POLITECNICO DI TORINO

Collegio di Ingegneria Informatica, del Cinema e Meccatronica

Department of Control and Computer Engineering

Master's Degree in Mechatronic Engineering

Functional Safety for Advanced Driver-Assistance Systems

Relatore
prof. Massimo Violante

Candidato
Giuseppe Allegra

A.A. 2017-2018

Functional Safety for Advanced Driver-Assistance Systems

“If a machine is expected to be infallible,
it cannot also be intelligent.”

Alan Touring, 1947.

Preface

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

MCA Engineering is part of MCA Group, an international player in engineering and high-tech consulting. MCA's consultants are engineers commissioned for strategic and technical in some of the biggest companies in the industrial and tertiary fields.

Acknowledgements

I would like to mention all those who helped me in writing the thesis with suggestions, criticisms and observations: my gratitude goes to them.

I want to thanks Luca, of MCA Engineering, for giving me the chance to realize this thesis and Vincenzo, Rubin and Rosanna for their support throughout the duration of the thesis.

I thank Professor Massimo Violante, of the Politecnico di Torino, for his support and advices during the thesis project.

Special thanks go to colleagues and friends who have encouraged me or who have spent part of their time to read and discuss work drafts with me.

Abstract

Automotive industry is currently looking for solutions to help people while driving. All these systems integrate several technologies subjected to increasing risk of failures and therefore OEMs need to implement safe system development processes. ISO 26262 provides guidance for safe system development processes and requirements for achieve an acceptable level of safety.

The purpose of this thesis in conjunction with *MCA Engineering* is to study the world of Advanced Driver-Assistance Systems and, starting from the concept phase of a safe system development, the object is to analyze the Forward Vehicle Collision Mitigation System (FVCMS) and some possible faults that can appear in an Autonomous Emergency Braking System (AEBS).

Contents

List of the Figures

List of the Tables

List of the Equations

Introduction

Nowadays, vehicle functions are one of the main forms of distinction through which OEMs tend to differentiate and increase their market. Advanced Driver-Assistance Systems represent one of the most important sector of vehicle industry and it is an ever-changing field that was revolutionizing the world of the transport.

In most countries, the road traffic is regulated through the "Vienna Convention on Road Traffic"; the international treaty, signed in 1968, established a standard traffic rules to facilitate traffic and to increase road safety. Regarding drivers, the Convention gives the following definitions (Vienna Convention on Road Traffic 1968):

- ARTICLE 8[1]:*"Every moving vehicle or combination of vehicles shall have a driver".*
- ARTICLE 8[5]:*"Every driver shall at all times be able to control his vehicle…".*

Defined these fundamental parameters of driving, it is clear that the development of ADAS is a crucial sector and, therefore, it is important to fix rules that can assert a high level of safety for the coexistence between drivers and vehicle systems.

In this thesis the world of Advanced Driver-Assistance Systems is investigated, considering classifications, interaction with drivers and related issues. Then it is analysed the safety in the automotive systems and the standard ISO 26262, giving special attention to chapter 3 “Concept phase”. The thesis continues with a section, dedicated to the longitudinal control and the Forward Vehicle Collision Mitigation Systems (FVCMS), with mathematical model and some simulations. The final part of the thesis includes the study of an Advanced Emergency Braking System (AEBS) with a Hazard Analysis and Risk Assessment (HARA), in accordance with the ISO 26262. Finally, a fault tolerant system is proposed and it is simulated by means of a Matlab/Simulink model.

The thesis is divided into the following sections:

- **Intelligent Transportation Systems and Advanced Driver-Assistance Systems:** it contains definitions and descriptions of advanced driver-assistance systems with historical and bibliographic references.

- **Safety of automotive system:** in this section it is analysed the safety cycle about the ISO 26262 and some safety analysis as a support for the functional safety.

- **Forward Vehicle Collision Mitigation System:** in this chapter the Forward Vehicle Collision Mitigation System is analyzed by means of the ISO 22839; then an Advanced Emergency Braking System is investigated and some simulation, based on Euro NCAP test scenarios are presented.

- **HARA analysis and Fault injection for AEBS:** it contains a HARA analysis for Advanced Emergency Braking System and some fault injection simulations of a fault tolerant system, using a Matlab model.

- **Conclusions:** the last chapter contains the conclusions of the thesis and some ideas for future works.

1 Intelligent Transportation Systems and Advanced Driver-Assistance Systems

1.1 Definitions of Intelligent Vehicles

Webster's Dictionary defined the term "intelligent" as "having or indicating a high or satisfactory degree of intelligence and mental capacity", and "intelligence" as "the ability to learn or understand or to deal with new or trying situations". Shifting these definitions to vehicles, the term "intelligent" is defined as "guided or controlled by a computer; *especially*: using a built-in microprocessor for automatic operation, for processing of data, or for achieving greater versatility" (Eskandarian 2012). An intelligent vehicle drives with autonomy or assists the driver improving safety and efficiency.

The term "autonomous" refers to the ability to operate without human command. The vehicle has to sense the scenario, analyze it and response. For example, if the vehicle hold a function to maintain the lane, it has to control the environment, perceive a possible change of lane and finally react by steering, accelerating or braking.

The term “Advanced Driver-Assistance Systems” defines all the handling functions that an intelligent vehicle provides to support the driver in every aspects of the trip or to drive autonomously.

1.2 The ARGO Project

The ARGO autonomous vehicle project was an Italian studies of the 1990s, about the field of ADAS. The main target of the ARGO Project was the development of an active safety system able also to act as an automatic pilot for a standard road vehicle (Broggi, et al. 1999). The project was based on two design choices: the only use of passive sensors and to keep the system costs low (production and operative costs). The experimental vehicle ARGO (Figure 1 and Figure 2) was equipped with vision system and an automatic steering capability and it was able to determine its position with respect to the lane, to compute the road geometry, to detect generic obstacles on the path, and to localize a leading vehicle. The images acquired were analyzed in real-time by a computer and the results of the elaborations were used to control an actuator on steering wheel and other devices (Broggi, et al. 1999). On ARGO the data were acquired through two synchronized cameras and a speedometer was used to detect vehicle velocity; then data were processed with a standard 450 MHz Pentium II processor. The output devices are acoustical, optical and mechanical.

Figure 1 - Argo prototype (Broggi, et al. 1999)

There were three level of intervention: Manual Driving (the system only monitors driver's activity), Supervised Driving (the system warns the driver in dangerous situations) and Automatic Driving (the system fully controls the trajectory) (Broggi, et al. 1999).

The functionality of the vehicle was extensively test by a 2000 km journey in June 1998 along Italian highway. After the tour, the collected logs were analyzed to compute the performance of the system. The weakest components of the system were proved to be the cameras because the change in the illumination caused degradation of the image quality (Broggi, et al. 1999).

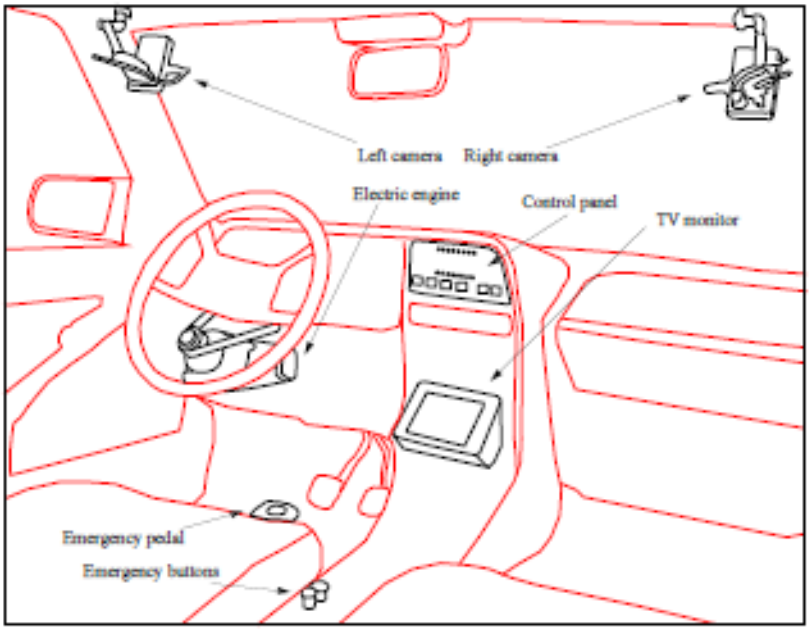

Figure 2 - Internal view of ARGO prototype (Broggi, et al. 1999)

The study on ARGO vehicle highlighted some of the problems of automated driving but the project was useful to open the way towards the development of ADAS system.

1.3 Classification of Intelligent Functions

With reference to the task of driving a vehicle, we can classify Intelligent Functions based on the driving task, the type of road, and the level of support.

1.3.1 Driving task

This method consists of a layered hierarchical structure with three level: strategic, tactical and operational level. (Michon 1985)

- Strategic or navigational level uses as target the destination, the route and the driving style. The time scale of the level is in the order of minutes.
- Tactical or maneuvering level involves road layout and road users (lane changing, turning). The time scale is evaluated in the order of 10 s.
- Operational or control level includes control of the vehicle (steering, brake, throttle and clutch). The time scale of the level is in the order of 1 s (Eskandarian 2012).

1.3.2 Type of traffic

An important characteristic of ADAS is the type of traffic. Classifying it from the least complex to the most complex, there are three groups:

- Motorway traffic
- Rural traffic
- Urban traffic

The characteristics of the type of traffic are summarized in Figure 3.

Motorway traffic	Rural traffic	Urban traffic
Most homogeneous class of roads with rather uniform traffic conditions	Non-motorway connections outside urban built-up areas	Heterogeneous class, widely different in terms of size and density
Sparse network, few intersections and entry/ egress points, traffic separated by direction	Moderately dense network, two-way traffic, limited intersections with traffic control	Dense and complex road networks, intersections and crossings; two-way traffic, traffic signals
Moderate to very high traffic flow levels, homogeneous traffic, generally rather high speeds except in congestion with stop-and-go conditions, standardized and predictable road geometry	Mixed traffic but mainly used by motorized traffic, wide range of driving speeds, wide variety of road geometry	Varying traffic loads, complex traffic composition
Low to moderate levels of driver attention, except in (nearly) congested conditions	Moderate to high driver loads	Low to moderate speeds, heavy driver load

Figure 3 - Type of traffic classification (Eskandarian 2012)

1.3.3 Support of intelligent transport

It is possible to distinguish three type of system: informing, supporting and automatic system.

- Informing system only informs but every decision belongs to the driver. The system can use visual or acoustic warnings.

- Supporting system supports but the driver is in control of the vehicle and can override the system.

- Automatic system performs some driving tasks and intelligent function can be overrulable or non-overrulable.

Informing systems have a high acceptance because the driver is freedom to act, instead supporting and automatic systems are more effective but require experience for people to trust them (Eskandarian 2012).

1.4 Issues related to automation

Technology is not the only issue within autonomous driving field. SMART64 report (van Schijndel-de Nooij, et al. 2011) gives the following definitions:

- ***Automated driving:*** *"Driving enhanced by dedicated control, existing of autonomous (sub)system that support the driver, while he/she is in control or able to timely get back in control and which is legally responsible throughout for carrying out the driving task. Automated systems can operate continuously (for example steer-by-wire) or can operate at specific moments when dedicated interventions become necessary (e.g. parking assist). Automation can cover a wide spectrum, from relatively weak support to highly automated driving".*

- ***Autonomous driving:*** *"The extreme end result of automated driving. In principle, no human driver needs to be active in operating the vehicle, although a driver can still be, but does not need to be in place".*

- ***Cooperative driving:*** *"Addresses automotive and road traffic systems that make use of information and communication technologies (ICT), in conjunction with automated or non-automated driving vehicles. These technologies are used to exchange specific information between vehicles (vehicle-to-vehicle communication, or V2V) and between vehicles and road infrastructure (V2I). ICT gives vehicles an additional input level that enhances their ability to make intelligent manoeuvre in traffic regardless of their level of automation*".

From these definitions it appears clear that there are some issues related to how much a driving functionality is automated (Okuda, Kajiwara e Terashima 2014).

1.5 Advanced Driver-Assistance Systems

ADAS system consists of a single or multiple sensors that sense a target and communicate with other ECU in the vehicle to assist the driving, providing also a visual or audio warning to the driver. Anytime the driver has to be able to take the control of the ADAS function and override it. However, not all systems work in the same way: some of them have only an assistance function and do not act on the guide. Table 1 lists some Advanced Driver-Assistance Systems and Table 2, instead, contains some of the sensors used for ADAS.

ADAS	Functionality
Adaptive cruise control	Maintains safe distance from vehicle ahead
Anti-lock braking system	Prevents the locking of the wheels during braking
Automatic parking	Moves vehicle into a parking spot
Automatic navigation system	Finds direction in a vehicle
Automotive night vision	Helps driver to see in darkness or poor weather
Blind spot monitor	Detects vehicles located side and rear
Collision avoidance system	Detects an imminent crash
Cruise control	Maintains the speed set by the driver
Driver drowsiness system	Prevents crash caused by drowsy driver
Driver monitoring system	Monitor the attention of the driver
Electric vehicle warning sounds	Alerts pedestrian to the presence of vehicle
Emergency driver assistant	Overrides driver in case of medical emergency
Intelligent speed adaptation	Ensures vehicle does not exceed safe/legal speed
Lane departure warning system	Warns driver when vehicle move out of its lane
Parking sensor	Alerts driver in case of obstacle while parking
Tire pressure monitoring	Monitors the air pressure inside tires
Traffic sign recognition	Recognizes traffic signs
Turning assistant	Monitor traffic while turning

Table 1 – ADAS examples

Sensors
Cameras
LIDARs
Ultrasonic
Short/Medium-range RADAR
Long-range RADAR
Infra-red

Table 2 – ADAS sensor

Figure 4 shows a view of vehicle sensors with their position.

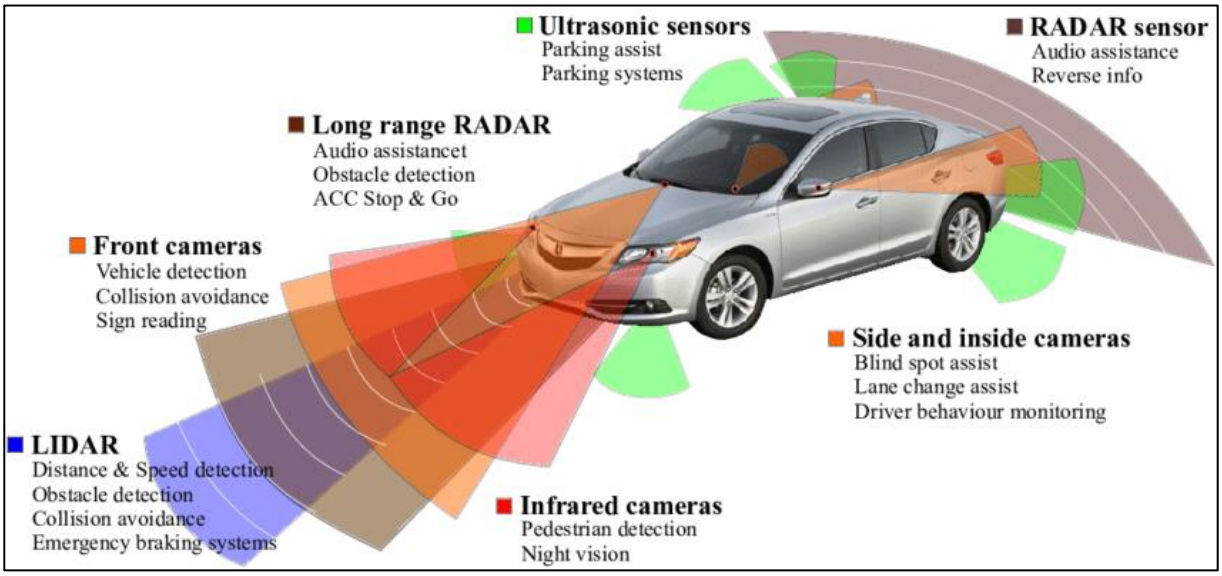

Figure 4 – Typical sensors for ADAS (Rezaei 2014)

1.5.1 Level of intervention

ADAS can be grouped according to the interaction with driver and driving control (Figure 5) (Eskandarian 2012):

Classification of driver assistance systems	Function or task (perception: sensing, estimating, computing)	Interaction with driver or intervention in driving task (response action)
Informational	Sense environment, road, weather, retrieve real-time or archival data	Enhances situational awareness and condition monitoring: display and present the relevant information
Warning-alerting	Sense condition, evaluate situations and potential hazards, decide when and what to do, decide corrective action	Alerts the driver of potential hazards and possibly recommend corrective actions (slow down, brake, steer)
Partial (semi) control	Sense condition, evaluate situations and potential hazards, decide when and what to do, decide corrective actions	Provide both warnings/alerts and partial control functions (e.g., apply partial brake force, stiffen gas pedal to retard speeding)
Automatic (full) control	Sense condition, evaluate situations and potential hazards, decide when and what to do, decide corrective actions	Apply the vehicle control function as needed (automatically apply the brakes, ESP, etc.)
Autonomous control	Have a trip plan (from origin to destination), have navigation plan, vehicle guidance and control, sense condition, evaluate situations and potential hazards, decide when and what to do, decide corrective actions	Execute the trip plan, generate navigation, guidance, trajectory plan, and execute vehicle control; execute collision avoidance and redirection, and reroute plan and control as necessary

Figure 5 - ADAS classification (Eskandarian 2012)

- ***Informational Systems***: provide only information to drivers in a nonintrusive way; they give alerts and advises but they are not projected for emergencies. Examples: traffic warning, wet road condition.

- ***Warning Systems***: support the drivers for specific safety situations; they provide warnings that can be visual in the instrument panel or in the display, auditory (beeping or buzzer sounds), haptic (vibrations), or a combination of the previous.

The mode, the timing and the frequency or the warning are planned during the design. Example: lane departure.

- ***Partial Control Systems***: improve the safety of the vehicles; they support the driver but do not take the control of the vehicle and the driver can overtake the control. Examples: ACC, brake assist.

- ***Automatic Control Systems***: are transparent to the driver in several dynamic functions; they act on suspensions, electronics, chassis, etc. Examples: TC, ESC, ABS.

- ***Autonomous Control System***: replace the driver through an autopilot system; they control all the aspects of the driving: trip planning, navigation, trajectory, guidance and control.

1.5.2 Adaptability and other classification

ADAS can be also categorized considering its level of adaptability to the driver and two methodologies can be adopted:

- Designing a generic system and the driver will adapt to it.

- Designing a customized system for a particular driver.

Generally the existing system are designed with the first method. They mitigate hazardous event or give information but they act without considering driver behaviour. Customized system are more difficult to design. Many parameters must be taken in consideration and all of these are specific for individual drivers. Furthermore, designing a system for a specific driver requires more time and lots of tests (Eskandarian 2012).

It is possible to consider a further method to distinguish ADAS:

- ADAS for normal driving.
- ADAS for emergency or hazardous driving.

Finally, we can classify them using a temporal method:

- Pre-crash region technology.
- Post-crash region technology.

1.6 Interaction with drivers

The main aim of ADAS system is to support driver experience improving the safety, the efficiency and the comfort. An important aspect to consider is related to the expectations of the end-user and how they approach the technology. This aspect was the goal of a research made in cooperation between the Vehicle and Traffic Safety Centre at Chalmers University of Technology, the Swedish National Road and Transport Research Institute, the Technical Research Institute of Sweden and the Division Design and Human Factors at Chalmers University of Technology (Strand, et al. 2011).

The aim of the study was the analysis of driver experiences of five driver assistance system: adaptive cruise control, blind spot monitoring, forward collision warning, lane departure warning and driver state warning. Data were collected by means of group interviews. The results revealed how drivers interacted with the systems. The research participants had different views for the functionality of the systems and they used them differently. Furthermore, there was a discrepancy between the driver understanding and how manufacturers described these systems. These difficulties sometimes resulted in different reactions, such as frustration or turning system off. The study revealed also positive effects on the drivers, including calmer driving, increased use of indicators and avoided accidents (Strand, et al. 2011).

It appears clear that a better explanation of the ADAS functionality is important to improve the effectiveness of the assistance functions.

1.7 Human performance capacity

To understand the links between driver, environment and vehicle, is important for the design of the driver assistance system. Particularly considerable is the human action of information processing which can be decomposed into three parts: perception, cognition and action. The *perception* is realized for the most part by sight (80-90%) and remaining information is perceived by hearing and touch. The frequency of stimuli can limit the performance and similar stimuli can interfere between themselves; consequently, the driver could lose data during the process of information intake. *Cognition* includes all processes made in order to take a decision about a possible action. The processing stage is influenced by individual tolerance and perception of risks and it affects the risk of accident. The *action* step is the last level of the information processing system; the decisions, made in the cognition stage, are translated into actions (Winner, et al. 2016). Three examples of this decomposition are shown in the following figures by means of simple driving tasks: maintaining a desired speed (Figure 6), lane changing (Figure 7) and avoiding of obstacles (Figure 8).

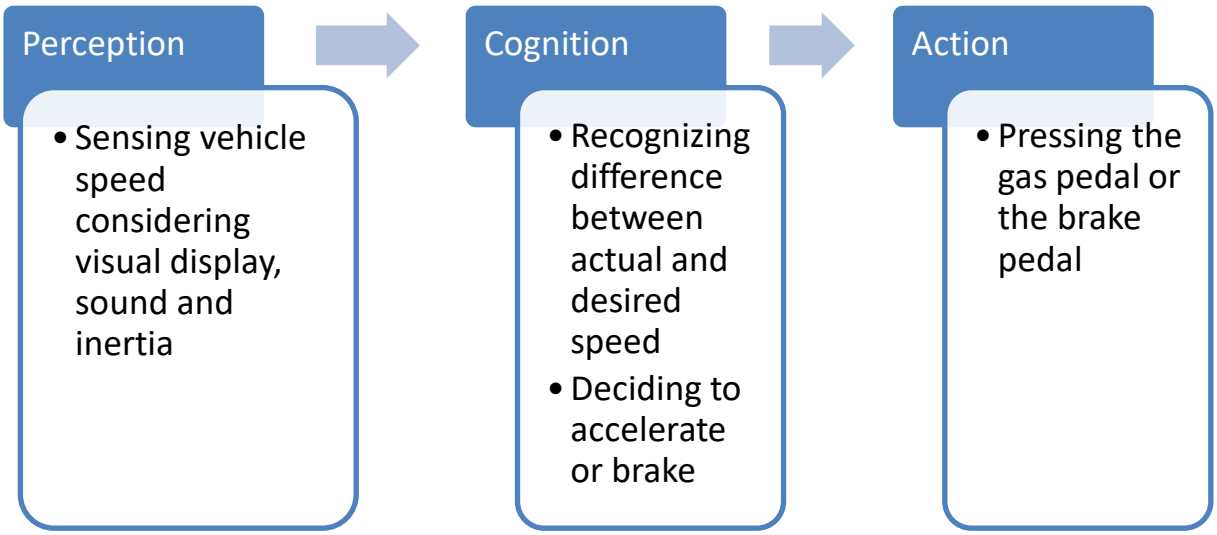

Figura 6 - Maintaining a desired speed

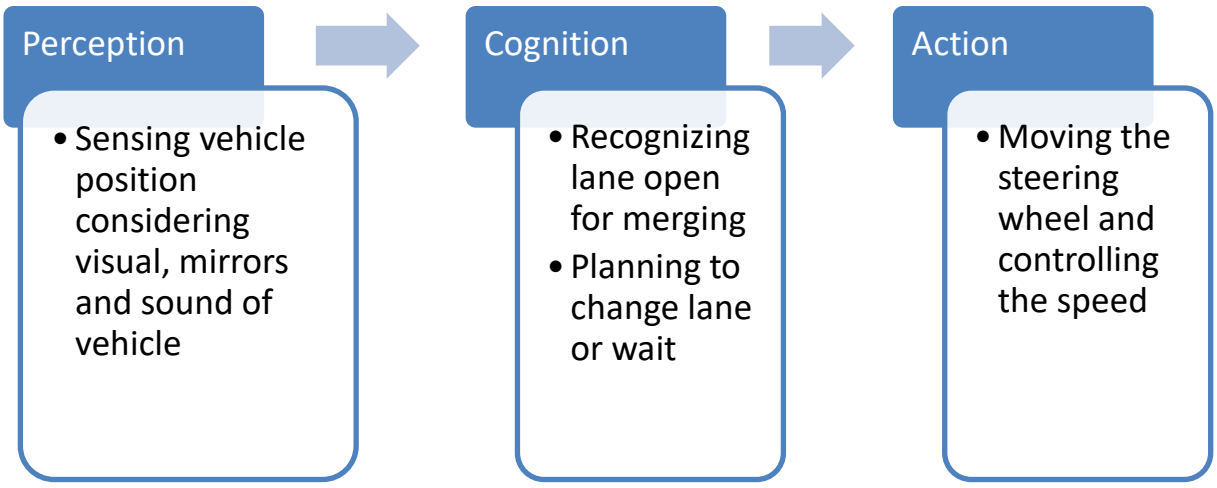

Figura 7- Lane changing

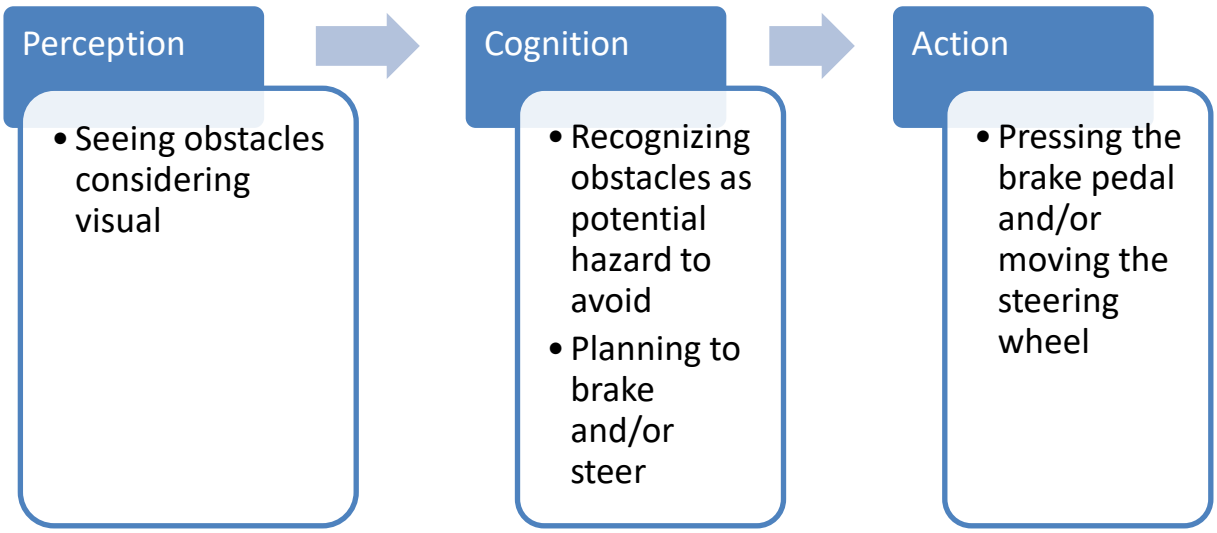

Figure 8 - Avoiding of obstacles

The variability of actions made by driver is the consequence of inter-individual and intra-individual variations, which can be classified into three groups: properties, capacities and skills. *Properties* are intra-individual variables and the most relevant are age, gender and personality. *Capacity* are time-dependent intra-individual variables and cause a reduced performance. These characteristics are affected by static and dynamic visual acuity, sensitivity to light and limitation of visual field. Finally, *skills* are human functions; among the skills we have to pay attention to driving experience, driving style and driver type (Winner, et al. 2016). In addition, there are other variables which affect the reaction time and the response of driver: urgency, mental load, fatigue, visibility and distraction.

The evaluation of human performance capacity starts from driving requirements (Winner, et al. 2016):

- *Information sources, sensory and perception processes*: visual displays, acoustic information (sirens and warning system) and secondary acoustic information (radio, conversation with passengers or on the telephone), road users, characteristics of the route, traffic signs, condition of the road and weather.
- *Evaluation*: longitudinal and horizontal distances, speeds and critical traffic situations.
- *Decision making and thought processes*: selecting suitable actions for navigating the vehicle and for vehicle guidance.
- *Vehicle manipulation*: controlling longitudinal motion (accelerating, braking) and horizontal motion (steering) and controlling actions (lights, radio, …)

These demand areas must be evaluated in order to find out which sectors need technical support.

1.8 SAE International Levels

SAE International (Society of Automotive Engineers) is a U.S. professional association and standard developing organization, especially, in the transport industry. SAE J3016 (SAE International 2016) provides detailed definitions for the levels of driving automation in the context of motor vehicles and their operation on roadways. The primary actors are three: the human driver, the driving automation system and other vehicle systems and components.

The levels of driving automation are six:

- Level 0 – No Driving Automation
- Level 1 – Driver Assistance
- Level 2 – Partial Driving Automation
- Level 3 – Conditional Driving Automation
- Level 4 – High Driving Automation
- Level 5 – Full Driving Automation

A summary of the SAE Levels, compared with those defined by the German Federal Highway Research Institute (BASt) and by the U.S. National Highway Traffic Safety Administration (NHTSA) is reported in Table 3.

0. ***No Automation:***
The driver controls lateral and longitudinal motion of the vehicle and the system assists the driver with only warnings.

1. ***Driver Assistance:***
The driver and the system share lateral and longitudinal motion of the vehicle; the driver monitors the environment.

2. ***Partial Automation:***
The system controls lateral and longitudinal motion of the vehicle and the driver monitors the environment; the driver must be available to take the control of the vehicle if it is necessary.

3. ***Conditional Automation:***
The system controls all the aspect of driving (lateral and longitudinal motion and monitoring of the environment); the driver must be available to take the control of the vehicle if it is necessary.

SAE level	Name	Narrative definition	Execution of steering and acceleration/ deceleration	Monitoring of driving environment	Fallback performance of dynamic driving task	System capability (driving modes)	BASt level	NHTSA level
Human driver monitors the driving environment			Human driver	Human driver	Human driver	n/a		
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 system					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			System	System	Human driver	Some driving modes		
3	Conditional Automation	The driving mode-specific 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					High automated	3
4	High Automation	The driving mode-specific by an automated driving system of all aspect 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 condition that can be managed by a human driver	System	System	System	Full driving modes		

Table 3 – SAE levels (Walker Smith 2013)

4. ***High Automation:***
   The system controls all the aspect of driving (lateral and longitudinal motion and monitoring of the environment) and it is able to react appropriately even if the driver does not respond to a request to intervene.

5. ***Full Automation:***
   The system controls all the aspect of driving (lateral and longitudinal motion and monitoring of the environment).

2 Safety of automotive systems

The most relevant factor for the safety of road vehicles is the behaviour of the driver. Several studies estimate that over than 90% of the road accidents occur due to human errors. The introduction of Advanced Driver-Assistance Systems is a way to improve road traffic safety because their usage allows a shifting of the driving responsibility from the driver to the functionality of the assistance system. Furthermore, ADASs, in addition to the capacity of mitigate hazardous event with respect to driver potentiality, are able to increase the general efficiency of the vehicle.

The benefits brought by ADASs are undeniable but these same systems are not immune from possible faults. The risks of possible malfunctions and failure must be taken into consideration and must be limited as much as possible. Functional safety of electrical and electronic (E/E) systems within road vehicle is the main goal of the ISO 26262 standard.

2.1 Development automotive model

The system development in the automotive industry is based on the V-model. It is a cascade model from project definition to system production (Figure 9). It provides a guide for designing and implementing the project. The goals of the V-model are: minimization of the risks, improvement of quality, reduction of total cost and better communication between all stakeholder. The development model can be divided into several phases:

- ***Requirements:*** during the initial phase, analysis are performed to describe user needs and requirements documents are created. Furthermore, some tests are designed.

- ***System design:*** during this stage, a specification set is filled in with detailed components and other system tests are designed.

- ***Architecture design:*** this phase consists of a high-level design for describing the links among all the components; as for the previous stages, integrations tests are created.

- ***Module design:*** the development goes on through a low-level design phase for all elements of a single module and unit tests are developed.

- ***Implementation/Coding:*** this stage is the bottom of the V-model; all previous specifications are converted into codes and the system is prepared for testing.

- ***Unit testing:*** during this phase the unit is tested for checking and eliminating bugs and faults. In software field software design, coding (and code optimization) and software integration compose the software-in-the-loop test.

- ***Integration testing:*** this stage verifies the functionality across the components of the system and their integration. Software integration and hardware/software integration compose the processor-in-the-loop test.

- ***System testing:*** during this phase performance of complete system is evaluated. Hardware/software integration and vehicle integration compose the hardware-in-the-loop test.

- ***Operation and maintenance:*** finally, the system is ready for the production; during operation phase, maintenance is implemented to repair possible issues and upgrade the system.

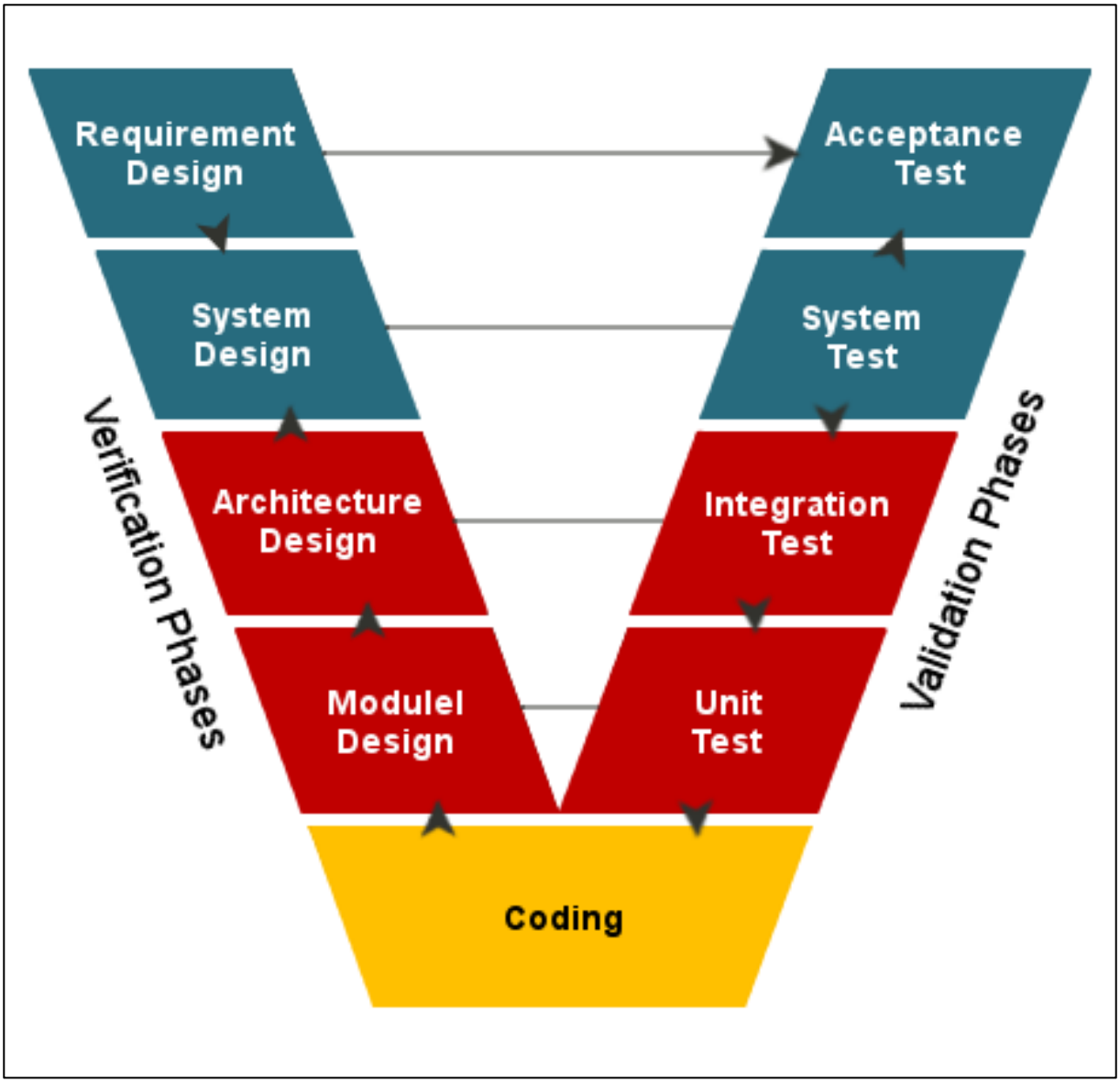

Figure 9 – Phases of V-model (ProfessionalQA.com 2016)

2.1.1 Safety cycle with ISO26262

ISO 26262 is an international standard for automotive industry that applies to safety-related road vehicle E/E system. It addresses hazards due to malfunctions and provides requirements for the lifecycle of the system. The thread of the ISO26262 is the functional safety. Functional safety is the part of the overall safety that depends on a system or equipment operating correctly in response to its inputs. It is the detection of a potentially dangerous condition resulting in the activation of a protective or corrective devise or mechanism to prevent hazardous events arising or providing mitigation to reduce the consequence of the hazardous event (IEC 2010). Functional safety can be asserted defining the risk of undesired effects during operation of the systems and the risk is determined by identifying the Automotive Integrity Level (ASIL). ISO26262 consists of 10 parts listed in Table 4.

Part	Title
1	Vocabulary
2	Management of functional safety
3	Concept phase
4	Product development at the system level
5	Product development at the hardware level
6	Product development at the software level
7	Production and operation
8	Supporting processes
9	Automotive Safety Integrity Level (ASIL)-oriented and safety oriented analyses
10	Guideline on ISO 26262

Table 4 – ISO 26262 chapters

ISO 26262 follows the V-model and the phases of the development are listed below and shown in Figure 10:

- Chapter 3. Concept phase:
  - Item definition
  - Initiation of the safety lifecycle
  - Hazard analysis and risk assessment
  - Functional safety concept

- Chapter 4. Production development at the system level:
  - Initiation of production development at the system level
  - Specification of the technical safety requirements
  - System design

- Chapter 5. Production development at the hardware level:
  - Initiation of production development at the hardware level
  - Specification of hardware safety requirements
  - Hardware design
  - Evaluation of the hardware architectural metrics
  - Evaluation of the safety goal violation due to random hardware failures
  - Hardware integration and testing

- Chapter 6. Production development at the software level:
  - Initiation of product development at the software level
  - Software architectural design
  - Software unit design and implementation
  - Software unit testing
  - Software integration and testing
  - Verification of software safety requirements

- Chapter 4. Production development at the system level:
  - Item integration and testing
  - Safety validation
  - Functional safety assessment
  - Release for production

- Chapter 7. Production and operation
  - Production
  - Operation, service (maintenance and repair), and decommissioning

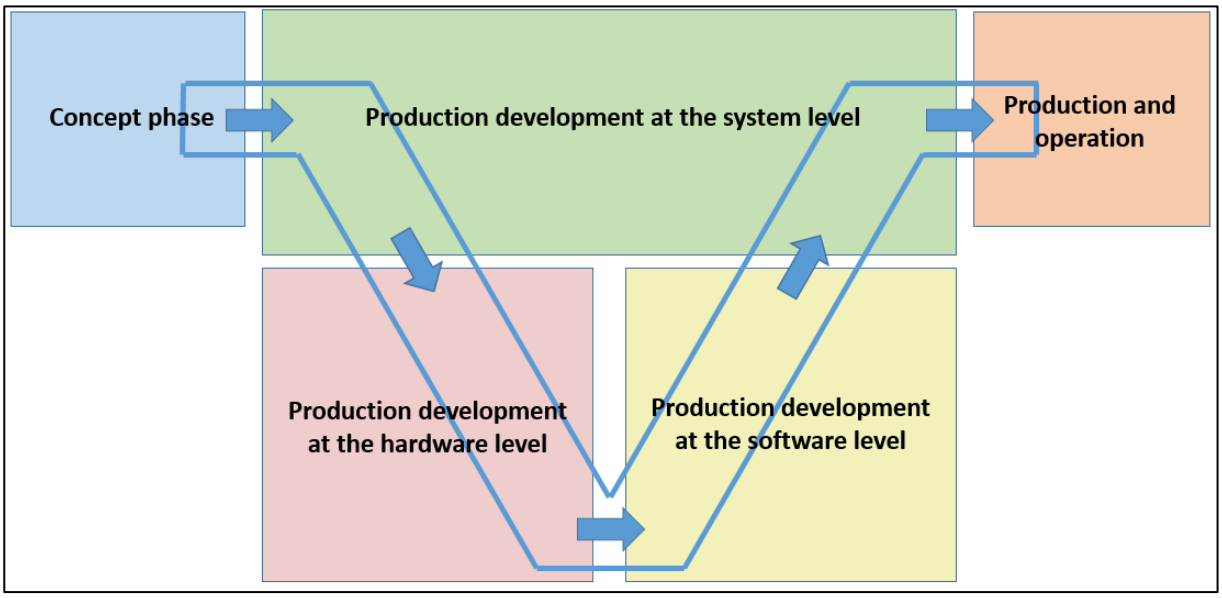

Figure 10 – Overview of ISO 26262

2.1.2 Preparatory activity for system and safety cycle

ISO 26262 provides the methodology able to develop an automotive system with a safety approach. However, system safety cycle needs a preliminary activity able to prepare for the following phases.

1. ***Need analysis:*** it is a process aimed to address human needs in order better meet the demands of the current market.

2. ***Concept exploration:*** it is a research aimed to compare all possible function able to fulfill the operational targets.

3. ***Concept definition:*** in this phase, a system concept, among those analyzed previously, is chosen and decomposed into elementary functions.

2.2 ISO 26262 Part 3: Concept phase

The third part of the ISO 26262 specifies the requirement for the concept phase for automotive applications, including (ISO 26262-3 2011):

- Item definition
- Initiation of the safety lifecycle
- Hazard analysis and risk assessment
- Functional safety concept

2.2.1 Clause 5: Item definition

The targets of this phase are (ISO 26262-3 2011):

a) To define and describe the item, considering the dependencies on, and the interaction with, the environment and other items.

b) To understand adequately the item for the following phases.

There are no prerequisites for this phase (ISO 26262-3 2011).

The requirements of the item shall be defined during the item definition phase (ISO 26262-3 2011), including information about:

a) Purpose, functionality, operating modes and states of the item.

b) Operational and environmental constraints.

c) Laws and standards.

d) Knowledge of the behaviour of similar items.

e) Assumptions on the item behaviour.

f) Shortfalls, failure modes and hazards.

The boundary, the interfaces and the external interactions of the item shall be defined in this stage (ISO 26262-3 2011), including information about:

a) Elements of the items.

b) Effects of the item on other items.

c) Interactions of the item with other items.

d) Functionality given to other items and the environment.

e) Functionality required from other items and the environment.

f) Function allocation and distribution in the elements of the item.

g) Operational scenario of the item.

2.2.2 Clause 6: Initiation of the safety lifecycle

The targets of this phase are (ISO 26262-3 2011):

a) To distinguish between a new item development and a modification of an existing item.

b) To fix the safety lifecycle operations in the case of a modification.

The prerequisite for this phase is the Item definition, resulting from Clause 5 (ISO 26262-3 2011).

If the item is a new development the process continues with Clause 7; if instead, it is the case of a modification the development shall be subjected to Clause 6 (ISO 26262-3 2011). The following step is to perform an impact analysis to identify the modifications and to assess their impact. The impact analysis includes (ISO 26262-3 2011):

a) Operational situations and modes.

b) Interfaces with the outside.

c) Characteristics of the installation and vehicle configurations.

d) Environmental conditions (temperature, humidity, vibrations, etc.).

e) Implications on functional safety.

f) Products that need to be update.

Finally, a safety plan shall be defined; the results of impact analysis are tailored according to lifecycle phases and modified products are reworked (ISO 26262-3 2011).

2.2.3 Clause 7: Hazard analysis and risk assessment

The target of HARA analysis are (ISO 26262-3 2011):

a) To identify the hazards that can occur.

b) To determine the safety goal to avoid risk.

The prerequisite for this phase is the Item definition, resulting from Clause 5 and as supporting information the impact analysis, resulting from Clause 6 (ISO 26262-3 2011).

Starting from item definition, HARA analysis follows some steps: situation analysis and hazard identification, classification of hazardous events, determination of ASIL and safety goals, verification.

1. Situation analysis
   This analysis evaluates the operational situations and operative modes of a malfunctioning item that can cause hazardous event; both correct and incorrect use of the vehicle shall be considered (ISO 26262-3 2011).

2. Hazard identification
   It is used to identify hazards based on observed behaviour at vehicle level and, also to determine the consequence of the hazardous events. Several technique can be chosen such as brainstorming, checklists, FMEA, quality history and field studies (ISO 26262-3 2011).

3. Classification of hazardous events
   Hazardous events shall be classified based on three parameters: severity (S), exposure (E) and controllability (C) (ISO 26262-3 2011).

Severity is classified from class S0 (no injuries) to class S3 (life-threatening injuries); the scale is reported in Table 5 (ISO 26262-3 2011).

	Severity class			
	S0	**S1**	**S2**	**S3**
Injuries	No injuries	Light and moderate injuries	Severe injuries (survival possible)	Fatal injuries (survival uncertain)

Table 5 – Severity class values (ISO 26262-3 2011)

Exposure is estimated from class E0 (incredible) to class E4 (high probability); the scale is reported in Table 6 (ISO 26262-3 2011).

	Exposure class				
	E0	**E1**	**E2**	**E3**	**E4**
Probability	Unlikely	Very low probability	Low probability	Medium probability	High probability

Table 6 – Exposure class values (ISO 26262-3 2011)

Controllability is classified from class C0 (controllable in general) to class C3 (difficult to control or uncontrollable); the scale is reported in Table 7 (ISO 26262-3 2011).

	Controllability class			
	C0	**C1**	**C2**	**C3**
Level of control	Controllable	Clearly controllable	Usually controllable	Hard to control or uncontrollable

Table 7 – Controllability class values (ISO 26262-3 2011)

4. Determination of ASIL and safety goal
   For each hazardous event, an ASIL shall be determined (ISO 26262-3 2011) using Table 8.

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

Table 8 – ASIL allocation table (ISO 26262-3 2011)

Four ASILs classes can be defined: ASIL A, ASIL B, ASIL C, ASIL D (from the lowest safety integrity level to the highest one). Class QM (quality management) does not require to comply with ISO 26262 (ISO 26262-3 2011).

Each hazardous event with its ASIL level leads to a safety goal; similar safety goals can be generate a single new safety goal and in this case the highest ASIL, among the hazardous event in consideration, shall be allocate to the combined safety goal (ISO 26262-3 2011).

5. Verification
   HARA analysis and safety goals shall show (ISO 26262-3 2011):
   - completeness for situations and hazards
   - conformity to item definition
   - completeness of hazardous events covered
   - uniformity of judgement for ASIL determination

2.2.4 Clause 8: Functional safety concept

The targets of this phase are (ISO 26262-3 2011):

a) To transform the safety goals into functional safety requirements.

b) To assign the functional safety requirements to the item or to external measures.

The objects covered by functional safety concept are: the safe state transition, the fault tolerant mechanisms that hold the item in a safe state, the detection of a fault, the mitigation of a failure, the driver alarm and the choice of the right control demand in case of multiple of them in the same time (ISO 26262-3 2011). The flow of the safety requirements is shown in Figure 11.

The prerequisites for this phase is the Item definition, resulting from Clause 5, the hazard analysis and risk assessment, resulting from Clause 6, and the safety goals, resulting from Clause 6 (ISO 26262-3 2011).

Each safety goal shall generate at least one functional safety requirement; then the functional safety requirement will be allocated to the components of the preliminary architecture; if functional safety concept concerns an external measures, functional safety requirements shall be reported and handled with ISO 26262 (ISO 26262-3 2011).

Finally, functional safety requirements shall be validate and verified, using Chapter 8 of the ISO 26262, to generate a verification report (ISO 26262-3 2011).

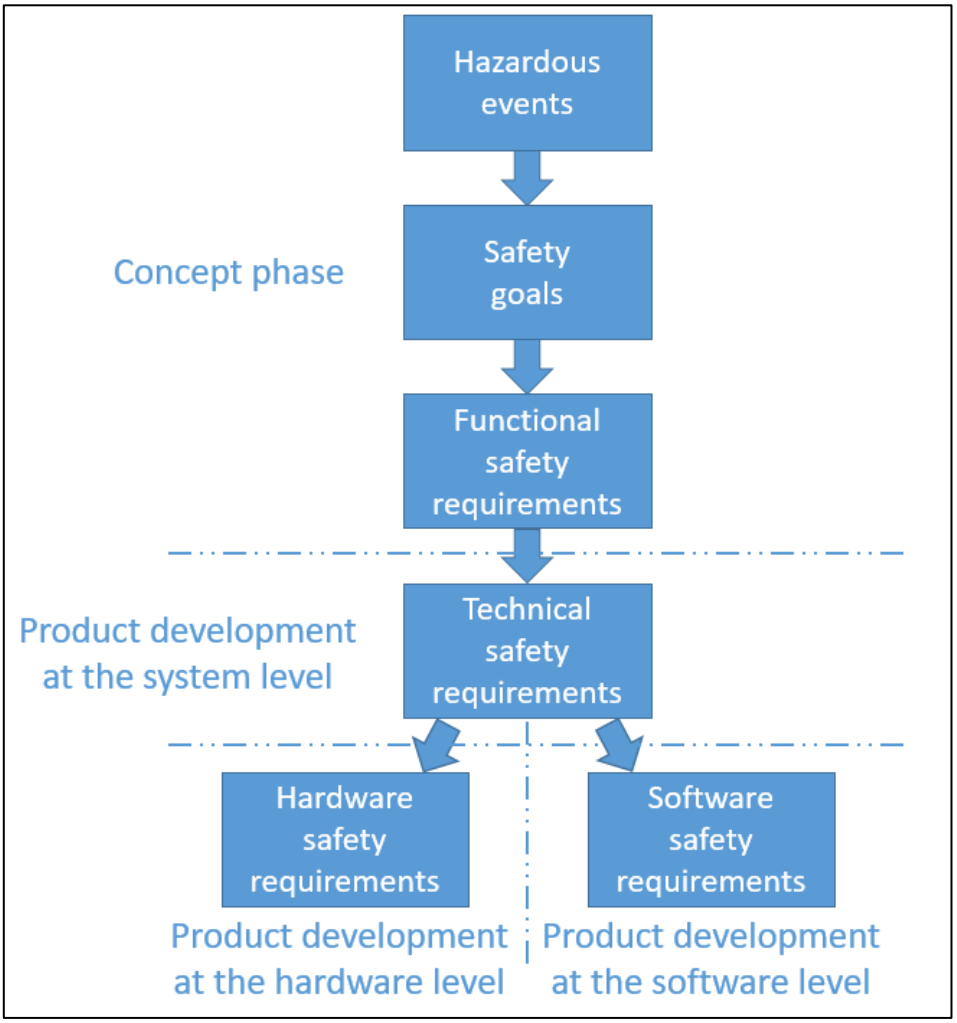

Figure 11 – Flow of safety requirements in ISO 26262

2.3 Functional safety activity supported by safety analysis

The methodology, implemented by ISO 26262 to allocate functional safety requirements starting from item definition, needs to be supported by external safety analysis in order to handle better hazard and safety analysis (see Figure 12). There are several types of analysis that can be used and the main ones are HAZOP, STPA and FMEA.

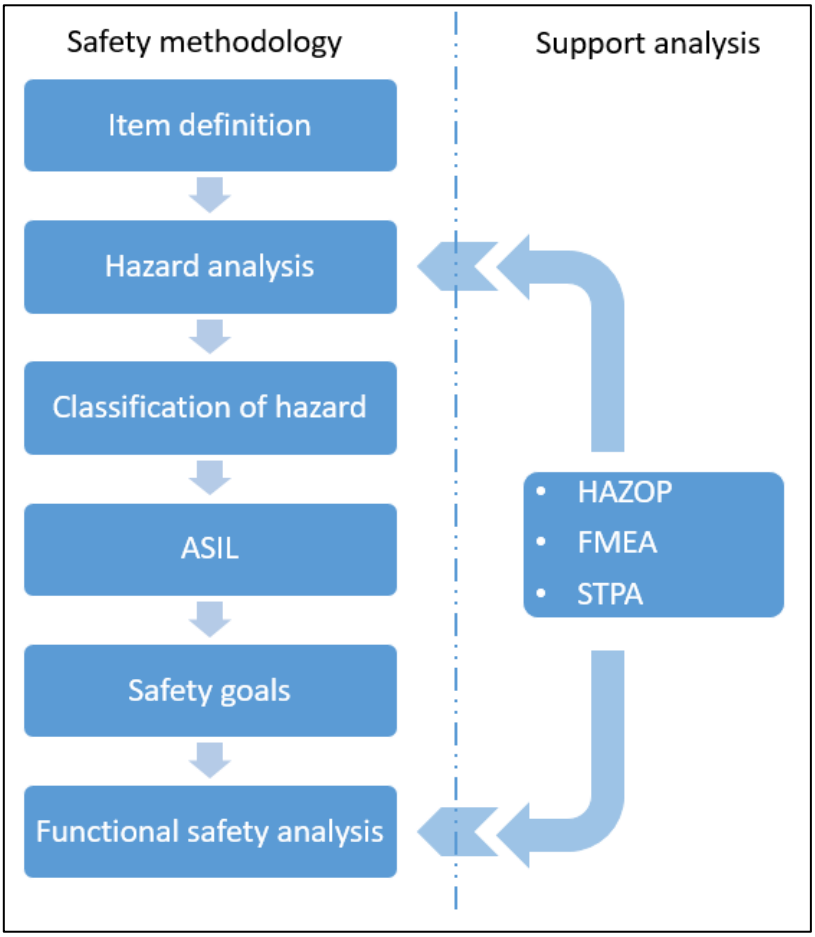

Figure 12 – Support analysis for functional safety

2.3.1 Hazard and Operability Analysis (HAZOP)

HAZOP is one of the most used technique for the process risk analysis and it is applicable for several fields of study. HAZOP procedure consists of a sequence of steps.

1. Define the project intention
2. Define if there are deviations from project intention
3. Define possible causes that can lead to failure
4. Value the effects of failure
5. Estimate the probability of a failure
6. Compare the failure risk with guide lines and safeguards
7. Design corrective or mitigation system to reduce the risks

2.3.2 System Theoretic Process Analysis (STPA)

STPA is a hazard evaluation process that has as object the identification of causes for vehicle performance losses and the generation of hazards and causal factors for safety requirements stage (Van Eikema Hommes 2015). STPA is a top-down approach based on three parts: analysis stage (system description, system-level losses and hazards), STPA step 1 (unsafe control action) and STPA step 2 (casual factors) (Van Eikema Hommes 2015).

1. ***Analysis stage:***
    - System description: it describes functionally the system and defines the scope of the system.
    - System-Level loss: event that can cause loss of life or injury, property harm, etc.
    - Hazards: potential source of system-level loss

2. ***Unsafe control actions (UCAs):*** controller actions that can lead to hazardous states of the vehicle systems. Every control action generates a tree flow as shown in Figure 13.

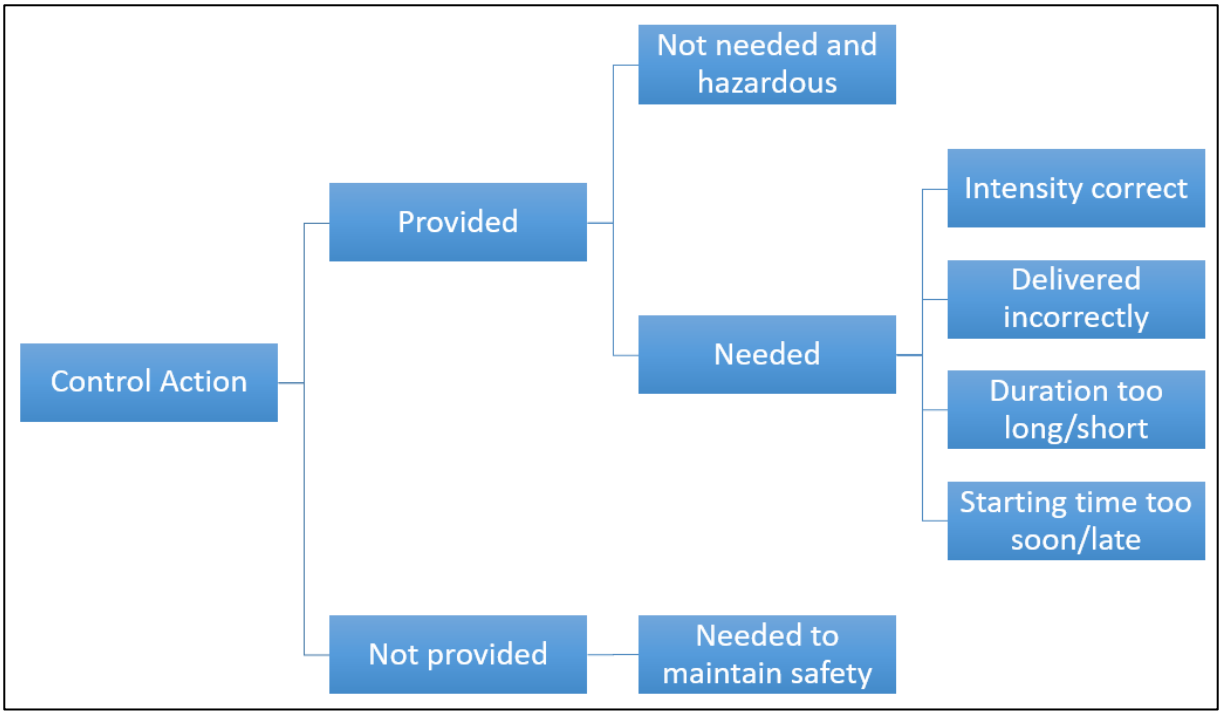

Figure 13 – Control action flow

3. ***Casual factors (CFs):*** factors that can lead to unsafe control action considering: controllers, sensors, actuators, processes, links, unsafe interaction with vehicles and environment.

2.3.3 Failure Mode and Effect Analysis

FMEA is a method aimed to analyze the mode in which a failure can occur and also the effect on the system. FMEA can be decomposed into some applicative phase, listed below:

1. ***Preliminary phase:*** it is necessary to choose the application, to identify the objects and to collect data.
2. ***Qualitative phase:*** it consists on decomposing the system and identifying modes and causes of failure and the effects.
3. ***Quantitative phase:*** this stage allows to fix some parameters; a level was assigned for occurrence, detection, severity and risk priority number (RPN).
4. ***Correction phase:*** it generates needed modifications and recommended action.
5. ***Final phase:*** it allows to value the correction action and to update the FMEA parameters.

Table 9 shows the FMEA matrix.

Item	Modes of failure	Effects	Causes	FMEA Parameters				Modification	Final Parameters			
				Occurrence	Detection	Severity	RPN		Occurrence	Detection	Severity	RPN

Table 9 – FMEA matrix

2.4 Safe transitioning of responsibility

An important aspect, related to safety on automotive system, is the transition of the responsibility from HM (human driver) and AD (automated driver) and vice versa. This relevant topic takes a crucial role in the passage from current ADASs to future autonomous vehicle.

Considering as reference the NHTSA level of automation L3, there are two strategies to handle the safe transition between drivers. The less conservative strategy investigates all possible scenarios that request the driver is available for occasional control. On the contrary, the more conservative one does not consider if the driver can regain the control

of the vehicle in a short time (Johansson, Nilsson e Kaalhus 2016). The transition between driver and autopilot generates two types of hazard (Johansson, Nilsson e Kaalhus 2016):

- ***Mode confusion:*** this hazard is generated when both the drivers try to control the vehicle or when no one takes care of it.

- ***Unfair transitioning:*** manual driver and autopilot drive using tactical plan that can be different and it can be difficult to distinguish a different tactical decision from a faulty one; moreover, this hazard is more dangerous if the transition occurs during a sequence of manoeuver.

A strategy to handle the unfair transition is the introduction of an agreement for a handover; in this way the driver (human or autopilot) keeps the control of the vehicle until the agreement. A strategy to solve the mode confusion consists of adding a mechanism to remember which driver is controlling the vehicle (Johansson, Nilsson e Kaalhus 2016).

Johansson, Nilsson and Kaalhus propose a protocol in which the transition is regulated by two actions and the use of a button for request a change, a lever for actuate the transition, a telltale light showing the AD preferred mode and a second telltale light to indicate that AD is ready for a change (Johansson, Nilsson e Kaalhus 2016). The sequence of the protocol is shown in Figure 14.

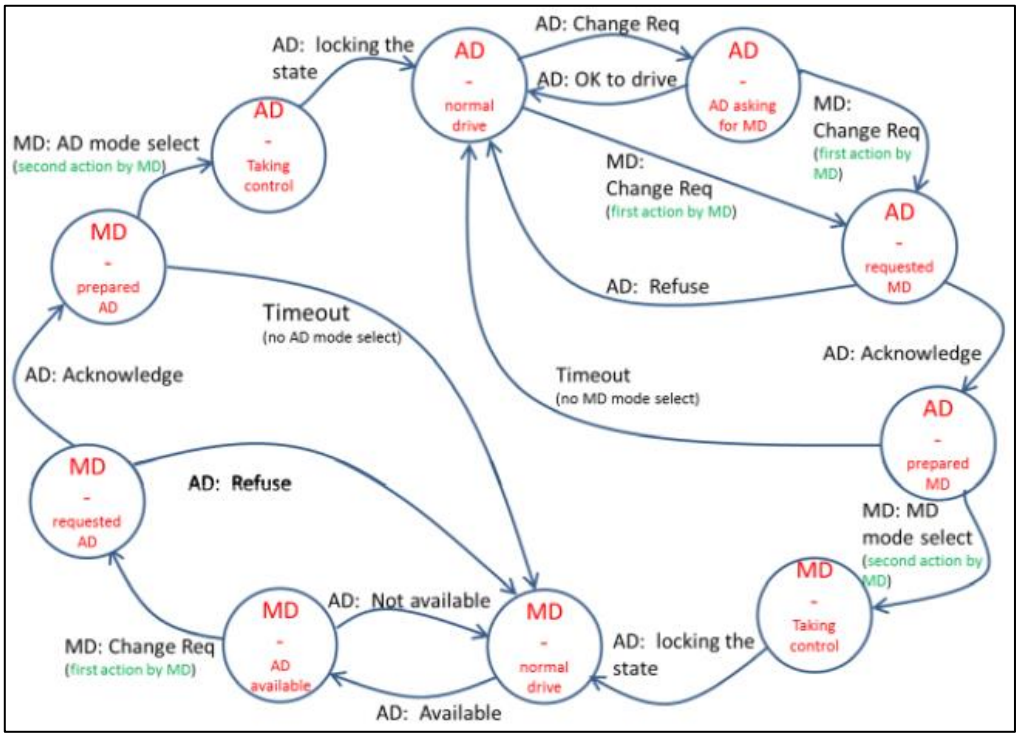

Figure 14 – Protocol for safe transitions (Johansson, Nilsson e Kaalhus 2016)

The safety analysis of the transition protocol was performed and all possible failures were investigated. Among all HMI failures only three of them cause an unsafe transition: the AD cannot sense the mode level position (mode confusion), the AD cannot lock the lever and the MD changes the position of level without noticing it (mode confusion and unfair transition), the AD cannot lock the lever and the MD changes the position of level without getting acknowledgment of a prepared AD (unfair transition). This implies to put ASIL D on faulty level sensor and ASIL D on lever lock faulty unlocked (Johansson, Nilsson e Kaalhus 2016).

3 Forward Vehicle Collision Mitigation System

Forward Vehicle Collision Mitigation System is currently one of the most crucial driver assist because they are able to avoid/mitigate accidents. Collision avoidance systems consists of several subsystems able to identify hazardous situation, warn the driver and take the control of the vehicle (braking and/or steering) without any driver input and prepare the vehicle in case of impact. Mainly, they use radar, but cameras and LIDAR are also used.

3.1 FVCMS input and output

Forward Vehicle Collision Mitigation Systems (FVCMS) require information about distance and motion of forward vehicles, movement of the subject vehicle, driver input and commands. Based on this data the system actuates some activities to mitigate the severity of the collision (ISO 22839 2013). Figure 15 shows a simple scheme of FVCMS.

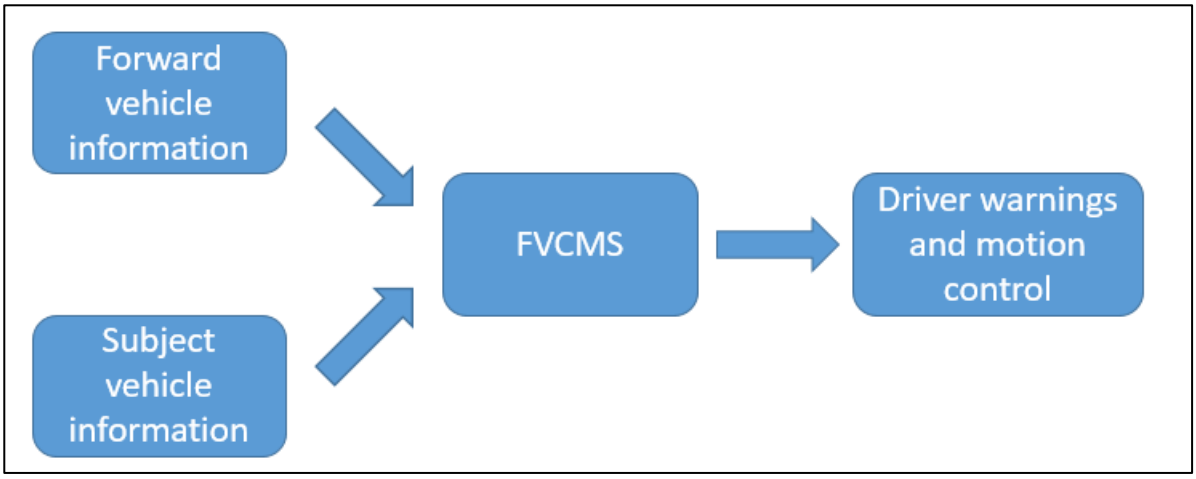

Figure 15 – Forward Vehicle Collision Mitigation System scheme

3.2 Classifications

FVCMS can be classified according to curve radius capability (ISO 22839 2013):

- ***Class I:*** the system shall detect forward obstacles in the trajectory of the subject vehicle along curves of radii down to 500 meters.

- ***Class II:*** the system shall detect forward obstacles in the trajectory of the subject vehicle along curves of radii down to 250 meters.

- ***Class III:*** the system shall detect forward obstacles in the trajectory of the subject vehicle along curves of radii down to 125 meters.

3.3 Countermeasures

FVCMS provide three levels of countermeasures that are activated when the pre-collision urgency parameter (PUP) exceeds the threshold given by the minimum countermeasure action point (MCAP) (ISO 22839 2013):

- ***Collision warning (CW):*** it is an alarm based on audible, visual and haptic sensory modes.

- ***Speed reduction braking (SRB):*** it is a braking function to reduce the vehicle speed. During SRB the driver can apply a braking, change the lane or deactivate the SRB and all these actions prevent the activation of the MB. SRB shall not be

initiated for time to collision (TTC) or enhanced time to collision (ETTC) above 4 s.

- ***Mitigation braking (MB):*** it is an automatic braking to avoid collision.

The previous countermeasures can be combined in three different FVCMS as shown in the following Table 10:

Type	MB	SRB	CW
1		•	•
2	•		•
3	•	•	•
• indicates the presence of the system			

Table 10 – FVCMS types

3.4 Operating modes

The FVCMS can have three operating modes (ISO 22839 2013):

1. ***FVCMS Off:*** No operations are performed during this state. When the vehicle is powered up the FVCMS will be in this mode and also if the self test detects a fault or if the driver disengages the system.

2. ***FVCMS Inactive:*** during this state FVCMS checks vehicle speed and decides if it is opportune to activate the system. The system enters this mode (from FVCMS Off state) when the engine is running and when the vehicle speed drops below the minimal velocity for the activation V_{min} or the Park mode is selected (from FVCMS Active state).

3. ***FVCMS Active:*** during this state FVCMS shall monitor the necessary conditions to activate the countermeasures. In case of a fault the system transfers to the FVCMS Inactive state and if is not possible to recover the failure it transfers to the FVCMS Off state.

The transition of the FVCMS state are shown in Figure16.

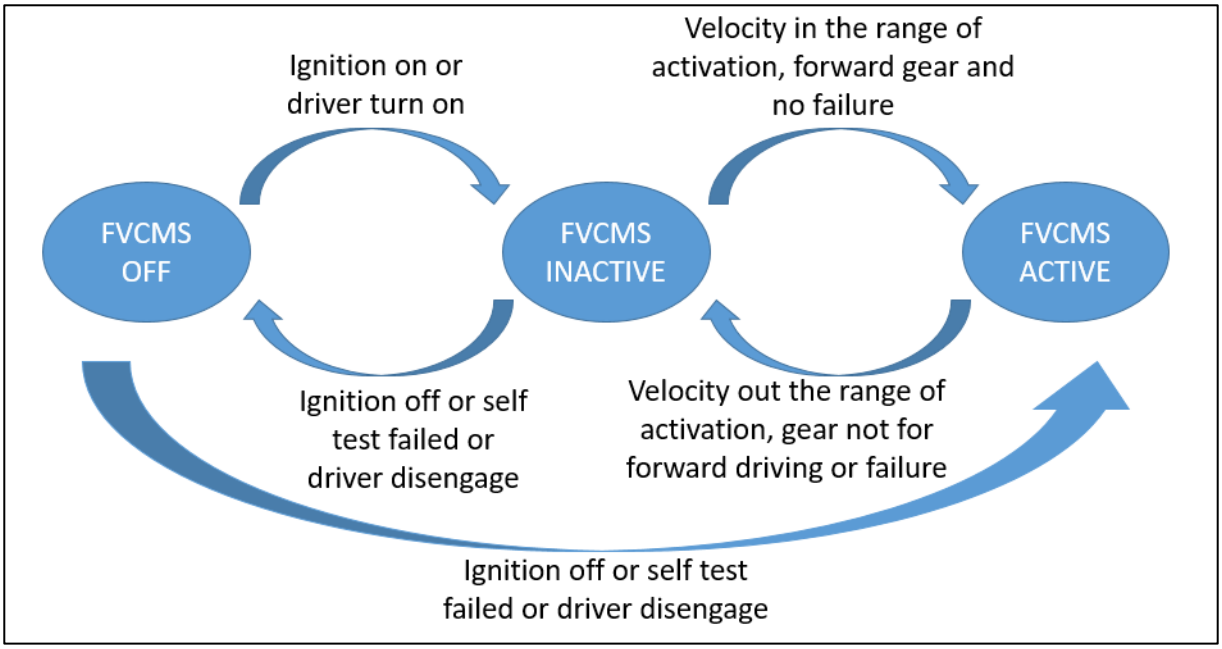

Figure 16 – State and transitions of FVCMS

3.5 Mathematical model for longitudinal control

The longitudinal control with constant deceleration can be mathematically modeled using the equations of the uniform accelerated linear motion. It is the motion of a point subjected to a constant acceleration and then we have (3.1):

$$\vec{a} = \frac{\mathrm{d}\vec{v}}{\mathrm{d}t} = costant \tag{3.1}$$

Integrating the equation 3.1 between two generic moment of time:

$$\int_{t_0}^{t} \mathrm{d}\vec{v} = \int_{t_0}^{t} \vec{a}\,\mathrm{d}t \tag{3.2}$$

Being the acceleration constant, from equation 3.2 we get:

$$\vec{v}(t) = \vec{v}_0 + \vec{a}t \tag{3.3}$$

where:

$v(0) = v_0$ is the initial velocity;

$v(t)$ is the velocity at the instant t.

Considering that:

$$\vec{v}(t) = \frac{d\vec{s}(t)}{dt} \tag{3.4}$$

Replacing the equation3.4 in the equation 3.3 and integrating:

$$\int_{t_0}^{t} \mathrm{d}\vec{s}(t) = \int_{t_0}^{t} (\vec{v}_0 + \vec{a} \cdot t)\mathrm{d}t \tag{3.5}$$

and from equation 3.5 we get:

$$\vec{s}(t) = \vec{s}_0 + \vec{v}_0 t + \frac{1}{2}\vec{a}t^2 \tag{3.6}$$

where:

$s(t)$ is the position at the instant t;

$s(t_0) = s_0$ is the initial position;

v_0 is the initial velocity.

3.6 Matlab simulations for a FVCMS equipped with SRB

Formulas shown in the previous paragraph are used in Matlab to simulate the braking of a vehicle equipped with a FVCMS and SRB mode. ISO 22839 establishes that the averaged deceleration generated by SRB shall not exceed, for a period T_1_SRB ($\geq 0{,}5\ s$) the line:

$$d_{SV} = 5{,}33\ \mathrm{m}/s^2 - 0{,}067/s * v_{SV} \tag{3.7}$$

where d_{SV} is the deceleration of the subject vehicle and v_{SV} is the current velocity of the subject vehicle. This constraint is valid for any vehicle speed between 5 m/s and 20 m/s. For $v_{SV} > 20\ m/s$ the deceleration generated by SRB shall not exceed $4\ m/s^2$ and for $v_{SV} < 5\ m/s$ the deceleration shall not exceed $5\ m/s^2$. After T_1_SRB the maximum deceleration can increase up to $6\ m/s^2$ (ISO 22839 2013). The braking profile is shown in Figure 17 and Figure 18.

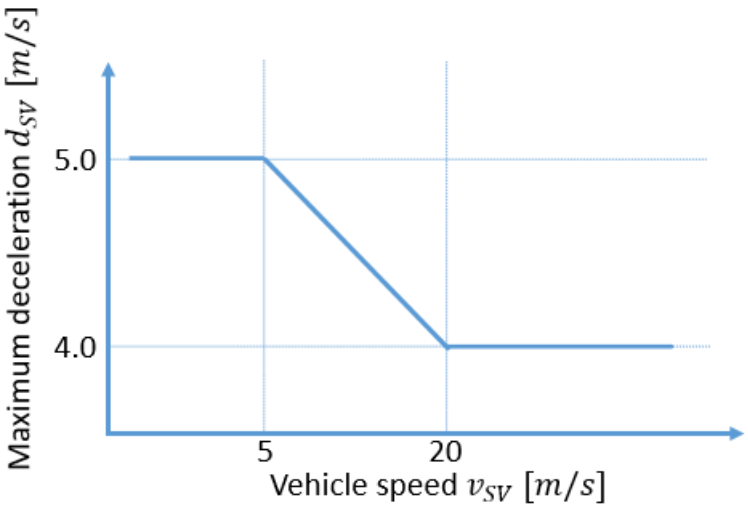

Figure 17 – Braking profile of SRB (t < T_1_SRB)

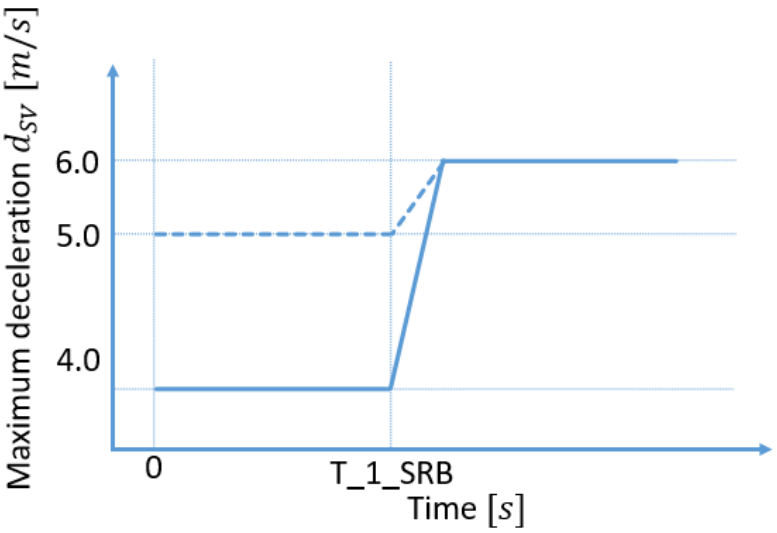

Figure 18 - Braking profile of SRB

This braking profile is applied to the model and simulation are carried out for different starting velocities from 30 km/h to 90 km/h. Distances, required to stop the vehicle, are reported in the Figure 19.

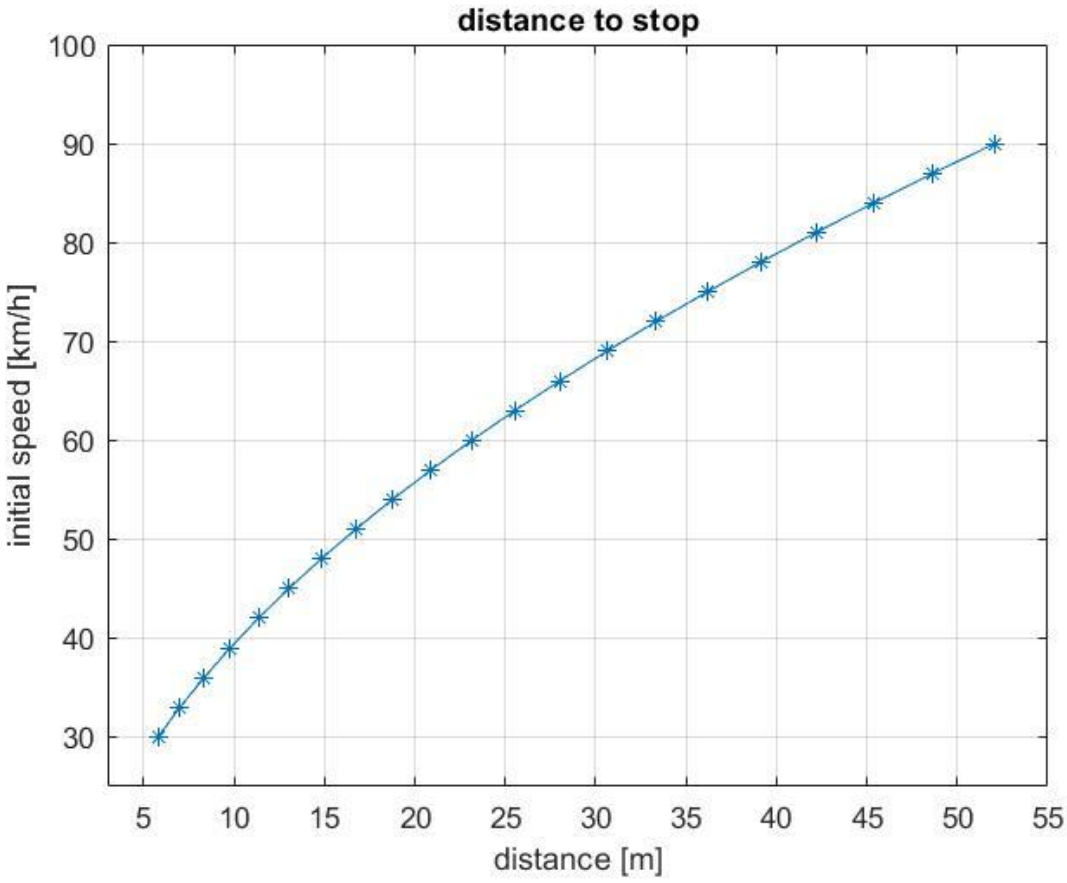

Figure 19 – Distance required to stop the vehicle equipped with SRB

3.7 Simulation of an Automated Braking Emergency System

Some simulations of an Autonomous Emergency Braking system (AEBS) were carried out. Scenarios of the simulations follow the guideline given by Euro NCAP for testing an AEBS, and can be divided into three groups (Euro NCAP 2017):

- ***Car-to-Car Rear Stationary (CCRs) scenario:*** a vehicle travels forwards towards another stationary vehicle and the collision happens between the front part of the vehicle and the rear part of the stationary one. The speed of the vehicle under test is changed in the range $10 - 50\ km/h$.

- ***Car-to-Car Rear Moving (CCRm) scenario:*** a vehicle travels forwards towards another vehicle which is moving at constant velocity and the collision happens between the front part of the vehicle and the rear part of the other. The speed of the vehicle under test is changed in the range $30 - 80\ km/h$ and the speed of the other vehicle is set at $20\ km/h$.

- ***Car-to-Car Rear Braking (CCRb) scenario:*** a vehicle travels forwards towards another vehicle which is moving at constant velocity and then decelerates, and the collision happens between the front part of the vehicle and the rear part of the other. The speed of the two vehicles is fixed at $50\ km/h$; the initial distance between the two vehicles is set to $12m$ or $40\ m$ and the deceleration of the forward vehicle is set to $2\ m/s^2$ or $6\ m/s^2$.

The characteristics of the scenarios are reported in Figure 20 and Table 11.

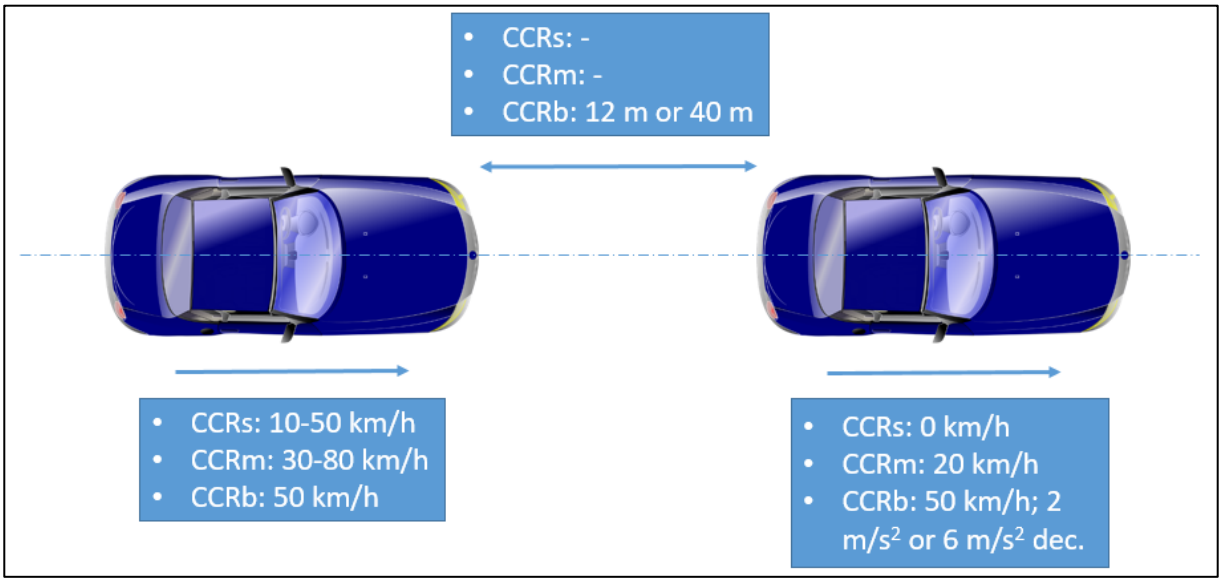

Figure 20 – Scenarios for CCR test

CCRs	**0 km/h**		
	10 – 50 km/h		
CCRm	**20 km/h**		
	30 – 80 km/h		
CCRb		**2 m/s²**	**6 m/s²**
	12 m	50 km/h	50 km/h
	40 m	50 km/h	50 km/h

Table 11 – CCR test characteristics

The logic of the system can be summarized as follows:

1) It was set a threshold for the activation of the Forward Collision Warning and for the activation of the Autonomous Emergency Braking. Thresholds are based on the necessary deceleration to stop the vehicle under test without having a crash. This deceleration can be calculate considering the following equation system:

$$\begin{cases} v_f = v + a * t = 0 \\ d = v * t + \frac{1}{2} * a * t^2 \end{cases}$$

(3.8)

where v_f is the final velocity, v is the current velocity, d is the distance needed to stop the vehicle that is equal to the distance between the vehicles, a is the acceleration and t is the time. Solving the equation system 3.8 we found that the necessary acceleration will be equal to:

$$a = -\frac{v^2}{2*d}$$

(3.9)

The FCW threshold has been set to 2 m/s^2 and the AEB one has been set to 3 m/s^2.

2) When the simulation starts, the system calculate the distance between the two vehicles, the velocities of the vehicles and the necessary deceleration to stop the vehicle under test without having a crash.

3) If the Forward Collision Warning threshold is exceeded, the FCW light is activated as it is shown in Figure 21.

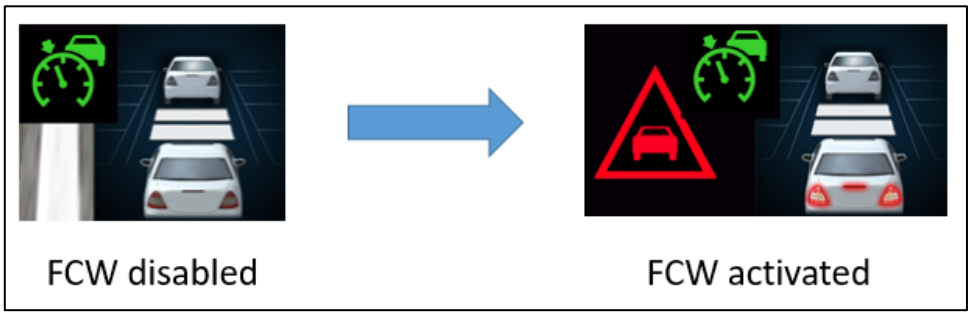

Figure 21 – FCW light

4) When the Autonomous Emergency Braking threshold is overlapped, the AEB signal is triggered; then the system measures the velocities of the two vehicles v_x (the speed of the vehicle under test) and v_{x_evt} (the speed of the target vehicle). If $v_x > v_{x\_evt}$ brakes are activated; if $v_x \leq v_{x\_evt}$ the AEB signal is disabled and simulation is aborted; the simulation is aborted also if $v_x = 0$.

3.7.1 Simulation results

Autonomous Emergency Braking threshold has been set to $3\,m/s^2$ for all simulations. The purpose of the simulations is to verify that the system is able to calculate the necessary deceleration to avoid the collision and if it is able to activate the brakes.

The Car-to-Car Rear Braking scenario has been simulated both with 12 m of starting distance and with 40 m. The initial velocities of the two vehicle have been set to 50 km/h. Moreover, for each simulation, it has been checked the behavior of the system both with

2 m/s^2 and 6 m/s^2 of forward vehicle deceleration. The system was able to behave in the desired way. Figure 22, Figure 23, Figure 24 and Figure 25 show the CCRb scenario results.

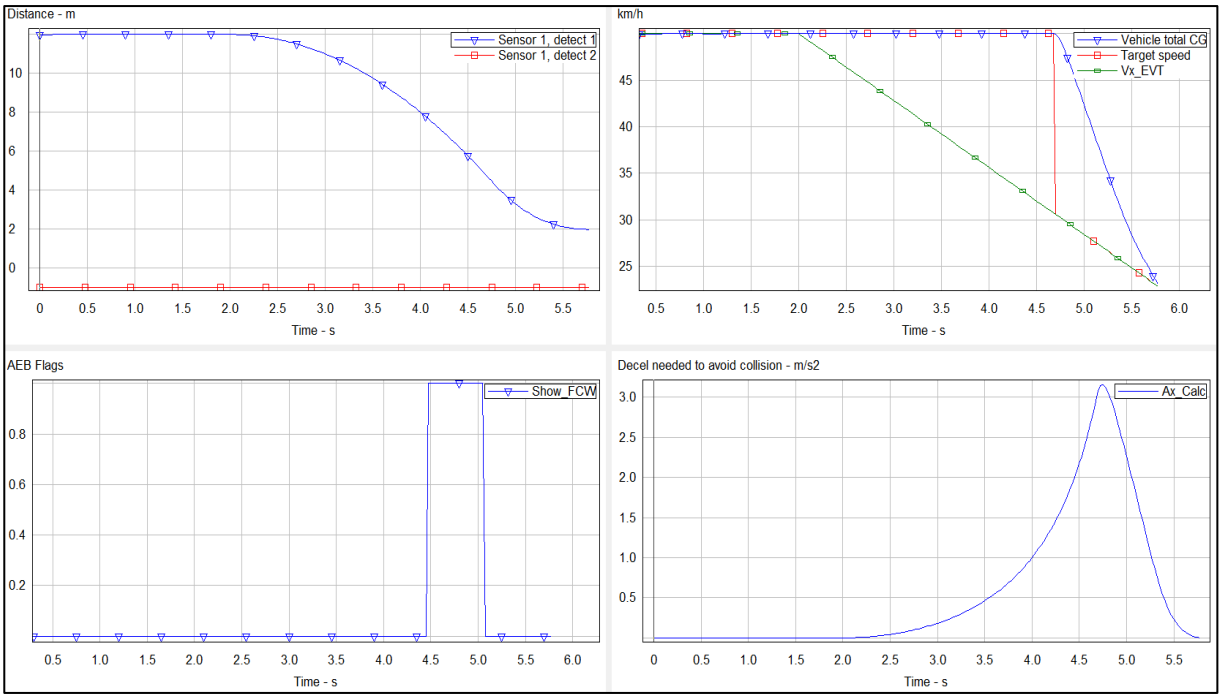

Figure 22 – CCRb test (12 m and -2 m/s²)

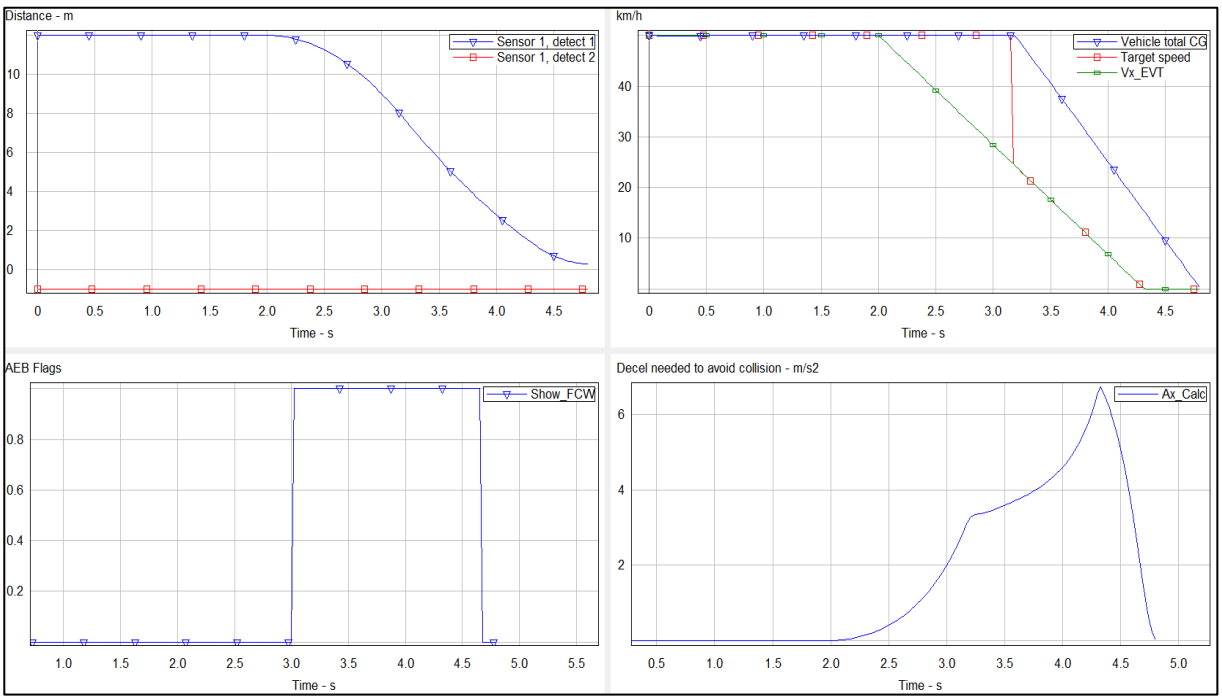

Figure 23 – CCRb tets (12 m and -6 m/s²)

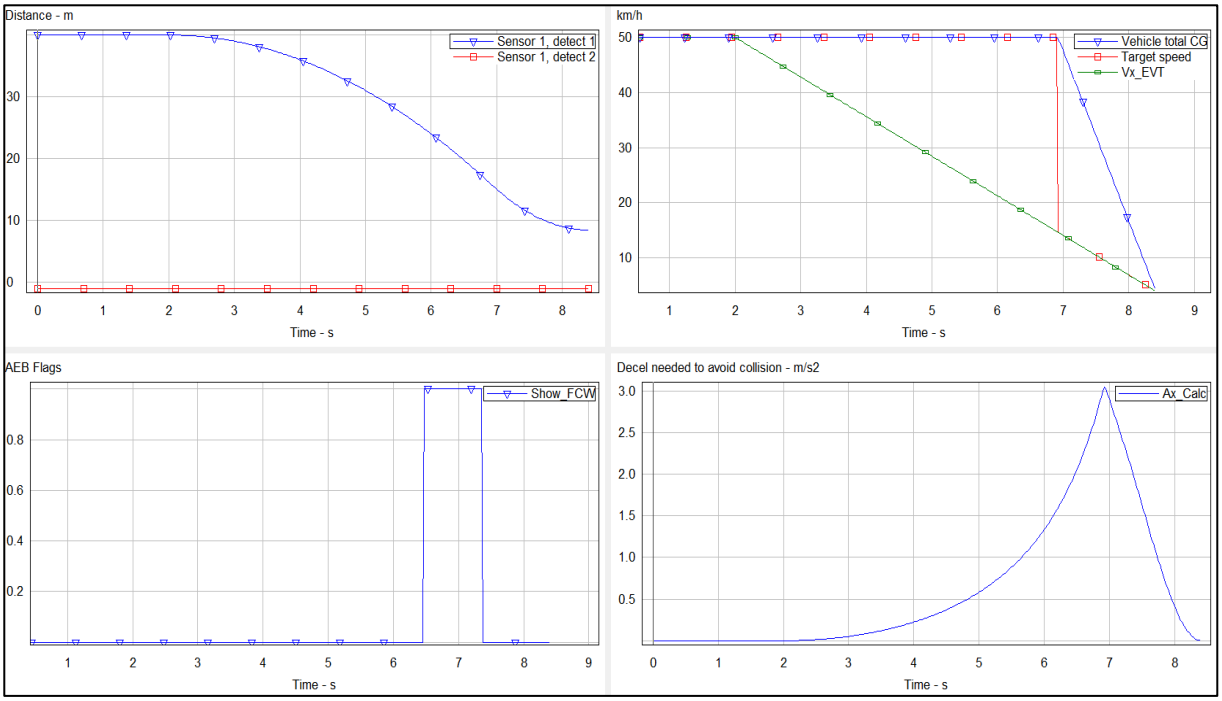

Figure 24 - CCRb test (40 m and -2 m/s²)

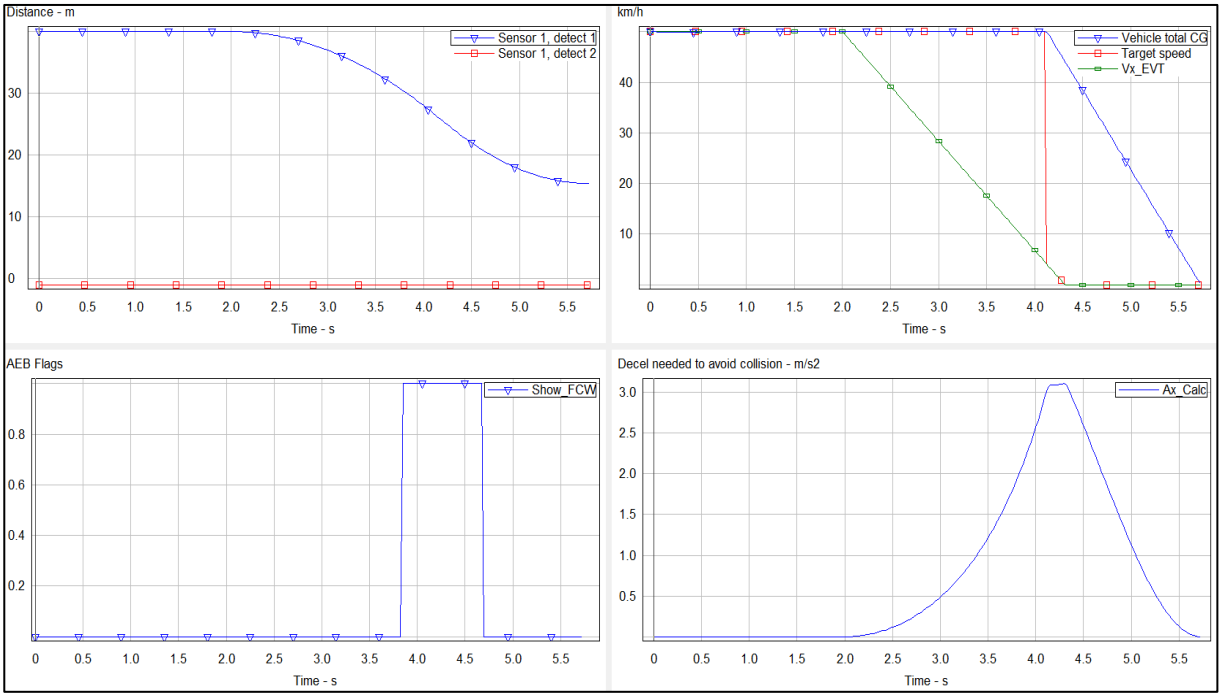

Figure 25 CCRb test (40 m and -6 m/s²)

The Car-to-Car Rear Moving scenario has been simulated with 50 m of starting distance and with a starting velocity of the ego vehicle in the range between 40 km/h and 100 km/h. The velocity of the forward vehicle has been set to 20 km/h. The system was able to behave in the desired way. Figure 26 show the CCRm scenario results.

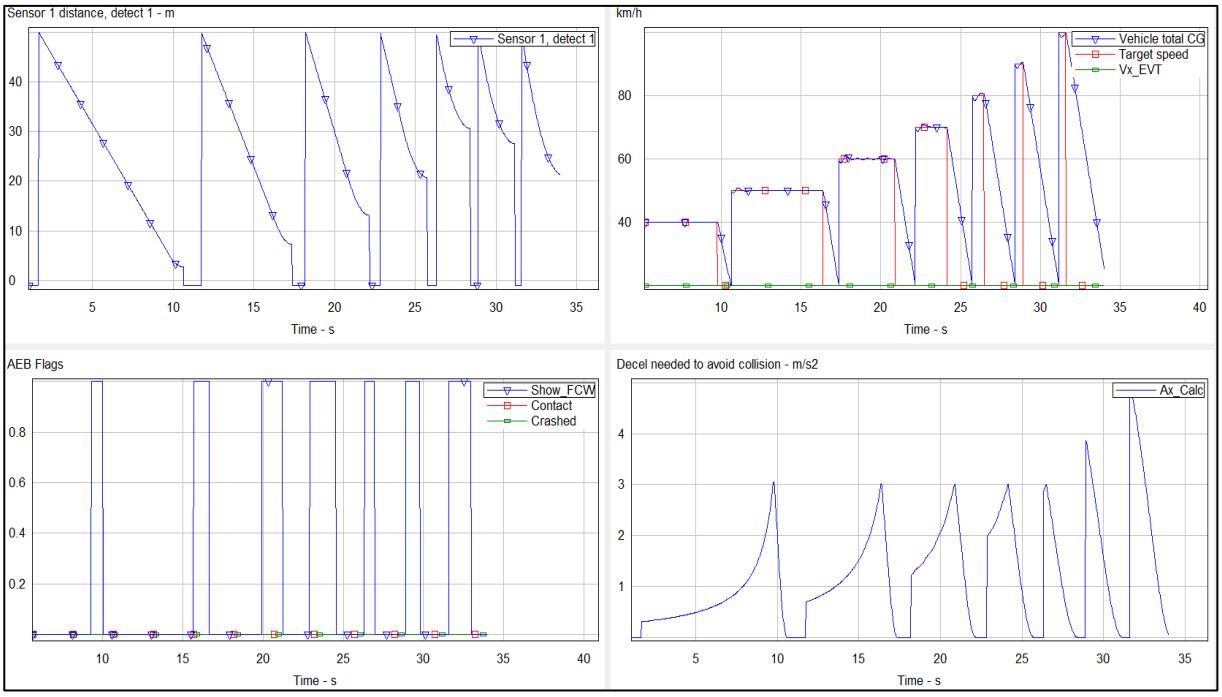

Figure 26 – CCRm tests

Finally, the Car-to-Car Rear Stationary scenario has been simulated with 50 m of starting distance and with a starting velocity of the ego vehicle in the range between 40 km/h and 100 km/h. The velocity of the forward vehicle has been set to 0 km/h. The system was able to behave in the desired way. Figure 27 show the CCRs scenario results.

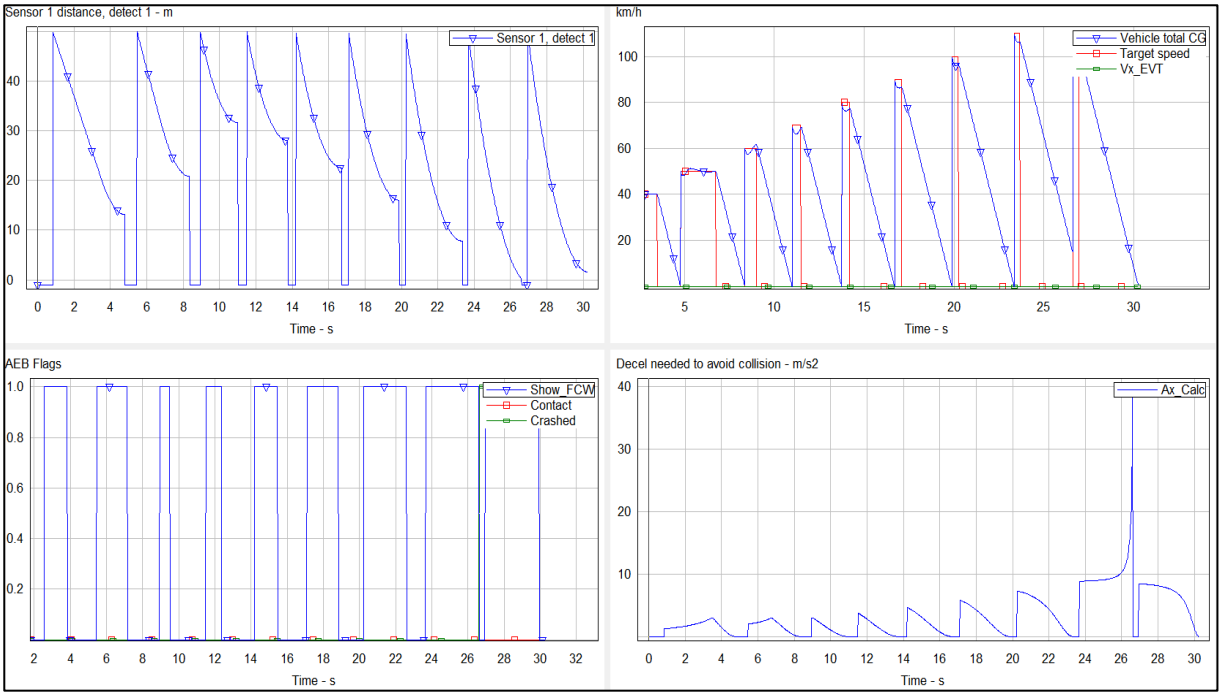

Figure 27 – CCRs tests

4 Hara Analysis and Fault Injection for AEBS

4.1 Item definition

4.1.1 Purpose

The purpose of the item is to reduce the velocity of the ego vehicle in case of possible crash. The item shall also display the imminent impact.

4.1.2 Functionality

The functionality of the item are:

a) The item shall use information from the sensors to calculate the time-to-collision.

b) The item shall monitor the environment and if there is the possibility of a crash it shall control the brakes.

c) The item shall allow the driver to brake with a higher pedal pressure with respect to the pressure actuated by the item.

4.1.3 Elements of the item

The elements of the item (Figure 28) are:

a) 1 CAMERA: to identify the objects

b) 1 RADAR: to measure the object relative distance and radial speed.

c) 1 ECU: to gather information from sensors and make decisions.

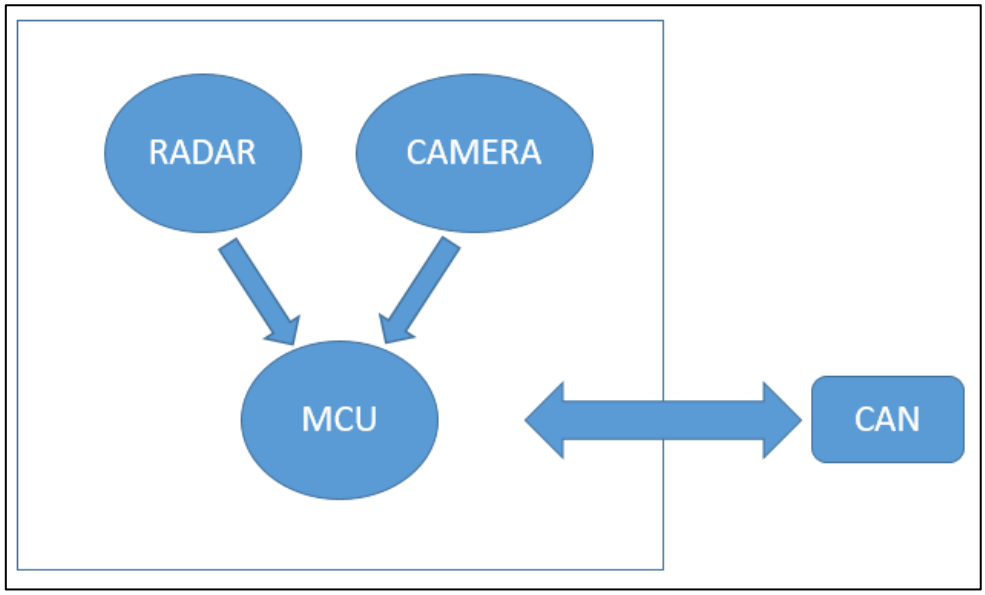

Figure 28 – Item elements

4.1.4 Interfaces

The item communicates through CAN network. It shall send longitudinal acceleration request. The item shall receive the ego vehicle velocity and status.

4.1.5 Operating modes and states

The item shall operate in 3 different modes as shown in Table 12.

OPERATING MODE	OPERATING STATE	FUNCTIONALITY
OFF	Item not switched on.	NA
INACTIVE	Item decides if it is opportune to activate the system.	Item monitors the vehicle speed.
ACTIVE	Item control the brakes if it is necessary.	Item checks distance and velocities of the vehicles and generates the necessary deceleration.

Table 12 – Operating modes of the item

4.1.6 Failure modes

Failure modes are:

a) Item sends wrong deceleration request on the CAN.

b) Item wrongly calculates the target distance and velocity.

4.2 HARA analysis and Functional Safety Concept

4.2.1 Situation analysis

Operational situations can be several but for current analysis it is considered only the following scenario; the item is intended to active during highway driving with ego vehicle speed between 50 km/h and 70 km/h. In case of a cut in manoeuver the item can generate a constant deceleration request between 1 m/s^2 and 5 m/s^2 to stop the ego vehicle. The scenario chosen to conduct the HARA analysis is shown in Figure 29.

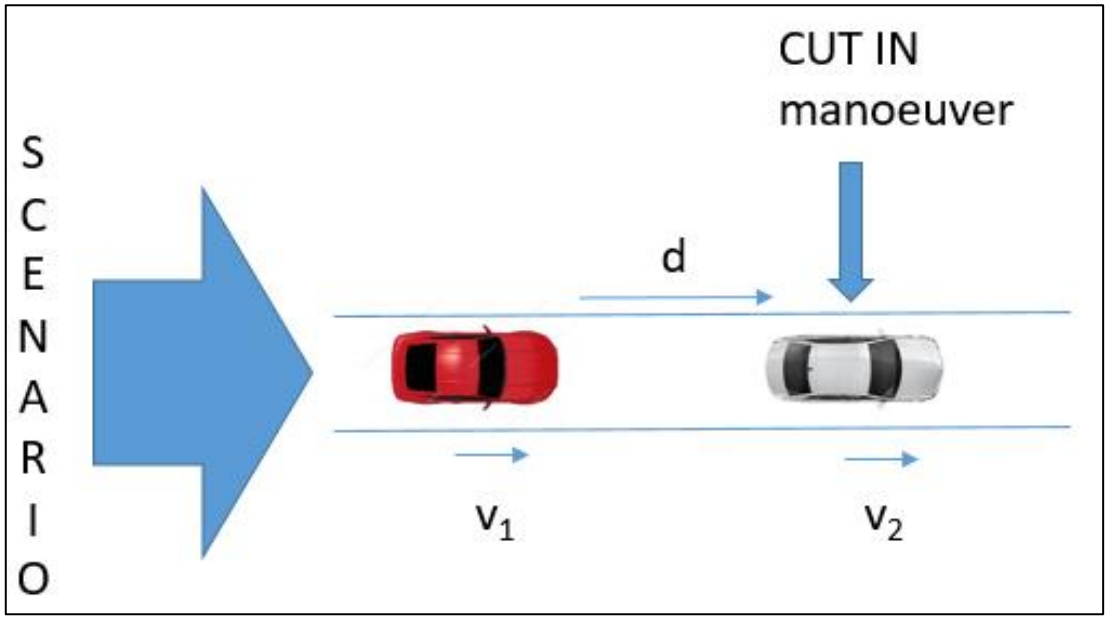

Figure 29 – Situation analysis

The necessary distance to stop the vehicle has been calculated for different value of velocity within the operative range of the AEBS; for every initial speed, steps of 0.5 m/s^2 has been considered. Figure 30, Figure 31 and Figure 32 show the needed distance to stop the vehicle for an initial speed of 50 km/h, 60 km/h and 70 km/h.

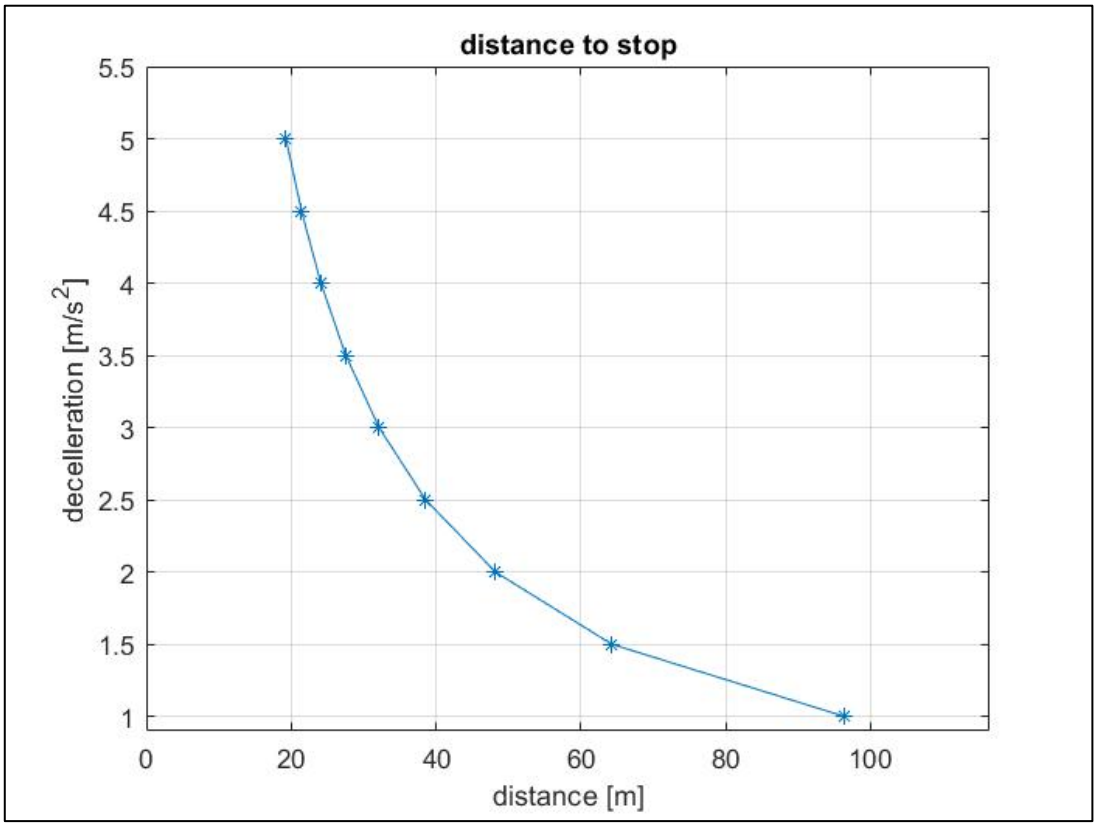

Figure 30 – Distance to stop the vehicle with initial speed = 50 km/h

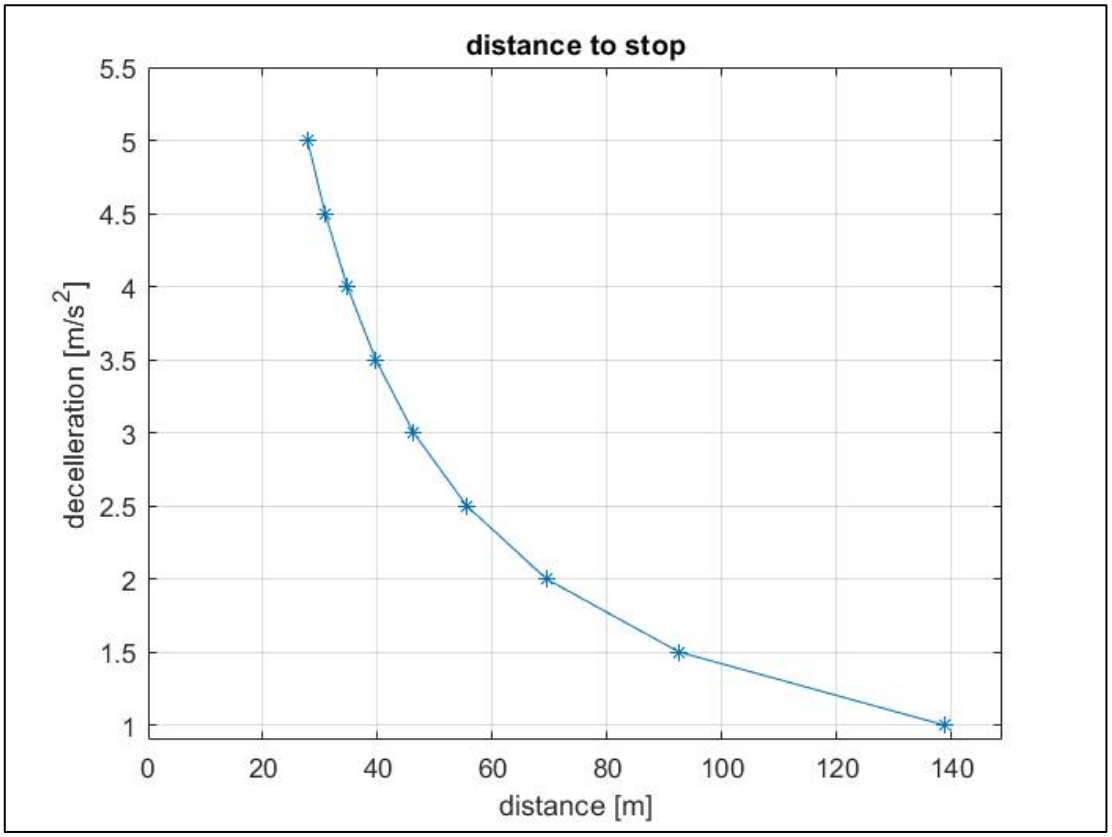

Figure 31 – Distance to stop the vehicle with initial speed = 60 km/h

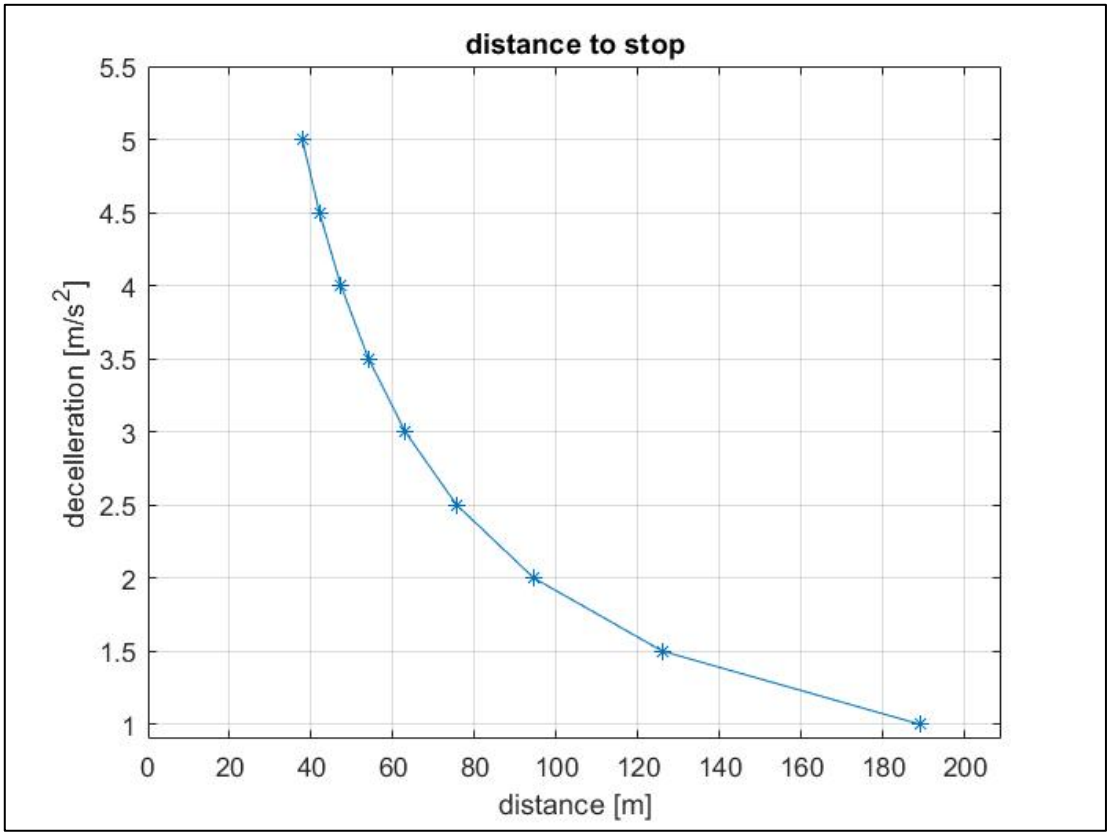

Figure 32 – Distance to stop the vehicle with initial speed = 70 km/h

4.2.2 Hazard identification

Considering the elements of the item, we can have the following FMEA:

1) Sensors fail in detecting the distance between the two vehicle:
    a. H1: braking request is lower than the right one
    b. H2: braking request is higher than the right one

2) Sensors fail in detecting the velocity of the forward vehicle:
    a. H1: braking request is lower than the right one
    b. H2: braking request is higher than the right one

3) Microcontroller fails in computing the deceleration:
    a. H1: braking request is lower than the right one
    b. H2: braking request is higher than the right one

4.2.3 Classification of hazardous events

4.2.3.1 **Exposure**

The item is designed to be active in highway. Hence, the value of exposure E is set to E4 for the entire analysis.

4.2.3.2 **Severity**

Severity S has been set depending on the range of the velocity if there is a crash. The ruleset adopted is reported in Table 13.

Velocity range	$0 - 10\ km/h$	$10 - 25\ km/h$	$25 - 45\ km/h$	$45 - \cdots\ km/h$
Severity	S0	S1	S2	S3

Table 13 – Severity allocation

4.2.3.3 **Controllability**

Controllability C has been set directly proportional to the severity (Table 14).

Severity	S0	S1	S2	S3
Controllability	C0	C1	C2	C3

Table 14 – Controllability allocation

4.2.4 Determination of ASIL

The ASIL determination has been carried out considering only the operational situation and the hazard event H1 (Table 15).

Operational situation	**Hazards H1**
OS1: crash with velocity between 0 and 10 km/h	S=0 C=0 no ASIL assignment is required E=4
OS2: crash with velocity between 10 and 25 km/h	S=1 C=1 **QM** E=4
OS3: crash with velocity between 25 and 45 km/h	S=2 C=2 **ASIL B** E=4

OS4: crash with velocity higher than 45 km/h	S=3 C=3 E=4	**ASIL D**

Table 15 – ASIL allocation

Figure 33, Figure34 and Figure 35 show ASIL allocation area associated to the applied deceleration and the necessary distance to stop the vehicle. The three different colored areas (red: ASIL D; yellow: ASIL B; green: QM) distinguish the combinations of distance, necessary to stop the vehicle, and deceleration, applied to the vehicle, for which it has the same value of ASIL. Going from right to left we can see that there is an increase in danger.

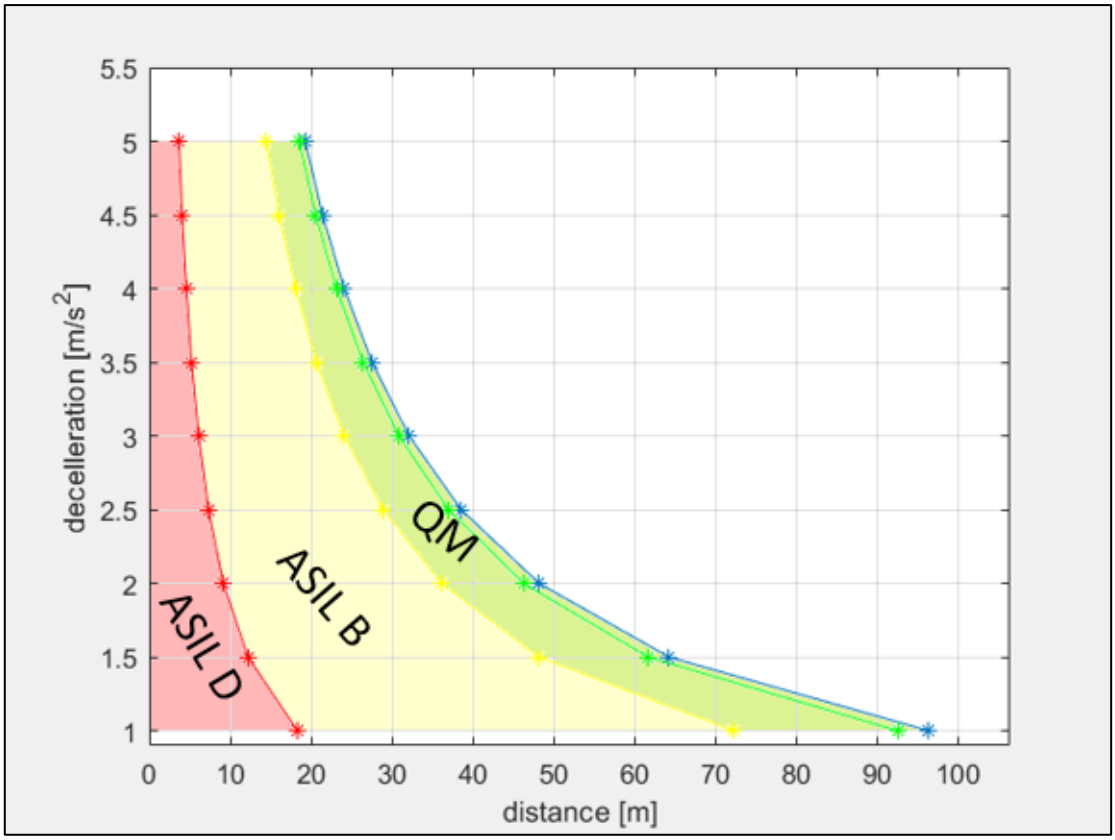

Figure 33 – ASIL allocation with initial speed = 50 km/h

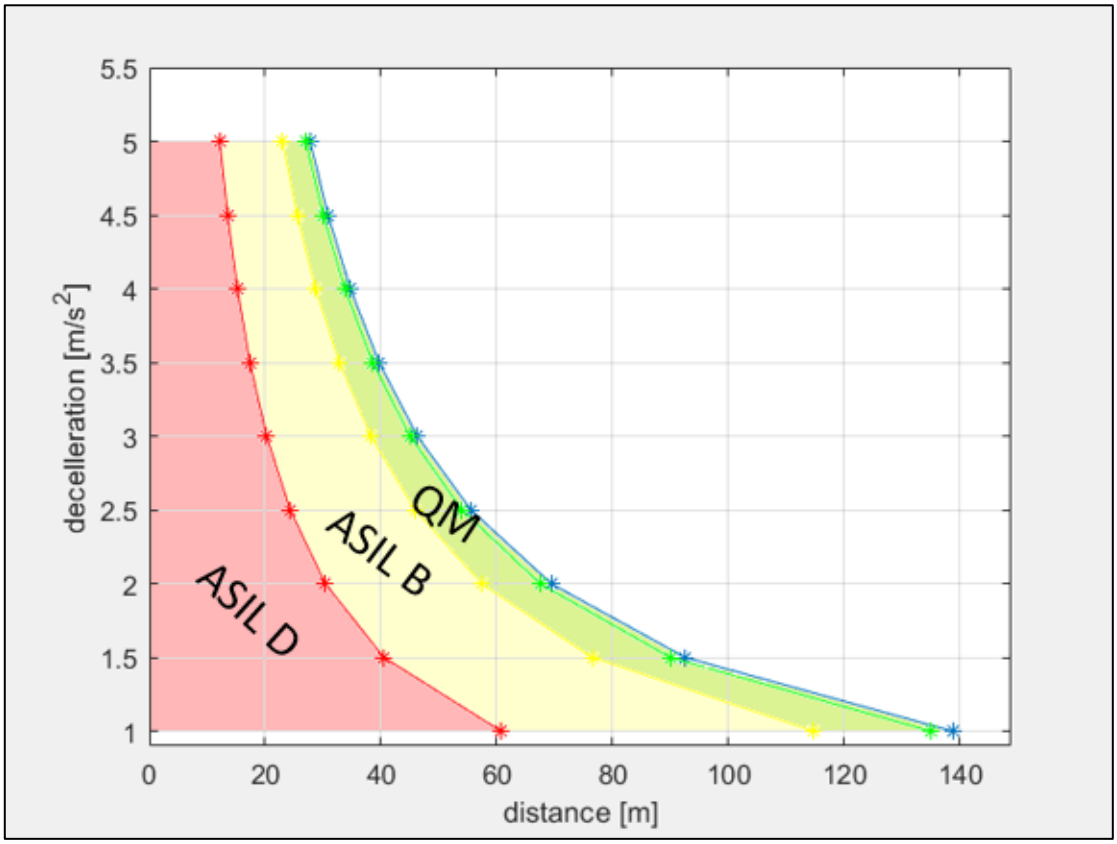

Figure 34 - ASIL allocation with initial speed = 60 km/h

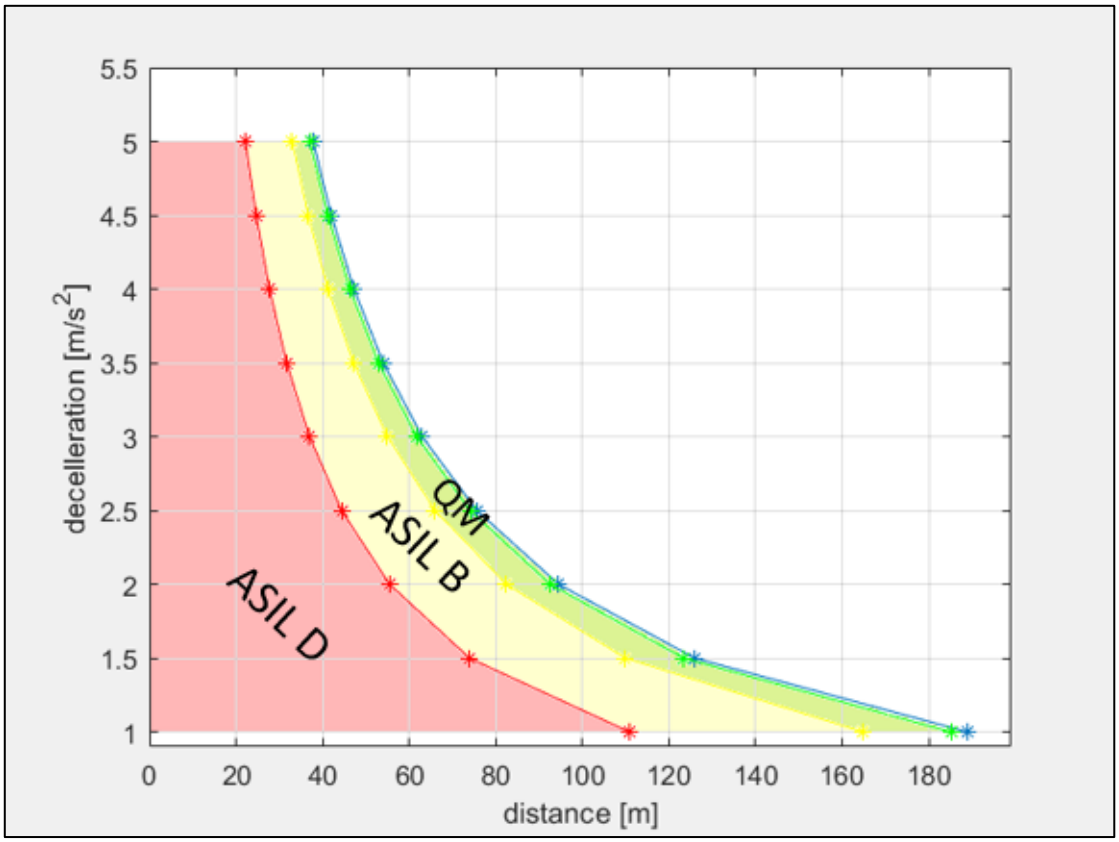

Figure 35 - ASIL allocation with initial speed = 70 km/h

4.2.5 Definition of safety goals

The following safety goals shall be applied:

- SG1: Distance between ego vehicle and forward vehicle shall be provided correctly.
- SG2: Relative velocity shall be provided correctly.
- SG3: Brakes shall be activated in the right moment.
- SG4: In case the AEBS ECU is not operational the safe state shall be entered.

4.2.6 Functional safety concept

Considering an ASIL D Item, the following functional safety concept shall be applied:

- FSC1: Sensors shall be duplicated.
- FSC2: An ASIL D microcontroller shall be used. In case of failure, the safe state shall be entered.
- FSC3: All the elements of the item shall be self-tested.

4.3 Fault Injection

4.3.1 Overview

The failures in the application sector of electrical and electronic systems, within road vehicle, can generate severe consequences. To obtain reliability, availability and safety, it has become very important to apply appropriate testing mechanism. The achievement of the system dependability is strictly connected to some topics during the design (Aidemark, et al. 2003):

- Defining the system dependability requirements.

- Designing and implementing the system considering the requirements.

- Validating the system.

To assert the dependability of a system several metrics can be attributed (Aidemark, et al. 2003):

I. ***Dependability:*** the property that allows reliance to be justifiably placed on the service it delivers.

II. ***Reliability:*** conditional probability that the system (given that it performs correctly at time t0) will perform correctly during the interval [t0, t].

III. ***Availability:*** probability that a system behaves correctly and is able to perform its function at the instant time t.

IV. ***Safety:*** probability that a system either behaves correctly or interrupts its functions without compromise the safety of any people.

V. ***Coverage:*** conditional probability that, given a fault, the system recovers.

VI. ***Maintainability:*** probability that a system can be repaired, once it has failed.

The main technique to validate the dependability of a system is the fault injection. It consists in introducing a fault into the system to observe its behavior. There are three type of fault injection:

1. ***Hardware-based fault injection:*** faults are injected in the integrated circuit of the target hardware system.

2. ***Software-based fault injection:*** faults are injected in the executing code of the target system.

3. ***Simulation-based fault injection:*** faults are injected in the simulation model of the target system.

For the validation of the HARA presented in the section 4.2 it is used a simulation-based fault injection.

4.3.2 AEBS Model

The AEBS model was created through Matlab/Simulink. The model (MathWorks) consists of two subsystem (Figure 36):

1. ***Subsystem 1:*** it models the AEBS controller, the speed controller, the accelerator robot and the Sensor Fusion that uses the Automated Driving System Toolbox.

2. ***Subsystem 2:*** it models the ego vehicle dynamics, the driver steering, the sensors and the scenario reader.

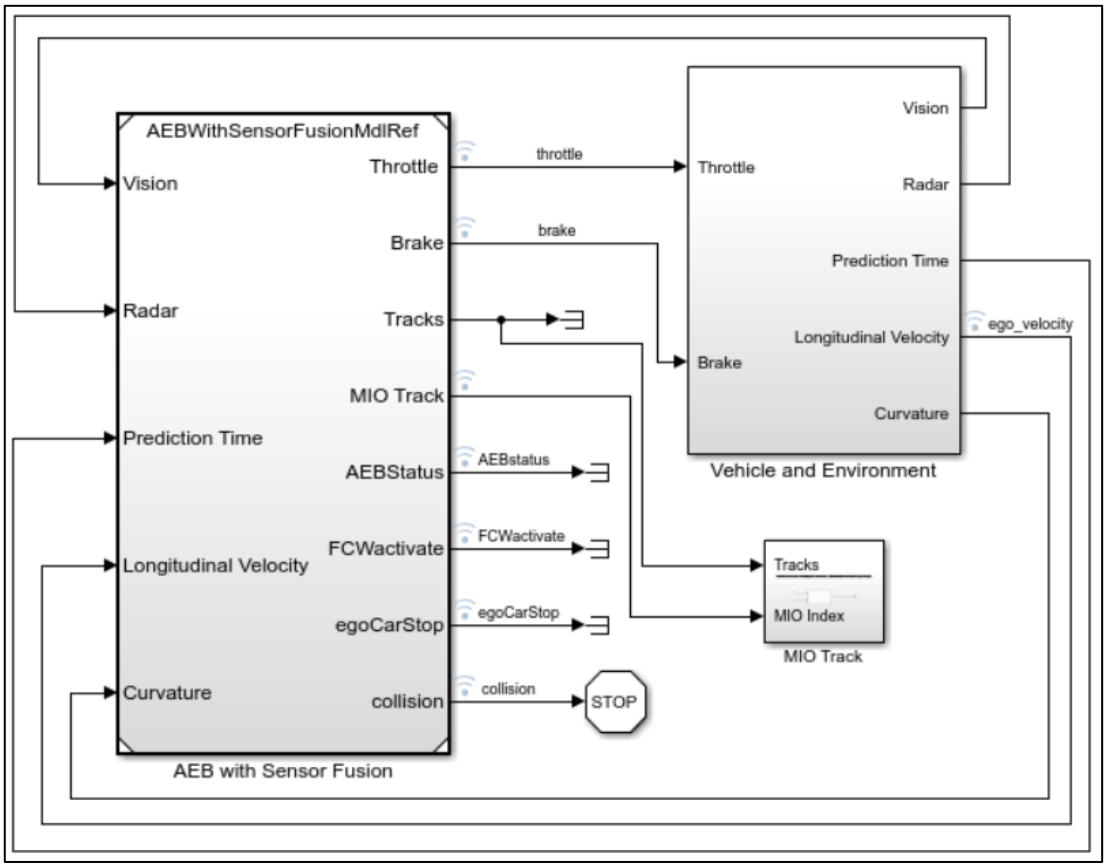

Figure 36 – Matlab model used for simulation

4.3.2.1 **Subsystem 1: AEB with Sensor Fusion**

AEB with Sensor Fusion subsystem contains the following parts (Figure 37):

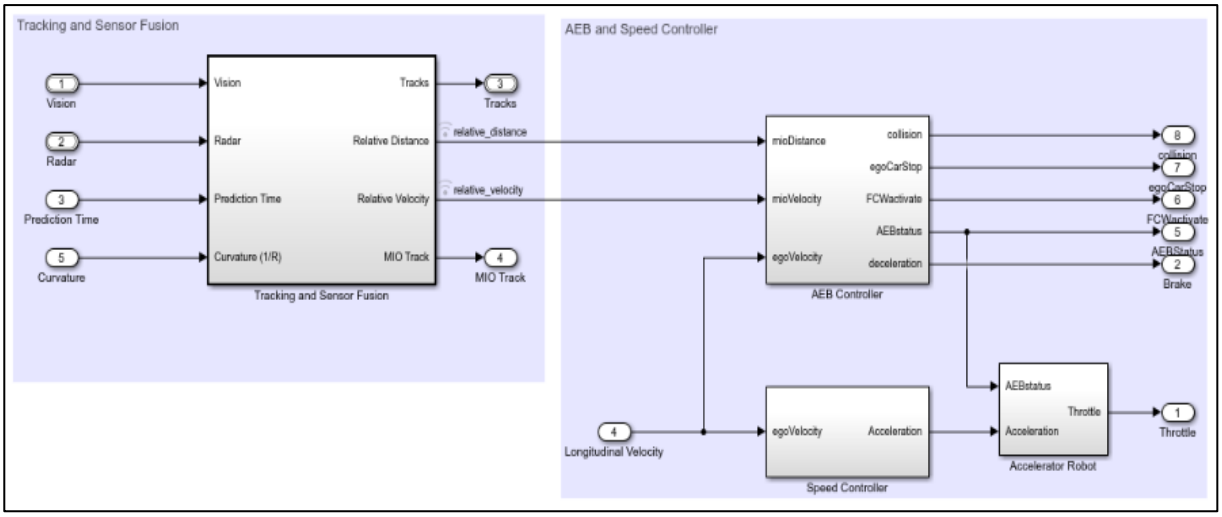

Figure 37 – AEBS model

- The Tracking and Sensor Fusion processes vision and radar detections coming from the Vehicle and Environment subsystem and obtains the position and the velocity of the objects near the ego vehicle.

- The Speed Controller takes the ego velocity and generates the acceleration.

- The accelerator Robot subsystem controls the accelerator and releases it during AEB activation.

- The AEB Controller models the forward collision warning (FCW) and AEB system.

The AEB Controller contains three subsystem:

- TTCCalculation: it takes the distance between vehicles and the relative velocity and calculates the time-to-collision (TTC).

- StoppingTimeCalculation: it calculates the timing for the FCW and for the phases of braking.

- AEB_Logic: it implements the logic of the AEB (Figure 38);

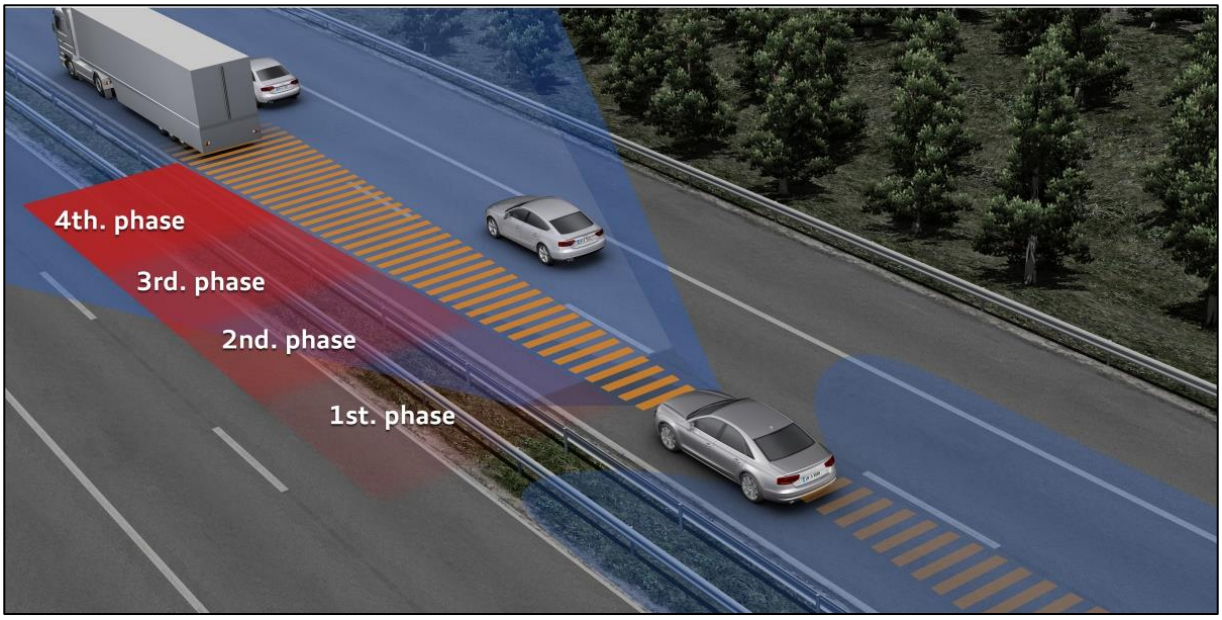

Figure 38 – AEBS functionality scheme, source (Audi 2011)

The logic of the AEB consists of some phases; if the driver fails to brake in time (during forward collision warning), the system try to avoid the collision applying a cascaded braking that consists of two partial braking (PB1 and PB2) followed by a full braking (Figure 39 and Figure 40).

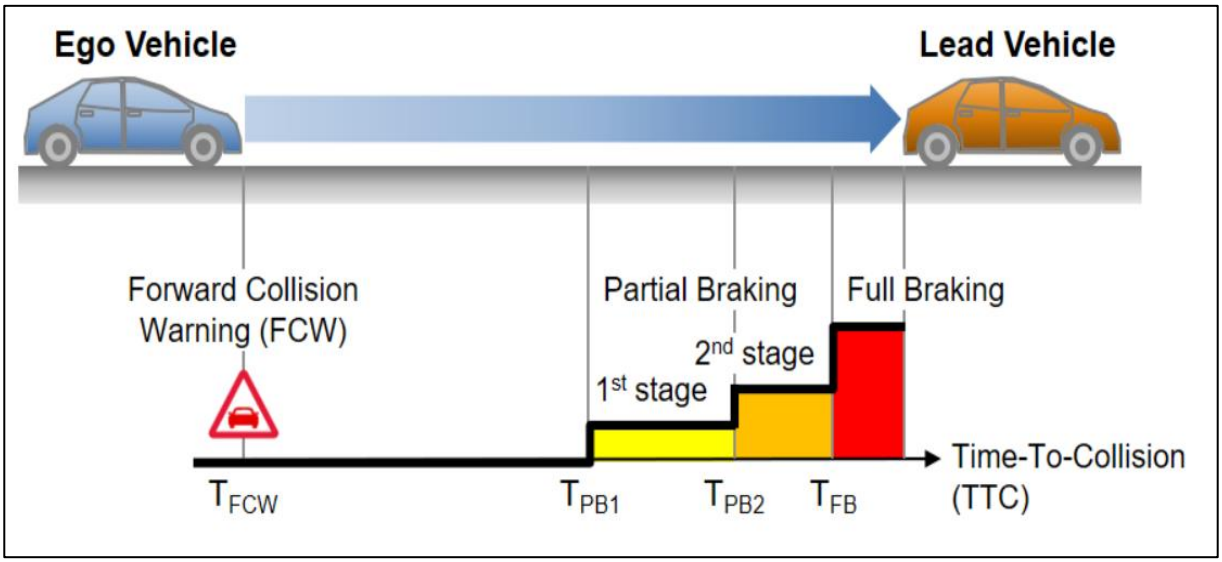

Figure 39 – AEBS cascade braking (MathWorks 2018)

First, the system checks if the time-to-collision is less than zero; the TTC is given by the following equation (4.1):

$$TTC = \frac{d}{\Delta v} \tag{4.1}$$

where:

d is the relative distance;

Δv is the relative velocity.

Then, the absolute value of the time-to-collision is compared, in cascade, with the forward collision warning time (FCWtime), the partial braking 1st stage time (PB1time), the partial braking 2nd stage time (PB2time) and the full braking time (FBtime). The results of the comparisons will be decisive in applying the right braking force (PB1decel, PB2decel and FBdecel).

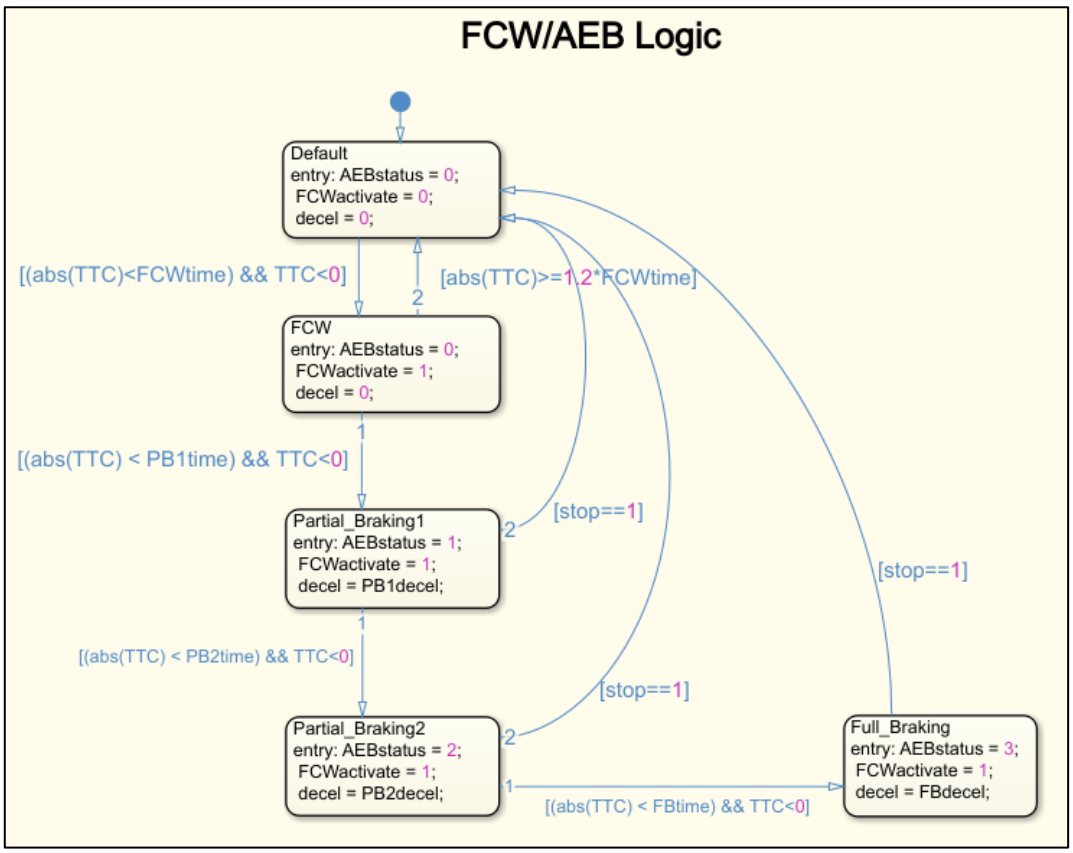

Figure 40 – FCW/AEB Logic

The timing of the AEB phases are regulated by the formulas listed in Table 16 and the values of deceleration are reported in Table 17.

Phases	Timing
Forward collision warning	$FCWtime = \frac{v}{FCW.driver\_decel} + FCW.timeToReact$ **(4.2)**
Partial braking 1st stage	$PB1time = \frac{v}{PB1decel}$ **(4.3)**
Partial braking 2nd stage	$PB2time = \frac{v}{PB2decel}$ **(4.4)**
Full braking	$FCWtime = \frac{v}{FBdecel}$ **(4.5)**
where v (m/s) is the vehicle longitudinal velocity, $FCW.driver\_decel = 4\ m/s^2$, $FCW.timeToReact = 1.2\ s$; $PB1decel, PB2decel$ and FB$decel$ are the phase decelerations and they are reported in Table 17.	

Table 16 – Timing for the AEB phases

Phases	Deceleration
Forward collision warning	$decel = 0\ m/s^2$
Partial braking 1st stage	$decel = PB1decel = 3.8\ m/s^2$
Partial braking 2nd stage	$decel = PB2decel = 5.3\ m/s^2$
Full braking	$decel = FBdecel = 8.0\ m/s^2$

Table 17 – Deceleration during AEB phases

4.3.2.2 **Subsystem 2: Vehicle and Environment**

Vehicle and Environment subsystem contains the following parts (Figure 41):

- The Vehicle Dynamics models the ego vehicle dynamics.
- The driver Steering Model calculates the driver steering angle.
- The Actor and Sensor Simulation models the sensors of the vehicle and contains a Scenario Reader to simulate the scenario (vehicles and environment) that is loaded when the Setup Script is running.

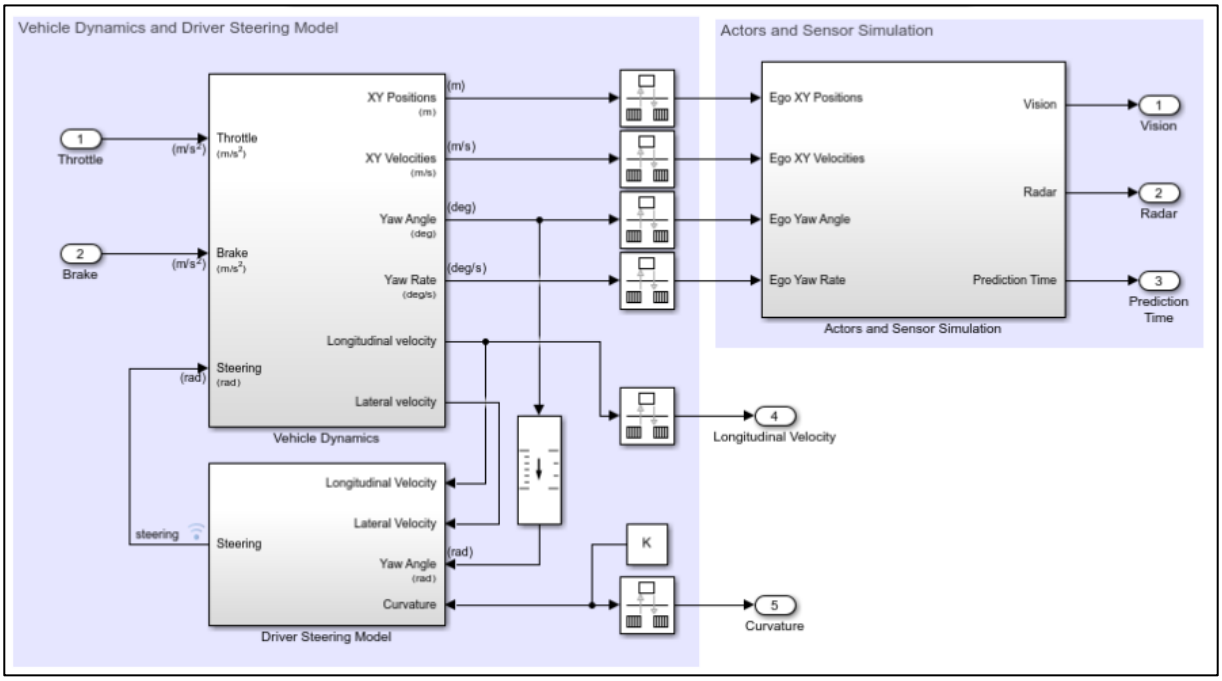

Figure 41 – Vehicle and Environment model

The scenario is contained in a file created by the Driving Scenario Designer. The Scenario Designer sets the characteristics of the actors (length, width and height of vehicles and objects) and of the road, the trajectories, the initial velocities and decelerations. The simulations have been carried out using the scenarios proposed by Euro NCAP AEB protocols for Car-to-Car Rear test.

An example of a scenario is reported in Figure 42.

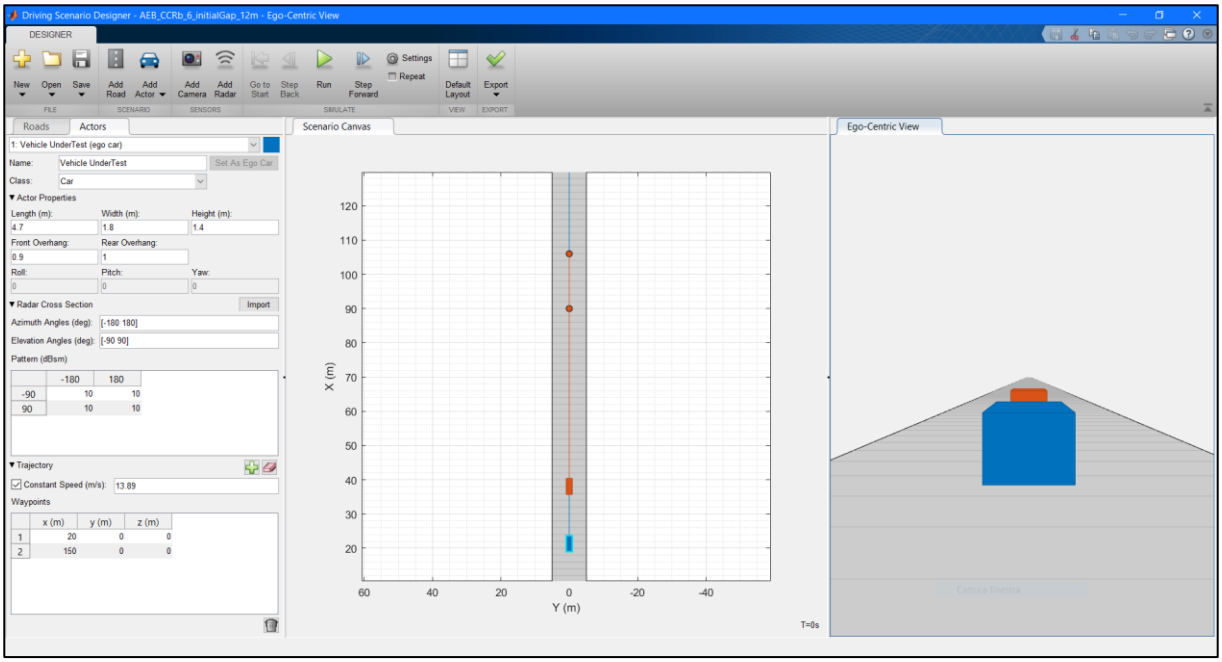

Figure 42 – Driving Scenario Designer

The detection characteristics of the sensors (Table 18) are:

- The maximum detection range of the Radar is equal to 174 m and its coverage area is tight (Figure 43).

- The maximum detection range of the Camera is equal to 150 m and its coverage area is larger (Figure 43).

Sensors	Maximum detection range
Radar	174 m
Camera	150 m

Table 18 – Maximum detection range of the sensors

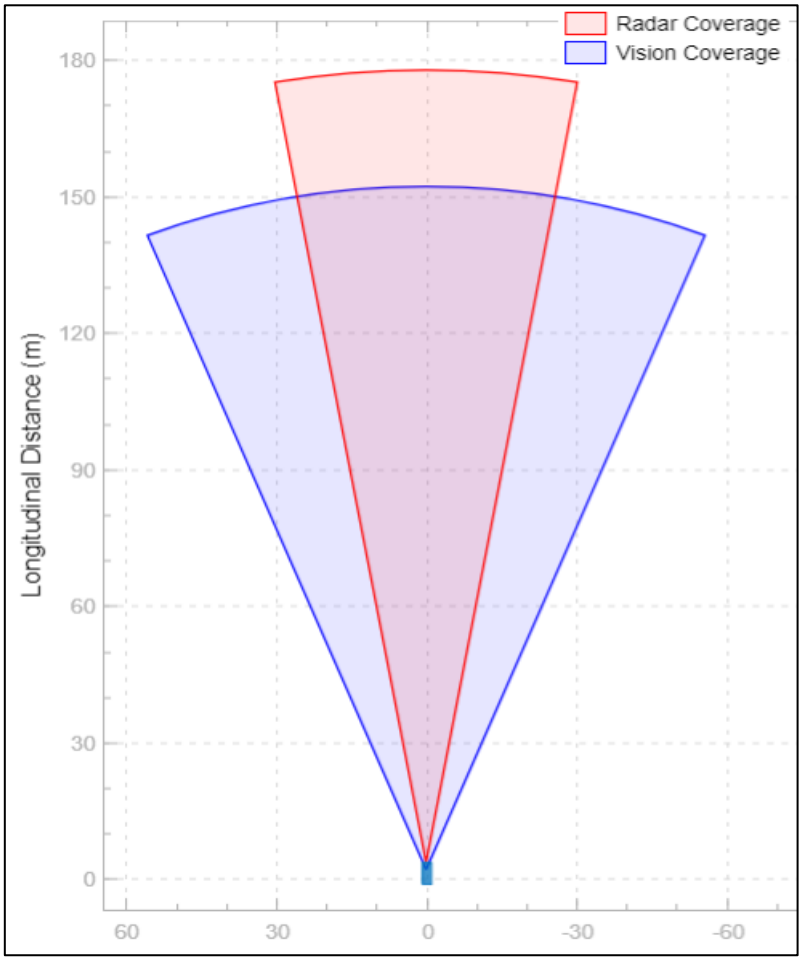

Figura 43 – Sensor coverage

4.3.3 Fault tolerant system

In order to validate the HARA, the model has been modified to create a fault tolerant mechanism, able to raise the robustness of the system. The sensors of the ego vehicle has been tripled. Then a subsystem has been added between Tracking and Sensor Fusion subsystem and AEB Controller subsystem; within the Fault Tolerant subsystem, two switches have been added and they have been connected to the signals of the sensors (Figure 44 and Figure 45); in this way, the outputs of a sensor are compared with outputs of the other sensors. When the measures are not equal, the activated sensor is released and another sensor is chosen. One switch is used for the relative distance measure and the other is used for the relative velocity measure.

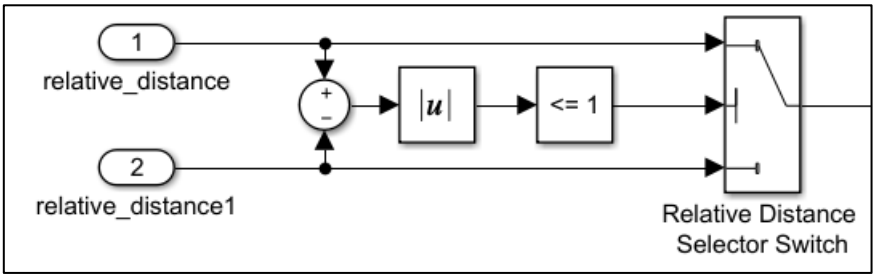

Figure 44 – Relative distance selector switch

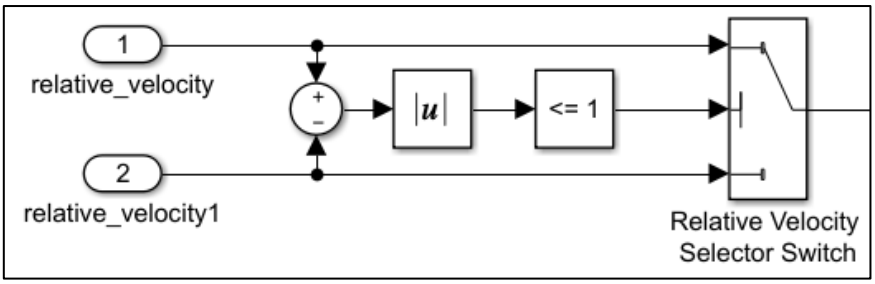

Figure 45 – Relative velocity selector switch

Some switches have been added in the subsystem to choose the active sensor for the visualization in the Bird Eye Scope. All the subsystem is shown in Figure 46.

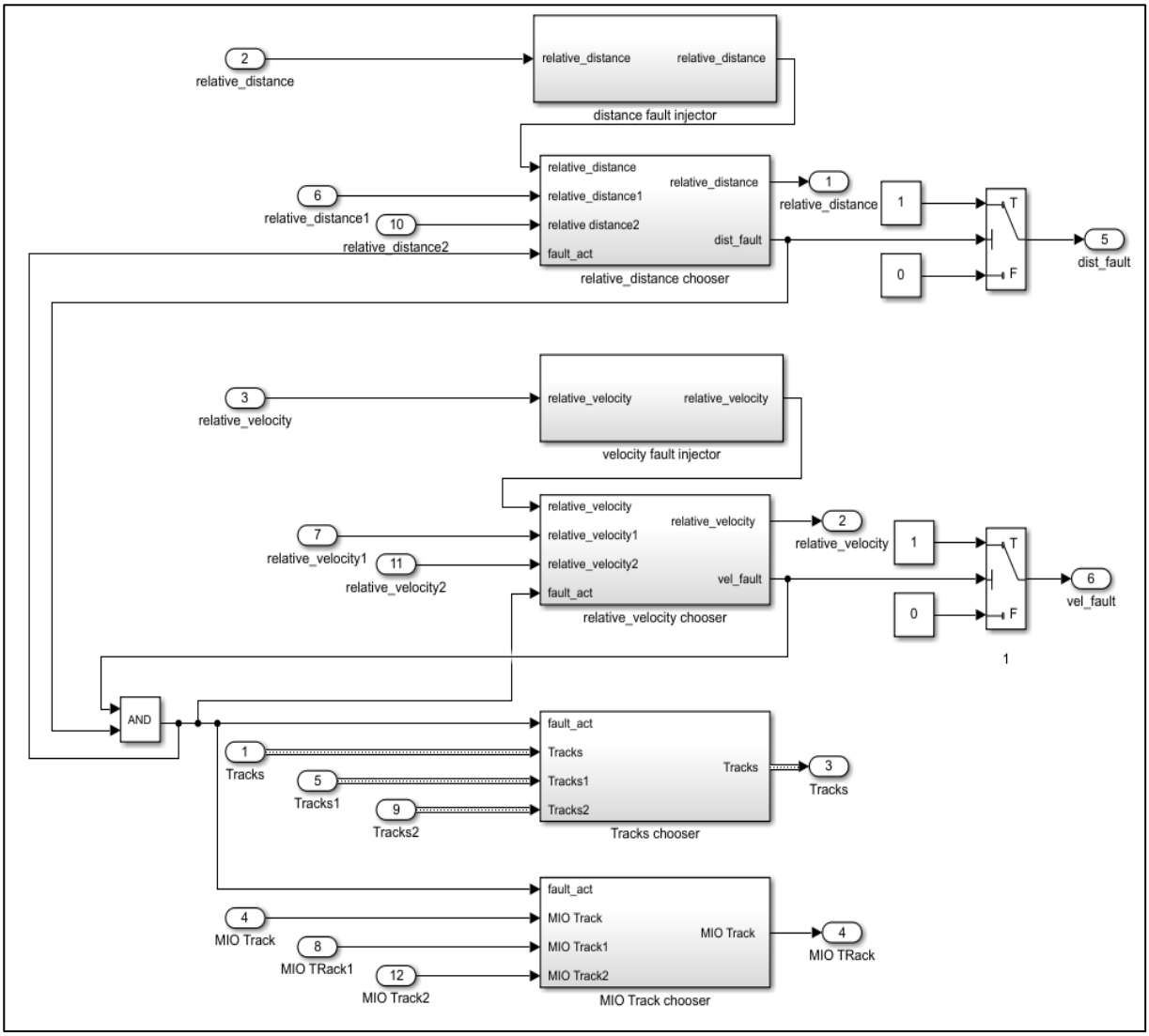

Figure 46 – Fault tolerant system model

4.3.4 Fault injection

The fault injection has been carried out by manipulating the signals of the relative distance and the relative velocity. Using two levers inserted in the dashboard, the injection of the fault is activated and two lamps will indicate if the fault has been discovered (Figure 47); this means that the relative distance signal and/or the relative velocity signal are altered with respect to their real values (Figure 48 and Figure 49). Subsequently, the resulting manipulated signal will be compared with that coming from another sensor and the tolerant system will decide which sensor to use.

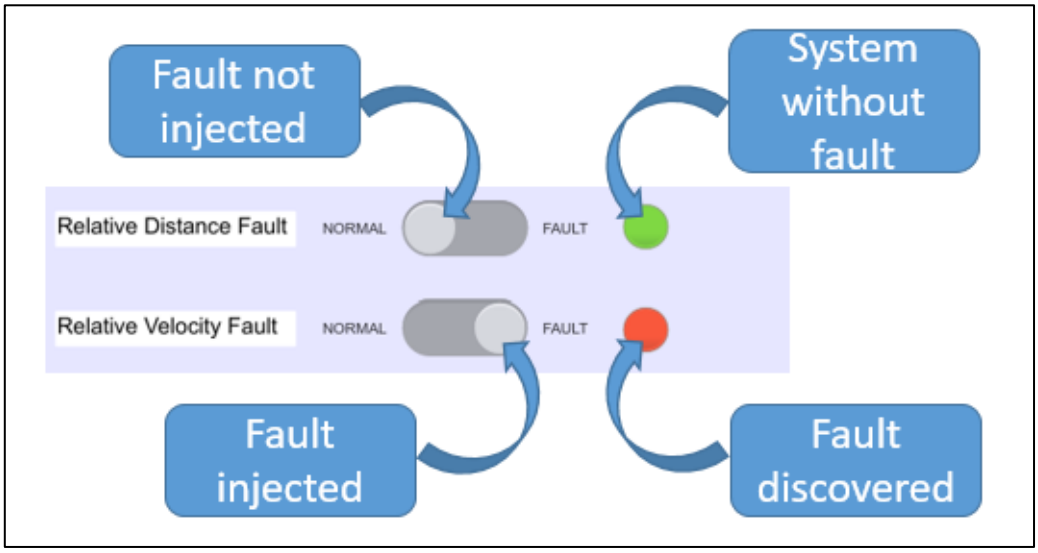

Figure 47 – Fault injector levers and fault lamps

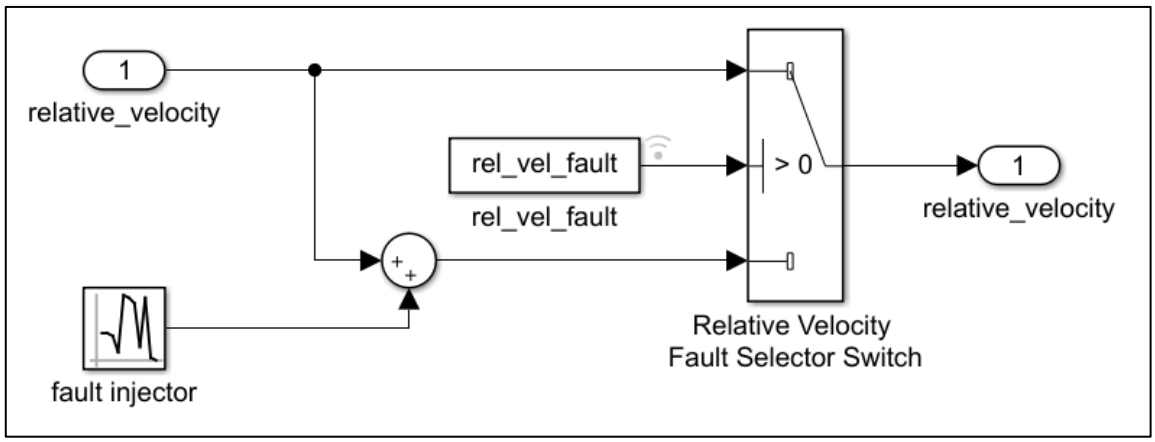

Figura 48 – Relative distance fault injector

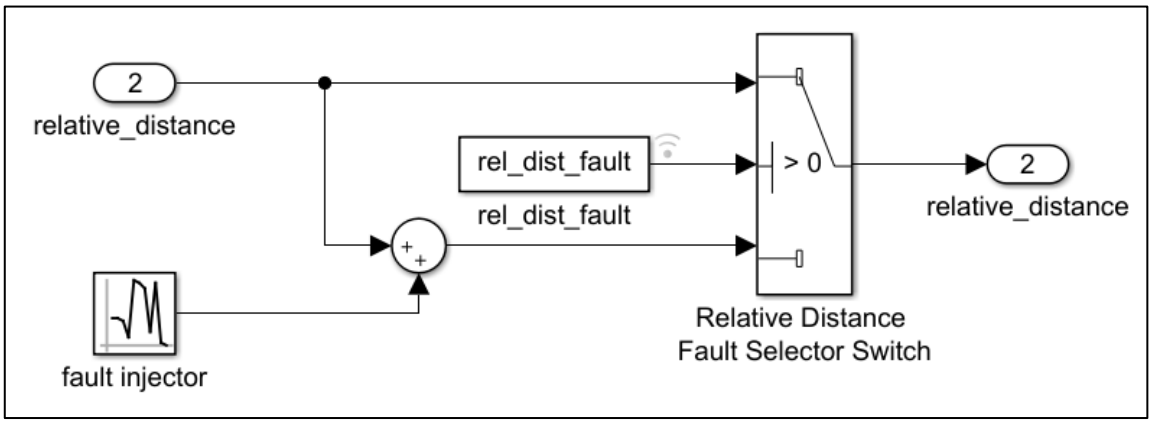

Figura 49 – Relative velocity fault injector

4.3.5 Simulation results

The simulations, as said previously, have been carried out using the scenarios proposed by Euro NCAP AEB protocols for Car-to-Car Rear test.

The result of the simulations, about a CCRb test, are shown below. The characteristics of the test are as follows (Figure 50):

1. Ego vehicle initial velocity $= 50\ km/h\ \ =\ \ 13{,}89\ m/s$
2. Target vehicle initial velocity $= 50\ km/h\ \ =\ \ 13{,}89\ m/s$
3. Initial distance $= 40\ m$
4. Ego vehicle velocity $=$ constant
5. Target vehicle velocity $=$ constant for 35 m; then it start to decelerate at 6 m/s^2

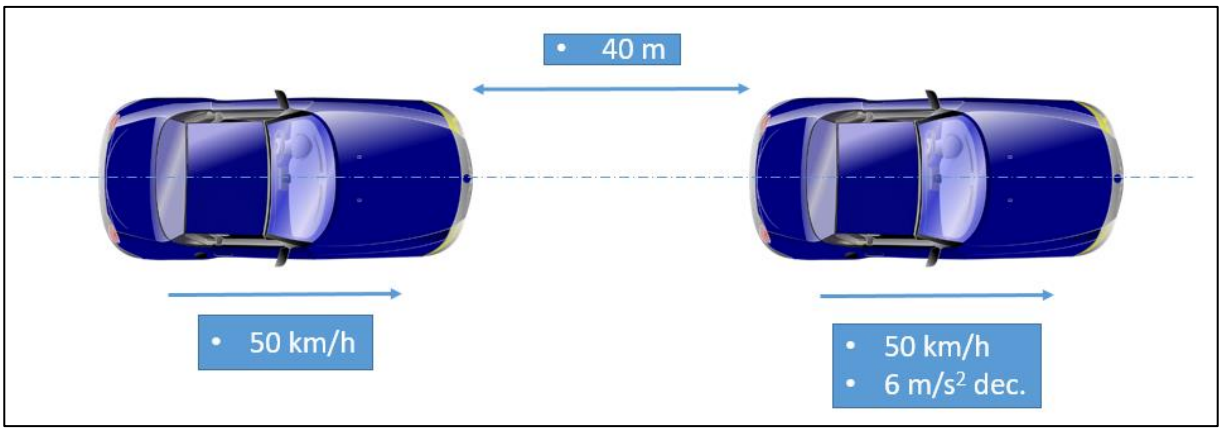

Figure 50 – Simulation scenario

A first test has been carried out, without fault injection, to check the behavior of the Automotive Emergency Braking System. The system was able to forecast the imminent crash, alert the driver, activate the brakes and avoid the collision. The data of the test are shown in Figure 51 and the initial and the final representation of the scenario are shown in Figure 52 and Figure 53.

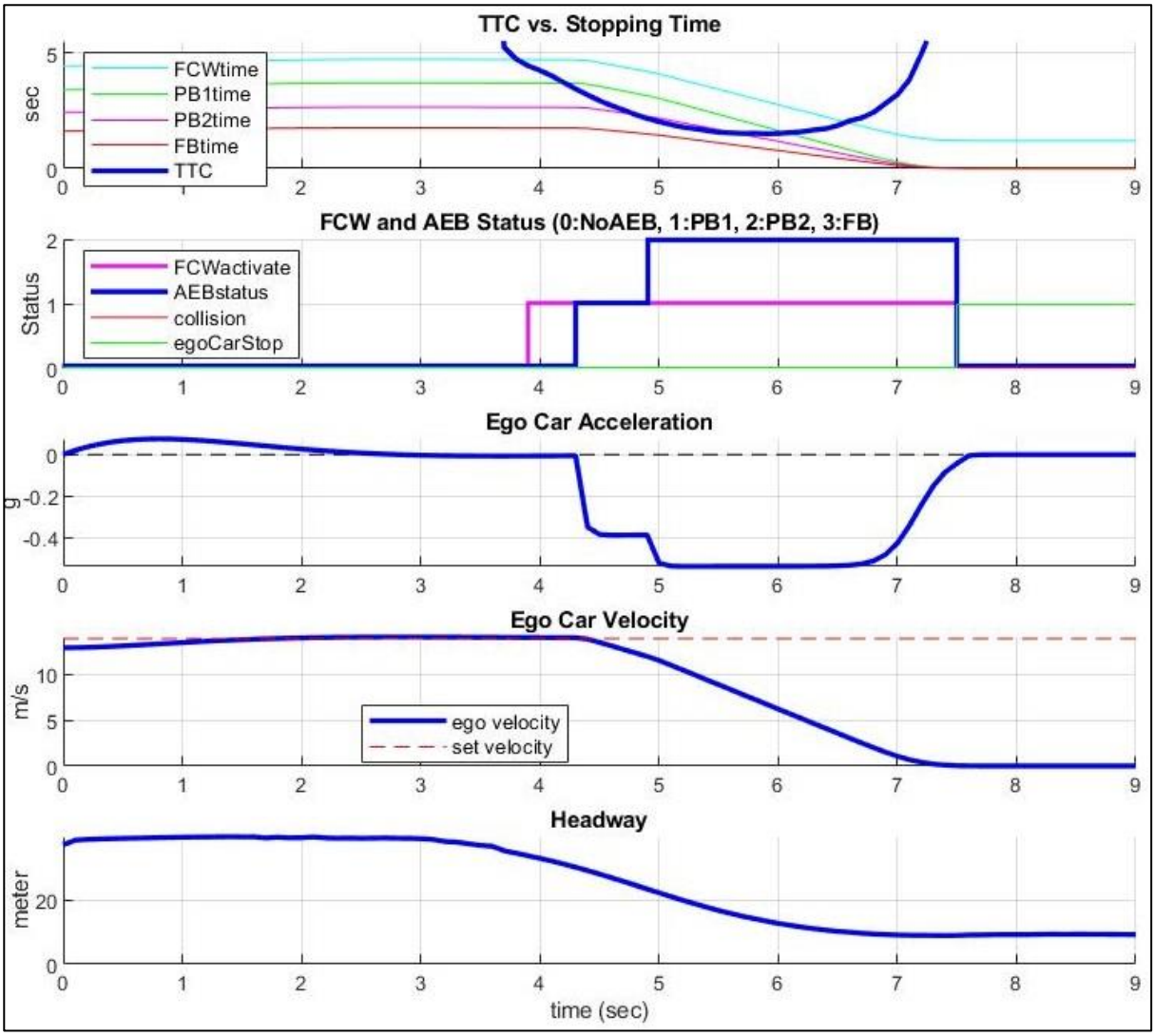

Figure 51 – AEBS test result without fault injection

The first plot of Figure 51 shows the time-to-collision compared with the stopping time of each phase and the second one shows the FCW and AEB status. The TTC decreases and, at first, it cuts the forward collision warning time line, activating the FCW (second plot, purple line); then it goes below the partial braking 1st stage time line and, subsequently, it cuts the partial braking 2nd stage time line; these two events trigger the partial braking 1st and 2nd stages (second plot, blue line). Finally, it starts to increase. During the FCW the deceleration is equal to $0\ m/s^2$; then during PB1 and PB2 the deceleration is equal, respectively, to $3.8\ m/s^2$ and $5.3\ m/s^2$ (third plot of Figure 51).

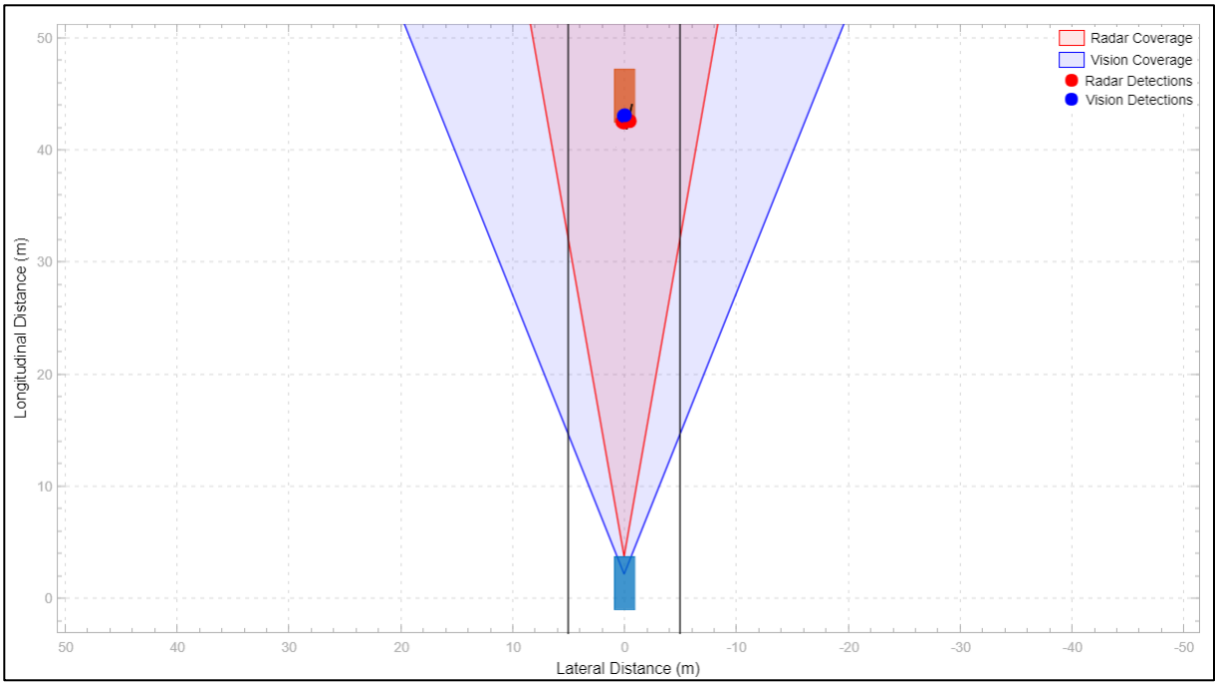

Figure 52 – Initial representation of the test

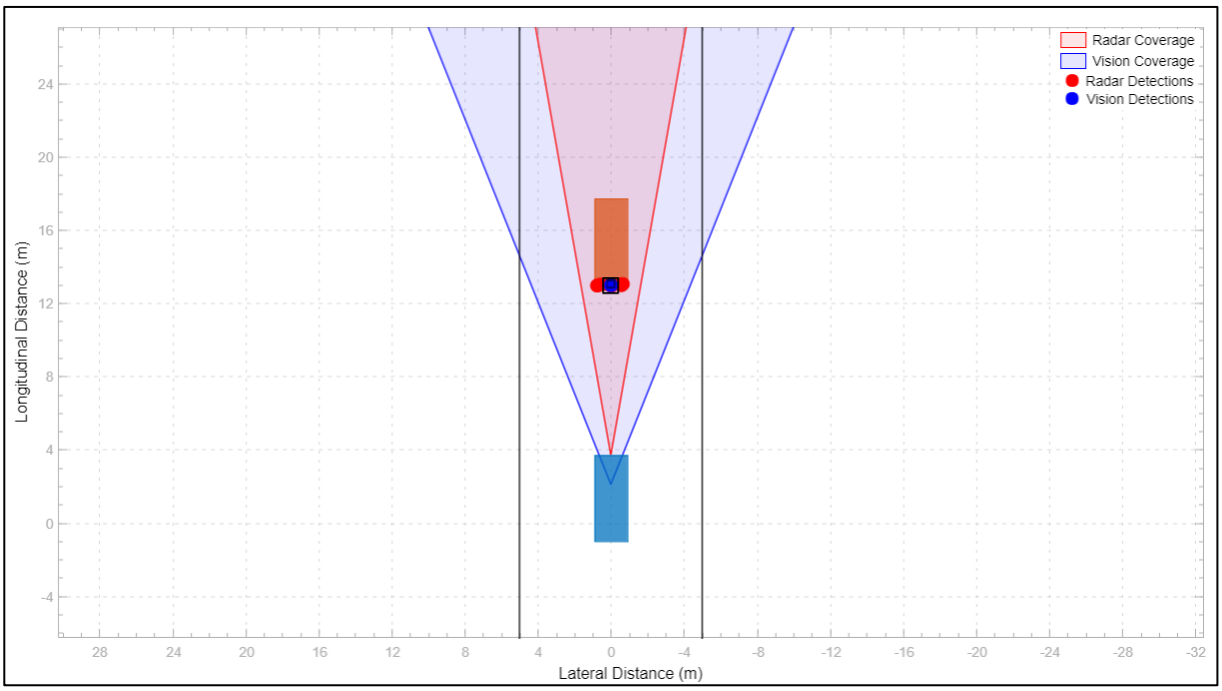

Figure 53 – Final representation of the test

Figure 52 and Figure 53 show the test scenario in the initial and final states. The two parallel grey lines are the edges of the road; the light blue rectangular is the ego vehicle and the orange one is the target vehicle. Moreover, the blue cone is the camera coverage

and the red one is the radar coverage. From the figures, it is possible to see that the detection areas of the sensors cover the space in front of the vehicle; the camera is able to detect the object (blue circle) and the radar detect the vehicle too (red circle).

A second test has been carried out, injecting a fault in the relative distance signal, to check the behavior of the Automotive Emergency Braking System. The system was able to discover the fault, release the faulty sensor and activate another one. Furthermore, it has been able to alert the driver, activate the brakes and avoid the collision. The data of the test are shown in Figure 54.

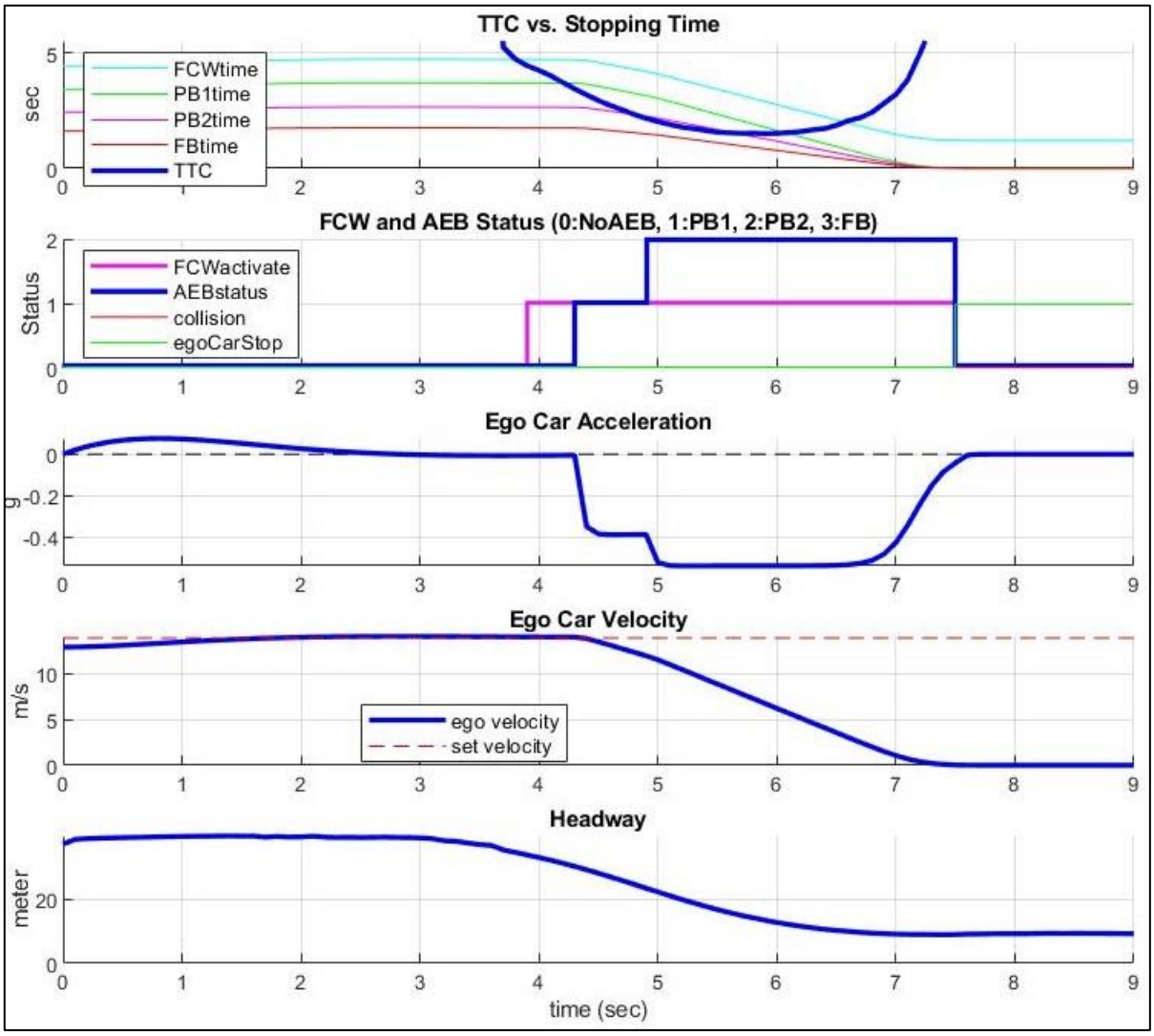

Figure 54 - AEBS test result with relative distance fault injection

A third test has been carried out, injecting a fault in the relative velocity signal, to check the behavior of the Automotive Emergency Braking System. The system was able to discover the fault, release the faulty sensor and activate another one. Furthermore, it has been able to alert the driver, activate the brakes and avoid the collision. The data of the test are shown in Figure 55.

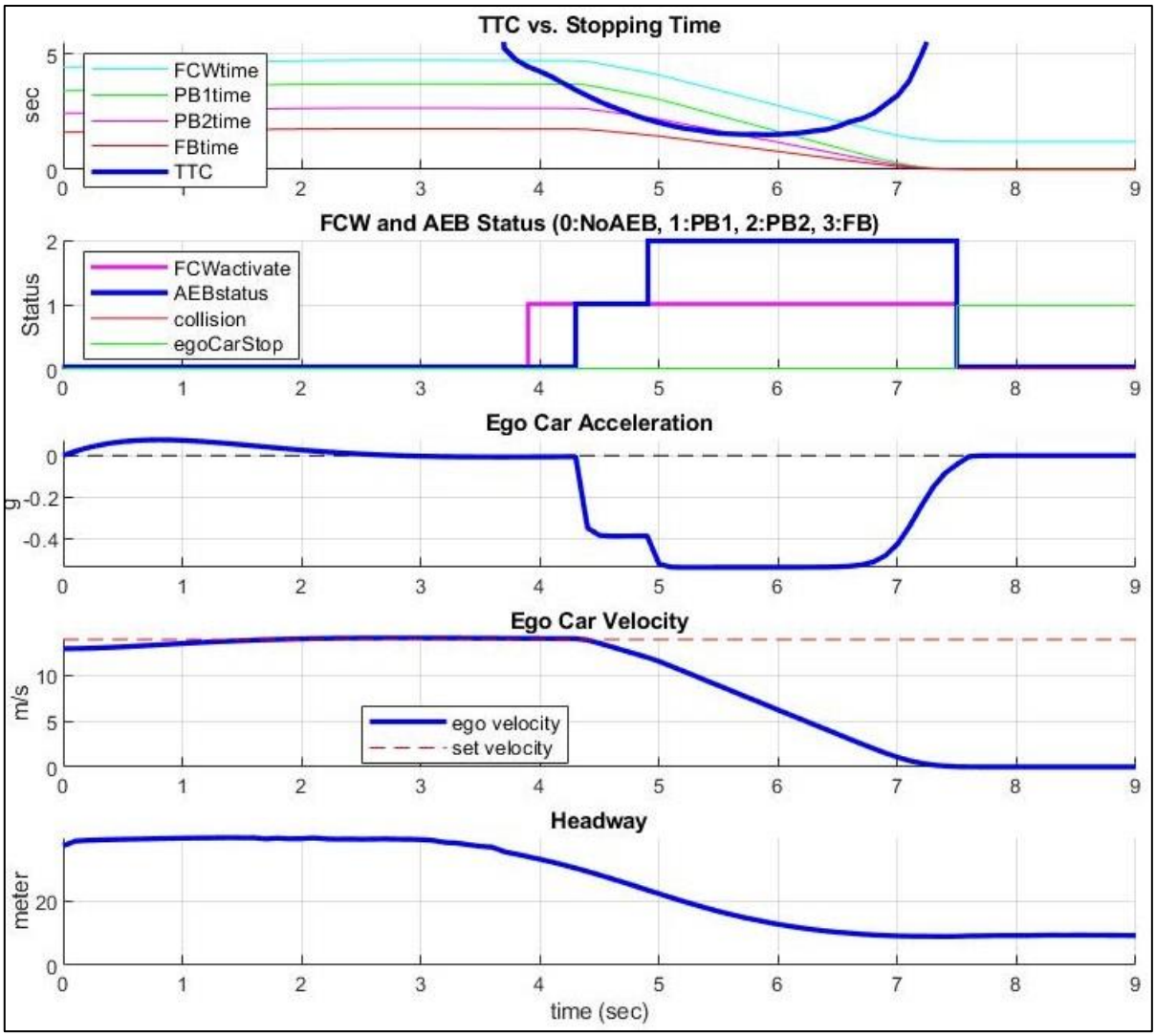

Figure 55 - AEBS test result with relative velocity fault injection

Finally, one last test has been carried out, injecting a fault both in the distance signal and in the relative velocity signal, to check the behavior of the AEBS. The system was able to discover the faults, release the faulty sensor and activate another one. Furthermore, it has been able to alert the driver, activate the brakes and avoid the collision. The data of the test are shown in Figure 56.

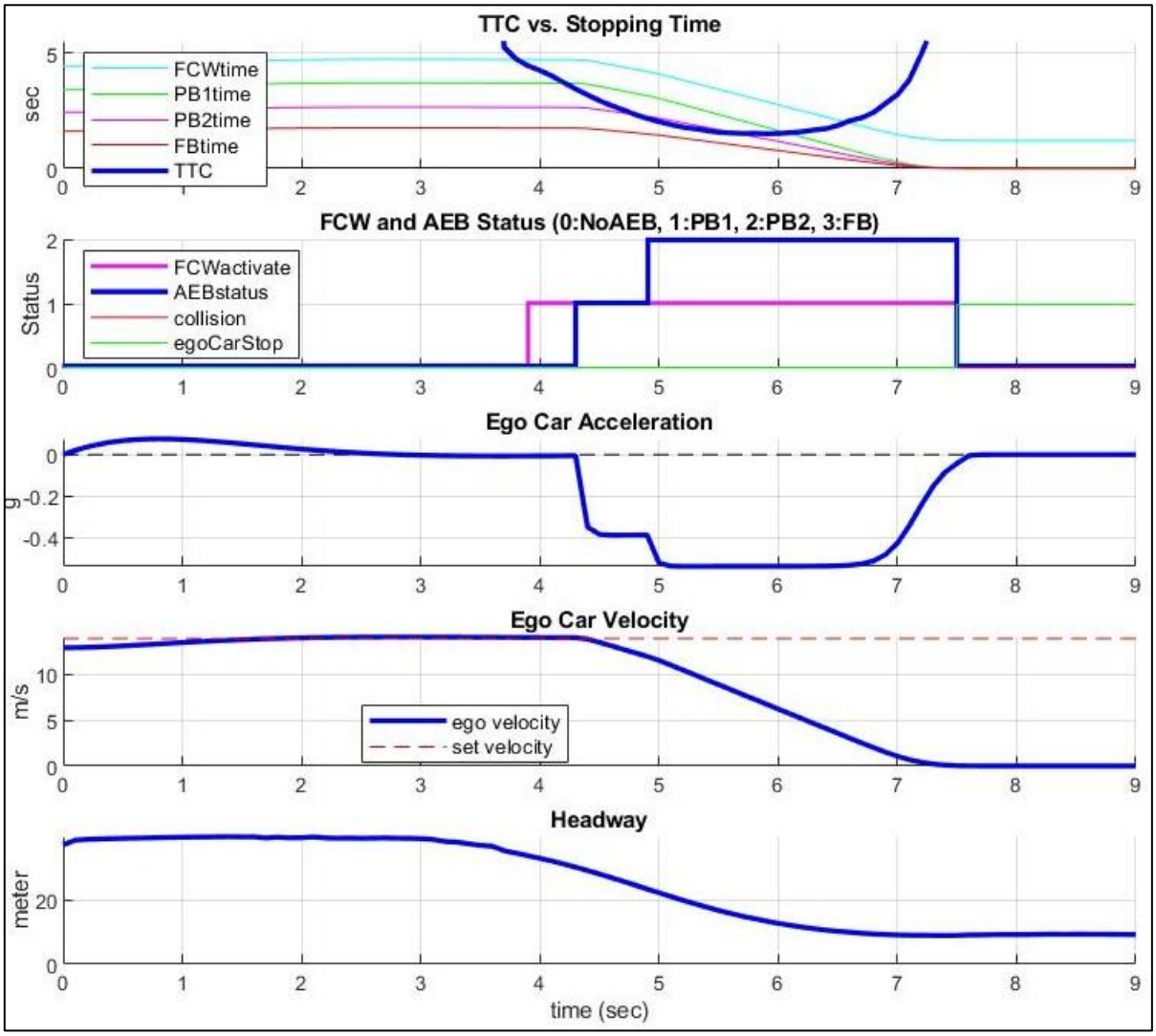

Figure 56 - AEBS test result with both relative distance and relative velocity fault injection

In each of the fault injection simulations, the Automotive Emergency Braking System behaves in the same way (Figure 54, Figure 55 and Figure 56) with respect to the simulation without fault (Figure 51). The time-to-collision decreases and it cuts, at first, the forward collision warning line, then, the partial braking 1st stage line and, finally, the partial braking 2nd stage line; subsequently, it starts to increase. In the same time, at first, the forward collision warning is activated, then, the partial 1st and 2nd stage brakings.

The same procedure, used for the CCRb test, has been exploited for other tests (CCRs and CCRm) and the system has been able to behave in a good way. Furthermore, further simulations have been carried out for scenarios in which there is a pedestrian or a bicyclist that is in the same trajectory of the ego vehicle or make a cut in maneuver. Also in these situations the system is able to detect faults and at the same time control the vehicle.

5 Conclusions

This thesis shows a brief view of the trend of the Advanced Driver-Assistance Systems, by providing definitions, historical reference and classifications about these systems.

Nowadays, the field of ADAS plays an important role in the design of the vehicle and in the future this relevance will grow exponentially. The controllability of the vehicle is a key target of the automotive industry and it will become one of the main points of distinction among the various car manufacturers, like motorization and aesthetic design.

It appears clear that the safety is a relevant factor within the development of a vehicle. The safety cycle, led by the ISO 26262, contributes significantly to the strengthening of the robustness of vehicles against various dangers caused both by man and by hardware and software malfunctions. Fault detection, failure mitigation and transitioning to safe state are three topics of the functional safety. Therefore, the HARA analysis, on the one hand (by the determination of the ASIL and the safety gaol), and the functional safety concept, on the other, are the main elements to be targeted in the development of the ADAS.

The design of fault tolerant mechanisms and driver warning systems are key points for the assessment of the safety in a vehicle. The validation of the functional safety concept

is an element of great importance and fault injection techniques are able to show the effectiveness of the results of the functional safety analysis.

If we consider the failures in driving control of vehicle, it appears clear that the critical situations to which they lead, can be very dangerous. In the final part of this thesis, faults on radar measurements are investigated. The main objective was to find a way to ensure that the system could be able to detect a possible fault and then fix it, thus preventing its propagation and the failure of the system. The proposed solution includes the duplication of the sensors and a mechanism for comparing the measurements. This system is able to test the operation state of the sensors, and if necessary, in the event of a fault, it can disable the faulty sensor and activate another.

However, faults can appear throughout the system, so more detailed analysis would be needed for complete validation of the AEBS; not only the sensors are subjected to faults but also actuators and other vehicle components. Furthermore, multiple faults can appear in the same time in different parts of the item and, for this reason, the ADAS control system shall be able to handle them. Fault-tolerant mechanisms improve the robustness of the systems, that is one the main target in the development of a product.

Moreover, in general, analysing the possible faults of the vehicle systems, it is necessary to take into account the presence of the drivers, and understand how their reaction can influence the countermeasures adopted by the same advanced driver-assistance system to prevent failures. The driver, in a critical situation, could approach the hazard situation differently than the system, or not consider particularly dangerous a manoeuver that, on the contrary, for the control algorithm instead is, or vice versa; therefore, the possible reaction of a driver shall be investigate, in the perspective of a better human-machine integration.

Several efforts shall be actuated to extend existing development procedures and/or create new ones in case they are not sufficient to satisfy the ever increasing introduction of new and more technological advanced driver-assistance system. Governmental institution, automotive industry and consumers shall cooperate and make sure that the safety that emerges from ADAS can grow, together with efficiency and appropriate knowledge.

5.1 Further improvements

The work carried out in this thesis can be extended in the future by studying the behavior of the system in case the failures make the system perceive the forward vehicle closer to the actual distance or in case the radar stops working. In the first case, the system would activate an unnecessary alarm and start a braking that could create a danger for the vehicles behind it. Furthermore, this situation could cause a disorientation of the

driver and a subsequent potentially dangerous manoeuver. Other research may be aimed at the injection of faults in the braking profile at the exit of the AEBS controller and some solutions must be generated to handle this kind of failures. Faults can also be injected into the controller, verifying the repercussions on the whole system. Finally, hardware-in-the-loop test and validation can be performed with IPG CarMaker and a real microcontroller.

6 Abbreviations

ADAS - Advanced Driver Assistance System

ABS - Antilock Braking System

ACC - Adaptive Cruise Control

AD - Automated driver

AEBS - Autonomous Emergency Breaking Systems

ASIL - Automotive Safety Integrity Level

FB - AEB Full Braking

FCW - Forward Collision Warning

FB - AEB Full Braking

FMEA - Failure Mode and Effect Analysis

FVCMS - Forward Vehicle Collision Mitigation System

HARA - Hazard Analysis and Risk Assessment

HAZOP - Hazard and Operability Analysis

HD - Human driver

OEM - Original Equipment Manufacturers

PB1 - AEB Partial Braking 1st stage

PB2 - AEB Partial Braking 2nd stage

RADAR - Radio Detection and Ranging

STPA - System Theoretic Process Analysis

TTC - Time-to-collision

7 Bibliography

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

Aidemark, J., A. Baldini, J. C. Baraza, M. Bellato, A. Benso, S. Blanc, J. Boué,J. Carreira, M. Ceschia, F. Corno, D. Costa, Y. Crouzet, J.-C. Fabre, L. Entrena, P. Folkesson, D. Gil, P. J. Gil, J. Gracia, L. Impagliazzo, E. Jenn, B. W. Johnson J.A. Arlat, J. Karlsson, C. Lopez, T. Lovric, and H. Madeira. *FAULT INJECTION TECHNIQUES AND TOOLS FOR EMBEDDED SYSTEMS RELIABILITY EVALUATION.* Kluwer Accademic Publisher, 2003.

Audi. *Audi Technology Portal.* 2011. https://www.audi-technology-portal.de/en/electrics-electronics/safety-systems/audi-pre-sense_en (accessed 2018).

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

Dodde, V., A. Masciullo, and G. Ricci. "Adaptive compensation of amplitude and phase conversion errors for FMCW radar signals." *2nd IET International Conference on Intelligent Signal Processing 2015 (ISP).* London: IET, 2015.

Elgharbawy, M., A. Schwarzhaupt, G. Scheike, M. Frey, and F. Gauterin. *A Generic Architecture of ADAS Sensor Fault Injection for Virtual Tests.* IEEE, 2016.

Eskandarian, Azim. *Handbook of Intelligent Vehicles.* London: Springer, 2012.

Euro NCAP. *Test Protocol - AEB Systems.* 2017.

IEC. *IEC61508.* International Electrothechnical Commission, 2010.

ISO 22839. *Intelligent transport system - Forward vehicle collision mitigation system - Operation, performance, and verification requirements.* International Organization for Standardization, 2013.

ISO 26262-3. *Road vehicles-Functional safety: Concept phase.* International Organization for Standardization, 2011.

Johansson, R., J. Nilsson, and M. Kaalhus. "Safe Transitioning of Responsability in Highly Automated Driving." *The Ninth International Conference on Dependability.* 2016.

Juez, G., E. Amparan, R. Lattarulo, J. P. Rastelli, A. Ruiz, and H. Espinoza. “Safety Assessment of Automated Vehicle Functions by Simulation-based Fault Injection.” *International Conference on Vehicular Electronics and Safety (ICVES).* Vienna: IEEE, 2017.

Low, Hoiman. *Attaining functional safety: Managing random failures.* Texas Instruments, 2015.

MathWorks. *Automatic Emergency Braking with Sensor Fusion.* n.d. https://it.mathworks.com/examples/automated-driving/mw/driving-ex96624516-automatic-emergency-braking-with-sensor-fusion?s_tid=srchtitle (accessed 2018).

Michon, J. A. “A critical view of driver behaviour models: What do we know, what should we do?” In *Human behavior and traffic safety*, by Evans L. and Schwing R.C. Boston: Springer, 1985.

Nilsson, J., N. Strand, P. Falcone, and J. Vinter. “Driver performance in the presence of adaptive cruise control related failures: Implications for safety analysis and fault tolerance.” *2013 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W).* 2013. 1-10.

Okuda, R., Y. Kajiwara, and K. Terashima. “A survey of technical trend of ADAS and autonomous driving.” *Proceedings of Technical Program - 2014 International Symposium on VLSI Technology, Systems and Application (VLSI-TSA).* Hsinchu, Taiwan: IEEE, 2014.

Pintard, L. *From safety analysis to experimental validation by fault injection - Case of automotive embedded system.* Toulouse: INP, 2015.

ProfessionalQA.com. 2016. http://www.professionalqa.com/v-model (accessed 2018).

Rezaei, M. “Computer Vision for Road Safety: A System for Simultaneous of Driver Behaviour and Road Hazards.” 2014.

SAE International. *J3016-Taxonomy and Definitions for Terms related to Driving Automation Systems for On-Road Motor Vehicle.* SAE International, 2016.

Stove, A. G. “Linear FMCW radar techniques.” In *IEE Proceedings F - Radar and Signal Processing*, 343-350. IET, 1992.

Strand, N., J. Nilsson, M. Karlsson, and L. Nilsson. “INTERACTION WITH AND USE OF DRIVER ASSISTANCE SYSTEMS: A STUDY OF END-USER EXPERIENCES.” 2011.

Svenningsson, R. *Model-Implemented Fault Injection for Robustness Assessment.* Stockholm: KTH Royal Institute of Technology, 2011.

Svenningsson, R., H. Eriksson, and J. Vinter. “Model-Implemented Fault Injection for Hardware Fault Simulation.” *Workshop on Model-Driven Engineering, Verification, and Validation.* Oslo: IEEE, 2010.

Van Eikema Hommes, Qi. *Safety analysis approaches for automotive electronic control system.* 2015.

van Schijndel-de Nooij, Margriet, et al. “Definition of necessary vehicle and infrastructure systems.” Study report, Brussels, 2011.

Walker Smith, Bryant. *SAE LEVELS OF DRIVING AUTOMATION.* 2013. http://cyberlaw.stanford.edu/blog/2013/12/sae-levels-driving-automation (accessed 2018).

Winner, H., S. Hakuli, F. Lotz, and C. Singer. *Handbook of Driver Assistance System.* Cham: Springer, 2016.