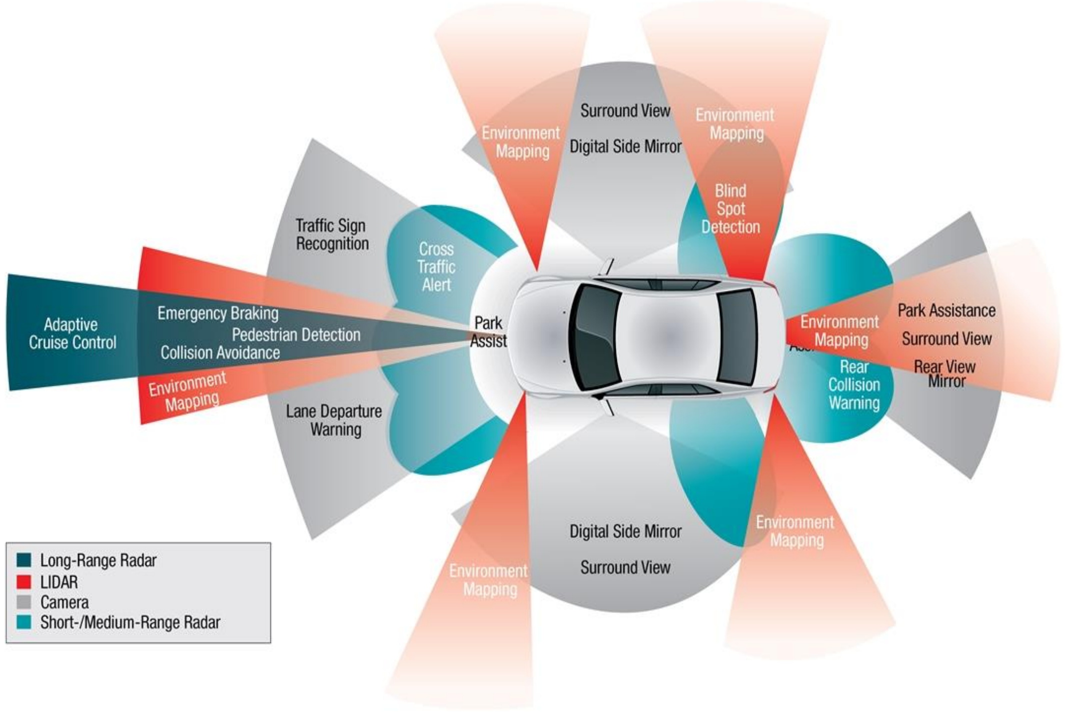


**Figure 3 Various ADAS functions and their sensors, source (SAE 2016)**

*Figure 3* shows the different sensors and their usage for ADAS vehicle function.

### 1.2.1 ADAS SENSORS

The sensors of ADAS provides awareness and perception of the environment; they are of two types:

- *Passive*: measure the radiation emitted or reflected from objects
- *Active*: emit radiation and measure the reflected waves from the objects

The sensors help in recognizing the road participants, their attributes like speed, direction and position and classify the objects as moving (MO), stationary (SO), incoming object or target object etc.

### 1.2.2 Ego Vehicle Model

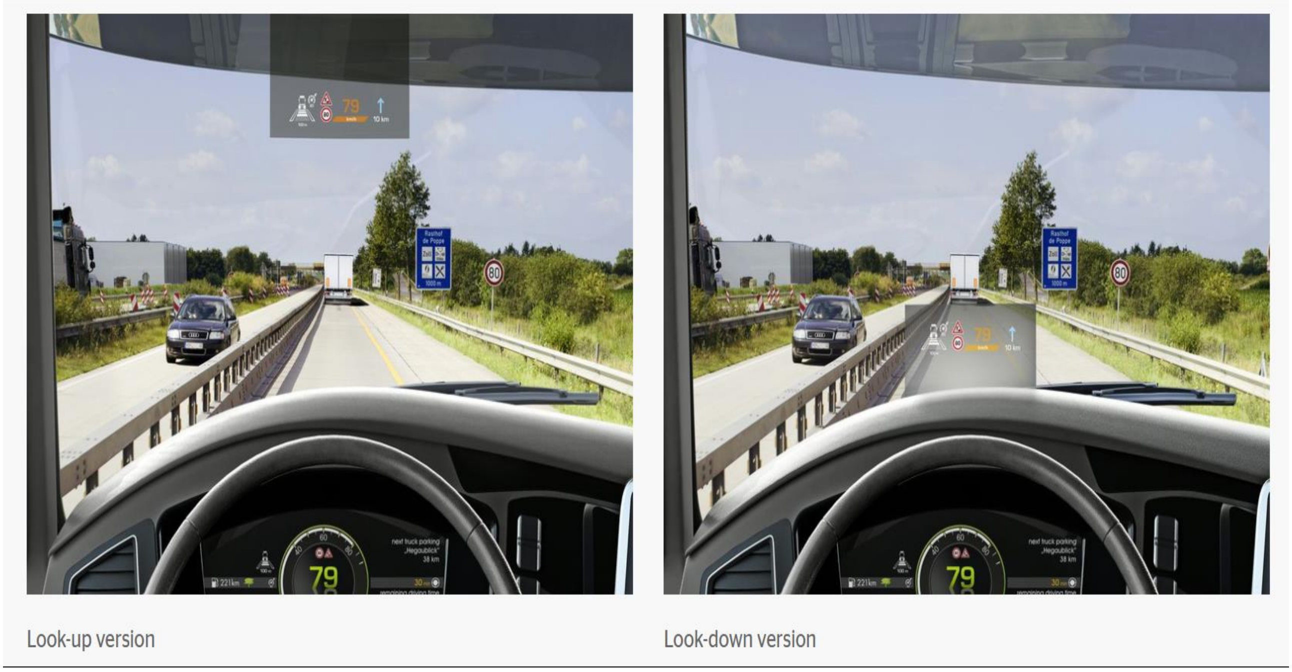
It is the vehicle with ADAS features and is part of the road traffic, following a target object. Along with the information regarding the environment provided by the ADAS sensors, there is a need in the system to understand the current state of the ego vehicle to achieve the driver's assistance function. The ego vehicle model helps in situation analysis, object classification, object detection and in deactivating the ADAS functionalities. *Table 1* describes some of the basic information needed to construct the ego vehicle model.

| Information | Uses |
|---|---|
| **Steering angle** | Steering input request by the driver |
| **Yawrate** | Curve calculation |
| **Acceleration** | Vehicle speed |
| **Brake pressure** | Brake request |
| **Brake stop light** | Visual warning to road users |
| **Wheel speed** | Vehicle speed and curve calculation |
| **Turn lights** | Driver intentions |
| **ESP activation** | To override AEBS |
| **Seat belt** | AEBS enabling |

**Table 1 Ego vehicle model construction**

### 1.2.3 User Interface

Functions like AEBS progress in multiple stages, for example starting with a warning until full intervention to mitigate the collision. During each individual stage, the driver will be displayed the status of the ADAS system and its action. This is achieved by ECU-HMI clusters. Care must be taken not to confuse the driver or divert their attention from the driving task when the indications and alerts are provided. HUD displays the alerts of functions on the windshield and keeps the attention of the driver on the road ahead.



Look-up version

Look-down version

Figure 4 Heads up display, source (Continental 2014)

## 1.3 Thesis Organization

The work presented is divided into the following sections:

*System Engineering*: guidelines for system engineers to incorporate system safety and methodology during system conception.

*System Safety Analysis*: overview of system safety analysis methods like FTA, FMEA and PHA and their applicability in the automotive industry, particularly in the context of the ISO26262

Definition of the *Usecase,* the need for it and a brief overview of the template created by MCA Engineering.

*ADAS:* a study of technology driven conceptualization of partial automation.

*Safety Life Cycle with ISO26262:* case study, incorporating functional safety (ISO26262) into the system requirements during the concept stage.

# 2 System Engineering

> "SYSTEMS ENGINEER FOCUSES THE PERSPECTIVE
> ON THE TOTAL SYSTEM, MAKING DECISIONS BASED ON THE IMPACTS AND CAPABILITIES
> OF THE SYSTEM AS A WHOLE."
>
> (Alexander, et al. 2011)

System engineering uses technical approach that simplifies the system design, operation and validation (Alexander, et al. 2011).

## 2.1 System

The system is a group of interacting entities working together to accomplish a task. The task could be accomplished by one or more systems. A system can be a sub-set (subsystem) of a larger system. The so-called larger system is referred as the *System of Systems* (Alexander, et al. 2011).

### 2.1.1 System Parameters

The system properties are based on their functions and behavior, and are expressed in the following parameters (Alexander, et al. 2011):

#### 2.1.1.1 Functions

Each system acts on three different units such as *Information, Material and Energy* (Alexander, et al. 2011)*.* System functions provide a decisive modification in some characteristics of these units to accomplish any task (Alexander, et al. 2011).

#### 2.1.1.2 Functional Elements

The system functions can be broken down into many functional elements also known as elementary functions (Alexander, et al. 2011).

Functional elements can perform actions such as processing data and transferring the processed signal to control the system (Alexander, et al. 2011). Any system can be visualized by using the functional elements and their interconnection (Alexander, et al. 2011). This is a useful asset to a system engineer for the design and analysis of any system.

### 2.1.1.3 Components

The functional elements are realized through multiple components which can be hardware (mechanical, electrical, pneumatic etc..), software or combinations of both (Alexander, et al. 2011).

### 2.1.1.4 Environment

The system environment is defined as everything outside of the system that is to be designed or analyzed. The interaction of system with the environment is of prime importance if the task to be accomplished involves multiple systems. System environment is defined by in the following parameters (Alexander, et al. 2011):

#### 2.1.1.4.1 Boundaries

The selection of system boundaries can be done based on *operational control, functional allocation, interfaces and purpose* of the system in multiple systems (Alexander, et al. 2011).

#### 2.1.1.4.2 Context Diagram

The system boundaries can be perfected by considering the system as a *black box* and can be accomplished with using the *context diagram*. Context diagrams are characterized by *external entities (Environment)* and their *interaction depicting the interface* (Alexander, et al. 2011).

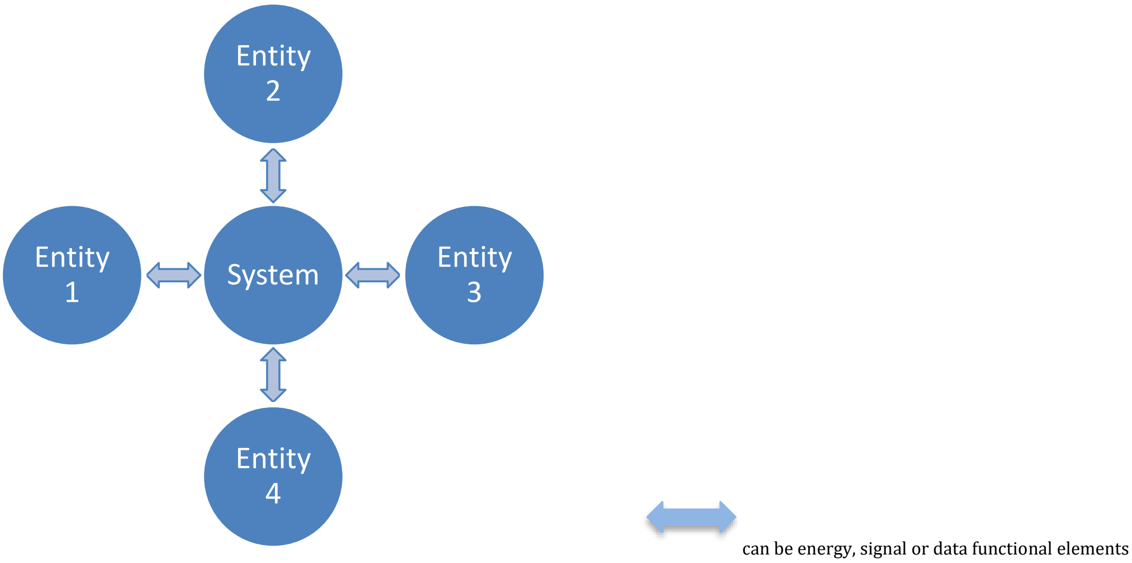


**Figure 5 Context diagram, based on (Alexander, et al. 2011)**

The context diagram in *Figure 5* gives out a pictorial description of inputs, outputs and system boundaries; it provides design depiction during the concept stage (Alexander, et al. 2011).

#### 2.1.1.4.3 Types of Interaction

The *primary interaction* is described as a direct functional interaction i.e. with elementary functions such as signals, data and energy, while the *secondary interaction* involves indirect functional interaction such as ambient temperature, rain etc., (Alexander, et al. 2011) and their effect on the system.

Interactions happen through interfaces and are of two types (Alexander, et al. 2011):

- *internal interaction*: occurring between two entities within the system
- *external interaction*: occurring outside the boundary of the system with different entities

## 2.1.2 System Life Cycle

The system life cycle provides a detailed action guide plan throughout the product evolution from the concept stage to its disposal. There are many models like the *Department of Defense (DoD) Acquisition Management model, International model ISO/IEC 15288* and the *National Society of Professional Engineers (NSPE) model* (Alexander, et al. 2011). The focus here will be more on the individual stages involved in the system engineering practice rather than the models.

### 2.1.2.1 Stage 1: Concept Stage

The need for a new system to accomplish a task is identified and a feasibility study is done at this stage. The stage consists of *Need Analysis, Concept Exploration & Concept definition* (Alexander, et al. 2011) (Belvoir Defence Acquisation 2001).

#### 2.1.2.1.1 Need Analysis

The need for a new system could be either based on commercial needs or technological improvements; the need for such a system is analyzed based on market, current system limitation and customer feedbacks. It is then translated into operational objectives which are realized with preliminary functions. It is also important to define the need for the system in an operational environment, which is the operational requirement for the system (Alexander, et al. 2011).

#### 2.1.2.1.2 Concept Exploration

The operational requirements and the preliminary functions are translated into system performance requirements. This is done by refining functions to fulfill operational requirements. Several viable functional concept which can carry out the functions are defined and the different functional concepts are analyzed for performance requirements (Alexander, et al. 2011).

#### 2.1.2.1.3 Concept Definition

The level of details in function definition is further extended to functional component blocks. Functional simulation provides a precise system performance measurement of all the defined concepts. Based on the project risk, cost and time, a suitable system configuration is nominated for realization and the chosen configuration is analyzed for dependability attributes like *reliability, maintainability, serviceability and safety* (Dubrova 2013). These are the system requirements and it is further expressed in architectural aspects using SysML (Alexander, et al. 2011).

### 2.1.2.2 Other Stages

Stages 2-5 include *development & test, production, operation* and *disposal* (Ericson II 2005) respectively. The scope of this study is about the concept phase and its safety-oriented approach.

## 2.1.3 Dependability

The *faults* in the system mature into *errors*, propagate beyond the system boundaries and manifest into *failures*. Failures affect the dependability of the system (Dubrova 2013). *Fault tolerance* is the design of the system which enables to perform correctly in the presence of faults; it is one of the means through which dependability of the system can be ensured (Dubrova 2013). Tolerance is achieved using redundancy in hardware, software, information and time (Dubrova 2013). The redundancy allows faults to be detected, localized, masked and contained within the system (Dubrova 2013). This allows the system to either recover to full operation, state called *fail operational*, or shut down some components and continue its partial operation in a degraded state called *fail safe*.

For example, if the cluster ECU that is responsible for the user interface *(1.2.3),* detects a fault inside its functions, it sends a diagnostic message to disable ADAS; this is done as there are no other means to communicate the activation and states of the ADAS function to the driver. The system is thus in fail-safe while the driver can still operate the vehicle without ADAS. Some OEMs might restrict vehicle speed so that the vehicle limps to the nearest repair shop.

## 2.1.4 System Safety

System safety is a specialized subset of system engineering that deals with risk management. It is a combination of engineering and management principles techniques made to enhance the safety of the system. The goal is to optimize safety by the identification of related risks and reducing them to an acceptable region, by design and with process procedures (Federal Aviation Administration 2000). The so-called acceptance region of risk is called *Residual Risk*.

System safety is achieved through safety requirements, consistent with function and performance requirements, that must be included in the system design (Federal Aviation Administration 2000).

System safety follows the system life cycle closely; in order to have a design which incorporates safety into the design, the system safety must start at the concept stages of the system life cycle (Ericson II 2005).

### 2.1.4.1 Automotive Life Cycle and Safety Cycle

The automotive industry follows the V-Cycle model *Figure 6* as the system life cycle. The left side of the V features the development of the product, while the right side is responsible for the integration and validation. The safety life cycle is mandated by *ISO26262* in the automotive industry.

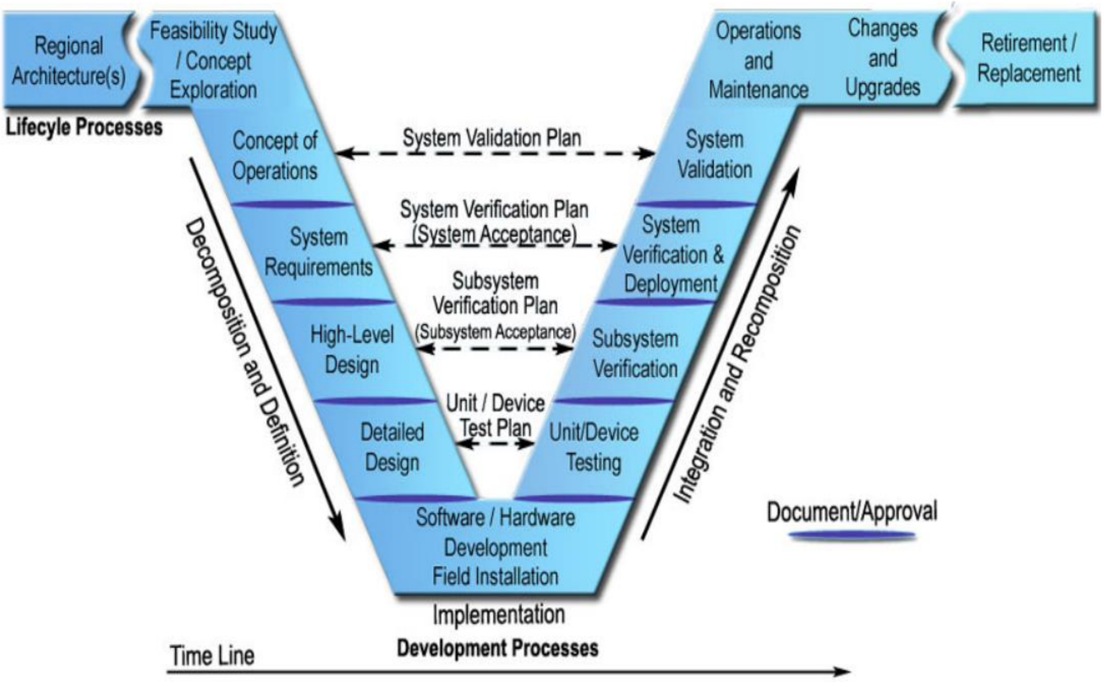


Figure 6 V model for system life cycle process, source (Federal Highway Administration 2007)

The concepts discussed in this section are relevant to the ISO26262 Part 3 work product - Item definition and their requirements.

## 2.2 ISO26262

> *"FUNCTIONAL SAFETY IS THE ABSENCE OF UNREASONABLE RISK DUE TO HAZARDS CAUSED BY MALFUNCTIONING BEHAVIOR OF E/E SYSTEMS." (ISO26262, 2011)*

ISO26262 is the automotive development guide based on *IEC61508*, specifically adapted for E/E architecture in road vehicles. ISO26262 is divided into 10 parts as described in *Table 2*. It deals with passenger vehicles only, with a mass equivalent to 3500 kg. It does not give out the nominal performance requirements of the system (ISO26262, 2011). It is expected that the second edition of the ISO26262 would include strategies for commercial vehicle like truck, bus etc...

| Part | Representation |
|---|---|
| **1** | Vocabulary and definition of terms used in IS026262 |
| **2** | Safety management activities |
| **3** | Concept phase activities to derive safety requirements |
| **4** | Product design: system level, design, integration and validation activities |
| **5** | Product development - hardware level: design, integration, validation and metrics for assessment of faults |
| **6** | Product development - software level: design, integration, validation |
| **7** | Production, operation, decommission, user manuals, field monitoring and service |
| **8** | Supporting process: configuration, change management and management of safety requirements |
| **9** | ASIL decomposition, safety analysis methods |
| **10** | Guidelines: informative section |

Table 2 Chapters overview based on (ISO26262, 2011)

### 2.2.1 Part 1

This part is dedicated to the definition of terms that are commonly used in other parts of the ISO26262. *Table 3* contains only terms relevant to this thesis.

| | **Glossary for ISO26262 Part 1** (ISO26262, 2011) |
|---|---|
| **Item** | The Item is a system or combination of systems, which represents functions at the vehicle level. |
| **Architecture** | Structured description of items, functions, elements and systems along with their interfaces and boundaries. |
| **Assessment** | Inspection of an item and representing its level of confidence in functional safety fulfillment. |
| **ASIL** | Automotive Safety Integrity Levels (ISO26262, 2011); they are QM, A, B, C and D, and are used to represent the risk assessment of an item. |
| **ASIL Decomposition** | Done to reduce the ASIL of an element, by decomposing the safety measures to another element. Care must be taken that there is independence on the partitioned element. |
| **Controllability** | Measure of control over the item during a critical situation to prevent harm from happening, through timely action on the system by the driver or by external measures. |
| **Degradation** | In the presence of active failures, the functionality of the system is reduced so that safety is ensured. The degradation is achieved by system design of hardware, software or the combination of both. |
| **Detected Fault** | The misbehavior of the system is detected through monitoring in software, hardware or the combination of both. |
| **E/E** | Combination of Electrical and Electronic systems. |

**Elements** Components of a system.

**Exposure** Item with active faults, operating in a situation which could be hazardous.

**External Measure** Design of safety in an item which mitigates some of the risks of the item under consideration. The measure is present outside the boundary of the item considered.

**Failure** The inability of the item to perform its intended task.

**Failure Mode** The ways in which the item can fail.

**Fault** The condition that makes the item to fail.

**Fault Reaction Time** The time between the detection and to bring the system to a safe state

**Fault Tolerance Time** The maximum time that the system can be dependable from the occurrence of a fault.

**Functional Safety** Safety-related requirements, that must be implemented in addition to the system's nominal requirements.

**Functional Concept** Specification of the item's functions to be implemented along with their interactions, boundaries and environment involved to respect the safety goal.

| | |
|---|---|
| **Harm** | Injury or damage to an item, human or property. |
| **Hazard** | Source of harm. |
| **HARA** | Hazard Analysis Risk Assessment, a methodology through which an item’s risk is studied through a hazardous event and ranked with ASIL. |
| **Hazardous Event** | Combination of hazard and operational situation. |
| **Operating Mode** | Possible functional state of the item during its operational time. |
| **Risk** | Combination of severity and occurrence of the harm. |
| **Safe State** | One of the operational states of the item, in which the behavior of the item is without any unintended risk. The item’s functionality could be in a degraded state. |
| **Safety** | Item’s ability to operate in a dependable manner, without any risk in all situation. |
| **Severity** | Amount of harm to a person or property. |

**Table 3 Glossary based on (ISO26262, 2011)**

### 2.2.2 Part 3

This part deals with the analysis of the system at its conception. The goal of this stage is to introduce system safety measures into the system design. System design requirements are responsible for the nominal performance of the system.

ISO26262 provides several clauses, most of them being binding requirements to system's concept definition (ISO26262, 2011).

#### 2.2.2.1 Clause 5.4.1

The item's definition shall be defined in this stage (ISO26262, 2011), specifying:

- Purpose, functionality, operating modes and states of the item.
- Standards relevant for the functions of the item and working constraints like the off-road, the region [EU, NA, JPN].
- Pre-existing knowledge related to the elements that are under design to achieve the functionality.
- Assumptions regarding the item or elements under consideration.
- Known failure modes and faults.

#### 2.2.2.2 Clause 5.4.2

The item's boundary shall be defined in this stage (ISO26262, 2011), specifying:

- Elements of the item, that are identified by using functional decomposition and functional allocation to the individual blocks.
- Type of information exchanged through the interfaces.
- Type of Interfaces.
- Functionality that the interfaces accomplish outside the item's boundary and its consequences.
- Functionality that is needed by the item outside the boundary to achieve its intended specifications.
- Function allocation that is achieved by different elements of the item.
- Common operational scenarios where the item is used in its life time.

#### 2.2.2.3 Clause 6

Once the item's definition and its boundaries are established, initiation of the safety cycle begins. At this stage, the item is checked to establish whether it is a new development or a modification of an existing item. If it is a modification of an existing item, an impact analysis is done, and HARA is carried out based on the impact analysis. If it is a new item, the entire item specifications are considered for HARA (ISO26262, 2011).

### 2.2.2.4 Clause 7: HARA

HARA is used for the determination of item's safety goals, the objective being that an unreasonable risk is avoided. This is done by assigning ASIL to hazardous events. The ASIL is the combination of *severity, probability of exposure* and *controllability* (ISO26262, 2011).

The steps in HARA are:

- Situation analysis
- Hazard identification
- Classification of hazardous events

#### 2.2.2.4.1 Clause 7.4.2.1: Situational Analysis

It is the definition of item's operational situations; it shall be as generic as possible and within the limits of the item. However, the reasonably foreseen misuse by the driver shall be considered (ISO26262, 2011).

#### 2.2.2.4.2 Clause 7.4.2.2: Hazard Identification

The hazard identification shall be expressed based on observable behavior at the vehicle level. ISO26262 does not give out any recommendation on the analysis technique in the identification of the hazards. HAZOP, Functional Failure Analysis are the traditional choices for hazard identification. However, in the thesis the analysis will be carried out on a modified version of STPA for the concept stage (ISO26262, 2011).

#### 2.2.2.4.3 Clause 7.4.2.3: Hazardous Events

Hazardous events are the consequence of hazards occurring in the worst possible situation during the item's operational situation. The consequence of each individual hazardous event and possible control mechanism available to the driver to avoid hazardous event shall be defined (ISO26262, 2011).

#### 2.2.2.4.4 Clause 7.4.3: Classification of Hazardous Events

Based on the consequences of the hazardous events, each event is classified based on the parameters S, E & C (ISO26262, 2011). A rational/ assumption must be provided for the assignment of S, E & C levels. These rational provide justification and the reasoning behind the classification of hazardous events.

#### 2.2.2.4.4.1 Clause 7.4.3.2: Severity

Severity is classified into S0, S1, S2 and S3 levels where S0 corresponds to no injuries and S3 corresponds to life threatening injuries (ISO26262, 2011).

| Severity Ranks | S0 | S1 | S2 | S3 |
|---|---|---|---|---|
| Injuries Ranks | No injuries | Light injury | Severe Injury | Severe, survival uncertain |

Table 4 Severity table based on (ISO26262, 2011)

#### 2.2.2.4.4.2 Clause 7.4.3.3: Exposure

Exposure of the item in the chosen situation is classified into E0, E1, E3 and E4, based on its likeliness (ISO26262, 2011).

| Exposure Ranks | E0 | E1 | E2 | E3 | E3 |
|---|---|---|---|---|---|
| Prospect Ranks | Not likely | Very less likely | Less likely | Likely | Highly likely |

Table 5 Exposure table based on (ISO26262, 2011)

#### 2.2.2.4.4.3 Clause 7.4.3.7: Controllability

Controllability is classified into C0, C1, C2 and C3 levels (ISO26262, 2011).

| Controllability Ranks | C0 | C1 | C2 | C3 |
|---|---|---|---|---|
| Classification ranks | Controllable overall | Typically controllable | Usually controllable | Uncontrollable |

Table 6 Controllability table based on (ISO26262, 2011)

#### 2.2.2.4.4.4 Parametrization Of S, E & C

S, E and C shall be parameterized based on *Table 4, Table 5, Table 6*. The parametrization makes the HARA process of determining ASIL scientific and reliable. The argument of parametrization using ruleset and its practices are explained in detail by (Khastgir, et al. 2017).

The argument provided by (Khastgir, et al. 2017) is that subjective interpretation of the allocation of S, E and C to individual hazardous events is based on the knowledge of the system. If there is a lack of understanding of the item under analysis, it could lead to an exaggeration of risk which in turn would result in increased ASIL or in the worst case, undermine the risk of hazardous event, which defeats the purpose of HARA (Khastgir, et al. 2017).

### 2.2.2.4.5 Clause 7.4.4.1: Determination of ASIL

ASIL for each hazardous event shall be determined based on *Table 7*.

| **Severity S** | **Exposure E** | **Controllability** | | |
|---|---|---|---|---|
| | | **C1** | **C2** | **C3** |
| **S1** | E1 | QM | QM | QM |
| | E2 | QM | QM | QM |
| | E3 | QM | QM | A |
| | E4 | QM | A | B |
| **S1** | E1 | QM | QM | QM |
| | E2 | QM | QM | A |
| | E3 | QM | A | B |
| | E4 | A | B | C |
| **S1** | E1 | QM | QM | A |
| | E2 | QM | A | B |
| | E3 | A | B | C |
| | E4 | B | C | D |

**Table 7 ASIL determination guide based on (ISO26262, 2011)**

ASIL is a combination *Figure 7* of probability of exposure of the vehicle to an operational situation, the degree of controllability available to the driver to avoid the hazardous event and severity is the degree of injury due to hazardous event.

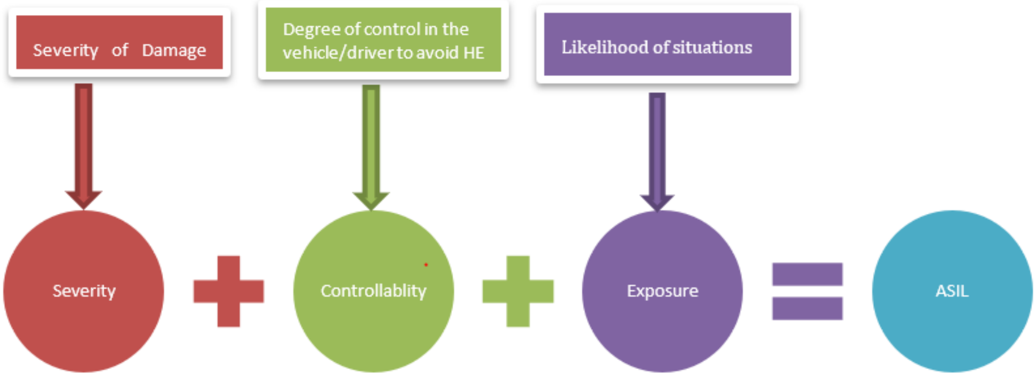


Figure 7 S, C and E based on ISO26262

### 2.2.2.5 Clause 7.4.4.3: Determination of Safety Goals

Each hazardous event with ASIL shall be assigned with safety goals. If similar safety goals are determined, they are combined into a single safety goal. Hazardous events with the highest ASIL will take precedence over others if the safety goals are similar (ISO26262, 2011)

Safety goals can have information's related to transition to a safe state, fault tolerance time and specifying the maximum/minimum physical characteristics of the items (ISO26262, 2011).

The safety goals are the objective assigned to the item, the item shall have strategies so that the safety goals are not violated.

### 2.2.2.6 Clause 8: Functional Safety Concept

The objective is to derive functional safety requirements based on the safety goals. Each safety goal shall have one or more functional safety requirements. Functional safety concepts are derived by specific failure mechanism. In functional safety concepts the functional safety requirement is allocated to the logical functional components of preliminary architecture. The allocation can be within or outside the item's boundary. Allocation to outside the boundary is defined as external measure (ISO26262, 2011). *The Figure* 8 shows the process of safety goals and functional safety derivation.

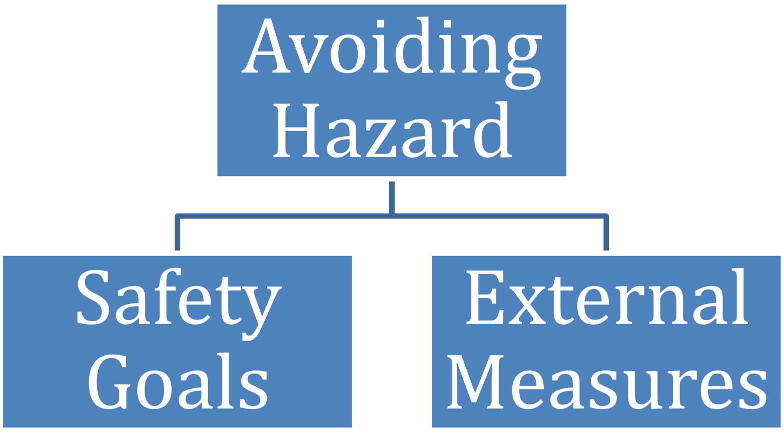


Figure 8 Safety through External measure based on (ISO26262, 2011)

The basic focus of functional safety is the risk reduction, risk is the combination of the probability of occurrence of harm and the severity of that harm (ISO26262, 2011)

The reduction by reducing the occurrence of harm by including safety measures is studied in this thesis.

ASIL is the estimation in effort/cost that is needed in the risk reduction to bring the risk to acceptable level, hence if a risk is ranked highly by a conservative approach the item might end up having more than needed safety and increased cost.

### 2.2.3 Methodology

The activities in *Part 3* are summarized into the following methodology:

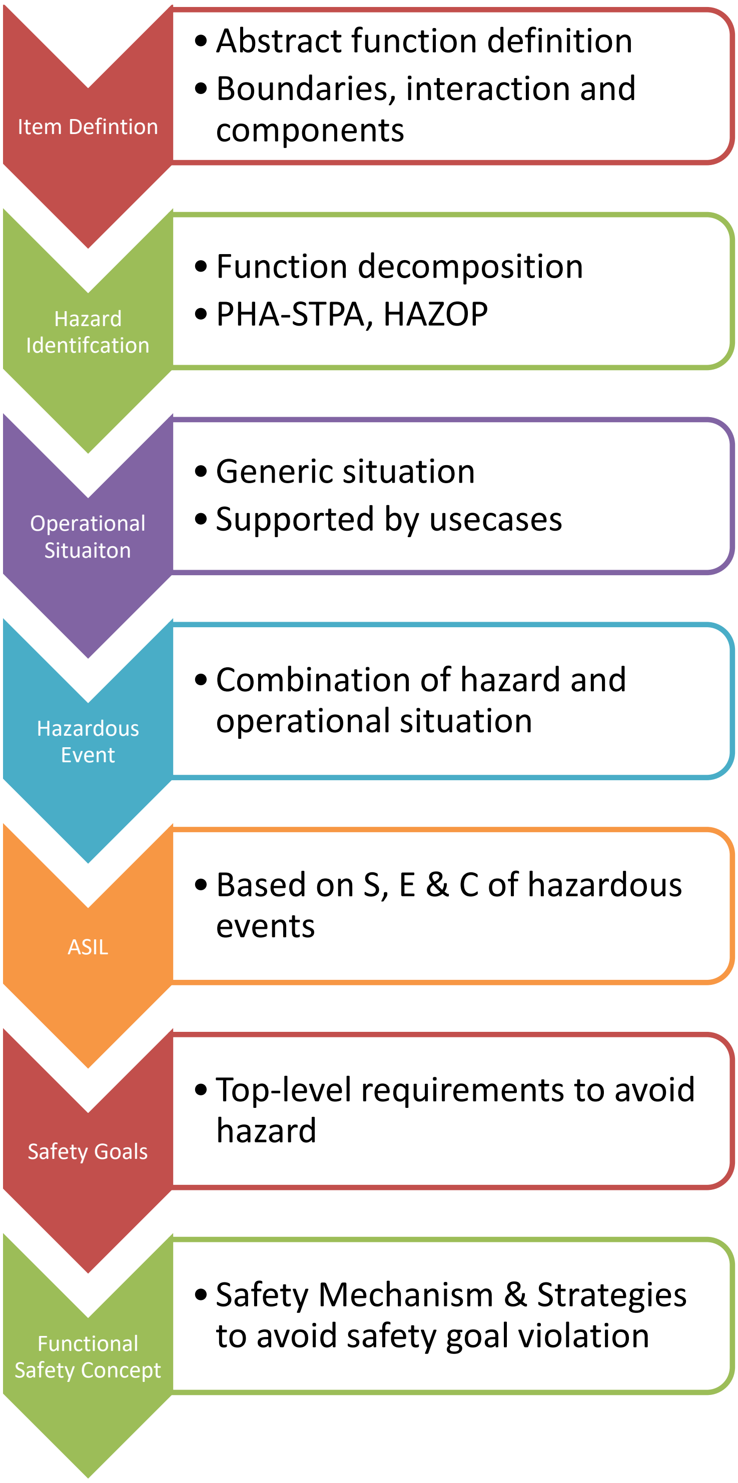
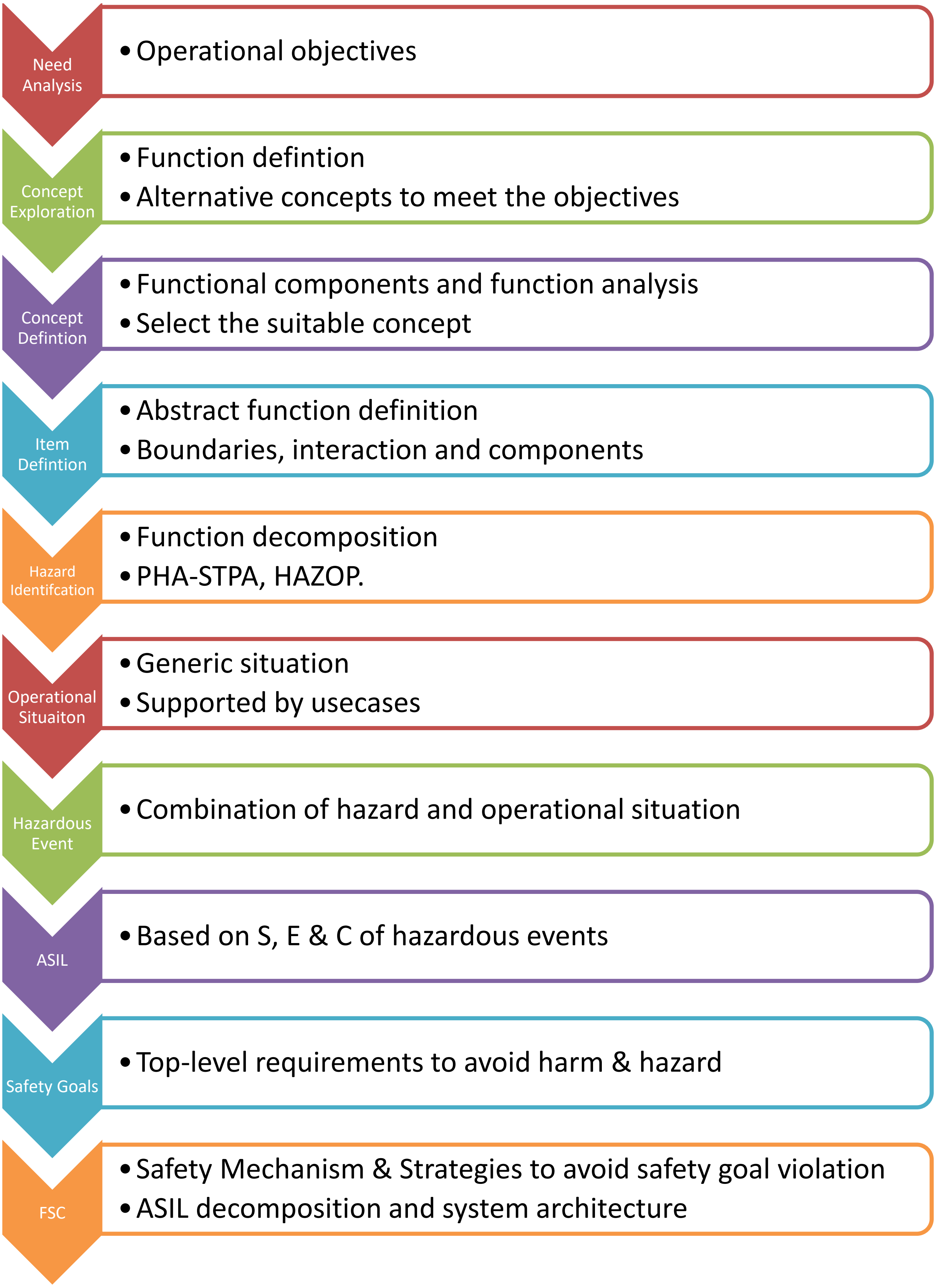

Item Defintion
Abstract function definition
Boundaries, interaction and components
Hazard Identifcation
Function decomposition
PHA-STPA, HAZOP
Operational Situaiton
Generic situation
Supported by usecases
Hazardous Event
Combination of hazard and operational situation
ASIL
Based on S, E & C of hazardous events
Safety Goals
Top-level requirements to avoid hazard
Functional Safety Concept
Safety Mechanism & Strategies to avoid safety goal violation

Figure 9 ISO26262 Concept phase methodology, based on (ISO26262, 2011)

## 2.3 System and Safety Life Cycle for the Concept Phase



Need Analysis
- Operational objectives

Concept Exploration
- Function defintion
- Alternative concepts to meet the objectives

Concept Defintion
- Functional components and function analysis
- Select the suitable concept

Item Defintion
- Abstract function definition
- Boundaries, interaction and components

Hazard Identifcation
- Function decomposition
- PHA-STPA, HAZOP.

Operational Situaiton
- Generic situation
- Supported by usecases

Hazardous Event
- Combination of hazard and operational situation

ASIL
- Based on S, E & C of hazardous events

Safety Goals
- Top-level requirements to avoid harm & hazard

FSC
- Safety Mechanism & Strategies to avoid safety goal violation
- ASIL decomposition and system architecture

Figure 10 Derived system engineering and safety life cycle methodology, based on (ISO26262, 2011), (Alexander, et al. 2011)

# 3 System Safety Analysis

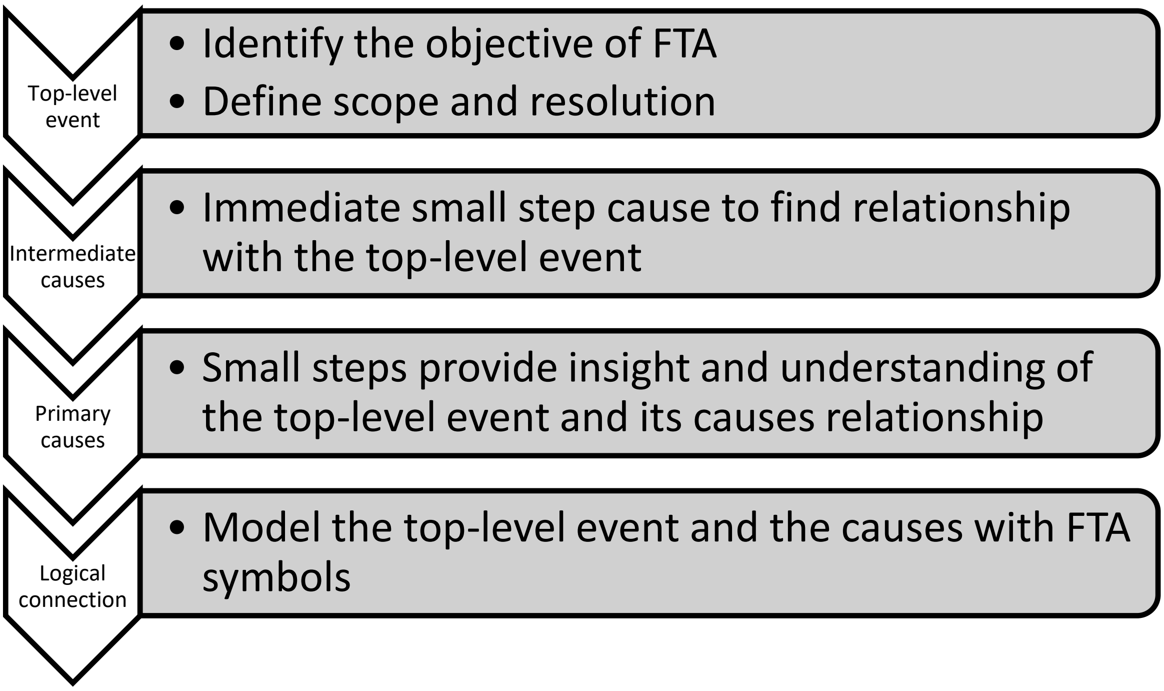
System analysis is a methodical technique used to gather information about a system. The information gained can be used in making decisions and improving the system design and its requirements (Vesely, et al. 1981). It can also be used to find out hazard in the design and enhance overall safety (Ericson II 2005).

There are two main approaches: *Inductive* and *Deductive methods*. Inductive methods are used to determine what are the failed system states, while the deductive methods are useful to find out how the system failure occurred (Vesely, et al. 1981).

## 3.1 FTA

FTA is a graphical deductive technique in which a top-level event/failure of the system is analyzed with respect to its operation and the causes that could lead to such failure (Stamatelatos, et al. 2002) (Vesely, et al. 1981).

### 3.1.1 Construction of FTA



- Identify the objective of FTA
- Define scope and resolution

- Immediate small step cause to find relationship with the top-level event

- Small steps provide insight and understanding of the top-level event and its causes relationship

- Model the top-level event and the causes with FTA symbols

Figure 11 Construction of FTA, based on (Stamatis 2003) (Vesely, et al. 1981)

### 3.1.2 Failure Effect, Mode and Mechanism

The top event describes the failure mode of the system. The failure to meet the system's success criteria is the top-level event (Stamatelatos, et al. 2002).

- *Failure Effect* - Effect of failure on the system
- *Failure Mode* - Likely means for the failure to occur
- *Failure Mechanisms* - causes behind the failure modes

| Failure Effect | Failure Mode | Failure Mechanism |
|---|---|---|
| **No AEB warning** | HMI malfunction | • CAN bus off<br>• HUD failure |
| | No deacceleration request | • Target object detection failure<br>• Radar misaligned<br>• Wrong object distance<br>• Communication failure |

Table 8 Failure - Effect, Mode, Mechanism

Each intermediate step in the construction of FTA is a failure mechanism (Stamatelatos, et al. 2002).

## 3.2 FMEA

FMEA provides a methodical mode of investigating all the behaviors in which a failure can happen. FMEA can help understand and provide counteractive actions required to prevent failures in the design. FMEA is categorized into *design, system, process* and *service* (Stamatis 2003).

FTA complements FMEA, helping in visualizing the analysis and providing potential failure effect and mechanism.

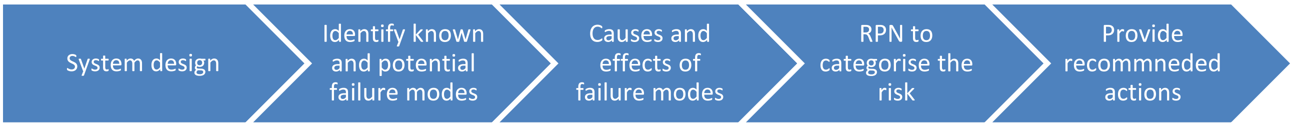

System design
Identify known and potential failure modes
Causes and effects of failure modes
RPN to categorise the risk
Provide recommneded actions

Figure 12 FMEA Process based on (Stamatis 2003)

### 3.2.1 Risk Priority Criteria

Risk Priority Criteria can be calculated by *Qualitative, Quantitative* and *Ranking* methods (Stamatis 2003). The ranking method will be used in the later stages; in this method, the priority is observed through RPN, which is the product of OSD. The ranking of OSD is done by assigning numbers from 1to10. If the RPN values are higher than a defined threshold value, then these failures are addressed through design changes. It is also common in the automotive world to focus on failures with high severity (Stamatis 2003).

- *Occurrence (O)* - frequency of the failure
- *Severity (S)* - effects of the failure
- *Detection (D)* - ability to detect the failure

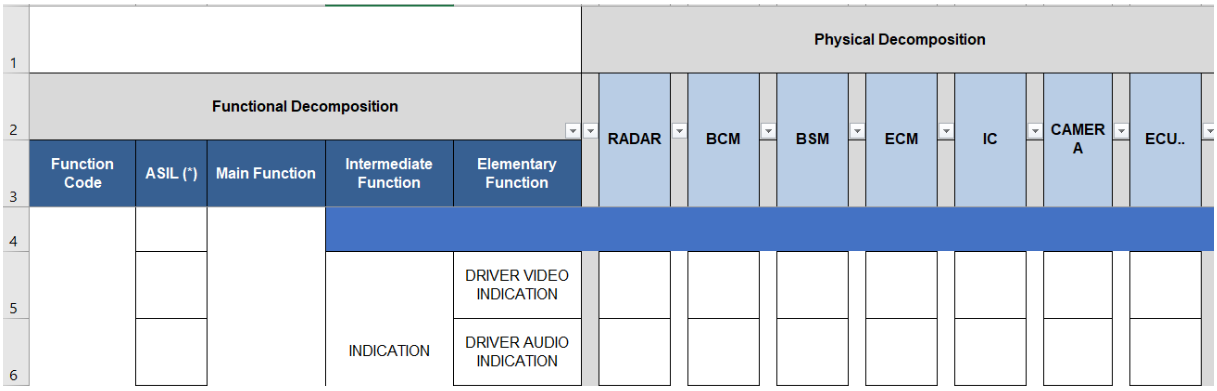
RPN helps in narrowing down the risk to be addressed as there could be many risks in the system design.

### 3.2.2 FMEA Document

FMEA is maintained in the FMEA sheet and is used throughout the life cycle of the system at various stages; it is composed of two matrices.

#### 3.2.2.1 Correlation matrix

The correlation matrix provides the dependency and interaction between the item's function and other systems external to the boundaries of the item. This helps visualize the failure modes effect of the item on the entire system.



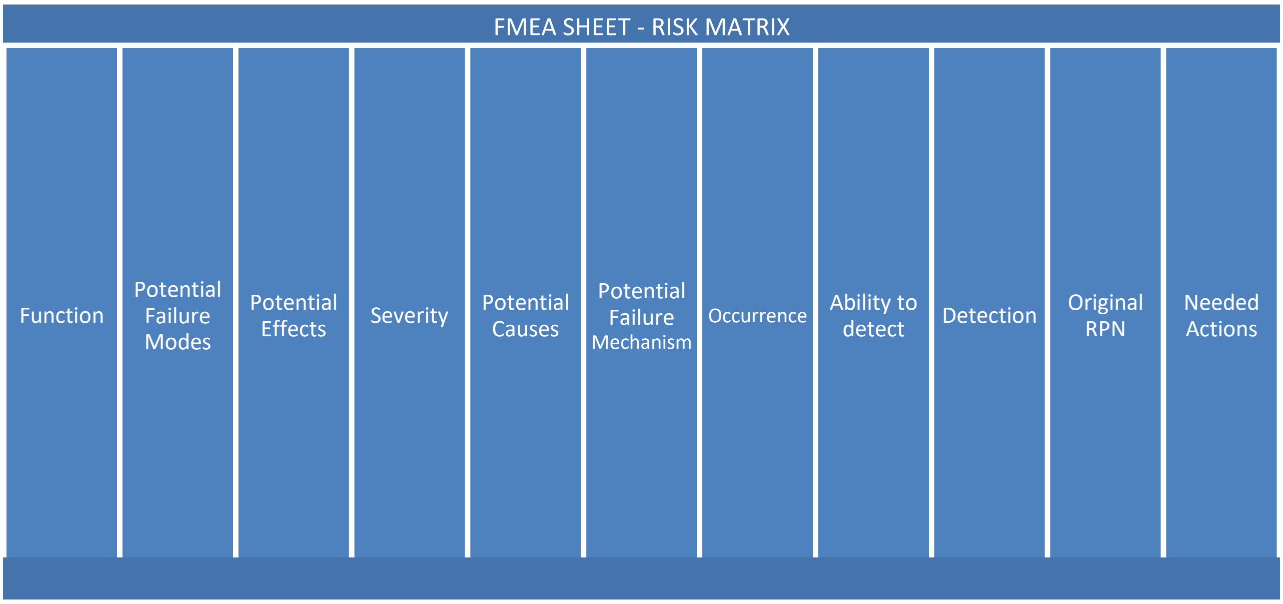
| | | | | | Physical Decomposition | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Functional Decomposition | | | | | RADAR | BCM | BSM | ECM | IC | CAMER A | ECU.. |
| Function Code | ASIL (*) | Main Function | Intermediate Function | Elementary Function | | | | | | | |
| | | | | | | | | | | | |
| | | | INDICATION | DRIVER VIDEO INDICATION | | | | | | | |
| | | | | DRIVER AUDIO INDICATION | | | | | | | |

Figure 13 Correlations matrix - MCA Engineering

The function decomposition in *Figure 13* is done to the elementary level to simplify the analysis and provide better resolution to the analysis.

Physical decomposition provides the correlation between the functions and their interaction with the rest of the system.

### 3.2.2.2 Risk Matrix



FMEA SHEET - RISK MATRIX

| Function | Potential Failure Modes | Potential Effects | Severity | Potential Causes | Potential Failure Mechanism | Occurrence | Ability to detect | Detection | Original RPN | Needed Actions |
|---|---|---|---|---|---|---|---|---|---|---|

**Figure 14 Basic FMEA Sheet – MCA Engineering**

The different columns of the risk matrix in *Figure 14* is described as follows:

- *Item/Function* – Specifies the purpose of the item or the function being analyzed
- *Potential failure modes* – List of possible failure modes, obtained using historical data and experience
- *Potential effects of failure* – Effects of the failure mode on the system
- *Severity (S)* – Severity of the effect of the failure
- *Potential causes of failure* – Use FTA to find the intermediate causes
- *Potential mechanisms of failure* – Use FTA to find the mechanisms of the failure
- *Occurrence (O)* – Number of times the failure modes can occur, based on historical data
- *Current design controls* – Ability to detect the failures with the detection mechanism that is currently available in the design
- *Detection (D)* – Effectiveness of the current detection mechanism to detect the failures
- *Recommended action* – Proposed method to reduce the level of RPN and improve the design through requirements and design changes

## 3.3 PHA

PHA stands for Preliminary Hazard Analysis; PHA is the risk analysis of a system during the concept stages of the design (Rausand 2013). It is used for recognizing hazards, causal factors and risks when there is no comprehensive design evidence (Ericson II 2005).

There are many ways of accomplishing PHA. In the automotive sector, especially at the concept phase of a new design, HAZOP is widely used and other traditional methods like concept FMEA and FTA can also be adopted for PHA analysis. In this thesis, a control theory-based approach proposed by (Leveson and Thomas 2013) called STPA is adopted to the concept phase analysis of hazards. STPA is recommended by (Hommes 2015) as an alternative to HAZOP in the concept stage analysis.

### 3.3.1 STPA

STPA stands for *System Theoretic Process Analysis* and is a top-down system level analysis (Hommes 2015). It provides the causal factors during the early stages of design and their relationship with hazards (Hommes 2015). The relationship, causal factors and hazards are pillars for specifying the safety requirements and their constraints (Hommes 2015).

#### 3.3.1.1 Methodology

The steps in STPA follow the process defined in *Figure 15*

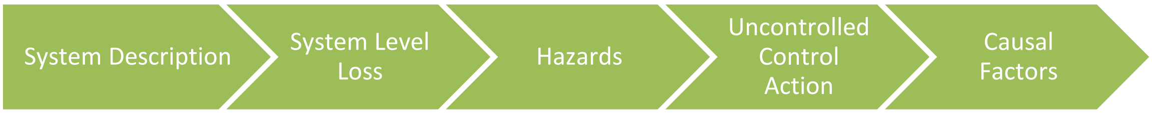


**Figure 15 STPA methodology, Source [John A Volpe National Transportation Systems Center]**

*Table 9* details the steps in STPA, in which *System Description* and *System Level Loss* are an easy adaptation and are derived from the *Concept Definition* while hazard, UCA and causal factors are derived by following further guidelines of STPA.

| Steps | Description |
|---|---|
| **System Description** | Functional description and system context diagram |
| **System Level Loss** | Event that results in loss of life and property |
| **Hazard** | System state, along with a set of worst-case scenarios, that leads to system level loss |
| **Unsafe Control Actions (UCA)** | Commanded by the controller that could lead to the transition of a safe vehicle state to a hazardous state. It is found out using 6 keywords |
| **Causal Factors** | Failures of actuators of the controlled process that can lead to UCA |

**Table 9 STPA steps, based on (Hommes 2015)  John A Volpe National Transportation Systems Center**

### 3.3.1.2 UCA Identification

The UCA identification is done using relevant system states and six words guidelines (Hommes 2015).

The ***guide words (red)*** are shown in *Figure 16*. They represent the hazard types that affect the system states which lead to system level loss.

### 3.3.1.3 Causal factors

Causal factors are the contributors to the UCA. The relation between hazards types (UCA) and the causal factors are found out using *FTA*. In *Figure 16* the ***causal factors*** are represented in ***violet.***

### 3.3.1.4 Scope & Limitation

Though STPA can provide safety requirements, only steps until causal factors are used extensively for the concept phase hazard analysis.

#### 3.3.1.5 Advantages

The advantages of STPA are the following:

- Incorporates control system theory
- Considers both component failures and system interactions
- Integrates driver-vehicle interface in the overall modeling
- Generates hazards and causal factors that are inputs to safety requirements and constraints

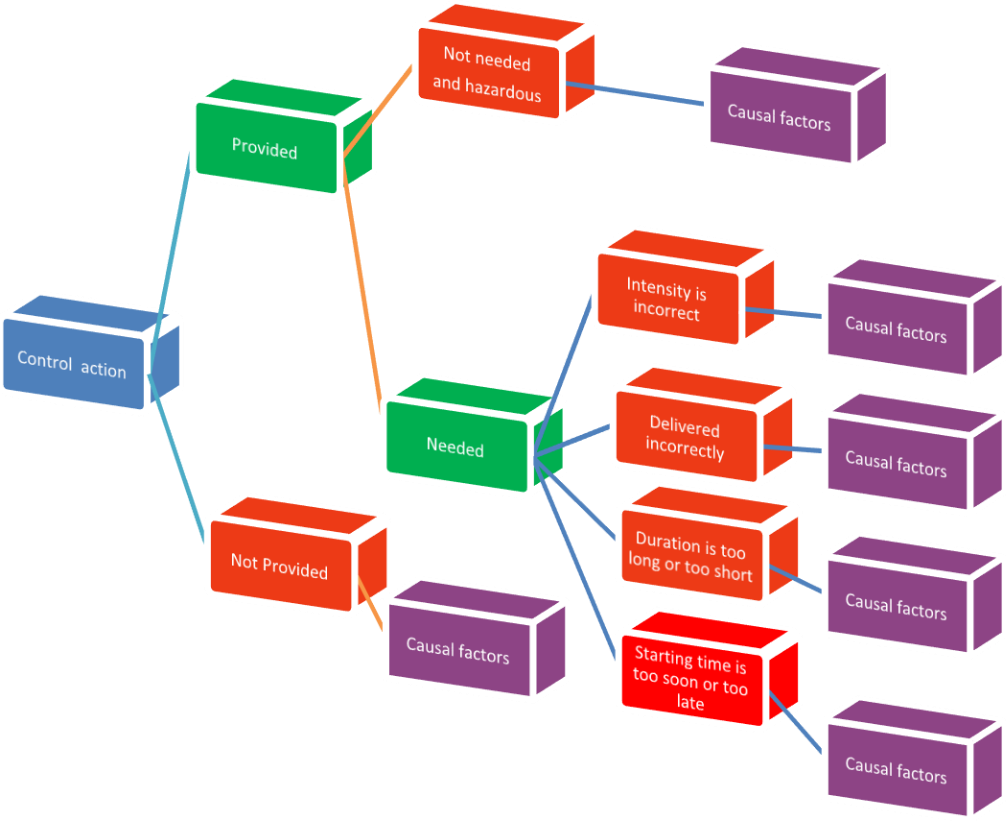


Figure 16 STPA, causal factors relations to hazards and system state

The safety analysis is used in Hazard Identifications, In improving the system requirements, in finding the faults that leads to hazards and also in analyzing if safety goals are violated by unknown hazards that are not considered during HARA.

# 4 Usecase

> *"A usecase is a complete course of events in the system seen from user perspective."*
>
> *Ivar Jacobson*.

Usecase is an essential method for the designer to conceptualize the system's behavior. The usecase defines the system's behavior under several conditions and its response to a request from one of the participants, called the *primary actor* (Cockburn 2000)*.*

## 4.1 Usecase

The primary goals of the usecases according to (Cockburn 2000) is the communication of the system's behavior to other designers and reviewers of the design. Usecases are defined in text form; they can be written using *flow charts, sequence charts, petri nets* and *programming languages* (Cockburn 2000).

The basic elements that are needed to define a usecase according to (Cockburn 2000) are:

- *Primary actor*
- *Scope*
- *Precondition & guarantees*
- *Stakeholder*
- *Main success scenario*
- *Extensions*

In (Cockburn 2000), the author further develops a template for usecases which is suited for generic applications.

## 4.2 Usecase by MCA

The idea and goal from (Cockburn 2000) is used behind *MCA Engineering*'s usecase definition. The adopted usecase template is focused on automotive applications tuned towards ADAS system development. Usecases offer a brief interpretation of what the system will do. The usecase captures the system level functional goals in a text-based modelling technique, that can be later refined and designed using modelling procedures.

Care must be taken when defining the operation requirement and in its refinement. The thumb rule is to define the requirement in terms of where and what, rather than defining the requirements in terms of how, to avoid design solutions.

*Table 10* gives the MCA equivalence of the template designed by (Cockburn 2000).

| Elements | Description | MCA Equivalence |
|---|---|---|
| **Context of use** | Goal of the use case | Functionality |
| **Scope** | Black box of the system | Functionality, objective |
| **Level** | Sub-functions involved | Functionality, objective |
| **Primary actor** | Description of the user | Actors and relations |
| **Stakeholders & Interest** | List of stakeholders and key interests in the use case | Actors and relations |
| **Precondition** | State of the system | Scenario, situation |
| **Minimal Guarantees** | Least expected goal of system | Desired behavior |
| **Success Guarantees** | The state of the environment if goal is achieved | Expected benefits |
| **Trigger** | What starts the usecase, may be a time event | Scenario, situation |
| **Main Success Scenario** | Steps of the scenario from trigger to goal delivery, and any steps after if any | Desired behavior, expected benefits |
| **Extensions** | Progression of main scenario | Situation |

**Table 10 Usecase Template based on (Cockburn 2000)**

*Table 11* gives a description of MCA engineering usecase template for ADAS design.

| | |
|---|---|
| **Usecase Definition** | |
| Description of functionality | Brief description of the functionality. |
| Objective | State here the objective of the system function or the system. |
| Desired behavior | State the intended behavior of the function or system goal. |
| Expected benefits | Positive influence of the design to the driver, road users, environment, traffic, fuel economy and driving pleasure. |
| **Use case description** | |
| Situation | What is happening in the scenario?<br>(insert a picure of the scenario) |
| Actors and relations | *Vehicle control*: manual pilot/autonomous pilot/partial pilot.<br>*Status of functionality*: active/failure/failsafe/not active.<br>*Warning to the driver*: HMI.<br>*Vulnerable road user*: traffic situations and others. |
| Scenario | *What is happening*: preconditions and present conditions.<br>*Road type and description*: slope, curve, autostrada etc.<br>*Weather condition*: snow, fog, rain, sun.<br>*Threat actions*: unexpected situation like lighting, cattle jumping on the road, flat tire. |
| **Use case implementation** | |
| Event | What is happening to the vehicle and what is the driver's state. |
| Functional architecture ID | ID of ADAS architecture. |
| Display / alert principle | Icon of warning and/or action on steering. |
| **Functional requirements** | |
| Messages information | List of involved messages on CAN/function interactions. |
| Standards | ETSI, ISO if it exists. |
| **Additional information** | |
| **Proprietary** | **2019 MCA All rights reserved** |

Table 11 Usecase template by MCA ENGINEERING

# 5 ADAS System Design

The system design of ADAS follows the methodology derived in *Figure 10*. The first activity is to explore the *Need Analysis* for the ADAS system and derive its operational objectives.

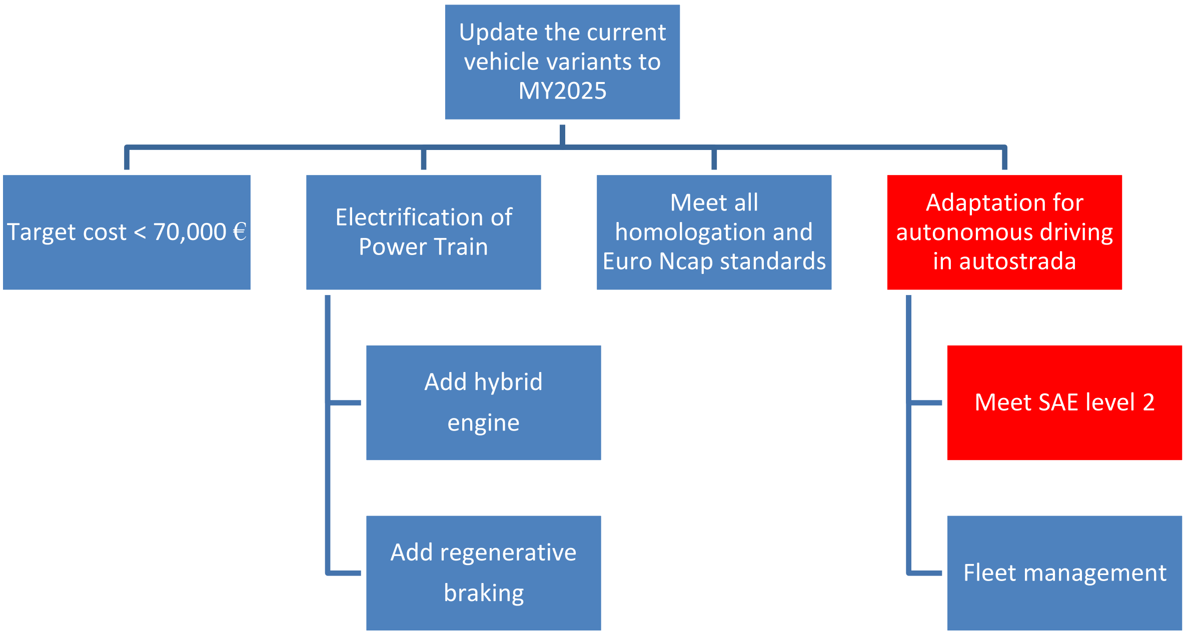

Update the current vehicle variants to MY2025
Target cost < 70,000 €
Electrification of Power Train
Meet all homologation and Euro Ncap standards
Adaptation for autonomous driving in autostrada
Add hybrid engine
Add regenerative braking
Meet SAE level 2
Fleet management

**Figure 17 Objective tree for ADAS system based on (Alexander, et al. 2011)**

## 5.1 Need Analysis

The need analysis model followed is technology oriented. It is based on the need to improve the current fleet with ADAS functions that can increase automation levels to meet the current market trends and users' needs. The need analysis is translated into operational objectives.

The operational objectives are to prepare the current vehicle models for future driving standards; objectives are identified at the organization level. The scope of the system design is the *highlighted objectives* as shown in *Figure 17* , it will be the adaptation for autonomous driving in autostrada.

### 5.1.1 Levels of Automation

It is necessary to understand the different levels of automation that are standardized in the automotive industry. *Table 12* compares *SAE's* levels corresponding to those developed by the *Germany Federal Highway Research Institute (BASt)* and by the *US National Highway Traffic Safety Administration (NHTSA)* (Smith Bryant Walker, Standford 2013).

| **Level** | **Name** | **Narrative definition** | **Execution of steering and acceleration/ deceleration** | **Monitoring of driving environment** | **Fallback performance of *dynamic driving task*** | **System capability (*driving modes*)** | **BASt level** | **NHTSA level** |
|---|---|---|---|---|---|---|---|---|
| ***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 | Driver only | 0 |
| **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 performs all remaining aspects of the dynamic driving task | Human driver and system | Human driver | Human driver | Some driving modes | Assisted | 1 |
| **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* performs all remaining aspects of the *dynamic driving task* | **System** | Human driver | Human driver | Some driving modes | Partially automated | 2 |
| ***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 | Highly automated | 3 |
| **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 | Fully automated | 3/4 |
| **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** | - | |

Table 12 SAE Levels of automation source (Smith Bryant Walker, Standford 2013)

*Table 12* shows the 6 different levels of automation. The description of each levels is translated in terms of ADAS vehicle functions to have a better chance of meeting the operational objectives.

#### 5.1.1.1 Level 0

The driver has the complete responsibility for lateral and longitudinal control of the vehicle. The assistance is in the form of warnings and alerts. It includes *blind spot warning* as well as *collision warning*. The warnings are just an assistance and driver have to be attentive in driving task.

#### 5.1.1.2 Level 1

The system and the driver share the responsibility of the vehicle control. The driver is responsible for control of the vehicle at all times, hands on the steering wheel and eyes on the road. The system performs a few maneuvers for longitudinal or lateral control assistance in specific situations.

Example: warnings for collision and lane departure mitigation system.

#### 5.1.1.3 Level 2

The system takes care of the vehicle control, while the driver does not need to provide steering or actuate the accelerator pedal. However, the expectation is that the driver is readily available to take control of the vehicle when called upon by the system. The driver is also expected to remain seated in their seat and must keep the eye on the environment. The level is the combination of 2 or more ADAS vehicle functions.

Example: longitudinal and lateral control in city/urban.

#### 5.1.1.4 Level 3

The system takes care of the entire vehicle control, the driver can essentially do other tasks and keep their eyes off the environment. When the system calls upon due to an event/failure in the system the driver is expected to take control of the vehicle.

Example: longitudinal and lateral control in city/urban environment and automatic lane change.

#### 5.1.1.5 Level 4 & Level 5

Full automation in which the driver can trust the system to depart from point A to arrival in point B without any intervention needed for driving task.

The operational objective in *Figure 17* is to meet SAE level 2 and must have adaptation for further automation levels, hence a combination of functions that is suitable to reach the objectives are studied in the *5.2.*

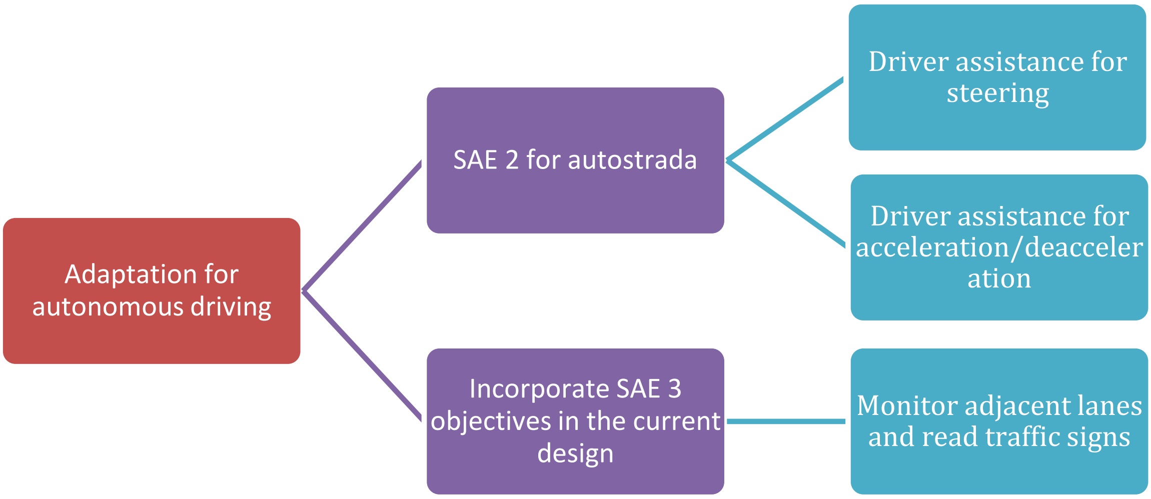

Adaptation for autonomous driving
SAE 2 for autostrada
Incorporate SAE 3 objectives in the current design
Driver assistance for steering
Driver assistance for acceleration/deacceleration
Monitor adjacent lanes and read traffic signs

**Figure 18 Operational objectives and their preliminary functions based on Table 12**

### 5.1.2 Operational Requirements

The operational objectives are translated into primary vehicle functions based on *Table 12*. The functions are driver assistance for steering, acceleration, deacceleration, monitoring of adjacent lanes and reading of traffic signs. The additional functions of monitoring adjacent lanes and reading traffic signs will ease the migration of SAE 2 automation to higher levels of automation *(Level 3, Level 4 & Level 5)* when the need arises.

The need for the system is defined in terms of operational situation. This is done to derive the requirements from operational objectives and assist the system design; the needs for the system in the operational situation are defined through the *Usecase by MCA* template. The operational objective in *Figure 18* is translated into text-based requirements in *Table 13*, which is used for monitoring adjacent lanes. The usecase produced in the need analysis stage is applied in system design, validation and during *HARA*.

Care must be taken not to provide design solutions during the definition of usecase and operational objectives.

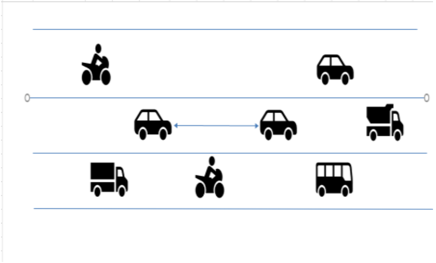
| **Usecase Definition** | |
|---|---|
| Description of functionality | Monitor the presence of vehicles in the adjacent lane |
| Objective | Monitor the presence of vehicles in the adjacent lane in order to assist the driver during lane change maneuver |
| Desired behavior | If the lane is occupied and the driver is doing a lane change with or without indication lights, warn the driver about adjacent lane collision |
| Expected benefits | Side collision is prevented, safety of the traffic and driver is ensured; the expectation is that the driver responds to the warnings and remains in the lane. |
| **Usecase description** | |
| Situation | What is happening in the scenario:<br><br>The adjacent lanes are occupied by a motorbike (left) and truck (right), if the driver of the ego vehicle attempts a lane change without indication light. |
| Actors and relations | *Vehicle control:* the steering wheel is held by the driver<br>*Status of functionality*: active<br>*Warning to the driver*: visual and auditory<br>*Vulnerable road user*: traffic situations and others |
| Scenario | *What is happening*: vehicle is about to do a lane change<br>*Road type and description*: autostrada<br>*Weather condition*: sunny<br>*Threat actions*: not applicable |
| **Usecase implementation** | |
| Event | Vehicle is doing a lane change, with vehicles present in the adjacent lane |
| Functional architecture ID | Not applicable now |
| Display / alert principle | Lamp on the HUD |
| **Functional requirements** | |
| Message information | Not applicable |
| Standards | ISO17387 |
| **Additional information** | |
| **Proprietary** | **2019 MCA All rights reserved** |

Table 13 Usecase for monitoring adjacent lanes

## 5.2 Concept Exploration

In this stage, the focus is now shifted towards finding existing technology to fulfill the operational objectives. Here, the different ADAS functions and sensors are analyzed and their performance characteristics and requirements are summarized.

### 5.2.1 Longitudinal Control

The driver assistance functions for acceleration and deacceleration are categorized as ADAS longitudinal control. The vehicle functions of this type of control include ACC and AEB and driver warning functions like traffic sign recognition and blind spot detection.

#### 5.2.1.1 ACC

ACC controls longitudinal acceleration and deacceleration; it allows the user to ease their foot off the gas pedal. It plays a prominent role in making a vehicle become autonomous, easing the driving burden off the driver.

There are two variants of ACC functions available, the *standard ACC* governed by ISO15622 and *FSRA* governed by ISO22179 (Dr. Azim Eskandarian 2012). The difference between them is the operating speed ranges. The standard ACC hands over the control back to the driver if the speed is below the threshold defined by ISO15622. The focus will be more towards the standard ACC as it can be designed for specific speed ranges. If the speed ranges chosen suits the highway driving, this can meet the operation objectives described in *Figure 18*.

##### 5.2.1.1.1 Operations

The OEMs usually provide means to activate the ACC using the toggle switch in the steering, to define the ACC speed, also known as the *set speed*, and the *time gap* that is to be maintained between the ego vehicle and the target vehicle. Based on the operation scenarios in *Figure 19*, the ACC operation can be summarized as follows:

- *Scenario 1*: the vehicle maintains the set speed when there is no traffic ahead.
- *Scenario 2*: it encounters a slower vehicle, based on the *time gap* in distance, the speed of the vehicle is reduced to match the slower vehicle (deacceleration).
- *Scenario 3*: once the slower vehicle is cleared out of its way, the vehicle is accelerated to its set speed.
- *User-action*: the driver can take control of the vehicle and overtake the slower traffic, hands on steering wheel, to deactivate press the brake pedal.

During *scenario 1*, the ACC is in speed control mode and request controlling torque on CAN to the engine control unit. ACC is in distance control in *scenario 2* and requests the deacceleration to the braking system. ACC is in standby mode during the user-actions.

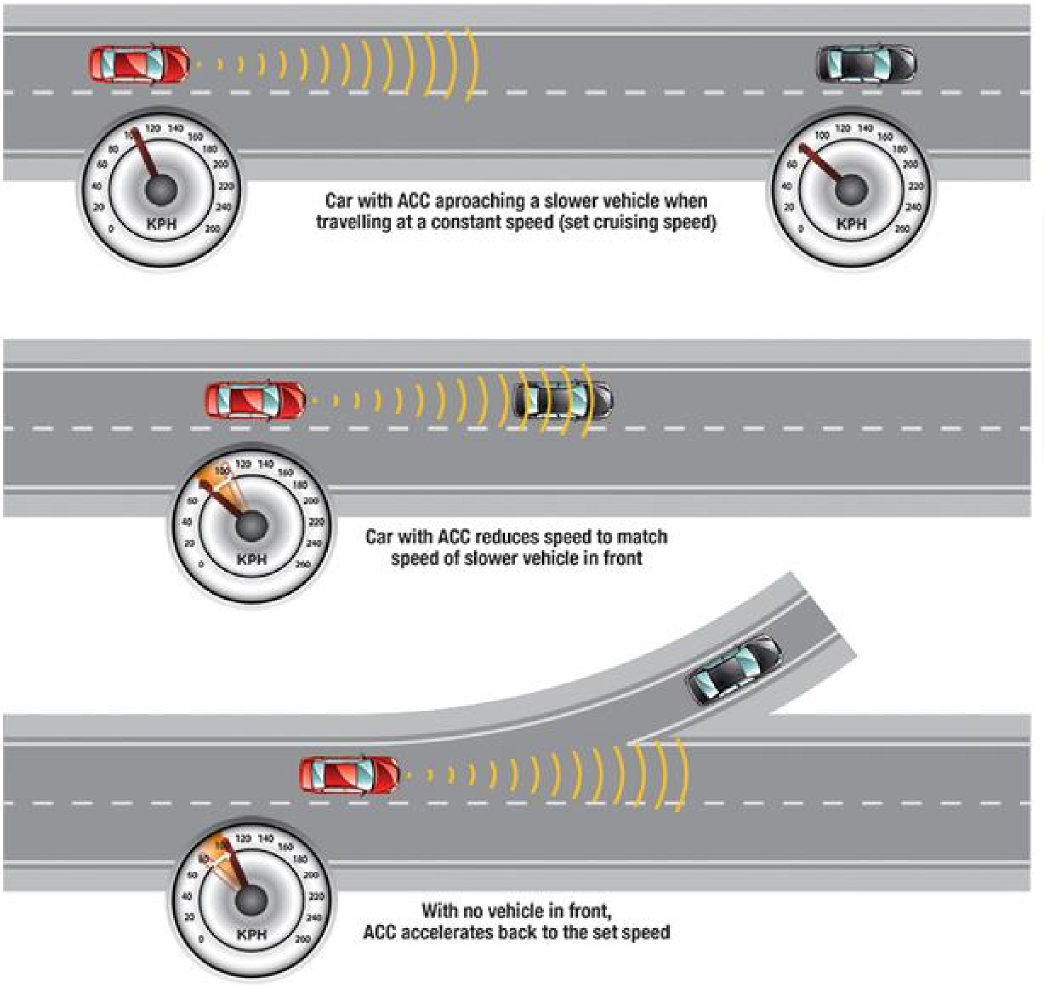

KPH
Car with ACC aproaching a slower vehicle when travelling at a constant speed (set cruising speed)
KPH
KPH
Car with ACC reduces speed to match speed of slower vehicle in front
KPH
With no vehicle in front, ACC accelerates back to the set speed

Figure 19 ACC operating principle, source (Transport Canada 2013)

### 5.2.1.1.2 Functional Parameters

The parameters that define the ACC operations are listed in *Table 14*. These parameters are useful when looking for alternative technologies in designing the system and to simulate their performance. An ACC system needs one or more sensors to identify, classify and follow the target object. A passive sensor in addition to an active sensor will make ACC robust. The sensor is mounted in the front of the vehicle.

| Parameter | Description |
|---|---|
| **User setting** | ACC set speed (min. 30 km/h) and time gap (1 s, 2 s, 3 s, min. 1 s. ISO5622 specifies min. 0.8 s to max 3.2 s) |
| **User intervention** | Priority to user intervention with deactivation during braking, override when using steering control and acceleration. Handover: During system failure and when the speed is lower than defined |
| **Binding parameters** | Longitudinal acceleration: max. -3.5 m/$s^2$ to 2 m/$s^2$ , lateral: 2 m/$s^2$ |
| **Deactivation** | Engine speed idle, invalid gear, parking break active, stability control failure and door status etc. |
| **Object distance** | Definition of sensor maximum and minimum detection capabilities (typical lengths needed are between 10 m to 100 m) |
| **Relative velocity** | Object classification based on the direction of movement, hence the sensor characteristic should be in such a way that there is no error in measurement |
| **Detection range** | Longitudinal: appropriate detection corridor such that only relevant objects are detected<br>Lateral: based on the curvature and azimuth angle |
| **Target selection** | For detection of target objects in curves, the curvature is measured from wheel speed, yaw rate, lateral acceleration, steering angle and object height |
| **Path prediction** | Additional sensor data like curvature of the road and lane classification to predict the future course of the objects tracked |
| **Target object** | Reaction only to moving object with positive relative velocity and stationary objects in detection corridor |
| **HMI** | Target object section, set speed, time gap and ACC status |

Table 14 ACC functional parameters based on (Dr. Azim Eskandarian 2012)

### 5.2.1.2 AEB

*AEB* is responsible for requesting deacceleration to the brake systems in emergency situations. It can be extended to stationary objects or pedestrians with the help of passive sensors, while the active sensors track the moving object.

#### 5.2.1.2.1 Operations

As shown in *Figure 20*, AEB is typically employed in four different phases. Based on the distance of the target object, the deacceleration request issued is noticeably greater than the ACC function (Dr. Azim Eskandarian 2012).

The environment of AEB function is the braking system, wheel speed sensors, steering angle, brake lights and HMI.

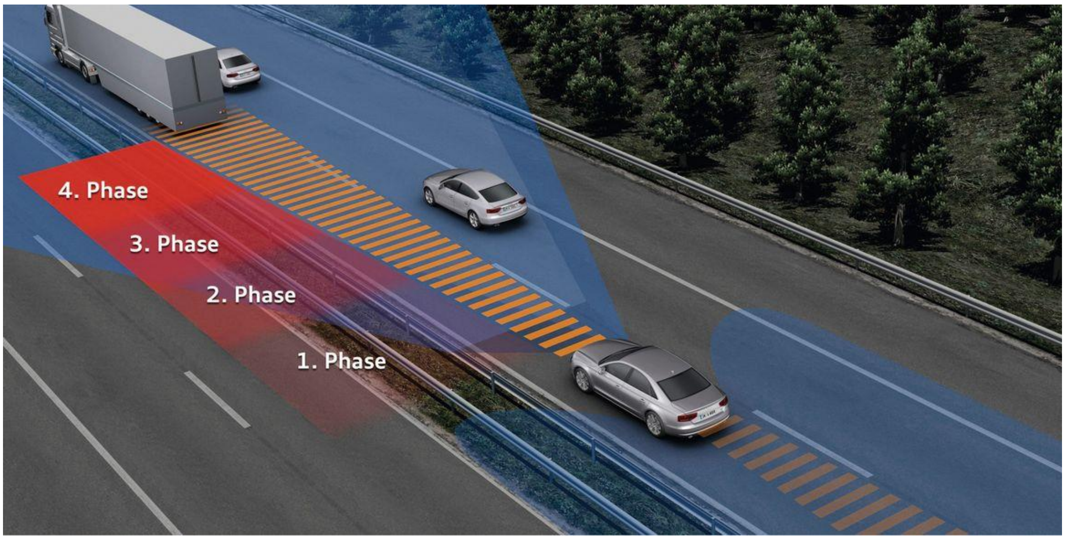


**Figure 20 Audi front sense, source (Audi 2011)**

- *Phase 1*: the system warns the driver about a potential collision with the target object through auditory alarm. During this stage the prefill of brakes is initiated.
- *Phase 2*: brake jerk and reduction in speed.
- *Phase 3*: partial braking.
- *Phase 4*: full braking

The user can intervene in the situation by pressing the brake pedal during any of the phases. The AEB assists the driver if extra braking pressure is needed to bring the vehicle to a complete standstill. The sensors are integrated to the front of the vehicle.

### 5.2.1.3 Blind Spot Warning

The area around the vehicle which cannot be observed directly or by using the mirror is referred to as blindspot, the various parts of the vehicle obstructing the view of vehicles in the adjacent lanes. The detection of the blindspot is possible with suitable sensors mounted on the rear side bumpers of the vehicle. Upon detection of vehicles in the blindspot, auditory and visual warnings are generated (Dr. Azim Eskandarian 2012). ISO17387 governs the blindspot detection and lane change assist functions.

#### 5.2.1.3.1 Operations

The system checks for occupancy of the adjacent lanes along with the user's intention to change the lane, which can be detected through activation of indication lights, and a blinking warning is issued if the occupancy is detected. It is possible to issue a warning even when the driver forgets the indication lights and attempts a lane change when there is a vehicle in the blindspot region.

It is advisable to record such attempts to change lanes without indication lights and provide feedback to the driver and encourage them to take a break from driving and also disable driver assistance system temporarily. *Figure 21* shows the operation of blindspot warnings on side mirrors of the vehicle.

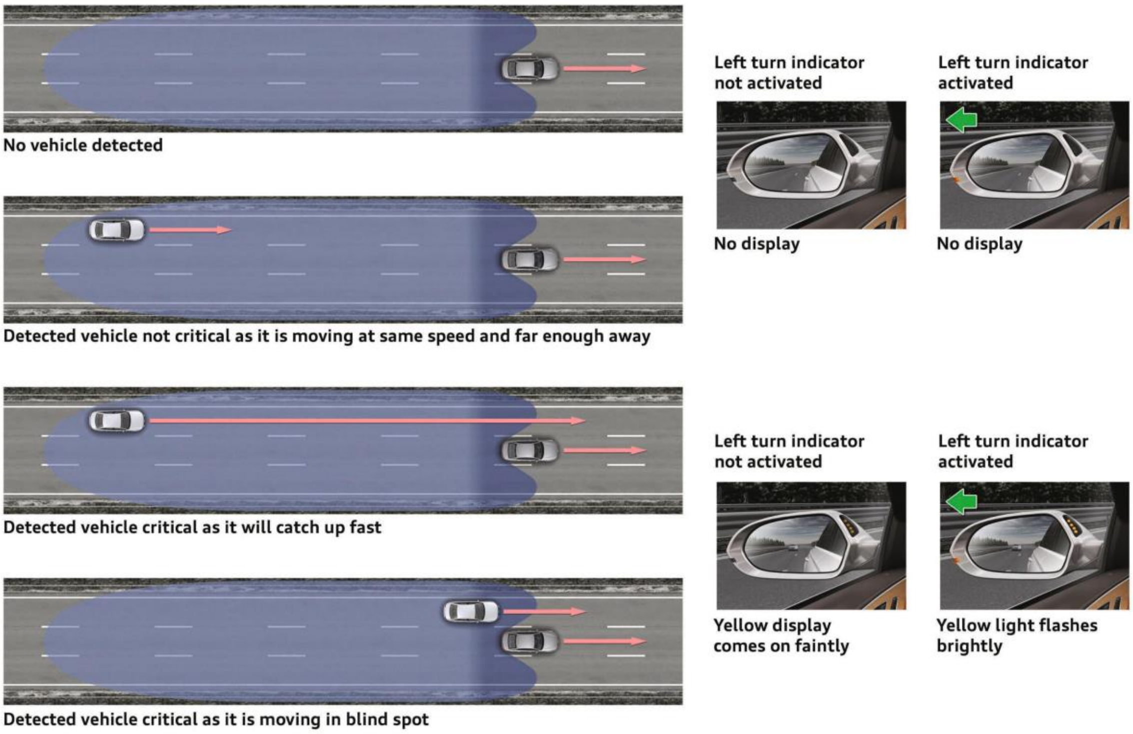

No vehicle detected
Detected vehicle not critical as it is moving at same speed and far enough away
Detected vehicle critical as it will catch up fast
Detected vehicle critical as it is moving in blind spot
Left turn indicator not activated
Left turn indicator activated
No display
No display
Left turn indicator not activated
Left turn indicator activated
Yellow display comes on faintly
Yellow light flashes brightly

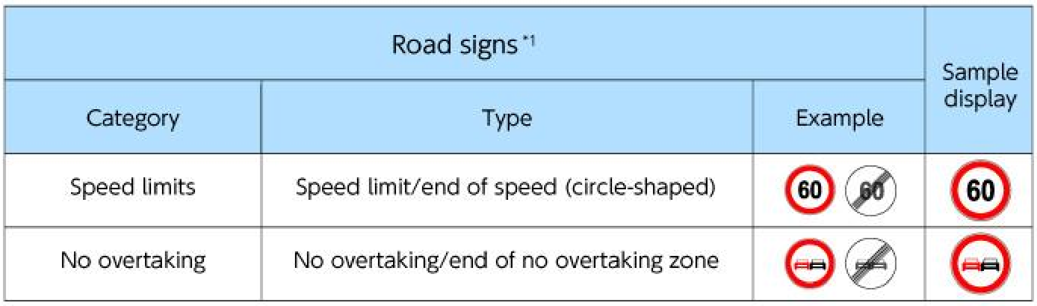
Figure 21 Audi side assist, source (Audi 2011)

#### 5.2.1.3.2 Functional parameters

The functional parameters that are used in evaluating the performance and in selecting the suitable technologies to implement blindspot detection are: road coverage radius by the sensors, target vehicle speed that is closing in and activation of function speed range (Dr. Azim Eskandarian 2012).

### 5.2.1.4 Traffic Signs Recognition

The front-facing passive sensors mounted behind the windshield recognize traffic signs and digital signs and display them on the HMI. This recognition system indicates to the driver the speed limits among others. The list of signs recognized include no passing zones, no overtaking, etc. The traffic signs recognition of the sensor can be verified with comparing the identified information with the data of the GPS and maps.



| Road signs *1 | | | Sample display |
|---|---|---|---|
| Category | Type | Example | |
| Speed limits | Speed limit/end of speed (circle-shaped) | 60 60 | 60 |
| No overtaking | No overtaking/end of no overtaking zone | | |

Figure 22 Toyota Road Sign Assist, Source (Toyota 2015)

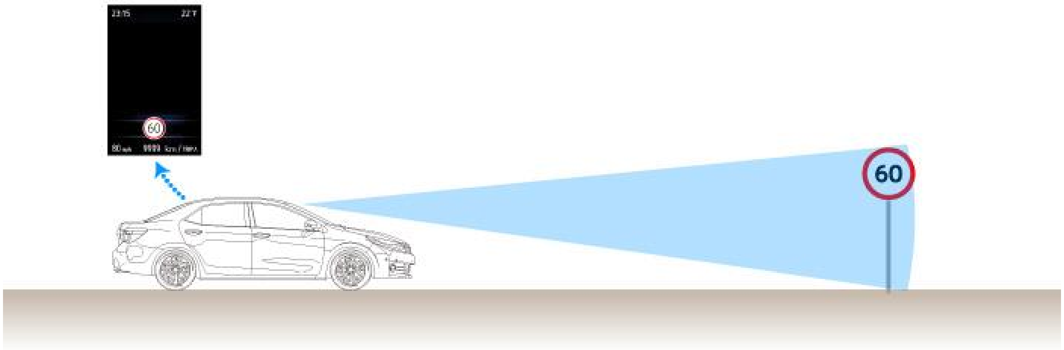


Figure 23 Toyota road sign assist, source (Toyota 2015)

## 5.2.2 Lateral control

The driver assistance for steering control and thus for preventing the vehicle from going out of lane or road is categorized into lateral control of the vehicle. The ADAS functions for this kind of control are based on warning, partial assist and continuous assist functions. *Table 15* explains the different types of controls available and their description.

| Assist Name | Function Type | Description |
|---|---|---|
| **RDM** | Partial | A corrective action on the steering control is performed to keep the vehicle in the lane or to avoid it going off the road |
| **LDW** | Warning | Sensor recognizes the lane patterns and warns the driver if the vehicle is departing the lane or going off the road |
| **LC** | Continuous | The vehicle control is tightly bound to the center of the lane |
| **LKAS** | Partial | A controlling torque is provided to keep the vehicle within the lane |
| **ESA** | Partial | Assist the driver with an additional steering torque to evade an obstacle |

Table 15 Lateral Control Types

The lane assisting systems are governed by ISO11270. All the lateral control functions in ADAS need a passive sensor to detect the lane markings along with an active sensor for object detection to calculate the trajectory in case of evasive assist. Most of the lateral control combined with functions like ACC provide comfort and safety to the driver (Dr. Azim Eskandarian 2012).

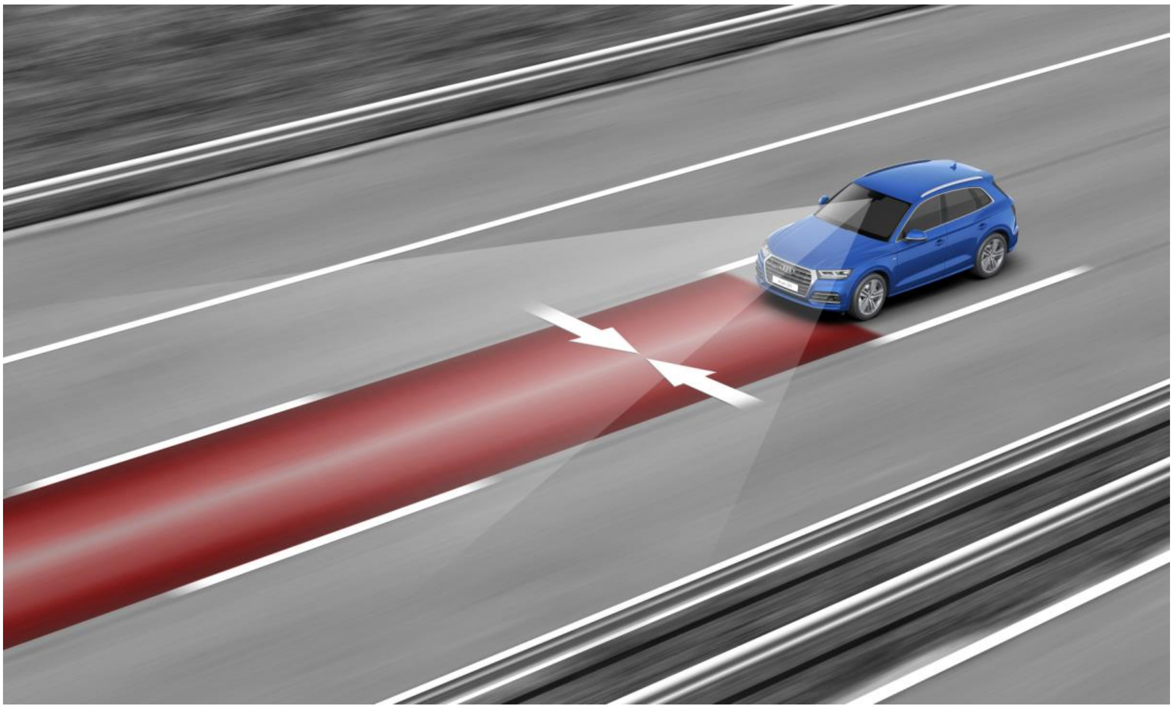


Figure 24 Audi active lane assist, source (AUDI 2017)

#### 5.2.2.1 Functional Parameters of LC

The interaction for LC is between the ADAS, braking system, wheel speed sensors, torque motor, brake lights and HMI.

Lane Centering (LC) is a type of continuous control. When designed to be active in a specific speed range and coupled with other ADAS functions like ACC, the autonomous capability of the vehicle in autostrada is increased in multitude. One of the important aspects of LC is the need to verify the driver's presence as the driver should be readily available to take over the control during certain situations. *Table 16* gives out the performance parameters of lane centering.

| Parameter | Description |
|---|---|
| **Speed Range** | Minimum and maximum active speed of the function |
| **Handover** | During system failure and when speed is not within the speed range |
| **User Intervention** | Priority to user intervention by deactivation during braking, override when using steering control and acceleration |
| **Deactivation** | Steering failure, driver not present, parking brake active, esp failure. |
| **Lane Detection** | Accuracy in detection of the lateral distance to the lane, curvature, future lane and course prediction |
| **Lane Patterns** | Patterns in the lane lines, dots, etc. |
| **Driver Monitoring** | Driver hands off monitoring to verify the presence of the driver |
| **Takeover/Hand over** | Takeover control by LC system based on situation and smoothness, handover control to the driver during failure with effective time to control the vehicle |
| **HMI** | Target object section, set speed, time gap and ACC status |

Table 16 Lane centering parameters based on (Dr. Azim Eskandarian 2012)

The transfer of vehicle control between the driver and the system that is responsible for the level 2 automation is refereed as the function transfer control.

The transfer control is of prime importance because in *level 2* automation, the driver needs to have hands on the steering wheel and be available readily when there is a need predicted by the system, while in automation *level 3*, the driver can have their eyes off the road and shall be available during the system limits or in case of failures and the system needs to handover the control of the vehicle. In order to make the migration towards the future autonomous design adaptable, the transfer control needs to be closer to automation *level 3*.

### 5.2.3 Partial Automation

Having explored different ADAS functions and their characteristics, the fulfillment of operational objectives in *Figure 18* can be accomplished with the combination of functions active during highway driving. They are as follows:

- Standard ACC
- Lane Centering (LC)
- Blindspot detection
- Traffic signs recognition

The addition of functions like blindspot detection and traffic signs recognition provide interfaces to implement automatic lane change maneuvers and automatic speed reduction based on speed limits. This will ease the migration to higher levels of automation when there is a need.

*Figure 25* shows different preliminary functions to accomplish the operation objectives.

#### 5.2.3.1 Performance Parameters

The preliminary functions derived from the operational objectives must be simulated to study the performance characteristic. In this thesis, few results of important parameters that affects the performance characteristics from other publications are cited.

The time taken by the vehicle, when there is not lateral control provided by the driver or by LC, to veer out of the ego lane into an adjacent lane is 13 *s*.[1]

In (Young and Stanton. 2007), the authors argue that a *brake reaction time of 2.4 s* is observed in drivers using adaptive cruise control responding to a critical situation.

[1] not a scientific value, extensive simulation of the vehicle behavior in different conditions and circumstance need to be carried out.

In (Merat, et al. 2014), the authors study the transfer control and human reaction behavior in a vehicle simulator and argue that:

- If the transfer control initiated is *"timed and expected"* (similar to *Level 2*) by the driver, the driver can control the lateral and longitudinal characteristics in *10 s*.
- When the transfer control *happens at irregular intervals* and is *not expected* by the driver because of eyes off condition (similar to *Level 3*), the *driver takes 40 s to control* the longitudinal and lateral characteristics of the vehicle.

Hence, making the transfer control behavior closer to SAE *Level 3* will make the migration easier for the future technological needs *Figure 17*.

At this stage, similar studies shall be conducted to derive the functional performance characteristics that are desired by the OEM's. Envisioning the customer needs and comfort can add unique identity to their vehicle functions. The functional performance characteristics shall be based on speed, limitations, activation conditions, deactivation conditions, human behavior with the system and vehicle dynamic parameters

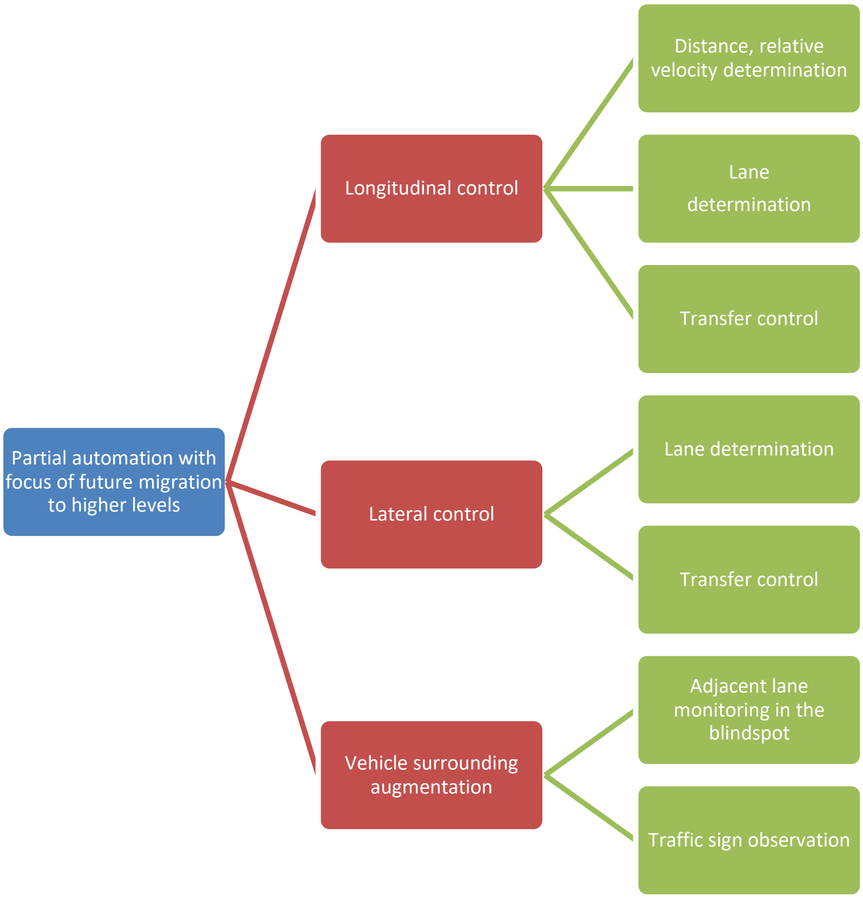

Partial automation with focus of future migration to higher levels
Longitudinal control
Lateral control
Vehicle surrounding augmentation
Distance, relative velocity determination
Lane determination
Transfer control
Lane determination
Transfer control
Adjacent lane monitoring in the blindspot
Traffic sign observation

**Figure 25 Objectives to preliminary function derived from concept exploration of ADAS functions**

### 5.2.4 Sensors of ADAS

To achieve the derived preliminary functions identified in *Figure 25*, different sensors that can fulfill the preliminary functions have to be analyzed. This is helps in narrowing down the perfect sensor system that would suit the performance characteristics of the derived functions. The sensors that are commonly used for ADAS systems are radar systems, vision-based systems, infrared sensors, laser scanners and ultrasonic systems (Dr. Azim Eskandarian 2012).

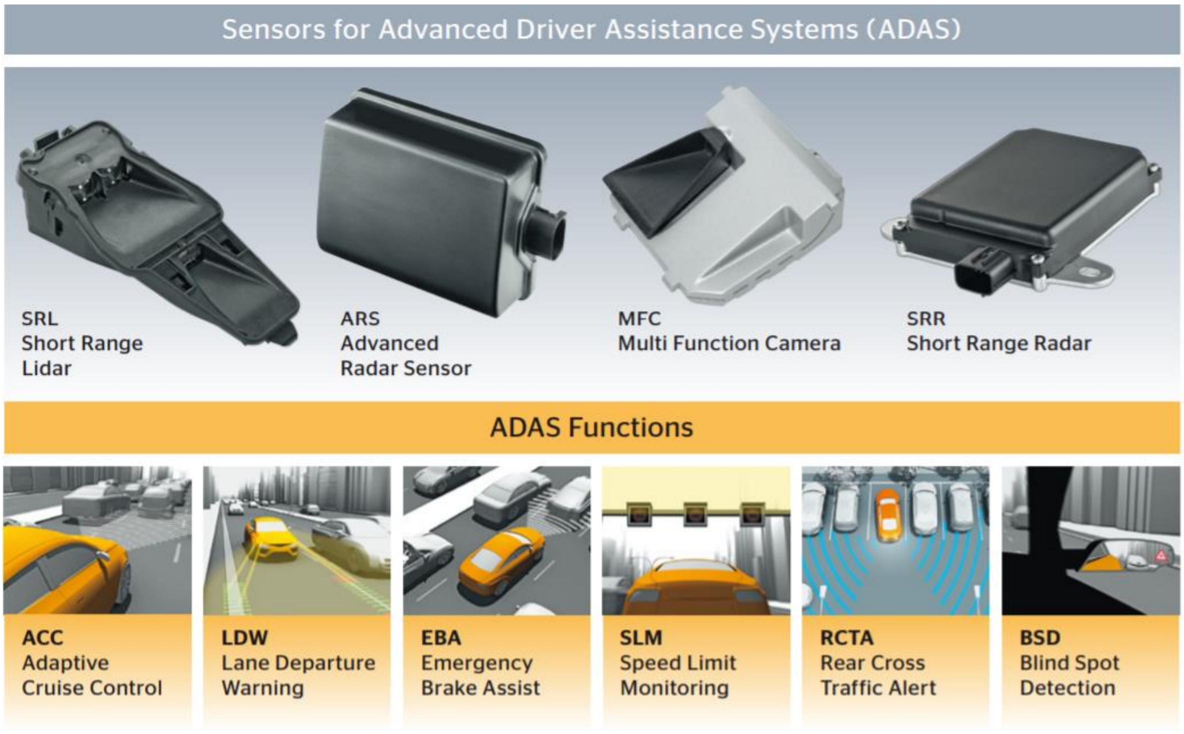


**Figure 26 Traditional ADAS sensors, source (Continental Engineering Services 2015)**

#### 5.2.4.1 RADAR

RADAR sensors used in ADAS are based on the *Doppler* effect. The Doppler effect is the change in frequency due to the target's movement relative to the ego vehicle. The types of RADAR used in the automotive application include *LRR, MRR (76.5 Ghz)* and SRR *(24GHz)* (Dr. Azim Eskandarian 2012). The 76.5 Ghz based LRR and MRR provide better accuracy in measurement of distance, speed and angular resolution than the 24Ghz based SRR system.

The so-called Doppler frequency is only used to detect relative speed. It is better to consider RADAR as a frequency detector; the position and vehicle speed are detected by the frequency of the reflected signal (Stove 1992).

#### 5.2.4.1.1 Working principle

A modulated wave with identifier is sent and a reflected sampled wave is used to measure the distance. The propagation of RADAR is based on the properties of the antenna diagram. The commonly used modulation technique is FMCW (Dr. Azim Eskandarian 2012). For the RADAR sensor in ADAS, it is necessary to track the objects and classify them based on their frequency spectral properties in distance and speed, with respect to the ego vehicle. This is done by *object hypothesis*. RADAR ASIC is responsible for FMCW, while the *object hypothesis* will be accomplished in the application microcontrollers.

#### 5.2.4.1.2 Integration in Vehicle

The installation will be handled by the OEM's through a process called alignment, this is finished before the vehicle is shipped from the factory to the dealers. Installation is based on the application and purpose of the radar. It is placed usually behind the vehicle's bumpers (at the front-end and/or rear-end) or on the corners or sides of the vehicle (Winner, et al. 2015).

#### 5.2.4.1.3 Performance Characteristics

The radar sensor's performance characteristics include scanning lobe, distance measurement, relative velocity, accuracy of point target, azimuth angle and lateral distance. Based on these characteristics, RADAR sensors are used in relevant ADAS function realization as follows (Dr. Azim Eskandarian 2012)*:*

- *MRR* – AEB due to its better lateral resolution
- *LRR* – ACC because of the longitudinal range and smaller FOV
- *SRR* - Blindspot detection because of high FOV

Objects acquired in the object hypothesis by detection are further analyzed to select a target object for ACC/AEB applications with the help of the ego vehicle state, decision based on the application is sent over the communication channel. The *Table 17* shows different steps in object hypothesis and tracking of the objects.

Object hypothesis in the following steps:

| Steps | Action |
|---|---|
| **Signal forming** | Modulation with ramp |
| **Data acquisition** | Sampling of reflected signals and demodulation |
| **Spectral analysis** | Target information |

| | |
|---|---|
| **Detection** | Sort based on the peaks in the spectrum over adaptive threshold (CFAR - Constant False Alarm Rate) |
| **Matching** | Assign detected peaks to objects |
| **Target information** | Determination of the azimuth elevation angles and relative speed |
| **Clustering** | Combining point like targets |
| **Tracking** | Assign current object data to previously known objects (association) to obtain a chronological data track that is filtered and from which the object data for the next assignment are predicted (Kalman filter and Joint Probabilistic Data Association (JPDA) |

**Table 17 RADAR hypothesis steps based on (Winner, et al. 2015).**

### 5.2.4.2 Video Sensor

The video sensor is a vision-based sensor in which the road scene is projected through the lens onto the image sensor. The photons that fall onto the image sensor are converted into an electronic output signal, which is analyzed by a processor unit and features of the road traffic like lanes, signs and vehicle types are extracted (Winner, et al. 2015). The exposure of the video sensor is controlled by either electronic or global shutter (Winner, et al. 2015).

#### 5.2.4.2.1 Types

The vision systems used in automotive applications can be categorized based on the image sensors (Dr. Azim Eskandarian 2012) (Winner, et al. 2015) into:

- Charge Coupled Device (CCD) sensors
- Complementary Metal Oxide Semiconductor (CMOS) sensors
- Infrared (IR) sensors

CMOS and CCD are used for visible light and near infrared applications (Winner, et al. 2015) (Dr. Azim Eskandarian 2012). For applications involving recognizing low light conditions, IR sensors are used (Winner, et al. 2015).

Based on the number of video sensors used in the architecture, they are categorized (Winner, et al. 2015) into mono and stereo systems. Stereo camera systems provide better object distance measurements and depth of the world (Winner, et al. 2015) than mono camera systems.

#### 5.2.4.2.2 Performance Characteristics

Some of the parameters that are suitable for the evaluation of the performance characteristics of the video sensor include *(Winner, et al. 2015):*

- Field of view
- Resolution
- Color reproduction
- Dynamic range

#### 5.2.4.2.3 Functionality

The vision-based sensors are used in traffic signs recognition, high-beam assist, lane detection and pedestrian detection (Winner, et al. 2015). The major advantages of vision systems are their capability in object classification based on shape and surface texture recognition (Dr. Azim Eskandarian 2012).

#### 5.2.4.2.4 Integration in Vehicle

The sensors are integrated in the vehicle based on the functionality and purpose as follows:

- Front view for ACC, AEB, etc.
- Rear view for parking assistance, etc.
- Surround view for autonomous driving
- Inside the vehicle for driver monitoring in drowsiness detection

### 5.2.4.3 LIDAR

LIDAR is based on the optical time of flight principle, in order to localize and measure the distance of objects and their relative velocity (Dr. Azim Eskandarian 2012).

#### 5.2.4.3.1 Performance Characteristics

The typical performance characteristics include: number of beams, detection distance, detection area, pollution detection, day and night recognition and object recognition (Winner, et al. 2015).

#### 5.2.4.3.2 Functionality

The laser scanners can be used for detecting vehicles, cyclists, pedestrians, obstacles and borders of the road (Dr. Azim Eskandarian 2012). The sensitivity of the LIDAR is decreased during rain and fog. The sensor is integrated behind the windscreen used for functions like LC, ACC and AEB.

### 5.2.4.4 Ultrasonic Sensors

The time of flight principle is used in the measurement of objects by the sensor. Ultrasonic sensors are low-cost, lightweight, have low power consumption and need low computational effort compared to other sensors (Dr. Azim Eskandarian 2012). They are integrated at the sides of the vehicles and are used mostly for the parking assistance systems (Winner, et al. 2015).

### 5.2.4.5 Wireless Sensors

The wireless standard is used to achieve real-time two-way communication among vehicles *(V2V)* and between vehicles and infrastructure *(V2I).* V2V and V2I add context to road traffic behavior like deacceleration of the target object in a motorway. These sensors have a higher range than the traditional sensors like RADAR and video and ultrasonic sensors. Thus, by making the vehicle a communication node, V2V and V2I extend the range of the traditional ADAS sensors (Winner, et al. 2015). GPS or Sat-Nav are sensor systems that can be used for ADAS. It provides terrain, speed limit and localization for lane assistance.

### 5.2.4.6 Sensor Data Fusion

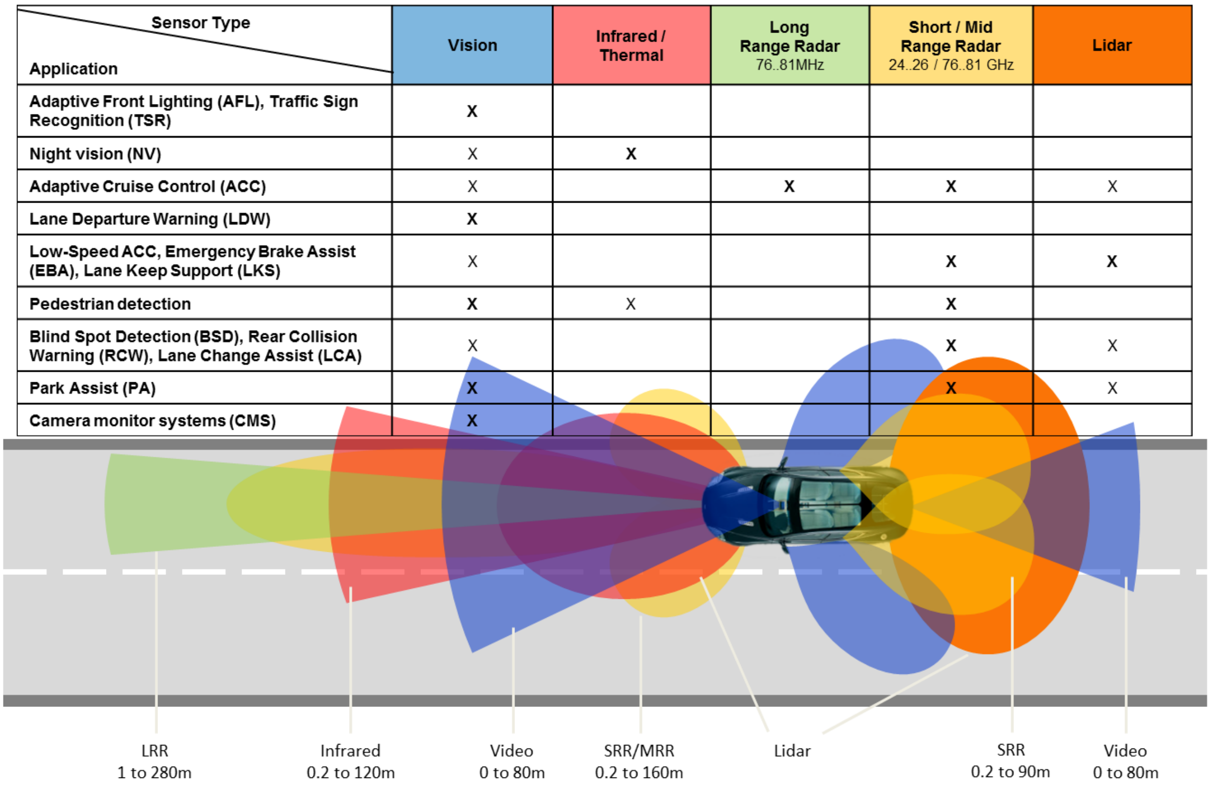
The main goal of the sensors in ADAS is to capture the environmental situation with thorough resolution and in the highest possible accuracy, from which a dependable decision can be calculated to assist the driver in their everyday life (Winner, et al. 2015).

Most of the ADAS functionalities like ACC or AEB can be achieved by using a standalone sensor like RADAR, which can calculate the target object's velocity accurately and RADAR's limitations like in recognition of object types, objects position with respect to the lane and ghost reflection in tunnels can make the system less reliable in certain situations. The safety and performance of the ACC and AEB can be improved by adding a stereo vision camera, to the architecture, which helps in detecting the object type and lane markings (Winner, et al. 2015).

The hypothesis of the environment is shared by the different sensors in the architecture and objects with same features are associated together and used to improve the object hypothesis of one of the sensors in the architecture (Winner, et al. 2015).

### 5.2.5 ADAS Benchmark

The *Figure 27* provides the summary of the ADAS sensors, their detection range along with their application in ADAS functions.



| Sensor Type<br>Application | Vision | Infrared / Thermal | Long Range Radar<br>76..81MHz | Short / Mid Range Radar<br>24..26 / 76..81 GHz | Lidar |
|---|---|---|---|---|---|
| Adaptive Front Lighting (AFL), Traffic Sign Recognition (TSR) | **X** | | | | |
| Night vision (NV) | X | **X** | | | |
| Adaptive Cruise Control (ACC) | X | | **X** | **X** | X |
| Lane Departure Warning (LDW) | **X** | | | | |
| Low-Speed ACC, Emergency Brake Assist (EBA), Lane Keep Support (LKS) | X | | | **X** | **X** |
| Pedestrian detection | **X** | X | | **X** | |
| Blind Spot Detection (BSD), Rear Collision Warning (RCW), Lane Change Assist (LCA) | X | | | **X** | X |
| Park Assist (PA) | **X** | | | **X** | X |
| Camera monitor systems (CMS) | **X** | | | | |

Figure 27 ADAS function and sensors benchmark, source (Peter Labaziewicz, Texas Instruments 2014)

The *Table 18* provides the summary of sensor system needed to achieve ADAS functions and their respective SAE interpretation. The function detection capability and proposed override are the essential parameters for system requirements.

| **Functionality** | **Sensor** | **Detection Capability** | **Description** | **Proposed Override** | **SAE** |
|---|---|---|---|---|---|
| AEB | RADAR/LIDAR &video | SO,MO and road users | Collision avoidance | Driver's brake intervention, steering-wheel | 1 |
| ACC/ACC stop & go | RADAR/LIDAR &video | MO & road users | Longitudinal control | Brake pedal, accelerator, steering angle | 2 |
| LDW | CAMERA/LIDAR | Pattern recognition (PR) | Lateral control | Turn indicators | 1 |
| Traffic-jam assist (QA+ LDW) | RADAR/LIDAR &video | SO, MO and PR | Lateral, longitudinal and driver monitoring | Brake pedal, accelerator, steering angle | 2 |
| Highway assist (ACC+LC) | RADAR/LIDAR &video | SO, MO and PR | Lateral, longitudinal and driver monitoring | Brake pedal, accelerator, steering angle | 3 |

Table 18 ADAS functional characteristics benchmark

### 5.2.6 Alternative Concepts

The concept exploration stage's goal is to provide a solution for the system design with various possible achievable alternative concepts. With all the ADAS functions and sensors that can be utilized to achieve the operational objectives analyzed, the 3 different concepts to attain the operational objectives are below.

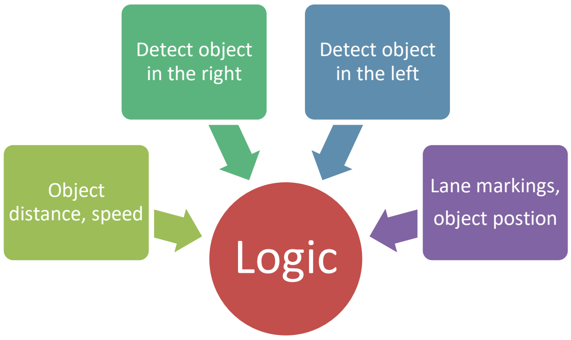

Detect object in the right
Detect object in the left
Object distance, speed
Logic
Lane markings, object postion

Figure 28 Preliminary functions

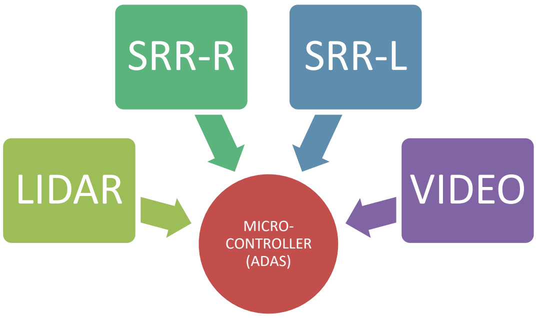


Figure 29 Concept 1

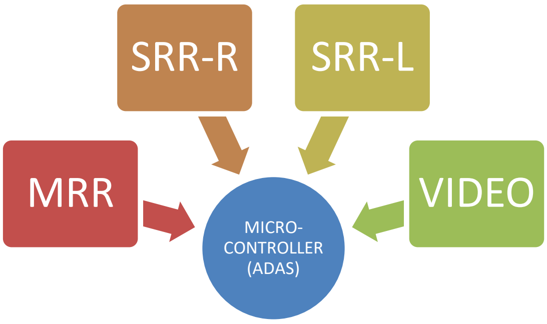


Figure 30 Concept 2

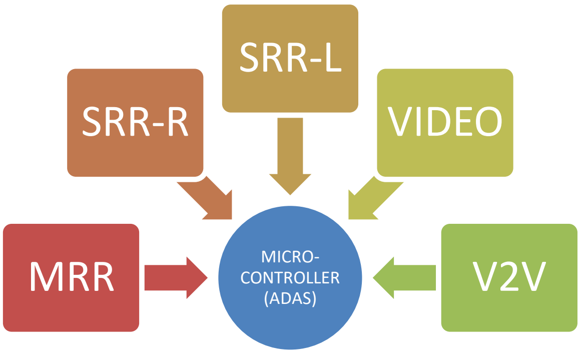


Figure 31 Concept 3

The preliminary functions can be accomplished through 3 different concepts. The *Figure 28* is the *Context Diagram* representation of the preliminary functions identified in *Figure 18*. The *Concept 3*, with V2V integration to the vehicles is not a feasible solution because of the adaptation of infrastructure that is needed in road traffic and further the V2V is not a matured technology yet.

*Concept 1* and *Concept 2* will be used in the concept definition stage; in this stage, a detailed performance evaluation of the functions is carried out and a concept is chosen for the design.

## 5.3 Concept Definition

In this stage, the best concept based on the functional performance of the sensor system to are evaluated, a system concept is chosen. The function of *Figure 25* are further decomposed into elementary function.

The *Table 19* contains the list of functions refined based on the need analysis and concept exploration of ADAS function longitudinal control. The functions marked in red influence the system states that are needed in the STPA.

| Functional Decomposition | | | |
|---|---|---|---|
| **Main Function** | **Function code** | **Intermediate Function** | **Elementary Function** |
| **LONGITUDINAL CONTROL** | MONITOR | TARGET VEHICLE STATUS | OBJECT DISTANCE<br>OBJECT RELATIVE SPEED<br>OBJECT POSITION |
| | | EGO VEHICLE STATUS | YAW RATE<br>VEHICLE SPEED<br>GEAR POSTION<br>STEERING ANGLE<br>SET SPEED<br>SET DISTANCE |
| | | DRIVER STATUS | BRAKE APPLICATION<br>STEERING ANGLE<br>HANDOVER/TAKE OVER |
| | ACTIVATION | BRAKING REQUEST | ACCELERATION/DEACCELERATION |
| | | TORQUE REQUEST | |
| | | CONTROL REQUEST | HANDOVER/TAKE OVER |
| | | STEERING REQUEST | STEERING TORQUE |
| | INDICATION | ACTIVATION ON | HMI |
| | | ACTIVATION NOT AVAILABLE | |

Table 19 Function decomposition of longitudinal control

The best suitable candidate to accomplish the elementary functions in black are analyzed by simulation or through evaluation studies with suppliers. While this stage lacks the scientific studies to define the concept of the functionality in terms of max object distance needed for the sensors, max speed of the functions (ACC and LC), lateral coverage distance, azimuth angle. These relevant data can be studied together with supplier of the ECU during the project accusation phase.

As seen during the concept exploration stage, the LIDAR sensor has a distinct advantage of supplementing video sensors with object measurement and identifying the borders of the road. Hence *Figure 32* is agreed upon as the candidate for achieving the operation objectives.

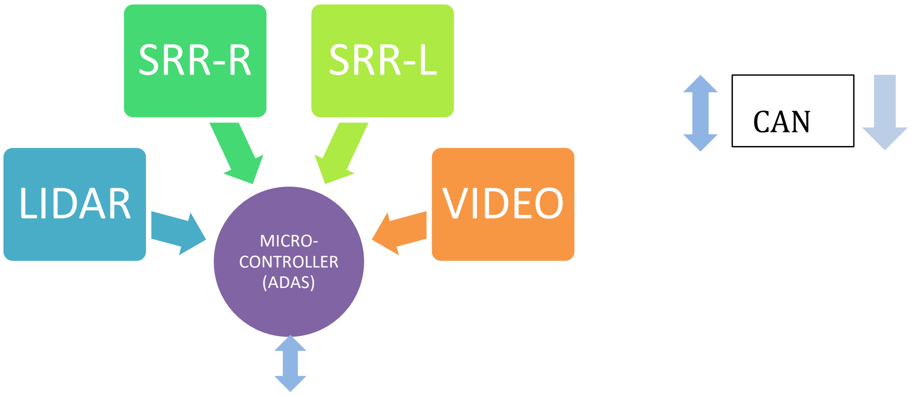


Figure 32 Concept 1 for ISO26262

### 5.3.1 Other Elements

The *Figure 32* shows the different elements of ADAS for accomplishment of operation objectives. The communication between ADAS and sensors is facilitated through private CAN and with the rest of the system through public CAN.

Since the ADAS needs to determine the ego vehicle status to fulfill the autonomous longitudinal and lateral control, a public CAN provides communication with the rest of the system. The interaction with the system is carried using interface defined in the CAN messages. The *Figure 34* shows the entire system, it is assumed that other system is working normally and has the interfaces to handle the request of ADAS.

### 5.3.2 System requirements [2]

The system requirements define the behavior of the system to be implemented so that objectives can be fulfilled. System requirements is a combination of OEM's vision of the vehicle function and sensor supplier's capability. The following are the list of system requirements:

1. The LIDAR and video are integrated together behind the windscreen responsible for ACC, LC and traffic sign recognition
2. Two SRR shall be placed on the rear corners of the vehicle to detect blindspot.
3. ACC, blindspot and traffic sign recognition shall be active above 30 km/h while LC after 50 km/h.
4. The functions shall be active between speed range 30 to 120 km/h adhering to requirement 3.
5. The ego vehicle model is calculated with the ECU available in the network represented in the *Figure 34*.
6. The driver shall be given 40s to take over the lateral and longitudinal control of the vehicle
7. The detection range for ACC shall be 100m.
8. The LC shall detect lanes up to 80m.
9. The operating modes of the functions should adhere to requirement 3 and 4.
10. The ADAS function shall be degraded when there is a failure in the system.

The other findings during the collaborative studies with ECU supplier is added to the system requirements and this ends the system concept definition. The safety life cycle is carried out on the *Figure 32* and the system requirements.

[2] The system requirements provided here has no scientific background, except when referenced with citation

# 6 Safety Life Cycle with ISO26262

The system requirements derived are analyzed for safety; this is done through the safety life cycle for concept stage. This chapter follows the *part 3* of ISO26262 briefed in *2.2.2*.

## 6.1 Item Description

The components of the system are SRR-R, SRR-L, Microcontroller, LIDAR and Video sensors. The communication between the components within the item and to the external elements is made through CAN.

### 6.1.1 Purpose

The purpose of the item is to maintain a safe distance from the moving target in front of the ego vehicle while localizing the ego vehicle in the centre of the lane. The item shall also display the speed limits from the traffic sign and warn if the adjacent lanes are occupied before a lane change maneuverer by the ego vehicle.

### 6.1.2 Functionality

The functionality of the item is based on the discussion in the *Concept Exploration* stage, the functionalities are as follows:

- The item shall use information from the sensors to keep the ego vehicle at the speed and lane defined by the driver. It also shall allow the driver to reduce/increase the speed and change lanes.

- The item shall monitor the environment. If there is a slower moving target vehicle, then the item shall maintain the ego vehicle in the same lane and keep a safe distance from the target object after alerting the driver.

- The item shall allow the driver to take control of the ego vehicle, reduce/increase the safe distance and change lanes when it is following a target object.

- The item shall monitor a lane change manoeuvre and warn the driver about the faster moving vehicle in its blindspot regions.

- The items shall display the traffic signs.

#### 6.1.2.1 Usecase Representation

The functionality of the item shall be supported by *Usecase* to provide better overview of scope, limits and controllability of the driver along with the item. The usecase shall support various scenarios that requires the activation of the functionality of the item. The usecase in *Table 13* is an example of blindspot monitoring definition using the usecase and providing the relationship of between the situation, expected driver behavior and the item's functionality.

### 6.1.3 Operating Modes and States

The Item shall operate in 6 different modes based on the functionality and failure modes of the item. The *Table 20* shows the different operating modes and state of the item this is derived in the *Concept Definition* stage are part of the system requirements.

### 6.1.4 Operational and Environmental Constraints

The items shall be used only with vehicles in autostrada in the EU region alone, items shall not be used in muddy off-road environments.

### 6.1.5 Relevant Standards

The relevant standards with respect to the functionality and usecase of the item are:

- *Lane Keeping Assistance Systems (LKAS):* ISO 11270-2014
- *ACC:* ISO15622-2010
- *Levels of Automation* : SAE J3016
- *Blindpsot* : ISO17387

### 6.1.6 Similar Item

The experience and knowledge of older relevant systems and history of dealing with similar functionalities gives valuable advantage in designing item, hence it is advisable to gather information about the older system's functionality and failure modes. The functionality of the item is a combination of ACC, LC, blindspot detection and traffic signs recognition, there is no experience with similar item in the organisation as single system. However, there exist number of individual item that are responsible for some the functionality of the item as follows:

- Longitudinal control: ESP and ACC
- Lateral control: ESP and power steering (EPS)

| Operating Mode | Operating State | Functionality |
|---|---|---|
| **OFF** | item not switched on | NA |
| **ON/PASSIVE** | item waits for valid set speed and distance | validate the data and monitor if the vehicle speed is above 30 km/h |
| **ON/SEMI ACTIVE** | item maintains the defined speed and the driver is responsible for the steering | monitor potential target object, traffic signs, blindspot and lane markings. Check if the vehicle speed is above 50 km/h |
| **ON/SEMI ACTIVE** | item maintains the safe distance and is responsible for steering | follow the target object, monitor the lane marking, traffic signs and blindspot Check if the vehicle speed is above 50 km/h |
| **ON/FULL ACTIVE** | item shall maintain safe distance and guide the ego vehicle in the centre of the lane | item maintains the safe distance and keep the vehicle in the lane, monitors the lane change request and warn the driver if the blind spot is occupied. Check for the presence of the driver in the driving seat. |
| **ON/PASSIVE** | item hands over the control of the vehicle to the user | monitors the blind spot, traffic sign and vehicle speed and waits for the handover of the control |
| **ON/LIMP HOME** | item/elements of the item are in error | item's performance is degraded |

Table 20 Operating modes and states of the item.

## 6.1.7 Assumptions

The items shall expect the driver to be present and be available to carry out transfer control when called upon.

## 6.1.8 Failure Modes and Hazards

The failure modes and hazards are defined based on the experience of similar system, they are:

**Failure modes**

- Item sends wrong information on the CAN
- Item wrongly calculates the target object distance and velocity
- Item wrongly detects blind spot region/traffic signs/lane markings
- HMI failure

**Hazards**

- Unintended acceleration or deacceleration
- Loss of steering control
- The driver panics and brakes to comply with the speed limit
- Vehicle veers out of the intended target lane collides with adjacent traffic

## 6.2 Item Characterization

The items characters like boundary definition and its interfaces for interactions, are described in this section.

### 6.2.1 Elements of the Item

The elements of the item are depicted in *Figure* 33. It includes, sensors, communication network (CAN) and an ECU to gather information from the sensors and make decision based on the situation.

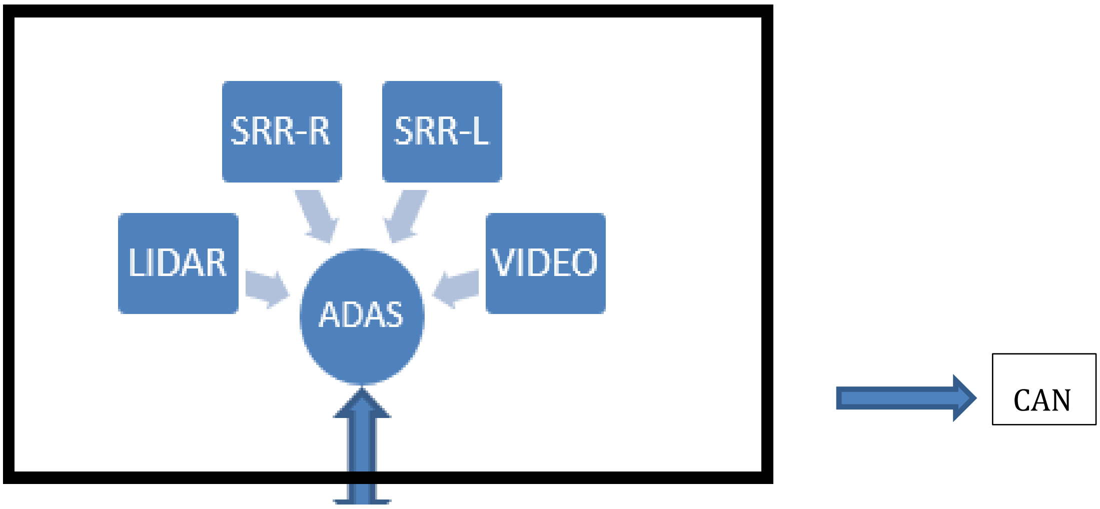


Figure 33 Elements of the item

### 6.2.2 Interfaces

The item shall send longitudinal acceleration/deacceleration request, lateral acceleration using steering torque, warnings signal about blindspot availability and traffic sign indications on the CAN. The item shall receive ego vehicle model status and information from the perception sensors about the environment.

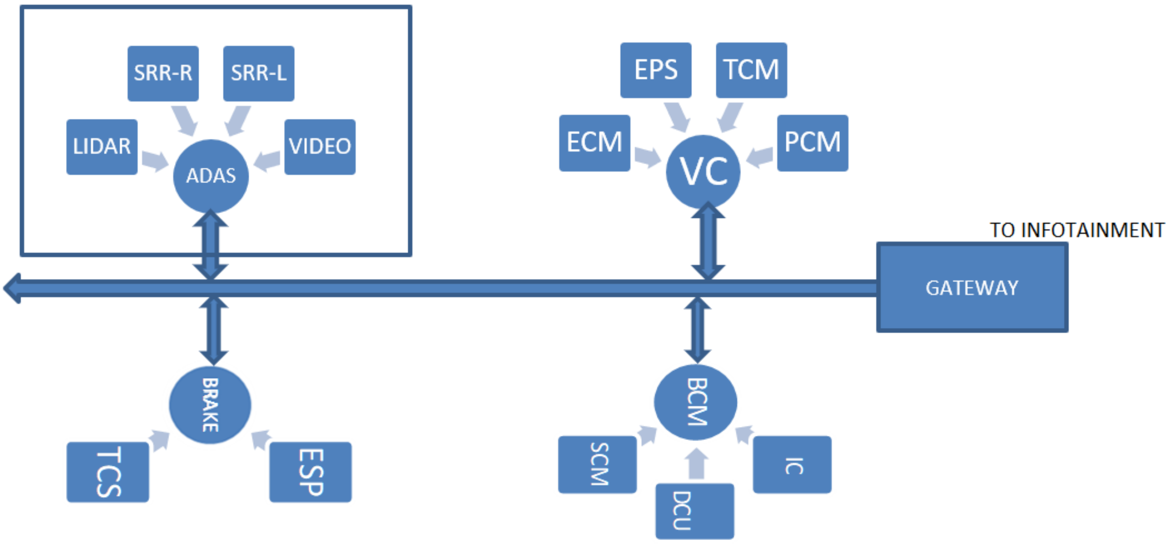


Figure 34 Item boundary and interaction

- VC- Vehicle Control
- TCM- Transmission Control Management
- ECM- Engine Control Management
- PCM- Power Train Control Management
- EPS- Electronic power steering
- ESP- Electronic Stability Program
- IC- Instrumentation Cluster
- TCS- Traction Control system

### 6.2.3 Interactions

The item communicates with other ECUs through CAN. The item is powered during the ignition ON.

### 6.2.4 External Interface

The item communicates to other items in the system outside its boundary with CAN. The *Figure 34* show the item's boundary and other systems. The other system provides the status of the ego vehicle and handles the functionality required by the item, following are functionality handled by other system:

- EPS: EPS module shall accept the steering torque control request, provide steering angle information.
- *EMS*: Engine module system shall accept acceleration request
- *ESP*: Stability module shall accept deacceleration request and shall provide wheel speed and yaw rate.
- *HMI*: HUD shall support the display of warnings and alerts
- *CAN*: Shall transmit and supply information without latency and data corruption
- *BCM*: Body module shall provide vehicle speed

#### 6.2.4.1 Functional Elements

The functional elements of the item are based on the function allocation discussed concept exploration and system requirements. They are as follows:

- *2 SRR*: for blind spot assist, as it requires only the information about objects in the rear-side area of the vehicle
- *1 Camera*: to follow lane markings, to monitor the traffic signs and to classify the object types
- *1 LIDAR*: to measure the object distance, speed and assist

The subsystem ADAS is responsible for sensor data fusion, it collects the objects information from different sensors and forms a data structure with relevant information about target object velocity, distance, ego lane and determines the needed acceleration/deacceleration, HMI alerts and steering torque request.

#### 6.2.4.2 Common Operational Situation

The item is intended to active during highway driving, it could involve the scenarios as follows:

- <30 km/h target object present
- >30 km/h with no target object
- <50 km/h with lane markings
- >50 km/h with lane markings
- >50 km/h with lane markings/no markings
- lane change maneuverer with blind spot occupied at all speeds

## 6.3 HARA

The HARA is an approach through which risk associated with the system can be studied. It is recommended to conduct the HARA with a scientific approach.

### 6.3.1 Situational Analysis

A simple scenario shown in *Figure 35* is chosen to conduct the HARA and visualize the risk associated with different functionalities of the item. The *Figure 35* shows the ego vehicle maintaining the distance a safe distance from the target vehicle and the adjacent lanes occupied in the blindspot region by a bike a truck.

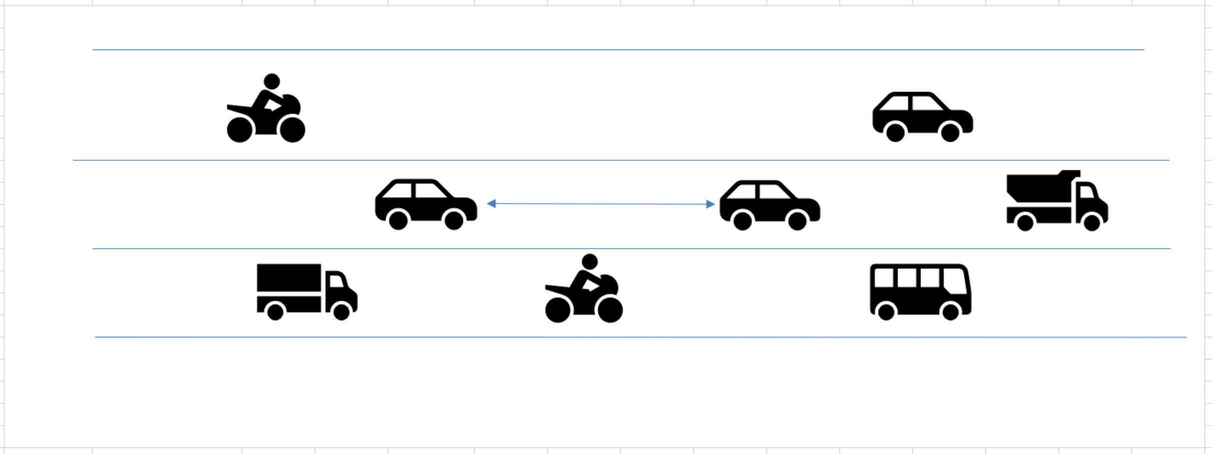


Figure 35 Operational situation for HARA

## 6.3.2 Hazard Identification

The preliminary hazard identification is accomplished with  STPA.

### 6.3.2.1 STPA

STPA is used to find out the hazard types within the boundary of the item and their respective causal factors. The methodology of STPA is described in *Figure 15*.

#### 6.3.2.1.1 System Description

The detailed functional scope for the item needs to be described in this step, description provided during the concept exploration and definition, item definition and description provides sufficient overview regarding the scope and functionality of the item.

The system description is supported by control block diagram. This is done through identifying the inputs and outputs of the item which helps achieving the controllability of the function at vehicle level. The functions decomposed during the concept definition in *Table 19* is provides the input and output functions for the context diagram.

The next step is narrow down the functions that affects the controllability of the vehicle i.e the system state.  The functions marked in red from the *Table 19* are the system state for the longitudinal control.

The *Figure 36* is the system control diagram for the item, with output represented by arrow heading out of the ADAS block, visualizing the system as a control blocks provides valuable insight for hazard identification.

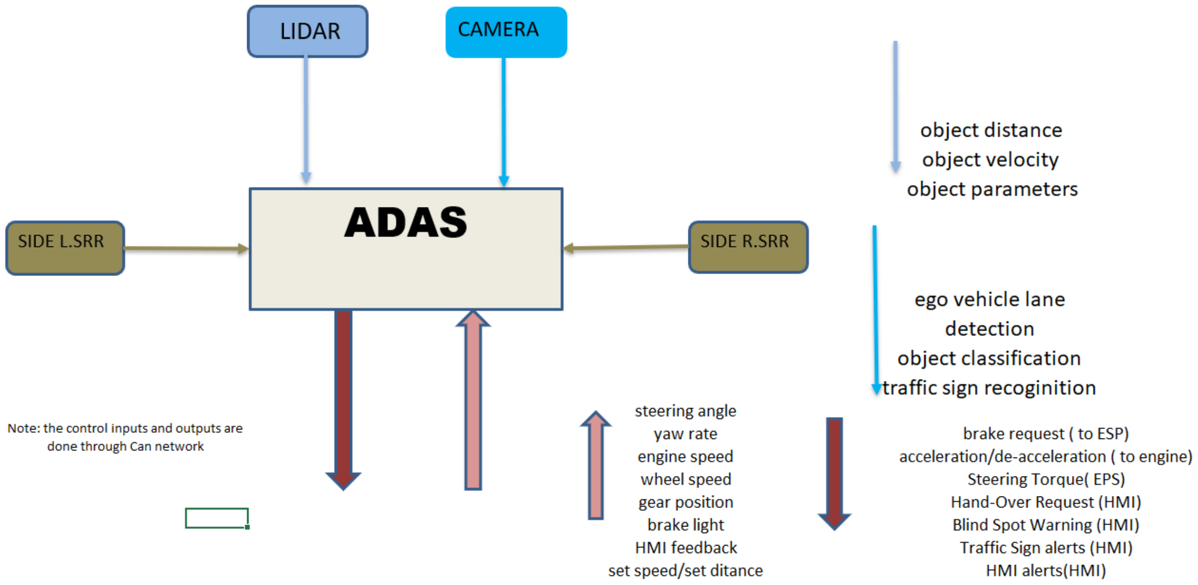


Figure 36 Control block for the item.

### 6.3.2.1.2 System Level Loss

The system level loss defined as a crash or loss of controllability at the vehicle level.

For the analysis,

- loss of controllability of the vehicle because of the item,
- loss of warning /alert by the item to the driver leading to loss of controllability
- item not granting the controllability/taking over the controllability of the vehicle from the driver leading to damage and loss of trust towards the item.

All these system level losses could potentially lead to the damage of life & property.

### 6.3.2.1.3 Hazards

The hazards are described as control action of the item that affects the system state thus by leading to system loss.

For the analysis,

- uncontrolled longitudinal control
- uncontrolled lateral control
- uncontrolled take over/ hand over request of vehicle control.
- uncontrolled blind spot warning and traffic sign alert.
- uncontrolled HMI warnings/alert

All these system level losses could potentially lead to a damage of life & property.

#### 6.3.2.1.4 UCA Identification

The UCA identification is done by using the six guide words discussed in *Figure 16*, the guide words are applied to the functions that affect the system states, i.e the interfaces to the elements outside the boundary of the item, while the causal factors of the hazards are the input functions, incorrect computation and communication errors.

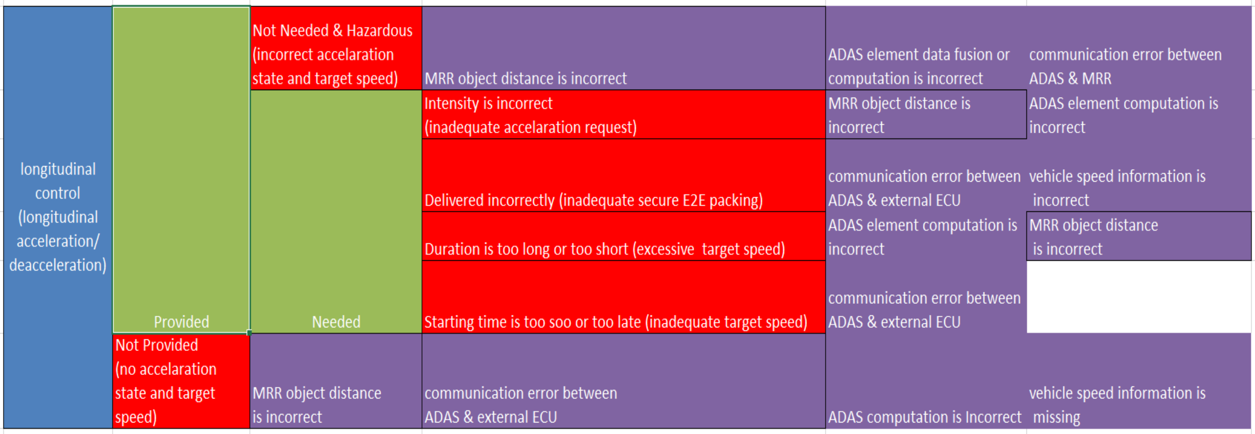

longitudinal control (longitudinal acceleration/ deacceleration)
Provided
Not Needed & Hazardous (incorrect accelaration state and target speed)
Needed
MRR object distance is incorrect
ADAS element data fusion or computation is incorrect
communication error between ADAS & MRR
Intensity is incorrect (inadequate accelaration request)
MRR object distance is incorrect
ADAS element computation is incorrect
Delivered incorrectly (inadequate secure E2E packing)
communication error between ADAS & external ECU
vehicle speed information is incorrect
Duration is too long or too short (excessive target speed)
ADAS element computation is incorrect
MRR object distance is incorrect
Starting time is too soo or too late (inadequate target speed)
communication error between ADAS & external ECU
Not Provided (no accelaration state and target speed)
MRR object distance is incorrect
communication error between ADAS & external ECU
ADAS computation is Incorrect
vehicle speed information is missing

Figure 37 UCA identification

The *Figure 37* has UCA in red and causal in violent, the UCA are translated into vehicle level hazards in the *Figure 38*, this helps in determining the hazardous event and its consequence.

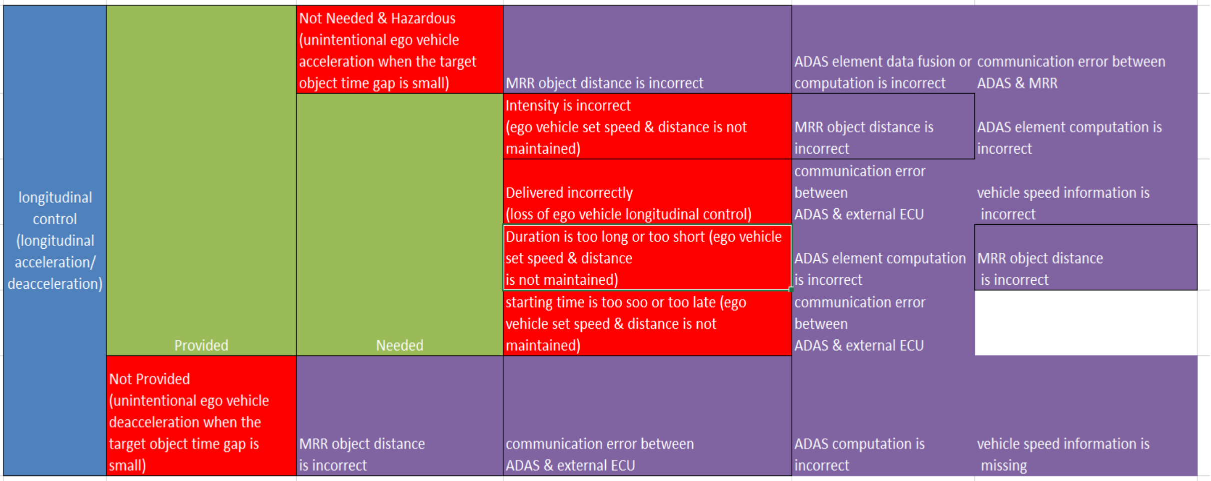

longitudinal control (longitudinal acceleration/ deacceleration)
Provided
Not Needed & Hazardous (unintentional ego vehicle acceleration when the target object time gap is small)
Needed
MRR object distance is incorrect
ADAS element data fusion or computation is incorrect
communication error between ADAS & MRR
Intensity is incorrect (ego vehicle set speed & distance is not maintained)
MRR object distance is incorrect
ADAS element computation is incorrect
Delivered incorrectly (loss of ego vehicle longitudinal control)
communication error between ADAS & external ECU
vehicle speed information is incorrect
Duration is too long or too short (ego vehicle set speed & distance is not maintained)
ADAS element computation is incorrect
MRR object distance is incorrect
starting time is too soo or too late (ego vehicle set speed & distance is not maintained)
communication error between ADAS & external ECU
Not Provided (unintentional ego vehicle deacceleration when the target object time gap is small)
MRR object distance is incorrect
communication error between ADAS & external ECU
ADAS computation is incorrect
vehicle speed information is missing

Figure 38 Vehicle level hazard

UCA to vehicle level hazard mapping in STPA provides the relationship between casual factors and hazard types to the system states.

| Hazard Types (UCA) | Manifestation (Vehicle Level) | Vehicle Level Hazard |
|---|---|---|
| Inadequate secure E2E packing | loss of ego vehicle longitudinal control | loss of ego vehicle longitudinal control (H1) |
| no acceleration state and target speed | loss of ego vehicle longitudinal control | loss of ego vehicle longitudinal control |
| inadequate acceleration request | ego vehicle set speed & distance is not maintained | unintended ego vehicle longitudinal control |
| incorrect acceleration and target speed | ego vehicle acceleration when the target object time gap is small | unintended ego vehicle longitudinal control |
| excessive target speed | ego vehicle set speed & distance is not maintained | unintended ego vehicle longitudinal control |
| inadequate target speed | ego vehicle set speed & distance is not maintained | unintended ego vehicle longitudinal control |

Table 21 UCA to vehicle level hazard mapping

The *Table 21* is an example of mapping of UCA to vehicle level hazard. The mapping is necessary and useful in deriving the safety goals. The casual factors mapping of the UCA to vehicle level hazard is useful in better understanding of the system and in deriving functional safety concept.

The hazards identification is continued for other system states like lateral control, transfer control, blindspot warning and traffic signs recognition.

### 6.3.3 Hazardous Events

It is the combination of hazards at vehicle level occurring during worst possible situation leading to loss of control of the vehicle. The focus must be given not only to the individual hazards but also to the combination of hazards that affects the controllability of the item or distracts the driver away from the driving task.

*Scenario:*

*Item gives a false alert about blindspot being occupied which distracts the driver and then followed by alert to handover control.*

#### 6.3.3.1 Parametrization Of S, E & C

One of the important tasks in HARA is the assignment of ASIL to the hazardous event, the draw backs of assignment of ASIL without scientific approach is discussed in *Parametrization Of S, E & C.* To overcome the shortcomings and to make HARA scientific a ruleset is defined for severity, exposure and controllability in the following section. It is recommended to have accurate results of the ruleset, by simulating the situation and hazards in virtual environments before proceeding to assignment of ASIL[3].

##### 6.3.3.1.1 Exposure

The item is designed to be active in autostrada, a normal passenger car spends more than half its life time driven in autostrada[4] and encountering various vehicle types. Hence, the value *of E is set to E4* for the entire analysis of the hazardous event.

##### 6.3.3.1.2 Severity and Controllability

The ruleset for controllability is defined in the *Table 22 S and C ruleset*, the parameters are identified by focussing on the functions of the item and driver behaviour that affect the overall vehicle controllability. It is advisable to consider HMI and HUD and alerts as it is the way of the item to communicate with the driver with warnings and visuals, poorly designed HMI/HUD can be detrimental to controllability of the vehicle by the driver.

| PARAMETER | DESCRIPTION |
|---|---|
| **TIME FOR TRANSFER CONTROL** | *40s* based on *(Merat, et al. 2014)* |
| **LANE DRIFTING** | time for the vehicle to go out of lane or road if lateral control is lost, for a *3.5m* width of lane is *13s* [5] |
| **BRAKE-REACTION TIME** | during ACC is *2.4s* based on *(Young and Stanton. 2007)* |

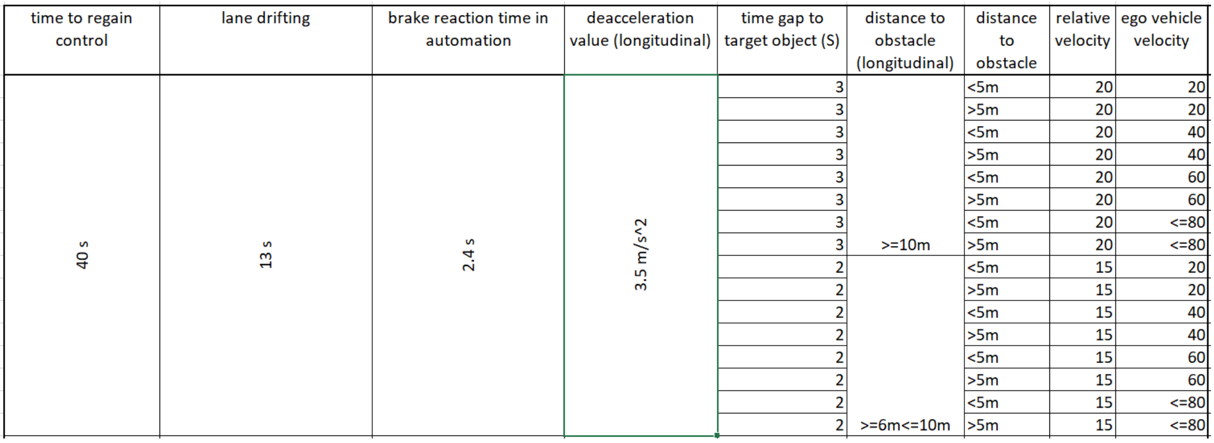
**Table 22 S and C ruleset**

Meanwhile the severity ruleset is identified by parameters like vehicle velocity of ego vehicle and road traffic, distance of the vehicles in the ego lane and neighbourhood lane, collision type.

[3] simulation is not carried out in this thesis and the ASIL assignment is based on the ruleset with brainstorming and review, though this reduces the assignment error. It is advisable to carry out the association of ASIL after evaluating the hazardous events in simulation.

[4] assumption

[5] no scientific proof



| time to regain control | lane drifting | brake reaction time in automation | deacceleration value (longitudinal) | time gap to target object (S) | distance to obstacle (longitudinal) | distance to obstacle | relative velocity | ego vehicle velocity |
|---|---|---|---|---|---|---|---|---|
| 40 s | 13 s | 2.4 s | 3.5 m/s^2 | 3 | >=10m | <5m | 20 | 20 |
| | | | | 3 | | >5m | 20 | 20 |
| | | | | 3 | | <5m | 20 | 40 |
| | | | | 3 | | >5m | 20 | 40 |
| | | | | 3 | | <5m | 20 | 60 |
| | | | | 3 | | >5m | 20 | 60 |
| | | | | 3 | | <5m | 20 | <=80 |
| | | | | 3 | | >5m | 20 | <=80 |
| | | | | 2 | >=6m<=10m | <5m | 15 | 20 |
| | | | | 2 | | >5m | 15 | 20 |
| | | | | 2 | | <5m | 15 | 40 |
| | | | | 2 | | >5m | 15 | 40 |
| | | | | 2 | | <5m | 15 | 60 |
| | | | | 2 | | >5m | 15 | 60 |
| | | | | 2 | | <5m | 15 | <=80 |
| | | | | 2 | | >5m | 15 | <=80 |

Figure 39 Parameterization of severity and controllability

The *Figure 39* provides the HARA parametrisation for the item's functionality, the data for the table can be populated with gaussian distribution.

## 6.3.4 Classification of Hazardous Events

The consequence of hazardous event is classified based on the *Figure 39*. During the classification, each hazardous event shall be assigned with an ASIL and accompanied by a safety goal. If multiple safety goals are similar due to identical consequence of hazardous event, the safety goals highest ASIL will be considered.

### 6.3.4.1 Association of ASIL

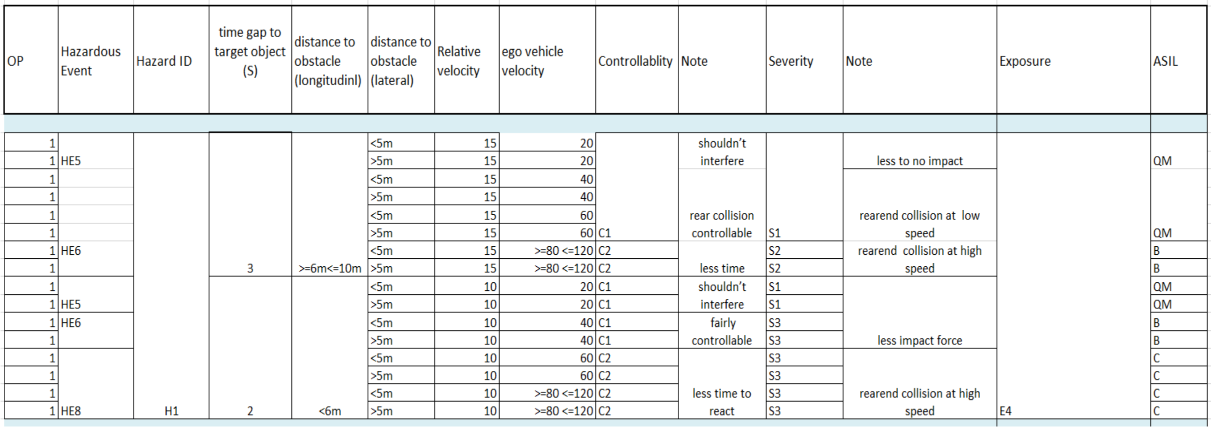
The association of ASIL is accomplished using the parameterization of S, E and C. The analysis for the hazard type *H1* in the *Table 21* is as follows:

*The loss of ego vehicle longitudinal control (H1),* occurring during the operational situation in *Figure 35*, with the velocity of ego vehicle between 80-120 km/h leads to read end collision at high speed. The hazardous situation is ranked as S3, C3 and E4 with an ASIL of C.

At low speeds below 30 km/h, if the item interferes with longitudinal control when the driver does not expect it to interfere. It could lead to rear end collision with slight damage to road traffic, hence ASIL assigned is QM.

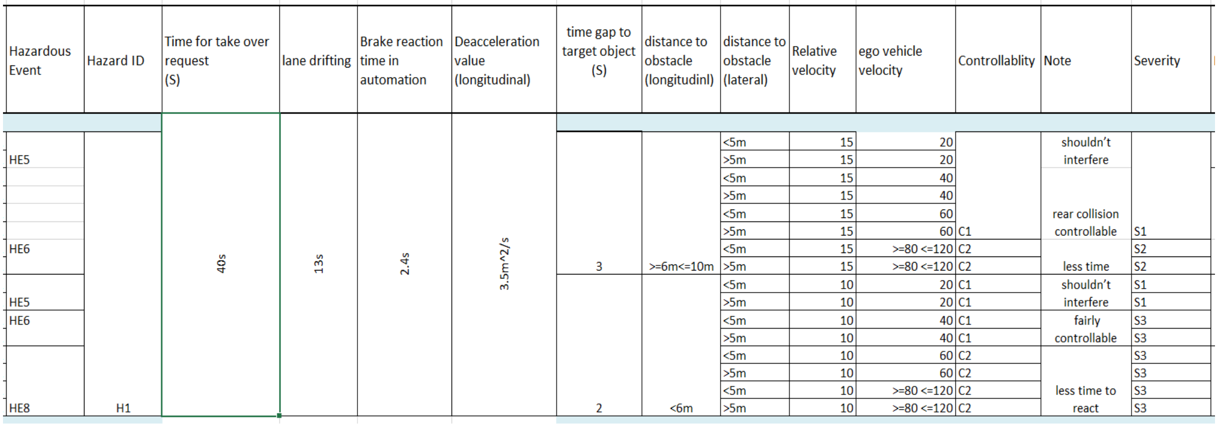
The safety goal to this hazardous event with QM will be different than the hazardous event with ASIL C because of the cause of the hazardous event is due to the loss of control longitudinal control when the item is not expected to interfere and function.

The other hazardous event with ranking ASIL B has the same consequence of that of ASIL C, hence the safety goal associated to hazardous event will be ranked as C.



| OP | Hazardous Event | Hazard ID | time gap to target object (S) | distance to obstacle (longitudinl) | distance to obstacle (lateral) | Relative velocity | ego vehicle velocity | Controllablity | Note | Severity | Note | Exposure | ASIL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | H1 | 3 | >=6m<=10m | <5m | 15 | 20 | | shouldn't interfere | | less to no impact | E4 | |
| 1 | HE5 | | | | >5m | 15 | 20 | | | | | | QM |
| 1 | | | | | <5m | 15 | 40 | | rear collision controllable | | rearend collision at low speed | | |
| 1 | | | | | >5m | 15 | 40 | | | | | | |
| 1 | | | | | <5m | 15 | 60 | | | | | | |
| 1 | | | | | >5m | 15 | 60 | C1 | | S1 | | | QM |
| 1 | HE6 | | | | <5m | 15 | >=80 <=120 | C2 | less time | S2 | rearend collision at high speed | | B |
| 1 | | | | | >5m | 15 | >=80 <=120 | C2 | | S2 | | | B |
| 1 | | | 2 | <6m | <5m | 10 | 20 | C1 | shouldn't interfere | S1 | less impact force | | QM |
| 1 | HE5 | | | | >5m | 10 | 20 | C1 | | S1 | | | QM |
| 1 | HE6 | | | | <5m | 10 | 40 | C1 | fairly controllable | S3 | | | B |
| 1 | | | | | >5m | 10 | 40 | C1 | | S3 | | | B |
| 1 | | | | | <5m | 10 | 60 | C2 | less time to react | S3 | rearend collision at high speed | | C |
| 1 | | | | | >5m | 10 | 60 | C2 | | S3 | | | C |
| 1 | | | | | <5m | 10 | >=80 <=120 | C2 | | S3 | | | C |
| 1 | HE8 | | | | >5m | 10 | >=80 <=120 | C2 | | S3 | | | C |

Figure 40 HARA

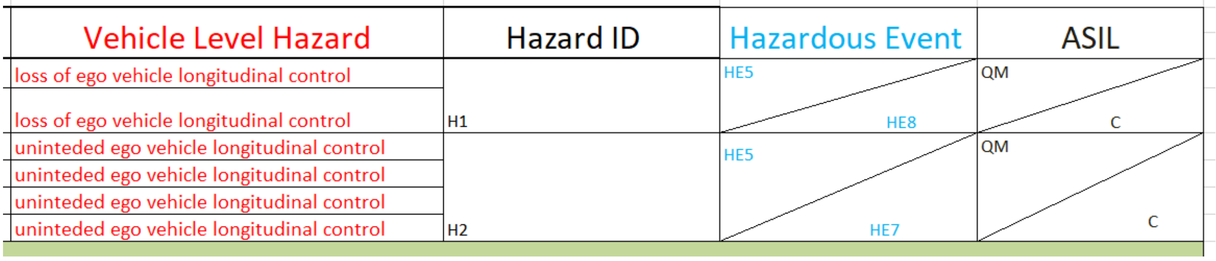


| Hazardous Event | Hazard ID | Time for take over request (S) | lane drifting | Brake reaction time in automation | Deacceleration value (longitudinal) | time gap to target object (S) | distance to obstacle (longitudinl) | distance to obstacle (lateral) | Relative velocity | ego vehicle velocity | Controllablity | Note | Severity |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | H1 | 40s | 13s | 2.4s | 3.5m^2/s | 3 | >=6m<=10m | <5m | 15 | 20 | | shouldn't interfere | |
| HE5 | | | | | | | | >5m | 15 | 20 | | | |
| | | | | | | | | <5m | 15 | 40 | | rear collision controllable | |
| | | | | | | | | >5m | 15 | 40 | | | |
| | | | | | | | | <5m | 15 | 60 | | | |
| | | | | | | | | >5m | 15 | 60 | C1 | | S1 |
| HE6 | | | | | | | | <5m | 15 | >=80 <=120 | C2 | less time | S2 |
| | | | | | | | | >5m | 15 | >=80 <=120 | C2 | | S2 |
| | | | | | | 2 | <6m | <5m | 10 | 20 | C1 | shouldn't interfere | S1 |
| HE5 | | | | | | | | >5m | 10 | 20 | C1 | | S1 |
| HE6 | | | | | | | | <5m | 10 | 40 | C1 | fairly controllable | S3 |
| | | | | | | | | >5m | 10 | 40 | C1 | | S3 |
| | | | | | | | | <5m | 10 | 60 | C2 | less time to react | S3 |
| | | | | | | | | >5m | 10 | 60 | C2 | | S3 |
| | | | | | | | | <5m | 10 | >=80 <=120 | C2 | | S3 |
| HE8 | | | | | | | | >5m | 10 | >=80 <=120 | C2 | | S3 |

Figure 41 HARA for longitudinal control

The *Figure 41, Figure 40* shows ASIL allocation and the argument for the association ASIL to hazardous event, similar approach is continued for other identified hazards.

The *Figure 42* shows the hazard to ASIL relationship. With the hazard to casual factors relationship derived during the STPA, the relationship between causal factors and ASIL can be visualized. This helps in allocating the ASIL to different functions, elements of the item and also in safety goals.



| Vehicle Level Hazard | Hazard ID | Hazardous Event | ASIL |
|---|---|---|---|
| loss of ego vehicle longitudinal control | H1 | HE5<br>HE8 | QM<br>C |
| loss of ego vehicle longitudinal control | | | |
| uninteded ego vehicle longitudinal control | H2 | HE5<br>HE7 | QM<br>C |
| uninteded ego vehicle longitudinal control | | | |
| uninteded ego vehicle longitudinal control | | | |
| uninteded ego vehicle longitudinal control | | | |

Figure 42 Vehicle level hazard and ASIL mapping

### 6.3.5 Determination of Safety Goals

The safety goals are requirements to avoid unreasonable risk, *Table 23* defines the safety goal and safe state for each hazardous event. Safe state is through which dependability attributes of the system is expressed. The derived safety goals should not hinder the item's functions and other system's safety mechanism.

| **Hazardous event** | **Safety goal ID** | **Safety goal** | **Safe state** | **ASIL** |
|---|---|---|---|---|
| HE2,HE9 | SG1 | item shall never distract or mislead the driver with false warnings/alerts about the occupancy of blindspot | failsafe: the unavailability of the item shall be informed to the driver | C |
| HE4,HE9 | SG2 | item shall never mislead or distract the driver with inaccurate traffic signs | failsafe: the unavailability of the item shall be informed to the driver | C |
| HE5 | SG3 | item shall never interfere with the longitudinal control of the vehicle when the vehicle speed is less than 30 km/h | fail operational: longitudinal control is the most important part of the level 3 automation, to enhance the dependability and user trust this item shall be designed with external to ensure that such take over is prevented | QM |
| HE7 | SG4 | item shall never apply unlimited longitudinal acceleration to prevent unintended longitudinal control, the longitudinal acceleration shall be limited 2 $m/s^2$ | failsafe: the unavailability of the item shall be informed to the driver | C |

| | | | | |
|---|---|---|---|---|
| HE8 | SG5 | item shall never lose the longitudinal control of the vehicle | fail operational: longitudinal control is the most important part of the level 3 automation, to enhance the dependability and user trust this item shall be designed with external to ensure that such take over is controlled | C |
| HE10 | SG6 | item shall never interfere with the lateral control of the vehicle when the vehicle speed is less than 50 km/h | fail operational: lateral control is the most important part of the level 3 automation, to enhance the dependability and user trust this item shall be designed with external to ensure that such take over is prevented | A |
| HE11 | SG7 | item shall never lose the lateral control of the vehicle | fail operational: lateral control is the most important part of the level 3 automation, to enhance the dependability and user trust this item shall be designed with external to ensure that such take over is controlled | C |
| HE12 | SG8 | item shall never apply unlimited lateral control acceleration to prevent unintended lateral control, the longitudinal acceleration shall be limited 1.5 m/$s^2$ | failsafe: the unavailability of the item shall be informed to the driver | C |
| H13 | SG9 | item shall never issue handover or take over request of lateral control when the vehicle is less than 50 km/h | fail operational: lateral control is the most important part of the level 3 automation, to enhance the dependability and user trust this item shall be designed with external to ensure that such take over is controlled | C |

| | | | | |
|---|---|---|---|---|
| HE14 | SG10 | item shall never hand over the control of the vehicle without providing adequate time for the driver to safely respond to take over request and to control the vehicle longitudinal and lateral task of driving | fail operational: lateral control is the most important part of the level 3 automation, to enhance the dependability and user trust this item shall be designed with external to ensure that such take over is controlled | D |
| H15 | SG10 | item shall never fail to communicate correctly through the HMI[6] | fail operational: HMI ECU shall have house measures such | D |
| H16 | SG11 | item shall take over control from the driver only after driver's approval[7] | fail operational: lateral control is the most important part of the level 3 automation, to enhance the dependability and user trust this item shall be designed with external to ensure that such take over is controlled | D |

**Table 23 Safety goals**

### 6.3.6 Functional Safety Concept

The functional safety concept provides measures through which the safety goals can be achieved in the system. The functional safety requirements are allocated to different elements of the system. The safety goals are achieved either by internal or external allocation of functions. The *Table 24* shows few of the concepts defined to achieve the safety goals. The *Figure 43, Figure 44* shows the allocation of functional requirements through which safety goals is achieved.

The Mission Monitor ECU (MM ECU) is an external measure created to achieve the safety goal *SG5*. During the complete failure of ADAS ECU the longitudinal and lateral control of the vehicle is taken over by the MM ECU for *20 s*[8] while altering the driver, if there is no response from the driver to take over the situation the item will lower the speed of the vehicle to a

[6] failure in cluster ECU can be dangerous to most of the vehicle functions
[7] approval can be a push switch in the steering wheel as an example for external measure
[8] not scientific

standstill in the middle of the lane while issuing warning lights for *20 s*. MM ECU will be active in controlling the vehicle only for a period of *40 s*.

If the driver understands the situation, the driver can override the system and can take over the control of the vehicle. In such situation the MM ECU will become passive and act as a diagnostic telemetric and begins the collection of diagnostic information for the rest of the trip while the vehicle function ADAS will be inactive for the driver.

It is also possible to add safety mechanism into the item from the rest of the system. For example, in case of steering system failure the ESP can request ADAS ECU to control the vehicle within the lane and deaccelerate the vehicle to a standstill, this can be possible because of the time to lane crossing calculation in the ADAS ECU. The risk involved in the addition safety mechanism in ADAS and ESP must be evaluated with HARA between the ADAS, ESP and EPS ECU's.

| Safety goal | Functional Safety Requirements | Allocation to the Elements | ASIL |
|---|---|---|---|
| **For all** | ADAS shall check for communication failure, sensor status always. | ADAS/Internal | C |
| **SG2** | MM shall verify the ADAS ECU traffic sign message with the data from GPS ECU(maps). | ADAS/External | C |
| **SG3** | MM shall verify the ADAS acceleration message with the vehicle speed from GPS ECU(maps). | ADAS and External | QM |
| **SG5** | MM shall monitor for ADAS failure and alert the driver with takeover request while controlling the longitudinal and lateral control of the vehicle for 40s in the ego lane with necessary warning to the road traffic. | ADAS and External | C |

Table 24 Functional safety concept with external measures

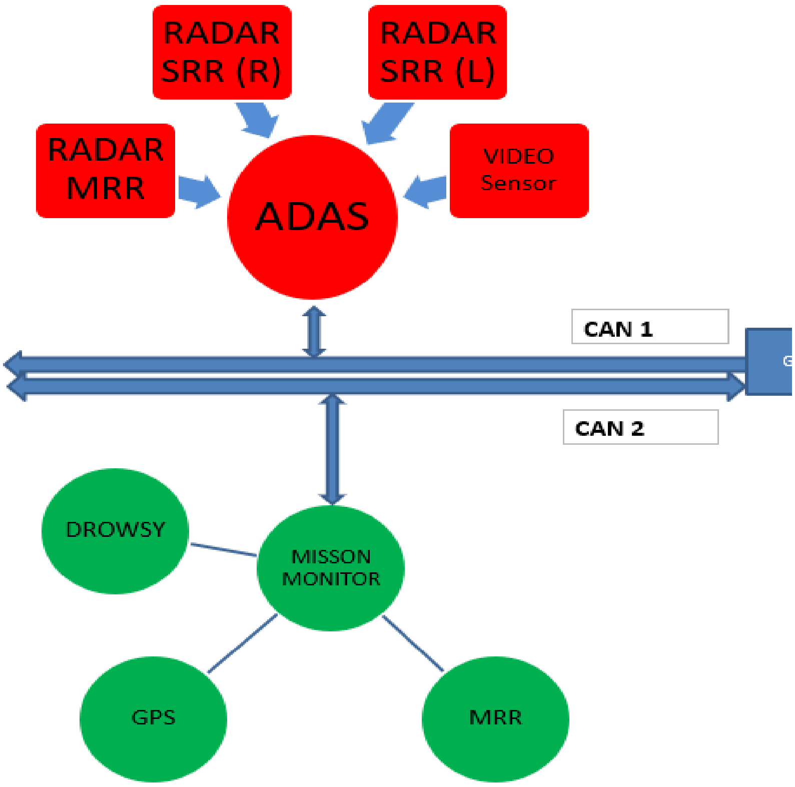


Figure 43 Functional safety concept using external measure

The addition of the second CAN channel ensures the independence between ADAS and the external safety measure.

## 6.4 S-FMEA

The functional safety concept and the system blocks in *Figure 44* are further analyzed with *System FMEA (S-FMEA)*, to ensure there are no hazards leading to improper vehicle behavior.

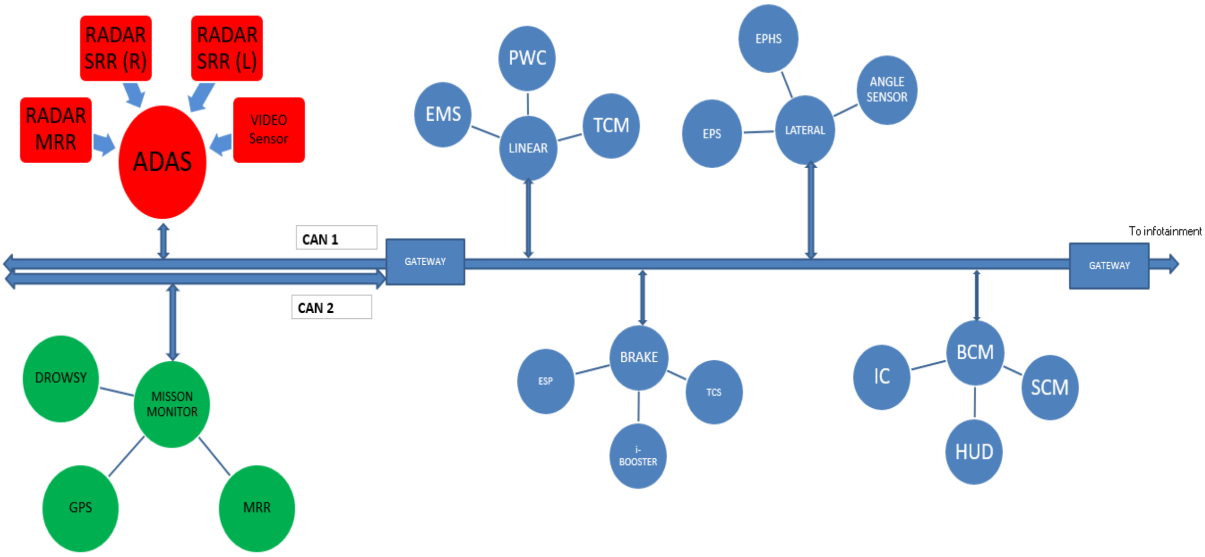


Figure 44 Evolved Safety Requirements

The S-FMEA also ensures that the functional safety requirement fulfills the safety goals. The Figure 45 represents the use of S-FMEA in the methodology.

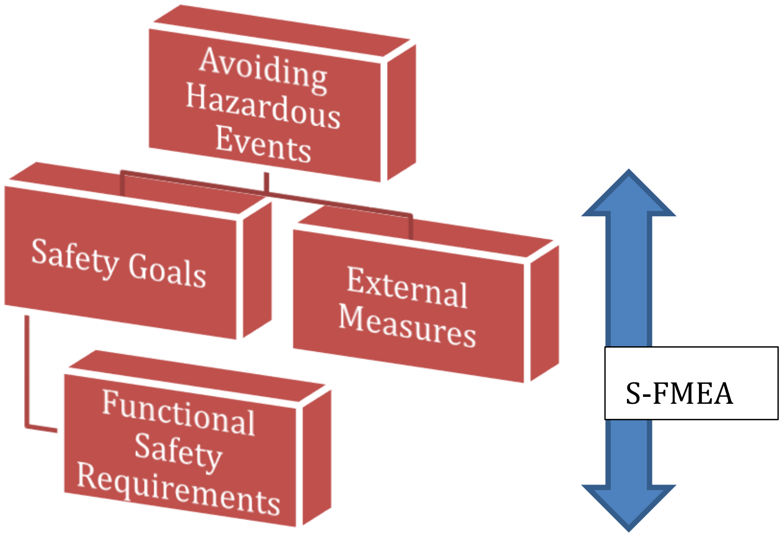
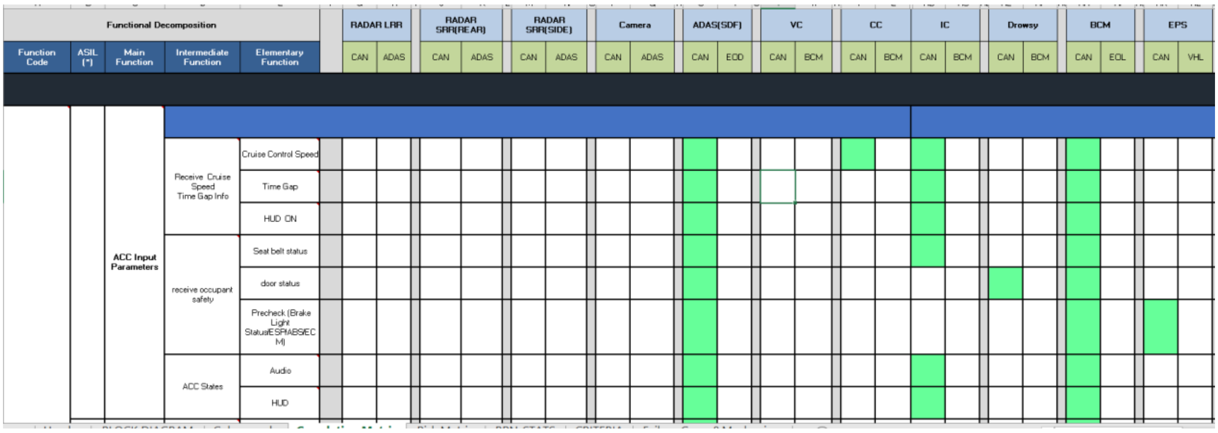


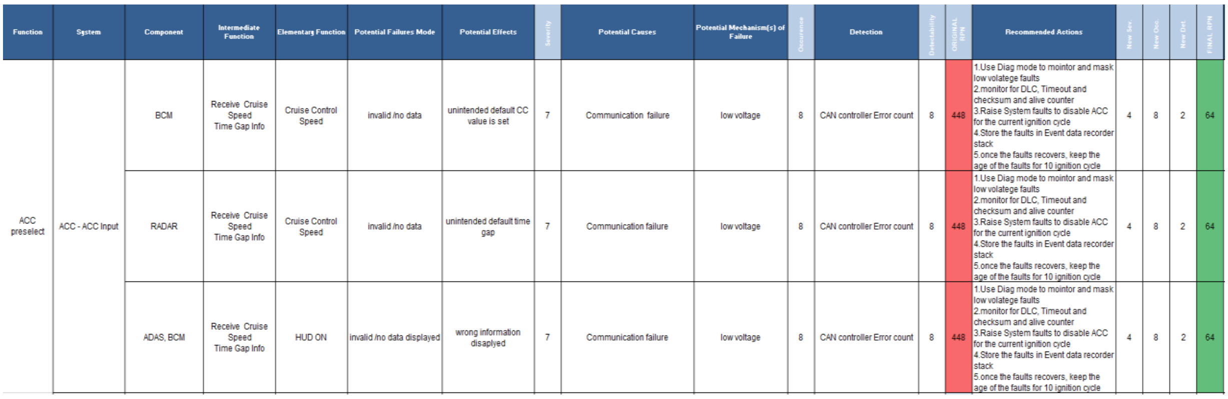
Figure 45 S-FMEA Use

The correlation matrix visualizes the interaction between different *ECU* to accomplish the functions of the ADAS. The risk matrix is done by decomposing the function to elementary level and analyzing the risk with RPN and countermeasures are produced for functions with higher RPN. If the countermeasures proposed are different from that of functional safety requirements, they are added to the system requirements.



| Functional Decomposition | | | | | RADAR LRR | | RADAR SRR(REAR) | | RADAR SRR(SIDE) | | Camera | | ADAS(SDF) | | VC | | CC | | IC | | Drowsy | | BCM | | EPS | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Function Code | ASIL (*) | Main Function | Intermediate Function | Elementary Function | CAN | ADAS | CAN | ADAS | CAN | ADAS | CAN | ADAS | CAN | EOD | CAN | BCM | CAN | BCM | CAN | BCM | CAN | BCM | CAN | EOL | CAN | VHL |
| | | ACC Input Parameters | Receive Cruise Speed Time Gap Info | Cruise Control Speed | | | | | | | | | 🟩 | | | | 🟩 | | 🟩 | | | | 🟩 | | | |
| | | | | Time Gap | | | | | | | | | 🟩 | | | | | | 🟩 | | | | 🟩 | | | |
| | | | | HUD ON | | | | | | | | | 🟩 | | | | | | 🟩 | | | | 🟩 | | | |
| | | | receive occupant safety | Seat belt status | | | | | | | | | 🟩 | | | | | | 🟩 | | | | 🟩 | | | |
| | | | | door status | | | | | | | | | 🟩 | | | | | | | | 🟩 | | 🟩 | | | |
| | | | | Precheck (Brake Light Status/ESP/ABS/ECM) | | | | | | | | | 🟩 | | | | | | | | | | 🟩 | | 🟩 | |
| | | | ACC States | Audio | | | | | | | | | 🟩 | | | | | | 🟩 | | | | 🟩 | | | |
| | | | | HUD | | | | | | | | | 🟩 | | | | | | 🟩 | | | | 🟩 | | | |

Figure 46 Correlation Matrix



| Function | System | Component | Intermediate Function | Elementary Function | Potential Failures Mode | Potential Effects | Severity | Potential Causes | Potential Mechanism(s) of Failure | Occurence | Detection | Detectability | ORIGINAL RPN | Recommended Actions | New Sev. | New Occ. | New Det. | FINAL RPN |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ACC preselect | ACC - ACC Input | BCM | Receive Cruise Speed Time Gap Info | Cruise Control Speed | invalid /no data | unintended default CC value is set | 7 | Communication failure | low voltage | 8 | CAN controller Error count | 8 | 448 | 1.Use Diag mode to mointor and mask low volatege faults<br>2.monitor for DLC, Timeout and checksum and alive counter<br>3.Raise System faults to disable ACC for the current ignition cycle<br>4.Store the faults in Event data recorder stack<br>5.once the faults recovers, keep the age of the faults for 10 ignition cycle | 4 | 8 | 2 | 64 |
| | | RADAR | Receive Cruise Speed Time Gap Info | Cruise Control Speed | invalid /no data | unintended default time gap | 7 | Communication failure | low voltage | 8 | CAN controller Error count | 8 | 448 | 1.Use Diag mode to mointor and mask low volatege faults<br>2.monitor for DLC, Timeout and checksum and alive counter<br>3.Raise System faults to disable ACC for the current ignition cycle<br>4.Store the faults in Event data recorder stack<br>5.once the faults recovers, keep the age of the faults for 10 ignition cycle | 4 | 8 | 2 | 64 |
| | | ADAS, BCM | Receive Cruise Speed Time Gap Info | HUD ON | invalid /no data displayed | wrong information disaplyed | 7 | Communication failure | low voltage | 8 | CAN controller Error count | 8 | 448 | 1.Use Diag mode to mointor and mask low volatege faults<br>2.monitor for DLC, Timeout and checksum and alive counter<br>3.Raise System faults to disable ACC for the current ignition cycle<br>4.Store the faults in Event data recorder stack<br>5.once the faults recovers, keep the age of the faults for 10 ignition cycle | 4 | 8 | 2 | 64 |

Figure 47 Risk Matrix

## 6.5 Iterative HARA

The refinement of system requirements and safety requirements can be accomplished by iterating methodology in *Figure 9 and Figure 10* until the resolution and system improvement has been achieved. This provide a better solution to the overall requirement and design.

Hence in the iterative HARA, the results from safety goal and the *S-FMEA* is added to the *System requirements* and the safety life cycle is restarted with a new item as shown in *Figure 48*

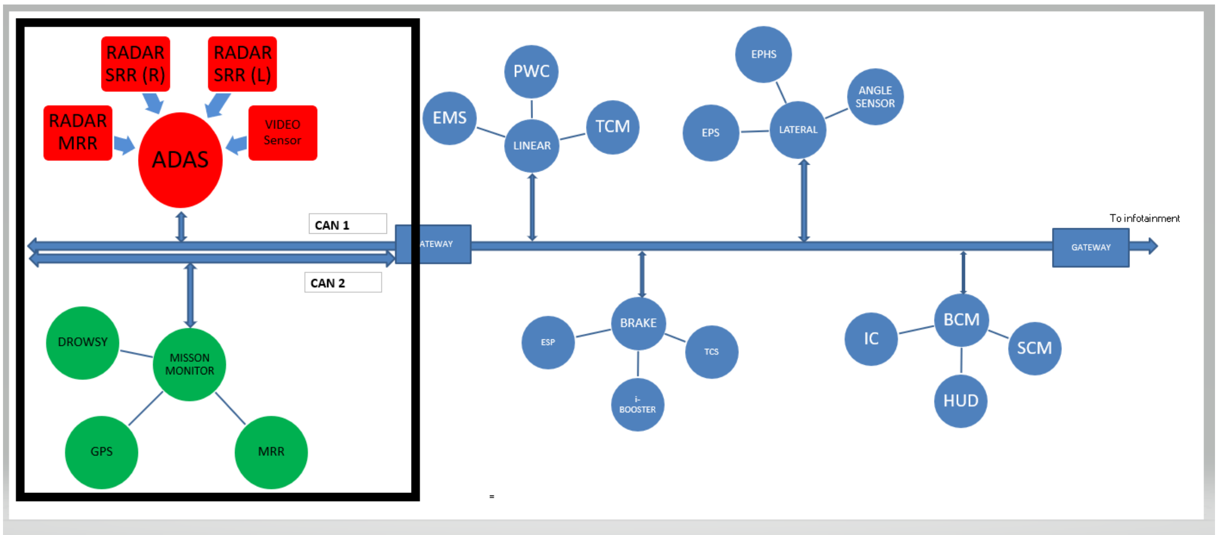


Figure 48 Iterative HARA: New Item

This could lead to following refinement,

- Planning the transfer control between the driver and item before the trip using the GPS information

In this function, the route planning isolates the zones where the speed of the vehicle falls less than 50 km/h and informs the user about the zones where autonomous control of lateral and longitudinal control will not be available. This will reduce the transfer control between the driver and the item, while the driver knows when to expect the transfer control from the item to resume driving in manual mode thus leading to a lower ASIL for *SG5*.

# 7 Conclusion

*Driver of a vehicle shall in all circumstances have his vehicle under control so as to be able to exercise due and proper care and to be at all times in a position to perform all maneuvers required– article 13 of (Vienna Convention on Road Traffic 1968)*

Controllability of the vehicle has been the very essence of automobile driving, from *System requirements* it is evident that the controllability of the vehicle is not available with the driver all the time. This contradiction of must be addressed with dependable system for higher levels of automation.

The methodology perfected with system design and safety life cycle in *Figure 9 and Figure 10* with added guidelines and inclusion of techniques like *STPA, FMEA and Parametrization Of S, E & C* will improve the accuracy in the finding the ASIL and deriving safety goals based on reasoning and scientific data. The methodology could be utilized in analyzing other work products of PART 3 and other PARTS of ISO26262.

The risk reduction that is ensured through safety goals and their respective functional safety concept assisted by external measures and adding a new CAN Channel is a starting point in understanding the complexity in design and resource needed in safe autonomous future.

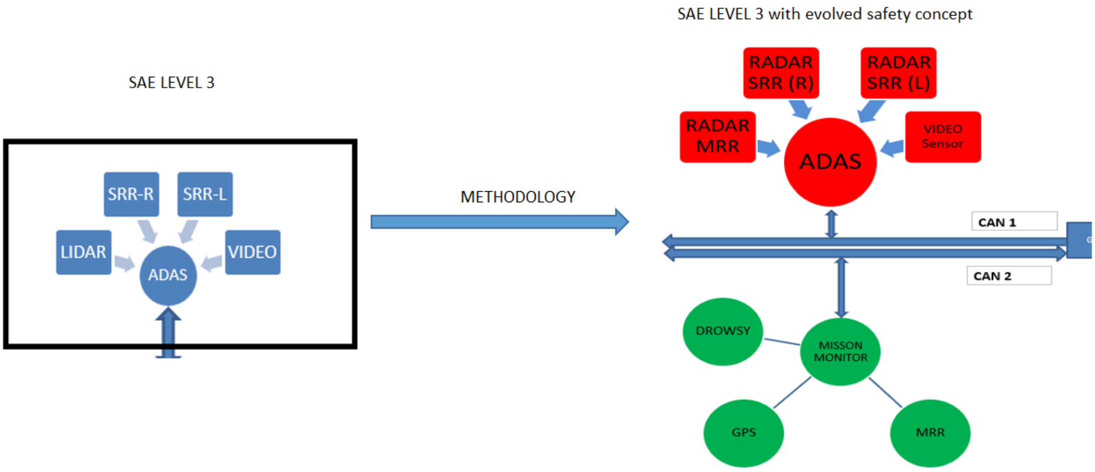


**Figure 49 Evolution of Architecture**

The difference between the system requirement which dictates the nominal performance and the safety requirements which adds function to keep the risk within the tolerable range is evident from *System requirements* and *Determination of Safety Goals*

The work carried out in this thesis can be extended in the future by exploring the following topics,

## 7.1 Usecase for Validation

Usecase from the system and safety life cycle of the concept stage can be extended to system validation and system performance characterization. By defining an usecase library with huge number scenarios that can be read by virtual simulators, the generation of test specification for the vehicle functions can be automated which could partially solve the burning how much validation is enough for higher levels of automation.

## 7.2 Simulation for HARA

Appropriate simulation tools can used to model the controller (AEBS, ACC, LKAS, LC etc..) and the fault injection methodologies can be used to observe vehicle dynamics and other relevant parameters which leads to HARA, ASIL, the assumptions and rational be scientific.

# 8 Abbreviations

| | |
|---|---|
| ADAS | Advanced Driver Assistance System |
| AEB | Autonomous Emergency Breaking Systems |
| ACC | Adaptive Cruise Control |
| AUTOSAR | Automotive Open Source Architecture |
| CMOS | Complementary Metal Oxide Semiconductor |
| CCD | Charge Coupled Device |
| ECU | Electronic Control Unit |
| ESA | Evasive Steering Assist |
| ESP | Electronic Stability Program |
| EPS | Electronic Power Steering |
| FSRA | Full Speed Range Adaptive Cruise Control |
| LDW | Lane Departure Warning |
| OEM | Original Equipment Manufacturers |
| GS | Global shutter |
| RADAR | Radio Detection and Ranging |
| RDM | Road Departure Mitigation |
| FMEA | Failure Mode Effective Analysis |
| FTA | Fault Tree Analysis |
| FSRA | Full Range Speed Adaptive Cruise Control |
| PHA | Preliminary Hazard Analysis |
| QA | Queue Assist |
| STPA | Systematic theoretic Process |
| HAZOP | Hazard and Operability Study |
| UCA | Uncontrolled Control Actions |
| HARA | Hazard and Risk Analysis |

# 9 Bibliography

Alexander, Kossiakoff, William N Sweet, Samuel J Seymour, and Steven M Biemer. 2011. *Systems engineering principles and practice.* John Wiley & Sons.

Audi. 2011. *Audi Technological Portal, Audi pre sense.* Accessed 12 21, 2017. https://www.audi-technology-portal.de/en/electrics-electronics/safety-systems/audi-pre-sense_en.

AUDI. 2017. *AUDI, Driver assistance systems.* 02 17. Accessed 12 21, 2017. https://www.audi-mediacenter.com/en/technology-lexicon-7180/driver-assistance-systems-7184.

Belvoir Defence Acquisation. 2001. *System Engineering Fundamentals.* Virginia: DEFENSE ACQUISITION UNIV FT BELVOIR VA. http://www.dtic.mil/get-tr-doc/pdf?AD=ADA606327.

Broggi, A, M Bertozzi, A Fascioli, C. G. L Bianco, and A. Piazzi. 1999. "The ARGO autonomous vehicle’s vision and control systems." *International Journal of Intelligent Control and Systems, 3(4), 409-441.*

Cockburn, Alistair. 2000. *Writing effective use cases,.* Addison-Wesley Professional Reading.

Continental. 2014. *Contienetal HUD.* 06 14. Accessed 01 2018. http://continental-head-up-display.com/.

Continental Engineering Services. 2015. *Continental Engineering Services ADAS.* 11 16. Accessed 01 08, 2018. https://www.conti-engineering.com/CMSPages/GetFile.aspx?guid=c3af2186-8330-4c66-bdbd-c082502ca609.

Dr. Azim Eskandarian, D.Sc, Bart van Arem-TU Delft. 2012. *Handbook of intelligent vehicles.* London: Springer.

Dubrova, Elena. 2013. *Fault-tolerant design.* . Berlin: Springer.

Ericson II, Clifton A. 2005. *Hazard analysis techniques for system safety.* Virginia: John Wiley & Sons, Inc.

Federal Aviation Administration. 2000. *System Safety Handbook.* Washington: Federal Aviation Administration.

Federal Highway Administration. 2007. *Systems Engineering for Intelligent Transportation Systems.* Washington: Department of Transportation.

FEV . 2013. *Vechicle Network Architecture and Validation* . 05 02. Accessed 01 05, 2018. http://www.fev.com/en/what-we-do/engineering-services/vehicle-electronics-infotainment-and-telematics/products/vehicle-network-architecture-and-validation.html.

Hommes, Qi Van Eikema. 2015. "Safety Analysis Approaches For Automotive Electronic Control Systems." John A Volpe National Transportation Systems Center, Office of the Secretary of Transportation - U.S. Department of Transportation.

ISO26262,. 2011. "Road vehicles-Functional safety." International Standard ISO.

J3016, SAE. 2014. *Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems.* SAE International.

Khastgir, Siddartha, Stewart Birrell, Gunwant Dhadyalla, Håkan Sivencrona, and Paul Jennings. 2017. *Towards increased reliability by objectification of Hazard Analysis and Risk Assessment (HARA) of automated automotive systems.* Safety Science.

Leveson, Nancy, and John Thomas. 2013. *An STPA primer.* Cambridge.

Merat, Natasha, A. Hamish Jamson, Frank CH Lai, Michael Daly, and Oliver MJ Carsten. 2014. "Transition to manual: Driver behaviour when resuming control from a highly automated vehicle." *Transportation research part F: traffic psychology and behaviour 27*, 274-282.

Peter Labaziewicz, Texas Instruments. 2014. *Texas Instrument behind the wheel blog.* 09 2014. Accessed 01 09, 2018. https://e2e.ti.com/blogs_/b/behind_the_wheel/archive/2014/09/25/cars-are-becoming-rolling-sensor-platforms.

PROMETHEUS. 1995. *PROMETHEUS.* http://www.eurekanetwork.org/project/id/45.

Rausand, Marvin. 2013. *Risk assessment: theory, methods, and applications.* John Wiley & Sons.

SAE. 2016. *Centimeter-accurate GPS for self-driving vehicles.* 11 02. Accessed 2018. http://articles.sae.org/15067/.

Smith Bryant Walker, Standford. 2013. *Stanford law school.* 12 18. Accessed 01 8, 2018. http://cyberlaw.stanford.edu/blog/2013/12/sae-levels-driving-automation.

Stamatelatos, M., W., Vesely, J., Dugan, J., Fragola, J., Minarick, and J. Railsback. 2002. *Fault tree handbook with aerospace applications.* Washington, DC 20546: NASA Office of Safety and Mission Assurance.

Stamatis, D. H. 2003. *Failure mode and effect analysis:FMEA from theory to execution.* . ASQ Quality Press.

Stove, Andrew G. 1992. "Linear FMCW radar techniques." *IEE Proceedings F (Radar and Signal Processing), vol. 139 no. 5,* (Stove, Andrew G. "Linear FMCW radar techniques." In IEE Proceedings F (Radar and Signal Processing), vol. 139, no. 5, pp. 343-350. IET Digital Library, 1992.) 343-350.

Toyota. 2015. *Road Sign Assist (RSA),Active Safety.* Accessed 2017. http://www.toyota-global.com/innovation/safety_technology/safety_technology/technology_file/active/rsa.html.

Transport Canada. 2013. *Transport Canada.* 12 10. Accessed 12 21, 2017. http://www.tc.gc.ca/eng/motorvehiclesafety/safevehicles-1175.htm.

Vesely, W. E.,, F. Goldberg, Roberts, F., and & Haasl, D. F. N. H. 1981. *Fault tree handbook (No. NUREG-0492).* Washington DC.: Nuclear Regulatory Commission .

1968. "Vienna Convention on Road Traffic." Vienna.

Winner, H, S Hakuli, F.,& Singer Lotz, C.Heinrich Gotzig, Geduld, Georg Martin Punke, and Stefan Menzel. 2015. *Handbook of Driver Assistance Systems: Basic Information, Components and Systems for Active Safety and Comfort.* Springer Publishing Company, Incorporated.

Young, Mark S.,, and Neville A. Stanton. 2007. "Back to the future: Brake reaction times for manual and automated vehicles." *Back to the future: Brake reaction times for manual and automated vehicle Ergonomics 50, no. 1*, 46-58.