**ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL**

# FUNCTIONAL SAFETY ANALYSIS FOR ADVANCED EMERGENCY BRAKING SYSTEMS

**M.Sc. THESIS**

**Semih UZUN**

**Department of Control and Automation Engineering**

**Control and Automation Engineering Programme**

**JULY 2021**

**ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL**

# FUNCTIONAL SAFETY ANALYSIS FOR ADVANCED EMERGENCY BRAKING SYSTEMS

**M.Sc. THESIS**

**Semih UZUN**
**(504181125)**

**Department of Control and Automation Engineering**

**Control and Automation Engineering Programme**

**Thesis Advisor: Assis. Prof. Dr. İlker ÜSTOĞLU**

**JULY 2021**

**ISTANBUL TEKNİK ÜNİVERSİTESİ ★ LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ**

# İLERİ ACİL FRENLEME SİSTEMLERİ İÇİN FONKSİYONEL EMNİYET ANALİZİ

**YÜKSEK LİSANS TEZİ**

**Semih UZUN**
**(504181125)**

**Kontrol ve Otomasyon Mühendisliği Anabilim Dalı**

**Kontrol ve Otomasyon Mühendisliği Programı**

**Tez Danışmanı: Dr. Öğr. Üyesi İlker ÜSTOĞLU**

**TEMMUZ 2021**

Semih UZUN, a M.Sc. student of ITU Graduate School student ID 504181125, successfully defended the thesis entitled "FUNCTIONAL SAFETY ANALYSIS FOR ADVANCED EMERGENCY BRAKING SYSTEMS", which he prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are below.

| | | |
|---|---|---|
| **Thesis Advisor :** | **Assis. Prof. Dr. İlker ÜSTOĞLU**<br>İstanbul Technical University | ..... |
| **Jury Members :** | **Prof. Dr. Metin GÖKAŞAN**<br>Istanbul Technical University | ..... |
| | **Prof. Dr. Tankut ACARMAN**<br>Galatasaray University | ..... |

**Date of Submission : 09.06.2021**
**Date of Defense : 05.07.2021**

***To my family,***

**FOREWORD**

First of all, I would like to thank my supervisor Assis. Prof. Dr. İlker ÜSTOĞLU for his support throughout the my thesis. I would also like to thank my friends Ersin Armağan and Abdullah Ömer Sevil and my family for their helps and support.

June 2021

Semih UZUN
Control and Software Engineer

**TABLE OF CONTENTS**

**Page**

**ABBREVIATIONS**

**ABS** : Anti-Lock Braking
**ADAS** : Advanced Driver Assistance System
**ADS** : Automated Driving System
**AEBS** : Advanced Emergency Braking System
**AIS** : Abbreviated Injury Scale
**ASIL** : Automotive Safety Integrity Level
**AUTOSAR** : Automotive Open System Architecture
**BCM** : Body Control Module
**BDCMS** : Bicyclist detection and collision mitigation systems
**BSW** : Basic Software
**CAN** : Controller area network
**CMBS** : Collision Mitigation Brake System
**cog** : Center of gravity
**CW** : Collision Warning
**ECU** : Electronic Control Unit
**E/E** : Electrical and Electronic
**ESC** : Electronic Stability Control
**ESS** : Emergency Steering System
**ETTC** : Enhanced Time to Collision
**FOV** : Field of View
**FDTI** : Fault Detection Time Interval
**FHTI** : Fault Handling Time Interval
**FTTI** : Fault Tolerant Time Interval
**FRTI** : Fault Reaction Time Interval
**FSR** : Functional Safety Requirement
**FVCMS** : Forward Vehicle Collision Mitigation Systems
**GPL** : General Public License
**GPS** : Global Positioning System
**GVW** : Gross Vehicle Weight
**HARA** : Hazard Analysis and Risk Assessment

**HIL** **:** Hardware-in-the Loop

**HMI** **:** Human-Machine Interface

**HMT** **:** Hazard Manifestation Time

**IEC** **:** International Electrotechnical Commission

**IIHS** **:** Insurance Institute for Highway Safety

**IMU** **:** Inertial Measurement Unit

**ISO** **:** International Organization for Standardization

**LIN** **:** Local Interconnect Network

**Lidar** **:** Light Detection and Ranging

**MB** **:** Mitigation Braking

**MBMT** **:** Malfunctioning Behavior Manifestation Time

**MIL** **:** Model-in-the Loop

**MMW** **:** MMW millimeter-wave

**MOST** **:** Media Oriented System Transport

**NHTSA** **:** National Highway Traffic Safety Administration

**OEM** **:** Original Equipment Manufacturers

**PCM** **:** Powertrain Control Module

**PCS** **:** Pre-Collision System

**RADAR** **:** Radio Detection and Ranging

**RCS** **:** Roll Stability Control

**RTE** **:** Runtime Environment

**SAE** **:** Society of Automotive Engineers

**SONAR** **:** Sound Navigation and Ranging

**SRB** **:** Speed Reduction Braking

**SV** **:** Subject Vehicle

**TCS** **:** Traction Control System

**TORCS** **:** The Open Racing Car Simulator

**TTC** **:** Time to Collision

**TV** **:** Target Vehicle

**UNECE** **:** United Nations Economic Commission for Europe

**VRU** **:** Vulnerable Road User

**SYMBOLS**

$A_F$ : Vehicle frontal area

$a_{SV}$ : Subject vehicle acceleration

$a_{TV}$ : Target vehicle acceleration

$a_{rel}$ : Relative acceleration

$B$ : Stiffness factor

$C$ : Shape factor

$C_d$ : Aerodynamic drag coefficient

$C_{roll}$ : Rolling resistance coefficient

$D$ : Peak value

$E$ : Curvature factor

$F_{aero}$ : Longitudinal aerodynamic drag force

$F_x$, $F_y$, $F_z$ : Tire Forces

$F_{xf}$ : Longitudinal tire force front tires

$F_{xr}$ : Longitudinal tire force rear tires

$g$ : Gravity

$l$ : Distance between the front and rear axles

$m$ : Vehicle mass

$M_x$, $M_y$, $M_z$ : Tire Moments

$r_e$ : Effective wheel radius

$R_{xf}$ : Rolling resistance force of the front tires

$R_{xr}$ : Rolling resistance force of the rear tires

$S_v$ : Vertical shift value

$v_{rel}$ : Relative velocity

$v_{SV}$ : Subject vehicle velocity

$v_{TV}$ : Target vehicle velocity

$Vwind$ : Wind velocity

$Vx$ : Longitudinal velocity of the vehicle

$w$ : Distance between steering points of the front wheels

$x$ : Distance value between two vehicles

$\boldsymbol{\delta_i}$ : **S**teering angle of the inner front wheel

$\boldsymbol{\delta_o}$ : Steering angle of the front outer wheel

$\boldsymbol{\theta}$ : Inclination angle

$\boldsymbol{\rho}$ : Air density

$\boldsymbol{\sigma_x}$ : Longitudinal slip ratio

$\boldsymbol{\omega}$ : Angular velocity of the tire

**LIST OF TABLES**

**Page**

**LIST OF FIGURES**

**Page**

## FUNCTIONAL SAFETY ANALYSIS FOR ADVANCED EMERGENCY BRAKING SYSTEMS

## SUMMARY

Studies have been carried out on Advanced Driver Assist Systems in order to reduce the death rates and severe injuries caused by traffic accidents. In this regard, using a Camera, Radar, and Lidar sensors that are being developed, the vehicle has begun to better perceive its environment while in motion. Thanks to these developing technologies, Advanced Driver Assist Systems have recently become very common in the automotive industry. In addition, with these systems that increase vehicle safety, comfort enhancement has also taken into consideration. Blind Spot Detection, Adaptive Cruise Control, Lane Keeping Assist System, Lane Departure Warning System, Advanced Emergency Braking System are examples of Advanced Driver Assist Systems.

The Advanced Emergency Braking System detects targets such as cars, trucks, motorcyclists, pedestrians, and cyclists, often using Radar and Camera sensors together. While Radars work more efficiently in selecting vehicle-type targets, they may be insufficient in detecting Vulnerable Road Users which are pedestrians and cyclists. Therefore, Camera sensors are used as well as Radar sensors to detect Vulnerable Road Users. As in this case, when two or more sensors are used, the data collected from the sensors are passed through the sensor fusion stage, thus the reliability of the selected targets has increased.

The vast majority of traffic accidents are caused by the lack of attention of drivers. Advanced Emergency Braking System aims to prevent traffic accidents or to minimize the impact of the accident. In order for this system to work, information about the distance to the target, the relative speed to the target, and the relative acceleration with the target are required. This information is obtained and processed by sensors. The Time to Collision is calculated by the system using the data of distance and relative velocity. When the calculated Time to Collision is smaller than the threshold time required for collision warnings and autonomous braking, the necessary warnings are initiated. Under normal circumstances, audible and visual collision warnings are given to alert the driver before autonomous braking. If the driver does not react to warnings and collision with the target becomes unavoidable, autonomous braking is activated. The two separated autonomous braking, namely Speed Reduction Braking and Mitigating Braking, can be requested by the Advanced Emergency Braking System. Speed Reduction Braking is primarily applied by the system. However, if the risk still continues despite the application of Speed Reduction Braking, Mitigating Braking is applied as the last step. But in some cases, for example; in cases where the target vehicle with slow speed in the side lane suddenly passes in front of us, collision warnings and autonomous braking can be initiated at the same time as the Time to Collision will be low.

Many standards and regulations have been published for the Advanced Emergency Braking System. These regulations and standards determine how the system should react to the targets recognized by the system and define test scenarios to measure the behavior of the system. It also specifies the appropriate weather and road conditions under which the advanced emergency braking system will operate and acknowledges that the behavior of this system may differ in each road and weather conditions.

In this thesis, two different goals are aimed. The first aim of the thesis is to develop the software of the Advanced Emergency Braking System. The software of Advanced Emergency Braking System has been developed on Matlab/Simulink. The tests of the software were carried out on The Open Racing Car Simulator (TORCS), which is an open-source simulation environment and can communicate with Matlab/Simulink. In addition, the fact that TORCS can run on the Windows operating system and give realistic results has made TORCS the most suitable program to be used for the simulation environment. In the tests carried out in the TORCS simulation environment, which data is taken from the vehicle and how the vehicle is controlled is explained in this thesis. The longitudinal motion of the vehicle is controlled by the desired speed request and the braking demand requested by the Advanced Emergency Braking System. In the TORCS simulation environment, the accelerator pedal can be controlled between 0 and 1 values. Therefore, the controller is designed to keep the vehicle at the desired speed and to control the demand of speed with the accelerator pedal. Likewise, in the TORCS simulation environment, the brake pedal allows the vehicle to slow down when the brake pedal values are between 0 and 1. Deceleration is requested by the Advanced Emergency Braking System to reduce the vehicle's speed. The controller is designed to slow down the vehicle with this requested deceleration and to control it with the brake pedal. In the TORCS environment, tests determined by UN Regulation 152 have been designed and the Advanced Emergency Braking System has been tested.

The increase in the number of electronic components used on the vehicle has made vehicles complicated. Therefore, the probability of malfunctions that may occur in vehicles has increased. In recent years, the importance given to functional safety has increased, as a malfunction in a vehicle that is traveling can lead to a serious accident. Normally, the technical standard IEC / EN 61508 is responsible for the functional safety requirements of electrical, electronic, and programmable systems. However, with the increasing importance of functional safety in the automotive industry, the ISO 26262 standard was generated to meet this demand, with being based upon the IEC / EN 61508 technical standard. The ISO 26262 standard provides guidance on how to develop and test an automotive safety system.

As a second aim in this thesis, it is aimed to perform the functional safety analysis of the Advanced Emergency Braking System according to the concept phase. For this, ISO 26262 – Part 3: Concept Phase has been examined and studies have been carried out in line with the guidance of the concept phase. In this study, firstly, the item definition of the Advanced Emergency Braking System was made. The purpose of the system, its working logic, the elements with which this system interacts and the interaction of this system with the environment are determined in the item definition. In addition, the operating modes of the Advanced Emergency Braking System were determined at this stage and the activation and inactivation conditions of the system were explained. After the item definition, the Hazard Analysis and Risk Assessment (HARA) has been done for the Advanced Emergency Braking System. The purpose of this is to determine the dangerous situations that may cause malfunctions in the system.

Next, safety goals were determined so that the system could compensate for these faults, and an Automotive Safety Integrity Level (ASIL) value was assigned to each safety goal.In dangerous situations caused by malfunctions, the difficulty in controlling the vehicle by the driver, how often the scenario where the malfunction occurs, and the level of injury of the driver in case of an accident are taken into account in determining the ASIL level. ASIL values are ranked as QM, A, B, C, D according to the impact of the damage on human life, where QM is the lowest value, and D is the highest value. The determination way of the ASIL value is detaily explained in ISO 26262 – Part 3: Concept Phase. There is a rule that says it is necessary to derive at least one functional safety requirement from each safety goal. By implementing this rule, functional safety requirements are established from safety goals in the final stage. The purpose of the functional safety requirements is to bring the vehicle to a safe state before the dangerous situation that may arise from the related failure occurs when the system malfunctions. For this, it is aimed that the vehicle will be in a safe state within the Fault Tolerant Time Interval (FTTI) after a malfunction in the system.

# İLERİ ACİL FRENLEME SİSTEMLERİ İÇİN FONKSİYONEL EMNİYET ANALİZİ

## ÖZET

Trafik kazalarından kaynaklı ölüm oranlarının ve ağır yaralanmaların önüne geçebilmek için ileri sürücü destek sistemleri üzerinde uzun zamandır çalışmalar yapılmaktadır. Bu bağlamda teknolojisi geliştirilmekte olan kamera, Radar ve Lidar sensörleri sayesinde, araç hareket halinde iken çevresini daha iyi algılamaya başlamıştır. Bu gelişen sensor teknolojileri ve araçlarda yazılım geliştirmek için kullanılan elektronik komponentlerinin teknolojilerinin de gelişmesi sayesinde, son zamanlarda ileri sürücü destek sistemleri otomotiv sektöründe çok yaygın hale gelmiştir. Ayrıca araç güvenliğini arttıran bu sistemler ile birlikte konfor attırımına da odaklanılmıştır. Kör Nokta Tespiti, Uyarlamalı Hız kontrolü, Şeritte Tutma Sistemi, Şeritten Ayrılma Uyarı Sistemi, İleri Acil Frenleme Sistemi gibi sistemler ileri sürücü destek sistemlerine örneklerdir.

İleri Acil Frenleme Sistemi, genellikle Radar ve kamera sensörlerini birlikte kullanarak otomobil, kamyon, motosikletli, yaya ve bisikletli gibi hedefleri algılar. Radarlar araç tipi hedefleri seçmede daha verimli çalışırken, yaya cinsi hedefleri algılamada yetersiz kalabilmektedirler. Bu yüzden insan hedeflerini de algılamak için Radar sensörlerinin yanında kamera sensörleri de kullanılır. Bu durumda olduğu gibi iki veya daha fazla sensör kullanıldığında, sensörlerden gelen datalar sensör füzyonu aşamasından geçirilir ve bu sayede seçilen hedeflerin güvenirliliği artmış olur.

Yollarda meydana gelen trafik kazalarının büyük çoğunluğu sürücülerin dikkatsizliğinden kaynaklanmaktadır. İleri Acil Frenleme Sistemi trafik kazalarını engellemeyi veya kazanın etkisini en aza indirmeyi hedefler. Bu sistemin çalışabilmesi için hedefe olan uzaklık, hedef ile olan bağıl hız ve hedef ile olan bağıl ivme bilgileri gereklidir. Bu bilgiler sensörler ile elde edilir ve işlenir. Sistem tarafından uzaklık ve bağıl hız verileri kullanılarak çarpışmaya kalan süre hesaplanır. Hesaplanan bu çarpışmaya kalan süre, çarpışma uyarıları ve otonom frenlemeler için gerekli olan çarpışmaya kalan eşik değer sürelerinden küçük olduğunda gerekli uyarılar başlatılır. Normal şartlarda, otonom frenlemeden önce sürücüyü uyarmak için sesli ve görsel çarpışma uyarıları verilir. Sürücü uyarılara tepki vermez ve hedef ile oluşacak olan çarpışma kaçınılmaz olursa otonom frenlemeler devreye girer. İleri Acil Frenleme Sistemi, hız azaltma frenlemesi ve hafifletme frenlemesi olmak üzeri iki ayrı otonom frenleme talep edebilir. Sistem tarafından öncelikle hız azaltma frenlemesi uygulanır. Ancak hız azaltma frenlemsi uygulanmasına rağmen risk hala devam ediyorsa, en son aşama olarak hafifletme frenlemesi uygulanır. Fakat bazı durumlarda, örneğin; yan şeritteki hızı yavaş olan hedef aracın aniden önümüze geçtiği durumlarda, çarpışmaya kalan süre düşük olacağından çarpışma uyarıları ve otonom frenleme aynı anda başlatılabilir.

İleri Acil Frenleme Sistemi için bir çok standart ve regülasyon yayınlanmıştır. Bu regülasyonlar ve standartlar, sistem tarafından tanınan hedeflere nasıl tepki vermesi

gerektiğini belirlemekte ve sistemin davranışını ölçmek için test senaryolarını tanımlamaktadır. Ayrıca, İleri Acil Frenleme Sistemi'nin çalışacağı uygun hava ve yol şartlarını belirtmekte ve her yol ve hava şartlarında bu sistemin davranışının farklılık gösterebileceğini kabul etmektedir.

Bu tezde, iki ayrı amaç hedeflenmiştir. Tezin ilk amacı İleri Acil Frenleme Sistemi'nin yazılımını geliştirmektir. Matlab/Simulink benzetim ortamında İleri Acil Frenleme Sistemi geliştirilmiştir. Yazılımın testleri ise, açık kaynaklı bir benzetim ortamı olan ve Matlab/Simulink ile haberleşebilen, The Open Racing Car Simulator (TORCS) benzetim ortamında gerçekleştirilmiştir. Ayrıca, TORCS'un Windows işletim sisteminde çalışabilmesi ve gerçekçi sonuçlar verebilmesi TORCS'u benzetim ortamı için kullanılacak en uygun program haline getirmiştir. TORCS ortamında yapılan testlerde, araçtan hangi verilerin alındığı ve aracın nasıl control edildiği bu tezde anlatılmıştır. Aracın boylamsal kontrolü, talep edilen hız isteği ve İleri Acil Fren Sistemi'nin talep ettiği fren isteği ile kontrol edilir. TORCS benzetim ortamında gaz pedalı 0 ile 1 değeleri aralığında kontrol edilebilmektedir. Bu yüzden aracı istenilen hızda tutmak ve hız talebini gaz pedali ile kontrol edebilmek için konrollör tasarlanmıştır. Aynı şekilde, TORCS benzetim ortamında, 0 ile 1 değerleri arasında olan fren pedalı değerleri ile aracın yavaşlaması sağlanır. Aracın hızını azaltmak için İleri Acil Frenleme Sistemi tarafından yavaşlatma ivmesi talep edilmektedir. Aracı bu talep edilen yavaşlatma ivmesi ile yavaşlatmak ve fren pedalı ile kontrol edebilmek için kontrollör tasarlanmıştır. TORCS benzetim ortamında UN Regulation 152' nin belirlediği testler tasarlanmıştır ve İleri Acil Frenleme Sistemi test edilmiştir.

Araç üzerinde kullanılan elektronik komponentlerin sayısının artması araçları karmaşık hale getirmiştir. Dolayısıyla, araçlarda oluşabilecek arızaların olasılığı artmıştır. Seyir halinde giden bir araçta meydana gelen bir arıza ciddi bir kazaya yol açabileceği için son yıllarda fonksiyonel emniyete verilen önem artmıştır. Normalde, IEC / EN 61508 teknik standardı, elektrik, elektronik ve programlanabilir sistemlerin fonksiyonel emniyet gereksinimlerinden sorumludur. Ancak, otomotiv endüstrisinde fonksiyonel emineyetin önem kazanmasıyla IEC / EN 61508 teknik standardı baz alınarak, bu talebin karşılanabilmesi için ISO 26262 standardı oluşturulmuştur. ISO 26262 standardı, otomotiv için emniyetli bir sistemin nasıl geliştirileceği ve nasıl test edileceğini konusunde rehperlik etmektedir.

Bu tezde ikinci amaç olarak, İleri Acil Frenleme Sistemi fonksiyonel emniyet analizlerinin konsept aşamasına göre yerine getirlimesi hedeflenmiştir. Bunun için, ISO 26262 – Part 3: Concept Phase incelenmiş ve konsept aşamasının rehberliği doğrultusunda çalışmalar yapılmıştır. Bu çalışmada ilk olarak İleri Acil Frenleme Sistemi'nin öğe tanımı yapılmıştır. Sistemin amacı, çalışma mantığı, bu sistemin etkileşimde olduğu öğeler ve bu sistemin çevreyle etkileşimi öğe tanımında belirlenmiştir. Ayrıca, İleri Acil Frenleme Sistemi'nin çalışma modları bu aşamada belirlenmiş ve sistemin aktivasyon, inaktivasyon koşulları anlatılmıştır. Öğe tanımından sonra, tehlike analizi ve risk değerlendirmesi (HARA) İleri Acil Frenleme Sistemi için yapılmıştır. Bunun amacı, sistemde oluşabilecek arızaların sebep olabileceği tehlikeli durumları belirlemektir. Daha sonra, sistemin bu hataları telafi edebilmesi için emniyet amaçları belirlenmiştir ve her emniyet amacına Otomotiv Emniyet Bütünlük Seviyesi (ASIL) değeri atanmıştır. Arızalardan kaynaklanan tehlikeli durumlarda, sürününün aracı ne zorlukla kontrol edebileceği, arızanın olduğu senaryonun ne sıklıkla gerçekleştiği ve eğer kaza olması durumunda sürücünün yaralanma seviyesi ASIL seviyesinin belirlenmesinde dikkate alınmaktadır. ASIL değerleri, oluşacak hasarın insan hayatına etkisine göre QM, A, B, C, D olarak sıralanır

ve QM en düşük değer iken D en yüksek değerdir. ASIL değerinin nasıl belirlendiği ISO 26262 – Part 3: Concept Phase incelemesinde detaylı olarak anlatılmıştır. Kural olarak her emniyet amacından en az bir tane fonksiyonel emniyet gereksinimi türetmek gerektiğinden, son aşamada emniyet amaçlarından fonksiyonel emniyet gereksinimleri oluşturulmuştur. Fonksiyonel emniyet gereksinimlerinin amacı, sistemde arıza olduğunda ilgili arızadan kaynaklanabilecek tehlikeli durum oluşmadan önce aracı güvenli duruma getirmektir. Bunun için sistemde arıza olduktan sonra Hataya Toleranslı Zaman Aralığı (FTTI) içerisinde aracın güvenli duruma geçmesi amaçlanır.

# 1. INTRODUCTION

Approximately 1.2 million people die each year due to traffic accidents. Many car manufacturers are dedicated to decreasing the number of dies and fatal injuries from traffic accidents. For that purpose, a lot of active and passive safety systems have already developed by car manufacturers. Passive safety systems do not prevent accidents, but collision affects are decreased during accident by passive systems. Systems such as airbags and seat belts are examples of passive safety systems. On the other hand, main purpose of active safety systems is preventing accidents or decreasing the collision energy when accident occurred.

Anti-Lock Braking System (ABS), Electronic Stability Control (ESC), Traction Control System (TCS), Roll Stability Control (RSC), Advanced Emergency Braking System (AEBS) are most common active safety systems in automotive industry. The ABS prevents the wheels from locking while the vehicle is braking. This allows the driver to gain more control over the vehicle. The Electronic Stability Control (ESC) improves the vehicle's stability by detecting and reducing the vehicle's side slip. When vehicle control is lost, individual wheels are braked to prevent the vehicle from skidding. The purpose of TCS is to enable traction and increase stability. That is done by reducing the torque of the engine and by applying brakes when the wheels start to spin. During high maneuvers or evasive steering maneuvers, the probability of rolling of the vehicle increases. RSC system applies individual brakes as soon as roll angle becomes critical in order to reduce rolling risk.

According to data supplied by European Union, more than 9,500 people died in 2016 and 38% of the accidents were taken place on the roads. Also, the proportions of fatalities of drivers and pedestrians were 50% and 40% respectively. In order to avoid these accidents United Nations Regulation for Advanced Emergency Braking Systems (AEBS) for vehicles was approved by 40 countries [1].

The most importantly it is predicted that AEBS can prevent 1000 European people from dying due to car accidents every year. Moreover, according to a study conducted

by Euro NCAP and Australasian NCAP, the ratio of the rear-end collisions at low speeds is diminished by 38%.

The European Union and Japan have declared there will be an obligation for car manufacturers after 2022 in the EU. With this regard, all new produced cars and light commercial vehicles will have to equipped with AEBS compulsorily. Therefore, the number of cars produced with this new technology in EU and Japan each year will be more than 15 million and 4 million respectively [1].

The National Highway Traffic Safety Administration (NHTSA) and the Insurance Institute for Highway Safety (IIHS) announced that ten car manufacturers produced more than 50% vehicles equipped with the crash avoidance technology between 2017 and 2018. This technology includes AEBS [2].

Among these 10 vehicle manufacturers, there are companies that produce a lot of vehicles such as Nissan, Toyota, and Honda. Tesla, Volvo, and Mercedes - Benz companies stated that more than 93 percent of their vehicles have AEBS. Additionally, Tesla has announced that all of the cars have been producing with AEBS. According to the list which demonstrates the number of vehicles produced with AEBS, Nissan is in the second-ranking and followed by Honda. Nissan stated that 1.1 million manufactured vehicles equipped with AEBS which corresponds to 78% of total manufactured vehicles. Similarly, Honda stated that 980,000 of its 1.6 million vehicles in total are equipped with AEBS (61%).

The rates of vehicles with AEBS reported by 20 vehicle manufacturers for their passenger cars and trucks weighing less than 3855 kg are shown in Table 1.1.

Many organizations have defined standard, regulation and testing protocols for AEBS. Commonly used documents for AEBS are listed below:

- ISO 22839:2013 - Forward Vehicle Collision Mitigation Systems – Operation, performance, and verification requirements [3].
- ISO 15623:2013 - Forward Vehicle Collision Warning Systems – Performance requirements and test procedures [4].
- ISO 19237:2017 - Intelligent transport systems — Pedestrian detection and collision mitigation systems (PDCMS) — Performance requirements and test procedures [5].

**Table 1.1 :** Passenger vehicles with AEBS [2].

| | PERCENTAGE OF VEHICLES PRODUCED WITH AEBS FROM SEPT. 1, 2017, TO AUG. 31, 2018 | PERCENTAGE OF 2019 MODEL VEHICLES WITH AEBS |
|---|---|---|
| **Tesla** | 100 | 100 |
| **Mercedes-Benz** | 96 | 89 |
| **Volvo** | 93 | 100 |
| **Toyota/Lexus** | 90 | 90 |
| **Audi** | 87 | 87 |
| **Nissan/Infiniti** | 78 | 54 |
| **Volkswagen** | 69 | 50 |
| **Honda/Acura** | 61 | 59 |
| **Mazda** | 61 | 67 |
| **Subaru** | 57 | 50 |
| **BMW** | 49 | 82 |
| **Maserati/Alfa Romeo** | 27 | 0 |
| **General Motors** | 24 | 0 |
| **Hyundai/Genesis** | 18 | 62 |
| **Kia** | 13 | 27 |
| **Fiat Chrysler** | 10 | 0 |
| **Porsche** | 8 | 17 |
| **Ford/Lincoln** | 6 | 36 |
| **Mitsubishi** | 6 | 0 |
| **Jaguar Land Rover** | 0 | 62 |

- ISO 19377:2017- Heavy commercial vehicles and buses - Emergency braking on a defined path - Test method for trajectory measurement [6].
- ISO 22078:2020 Intelligent transport systems - Bicyclist detection and collision mitigation systems (BDCMS) - Performance requirements and test procedures [7].
- UNECE Regulation No 131:2013 - Uniform provisions concerning the approval of motor vehicles with regard to the Advanced Emergency Braking Systems (AEBS) [8].
- UNECE Regulation No 152:2020 - Uniform provisions concerning the approval of motor vehicles with regard to the Advanced Emergency Braking System (AEBS) for M1 and N1 vehicles [9].

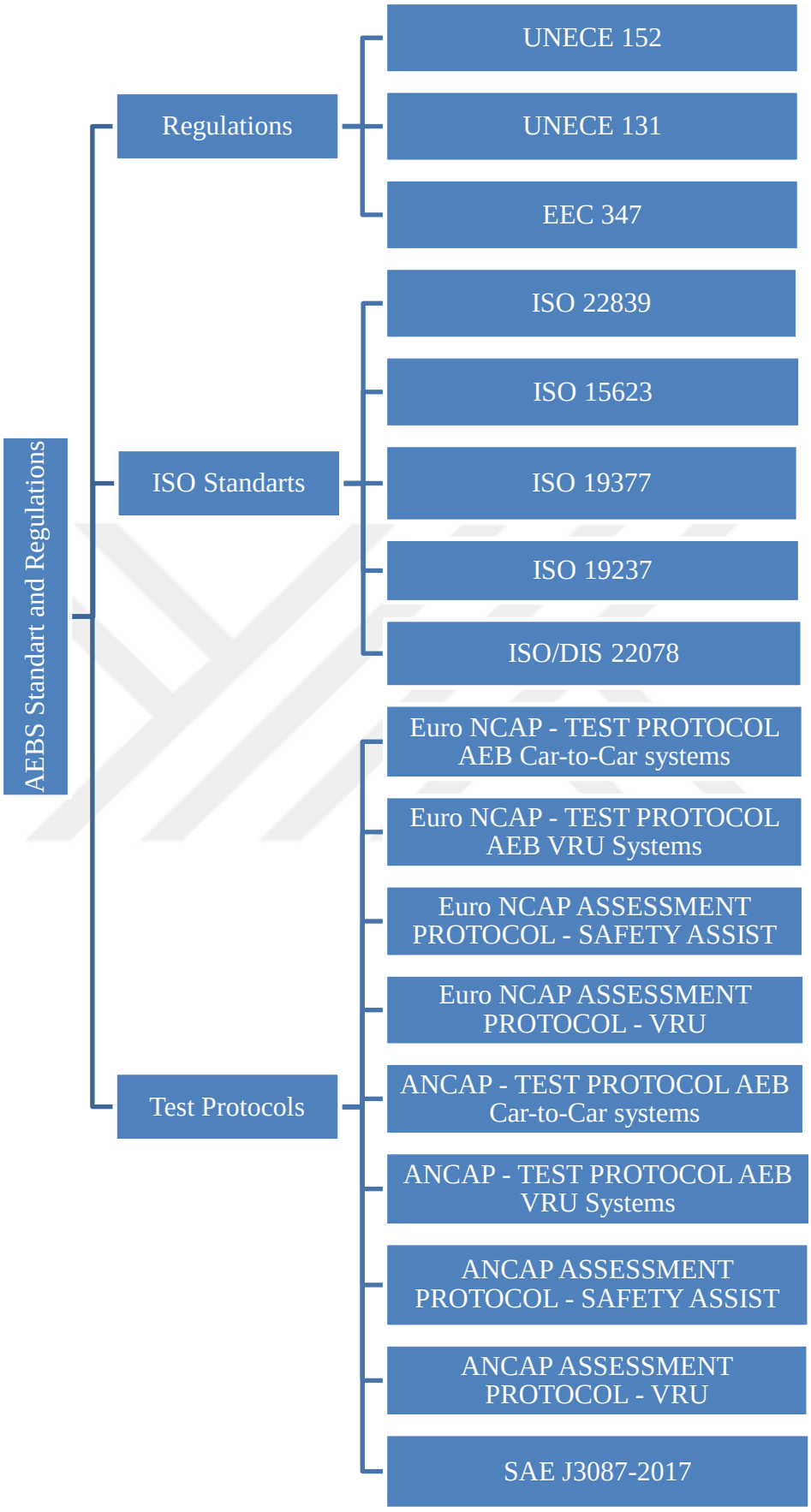


**Figure 1.1 :** AEBS Regulations and Standarts.

- European Parliament Regulation No 347:2012 - Type-approval requirements for certain categories of motor vehicles with regard to advanced emergency braking systems [10].
- Euro NCAP TEST PROTOCOL - AEB Car-to-Car systems -Version 3.0.2 [11].
- Euro NCAP TEST PROTOCOL - AEB VRU systems - Version 3.0.3 [12].
- Euro NCAP ASSESSMENT PROTOCOL - SAFETY ASSIST - Version 9.0.3 [13].
- Euro NCAP ASSESSMENT PROTOCOL - VULNERABLE ROAD USER PROTECTION - Version 10.0.3 [14].
- AUSTRALASIAN NCAP TEST PROTOCOL - AEB Car-to-Car systems - Version 3.0.2 [15].
- AUSTRALASIAN NCAP TEST PROTOCOL -AEB VRU systems - Version 3.0.3 [16].
- AUSTRALASIAN NCAP ASSESSMENT PROTOCOL - SAFETY ASSIST - Version 9.0.3 [17].
- AUSTRALASIAN NCAP ASSESSMENT PROTOCOL - VULNERABLE ROAD USER (VRU) PROTECTION - Version 10.0.3 [18].
- SAE J3087-2017: Automatic Emergency Braking (AEB) System Performance Testing [19].

These standards have been added for both heavy vehicles and passenger cars. Figure 1.1 shows the AEBS related standarts and regulations. However, in this thesis, documents related to heavy vehicles are not taken into consideration.

## 1.1 SAE International Levels

SAE International (Society of Automotive Engineers) publishes standards, especially for the automotive field. SAE J3016 is one of those standards and it defines the autonomous driving levels for motor vehicles. There are 6 autonomous driving levels according to SAE. These levels are listed below:

- Level 0 (No Driving Automation): Currently, most of the vehicles which are available on the road have level 0 autonomous level. Those vehicles are always controlled by the driver.
- Level 1 (Driver Assistance): An advanced driver assistance system (ADAS) is available on the vehicle and it helps to driver. Steering or braking/accelerating can be controlled by the ADAS, but they shall not work at the same time.
- Level 2 (Partial Driving Automation): For some situations, steering and braking/accelerating may be controlled at the same time by the advanced driver assistance system (ADAS) if it is necessary. But the driver shall keep always its attention and the drive is needed to perform dynamic driving task.
- Level 3 (Conditional Driving Automation): For some situations, all driving task aspects can be performed by an automated driving system (ADS). For those situations, the driver should be ready to control the vehicle if the ADS is not capable to control the vehicle.
- Level 4 (High Driving Automation): For some driving modes, an automated driving system (ADS) can issue all driving tasks and monitor its surrounding.
- Level 5 (Full Driving Automation): Driving can be done by an automated driving system (ADS) for all driving conditions. The driver is not necessary for driving.

Figure 1.2 demonstrates the driver's control over the vehicle according to SAE levels. At level 0, it is seen that the driver is fully responsible for vehicle control, and towards level 5 the driver's control obligation is reduced. At level 5, it is seen that the driver is completely removed and it is a fully autonomous vehicle.

Thanks to autonomous vehicles, safety has increased considerably in new vehicles. 94% of serious accidents occurring are caused by human errors [20]. With the development of autonomous driving systems, human errors will decrease, and the possibility of accidents will decrease. Thus, it will protect not only drivers and passengers, but also other drivers, cyclists, and pedestrians.

As seen in Figure 1.3, the AEBS function is in the SAE level 0 function category. In this case, the responsibility lies entirely with the driver. While performing Hazard

Analysis and Risk Assessment (HARA) analysis, since AEBS is SAE level 0 function, in many cases the responsibility is left to the driver.

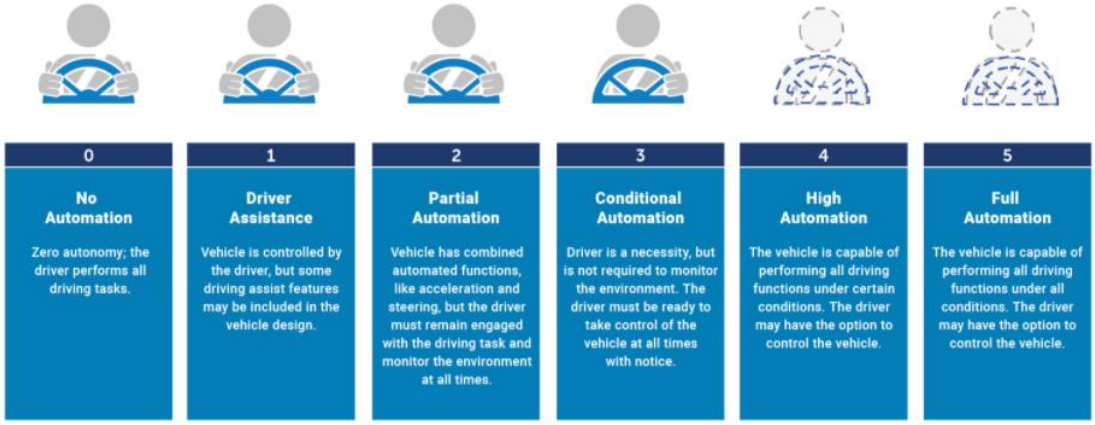


**Figure 1.2 :** SAE Autonomous Levels [20].

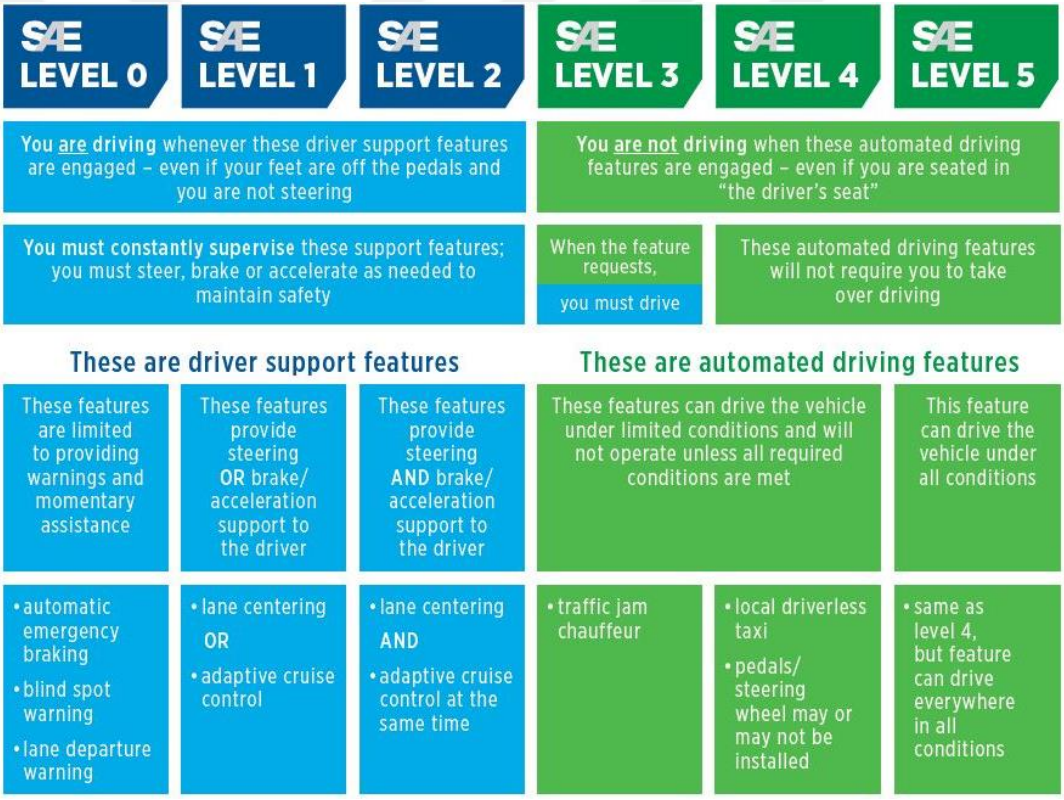


**Figure 1.3 :** Driving tasks of features based on SAE Automation Levels [23].

## 1.2 Literature Review

Toyota introduced its first emergency braking system on the Harrier model in 2003. Toyota called this system pre-collision system (PCS) which was working with Radar. As soon as an unavoidable collision detected for an object, the seat belts were tightened and mitigation braking was activated by the system [21]. Today, PCS is available

under Toyota Safety Sense 2.0. PCS uses both Radar and front-facing Camera and is able to detect pedestrians, cyclists, and vehicle targets. When a high collision possibility is detected, the system firstly gives collision warning and increases the brake pressure. If the collision probability becomes critical then the system initiates mitigation braking in order to prevent accident or reduce the collision energy.

Features in addition to the Pre-Crash Safety (PCS) system have been launched in the LS 460 model of Lexus of 2007. This is an obstacle detection system that works in different conditions from daylight to darkness and detects not only pedestrians but also animals in addition to vehicles. The near-infrared radiation is monitored by the Camera. The working way of this Camera sensor is like this; special units embedded into headlamp high-beam projectors of the car emit this light and objects reflect the light in advance to 25 m. So, the targets are obtained by the sensor. The probability of colliding with an obstacle in front of it is evaluated by the PCS system according to the position, speed, and trajectory of the vehicle. If there is a high probability of collision with the target, a warning sound and a red brake visual warning would be displayed on the screen. Also, when the collision is unavoidable, thn the seat belt is tightened before the collision [28].

Collision Mitigation Brake System (CMBS), originally Collision Mitigation System (CMS) was introduced by Honda on the model of Inspire in 2003. That system was the first production of autonomous braking system [22]. Millimeter-wave Radar was used to detect the objects and the detection range was 100 m. This system was helping the driver to reduce collision damage for the vehicle and passengers if the force applied on the brake by the driver were not enough. The CMBS, which is part of Honda Sensing technology currently used by Honda, detects both pedestrians and vehicles using both Radar and Camera sensors and is able to avoid accidents or mitigates collision for both target types. However, the system works when the relative speed with the target object is higher than 5 km/h.

The equipment of the 2006 model Mercedes-Benz S-Class includes Brake Assist PLUS (BAS PLUS) and PRE-SAFE Brake systems. In these systems, a single 77 GHz Radar sensor is used. This sensor which degree of view field is nine, in the vehicle is able to monitor the three-lane road with a distance that can reach up to 150 m. Also, there are two extra 24 GHz Radar sensors that can have a view area with an 80° field, and monitor a 30 m distance from the vehicle. Also, if it is required, the system

automatically brakes the vehicle and maintains the distance to the vehicle in front, finally it speeds up the vehicle when the traffic situation permits [24].

As stated in [24], Brake Assist PLUS (BAS PLUS) has a system that has the ability to anticipate and by monitoring the distance between the vehicle and the forward vehicle. If the distance is very small the driver is warned audibly and visually that are supplied by the system. Moreover, the required deceleration is calculated for collision avoidance. When the driver pushes the brake, the recommended deceleration will be applied automatically. According to [24], PRE-SAFE Brake is developed as supplementation to BAS PLUS. Although the signal is supplied by BAS PLUS, if the driver does not react to this, and an acute accident danger exists, the vehicle speed is reduced by 4 $\mathrm{m/s^2}$ deceleration by the PRE-SAFE Brake system. This deceleration demand is called partial braking. The order of countermeasures for rear-end collision scenario is illustrated in Figure 1.4 and explained following:

- The driver is warned with sound by S-Class assistance systems before the moment of collision. The time difference between the warning and collision is approximately 2.6 seconds which the system calculates. Also, a red symbol is provided in order to give signs and so warn the driver about the risk of the collision.
- Despite these warnings, if the reaction is not provided by the driver the autonomous partial braking is applied by the PRE-SAFE Brake System. The time difference between the application of the autonomous partial braking and collision is 1.6 seconds.
- The driver has the last chance before the collision. The reaction should be provided approximately 0.6 seconds before the collision. The driver can swerve rapidly or apply full braking in order to prevent the accident.

When the speed range of the vehicle is between 10 and 180 $\mathrm{km/h}$, the system is active. Also, while the vehicle is closing to a stationary queue of traffic the system gives reaction if the vehicle velocity does not reach and exceed the limit 70 $\mathrm{km/h}$.

Ford Motor Company's Research and Advanced Engineering group and the Volvo Safety Centre have developed the Collision Mitigation by Braking (CMbB) [26]. The Radar and Camera sensors are used for the detection of the forward vehicle and determine collision probability based on the other vehicle's position, speed, and

direction. The Radar sensor is working up to 150 meters and the camera sensor up to 55 meters that are used in this system. The CMbB system uses predictions of both threats of the collision and the intention of the driver. Driver warning is provided by the system and when the driver pushes the brake the system improves the braking. Also, when it is not possible to avoid the accident the full braking is applied by the system automatically [27].

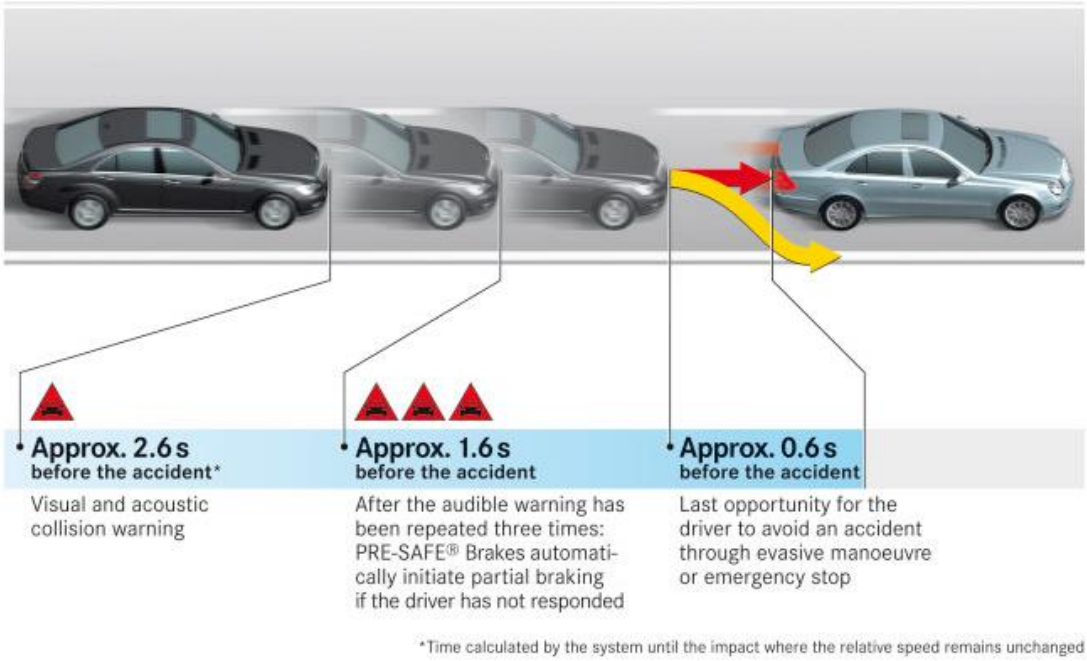


**Figure 1.4 :** Warning Times of PRE-SAFE System [25].

Currently, newly produced vehicles consist of Forward Collision Warning and Collision Mitigating Braking System. These systems are the only function for collisions both rear-end collision between vehicles and forward collision between the subject vehicle and objects that do not move. There are a lot of research papers that refer to other types of collisions and describe the systems' development. In 2002, impact configurations are aimed to functionalize the systems. Also, the results of computer simulations and decision-making algorithms are described for them by [29]. They presented a method of calculating the collision risk and initiated mitigation braking when the risk became one. They carried out this study based on many accident statistics and also tested it in a simulation environment [29].

The ALASCA laser scanner's possible automotive applications are discussed with attributing the warning and emergency brake systems by Nitsche and Schulz in [30]. It is claimed that the device which is combined with suitable analysis algorithms can

detect and classify trucks, cars, bicycles/motorcycles, and pedestrians separately. Sensor system to be used in ADAS systems such as Automatic Emergency Braking, Stop and Go, Front Collision, Park Assist, Pedestrian Detection and Turn Assist was introduced [30].

A proof-of-concept sensor system was developed. This system can be used for vehicle braking potentially, the implementation of active secondary safety features, and the detection of pedestrians in front of the vehicle in [31]. Also, it was claimed that this system can provide significant benefits in accidents related to pedestrians. In the developed prototype system, a passive infra-red sensor is used in addition to a high-resolution Radar that is a 24 GHz short-range sensor. These systems are used to accurately describe distance and relative speed. In addition, the VRUs detected by the Radar and infrared sensor are fused, that allowing targets to be detected as VRUs as well as tracked.

# 2. AUTOMATIVE FUNCTIONAL SAFETY

## 2.1 Literature Review

Along with developing technologies, electrical and electronic (E/E) devices are of vital importance in road vehicles. Electrical and electronic (E/E) devices are responsible for decision-making in all new vehicles. In the 1990s, with the development of systems such as electronic fuel injection, electric power steering system and anti-lock braking system, the use of electrical and electronic (E/E) devices began. In 2011, ISO 26262 standard was created based on IEC 61508 for E/E systems of road vehicles. In the version released in 2011, only light passenger vehicles not exceeding 3.5 tons were covered, but the version released in 2018 covers all road vehicles except mopeds and special vehicles produced for disabled people.

ISO 26262 standard takes into account the incorrect behaviours that will occur in the operation of E/E systems in terms of safety. ISO 26262 standard aims to control the dangerous situations that may occur in the vehicle in the event of a malfunction in the E/E system. However, this standard does not consider dangerous situations that do not directly affect the E/E system. For example, errors caused by electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, energy release and similar hazards are not covered by this standard. In the design of E/E systems, the ISO-26262 standard does not take into consideration the nominal operating states of these systems. For example, the strength of the brakes or the deployment speed of the airbag is not specified by ISO-26262. Instead, it advises the development of E/E systems to avoid any dangerous situation [33]. The development phases and contents of safety standards are displayed in Figure 2.1.

With the widespread use of autonomous vehicles and ADAS systems, functional safety has become very important for cars and people to avoid dangerous situations. ISO 26262 defines the Automotive Safety Integration Level (ASIL). While making ASIL classification, the probability and severity of the situation that is dangerous for human life are taken as basis. The ASIL grading is QM, A, B, C, D from the lowest to the

highest respectively. Functional safety requirements for the development of software systems in autonomous vehicles have been examined in 4 different aspects in [32]. In order to prevent malfunctions in vehicles and do not affect the operation of systems, the usage of redundancy was discussed in the first aspect. It is expected that the system backed up with the use of multiple sensors and various data processing will obtain safe results in terms of functional safety. In the second aspect, based on redundancy requirements, a hardware and software architecture that can help to meet these requirements is suggested. It is aimed to prevent systematic errors. The third aspect aims to allow secure and unsafe subsystems to be used together and to work according to their characteristics. To do these operations, mechanisms such as Memory Management Unit (MMU) and Firewalls investigate the use of freedom from interference (FFI). In the last aspect, it deals with detecting and correcting random errors in software and hardware.

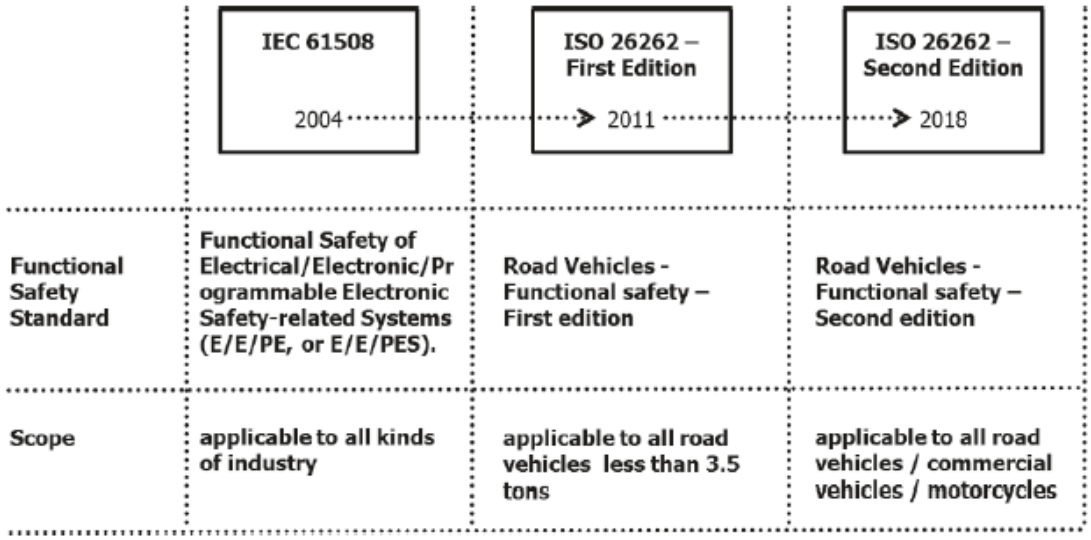


**Figure 2.1 :** History of the safety standard [34].

Giuseppe Allegra focused on the development of the Forward Vehicle Collision Mitigation Braking System (FVCMS) function and functional safety analysis of that function according to ISO 26262 Concept Phase, in his master's thesis. The Hazard Analysis and Risk Assessment (HARA) was carried out by considering the faults that may occur in the speed or distance measurements of the sensors. The developed software has been tested with fault injection method in order to detect the measurement failures of sensors. Another purpose here is to prevent the failure of the system by tolerating the faults that occur. As a solution, duplication of sensors has been proposed.

According to this suggestion, the faulty sensor will be disabled and the backup sensor will be activated [35].

## 2.2 ISO 26262 Part 3: Concept Phase

### 2.2.1 Item definition

#### 2.2.1.1 Objectives

There are 2 objectives for this clause. First one is determination of item's functionality, the interaction between the driver, environment and other items in the vehicle, and what it depends on in order to identify and describe the item.

Second one is making the item understandable sufficiently. In order to reach this the processes in subsequent phases can be carried out.

#### 2.2.1.2 General

In this clause to define the item's requirements and recommendations are specified. In this regard, functionality, interfaces, environmental conditions, legal requirements and hazard are determined.

#### 2.2.1.3 Requirements and recommendations

The item requirements are supplied by in these circumstances;

a) Standards approved internationally and nationally, legal requirements,

b) The functional behavior which involves states and operating modes at the vehicle level,

c) If it is possible to apply, the required quality, performance and availability of the functionality,

d) Restrictions related to the item about dependencies of functional, between other items and environmental conditions,

e) Possible outcomes of behavioral shortfalls that might be known failure modes and hazards,

f) The properties of actuators and its estimated capabilities such as torque output, force exerted, brightness and speed of operation. In order to evaluate the

magnitude of the effect that is considered to make decision of severity and controllability and emerge analyzing of hazards and risk assessment.

The item's boundary, interfaces, and the presumptions of interactions between the item and other items and elements are defined;

a) Item's elements,

b) The assumptions related to the effects of the behavior of the item on the vehicle,

c) Under consideration, other items and elements require some item' functionality,

d) Under consideration, the item requires the functionality of other items and elements,

e) There are functions among elements and relevant systems, and distributing and allocating of them,

f) Some operational situations affect the item's functionality.

### 2.2.2 Hazard analysis and risk assessment

#### 2.2.2.1 Objectives

There are two main aims of this clause. First one is identification and classification of the hazardous events. The malfunctioning behavior of the items brings about these events. The second one is formulization of the safety goals with regard to their ASILs. These assist the inhibiting and alleviation of hazardous events and preventing risks that are unreasonable.

#### 2.2.2.2 General

In order to identify item's safety goals hazard analysis, risk assessment and ASIL are determined. The ASIL is identified in terms of severity, exposure probability and controllability. For this process functional behavior of the items should be taken into consideration, so knowing the design of the item in detail is not required.

#### 2.2.2.3 Inputs to this clause

Item definition is needed for this clause.

#### 2.2.2.4 Requirements and recommendations

**Initiation of the hazard analysis and risk assessment**

- While identifying Hazard Analysis and Risk Assessment, item definition shall be taken into consideration as a basis.
- The assessment of the item which does not include internal safety mechanisms shall be carried out during analyzing the hazard and risk assessment, i.e., while analyzing the hazards and evaluation of the risk assessment safety mechanisms proposed to be implemented or that have already been implemented in the predecessor items shall not be taken into account.

**Situation analysis and hazard identification**

- The malfunctioning behavior of the item will cause a hazardous event. In this regard the operational situations and operation's modes will be determined in this clause. Those are held for both using the tool correctly and predictably misused. The conditions are determined in terms of behaving safety manner for operational situations.
- The item's probable malfunctioning behavior should be used as a base in order to describe hazards in a systematical way. It is important to state that the additional risks that can be caused by transportation of good are not included.
- Hazard that is resulted from item's malfunctioning behavior shall be determined at the vehicle level.
- If the hazards that have not been identified within the scope of ISO 26262 (see Clause 1) have existed, the organization-specific procedures shall be taken into consideration to address these hazards.
- Hazardous events that is relevant should be identified.
- This clause includes the identification of the outcomes of hazardous events. For example, the driver assistance functions cannot be available simultaneously as a result of function loss of a braking system (ESC).
- The detail level should be chosen from the list of operational situations and this level shall not cause inappropriate reduction in the ASIL.

**Classification of hazardous events**

- Hazardous situations shall be classified if they are scope of ISO 26262. It might be difficult to classify given hazards in terms of severity (S), exposure probability (E) or controllability (C). In order to make it easy the conservative classification can be preferred. For example, a higher S, E, C classification is selected if the doubt is reasonable.
- In order to characterize the severity, the description of the Abbreviated Injury Scale (AIS) can be used. There are 4 severity classes: S0, S1, S2 and S3. The severity of hazardous events shall be defined according to these classes given in the Table 2.1. Also, the AIS levels are indicated in the Appendix A besides different severity and accident types. The combination of injuries can be used as a base in classification of the severity. Therefore, instead of looking at a single injury, the higher severity classification is required.

**Table 2.1 :** Severity classes [33].

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

- In some operational situations that causing harm like an accident, the subsequent malfunctioning behavior of the item may increase the harm resulted or fail to reduce. When operational situations lead to harm, the severity classification can be restricted to the difference from the severity resulted between the initial operational situation such as an accident and the item's malfunctioning behavior.
- When the severity class S0 is assigned for a hazardous event, it is not needed of the determination of ASIL.
- In order to make an estimation of the exposure probability in terms of each operational situation, the rationale which is defined for each hazardous event shall be used as a base. The exposure probability shall be assigned according to Table 2.2.
- While making an estimation of the exposure probability, the number of vehicles which are equipped with the item shall not be taken into consideration.

- When the exposure class E0 is assigned for a hazardous event, it is not needed to the determination of ASIL.

**Table 2.2 :** Exposure probability classes [33].

| | E0 | E1 | E2 | E3 |
|---|---|---|---|---|
| Description | Incredible | Very low probability | Medium probability | High probability |

- The rationale is defined for each hazardous event. According to this defined rationale, the driver or other people who are involved in the operational situation should control each hazardous event. There are 4 controllability classes: C0, C1, C2 and C3. The controllability of hazardous events shall be defined according to these classes given in the Table 2.3.

**Table 2.3 :** Classes of controllability [33].

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

- In some cases, like driver assistance systems, the vehicle operates safely without being affected by hazards or drivers can prevent the accident by their routine actions. In these situations, the C0 class can be used for hazards associated with the unavailability of the item. When the controllability class C0 is assigned for a hazardous event, it is not needed to the determination of ASIL.
- In Table 2.4, the ASIL determination is given. This includes three different classes: severity, probability of exposure and controllability. Also, these classes should be used as a base when identifying an ASIL for each specific hazardous event.
- If the exposure probability is lower than E1 as a result of combining unlikely situations, QM might be discussed for S3, C3 depend on this combination.

**Determination of safety goals**

- The ASIL is assessed with regard to Hazard Analysis and Risk Assessment. Based on this evaluated ASIL, a safety goal shall be identified for each hazardous event. If determined safety goals are similar to each other, they can be combined under a single safety goal.

**Table 2.4 :** ASIL determination [33].

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

- The identified ASIL for each hazardous event should be assigned to related safety goal. When similar safety goals are combined under a single safety goal, the combined safety goal should be selected as an assignment and the highest ASIL should be allocated to this.
- The safety goals shall be determined in terms of their ASIL, ISO26262-8:2018, Clause 6.
- While analyzing hazards and evaluating risk assessment corresponding to ASIL identification, the assumptions shall be determined. Also, if it possible it should be included those hazardous events classified as QM or assigned without ASIL. The assumptions shall be confirmed in terms of ISO26262-4:2018 and Clause 8.

### 2.2.3 Functional safety concept

#### 2.2.3.1 Objectives

There are five main objectives for this clause;

- Identification of item's functional or degraded functional behavior according to its safety goals,
- According to safety goals, indication of the constrains in order to detect and control suitable faults in time,
- Determination of strategies at item level or measures. This should be done in order to get the required fault tolerance or to alleviate the effects regarding faults sufficiently by the item itself, the driver or external measures,
- Allocation of the functional safety requirements to architectural design of the system, or external measures,
- Verification of concept of the functional safety and indication of validation criteria of the safety.

#### 2.2.3.2 Prerequisites

This clause shall include three main properties. Those are;

- Description of item,
- HARA report,
- The architectural design of the system by using an external source.

#### 2.2.3.3 Derivation of functional safety requirements

- Determination of functional safety requirements shall be based on the safety goals related to the architectural design of the system.
- At least one derivation of functional safety requirement shall be done based on each safety goal.
- If it is implemented, the identification of strategies according to the functional safety requirements for these nine properties;
    a) Avoidance of fault,
    b) Detection and control of fault or faults or resulted malfunctioning behavior,
    c) Transition from present state to safety state, and if it is possible, it should be from safety state,

d) Tolerance of fault,

e) Functionality deterioration in the existence of a fault, and interaction of it with f) and g),

f) In order to cut down the exposure time to risk to reasonable duration determine required driver warnings,

g) An order to raise the controllability by the driver determine required driver warnings for example, ABS fault lamp and engine malfunction indicator lamp,

h) At the vehicle level, how requirements of timing are met,

i) Multiple control requests can be generated simultaneously by different functions. The inappropriate arbitration of those requests can be resulted in a hazardous event. It is required to avoid or decrease them.

- If it is implemented, each requirement of functional safety shall be identified in terms of followings;

  a) Modes of operating,

  b) Time interval of fault toleration,

  c) Safe states,

  d) Time interval of emergency operation,

  e) Functional redundancies such as tolerance of fault.

- If it is possible to avoid from a violation of safety goal by transitioning to, or pursuing, the specification of related safety state(s) should be done.

- If it is not possible to obtain a safe state by transition in the time interval that is acceptable, the specification of an emergency operation shall be done.

- The assumptions regarding to necessary driver actions or actions made by other people are made to avoid from safety goal violation. Two main concepts that are given below shall be applied if these assumptions are made;

  a) Specification of these actions shall be done within the concept of functional safety,

b) If the sufficient means and controls are available for the driver and other people, they shall be identified within the concept of functional safety.

Figure 2. shows the flow mechanism of safety requirements. After the item definition is made, HARA analysis is performed. The purpose of HARA analysis is to determine the malfunctions that the system will encounter. Safety goals are determined at the HARA phase in order to take the necessary precautions against these malfunctions. When determining safety goals, ASIL level calculation is also made. The next step is to produce Functional Safety Requirements from the determined safety goals. Technical Safety Requirements are derived from the determined Functional Safety Requirements in the Technical Safety Concept section. In the last stage, Hardware Safety Requirements and Software Safety Requirements are produced from Technical Safety Requirements.

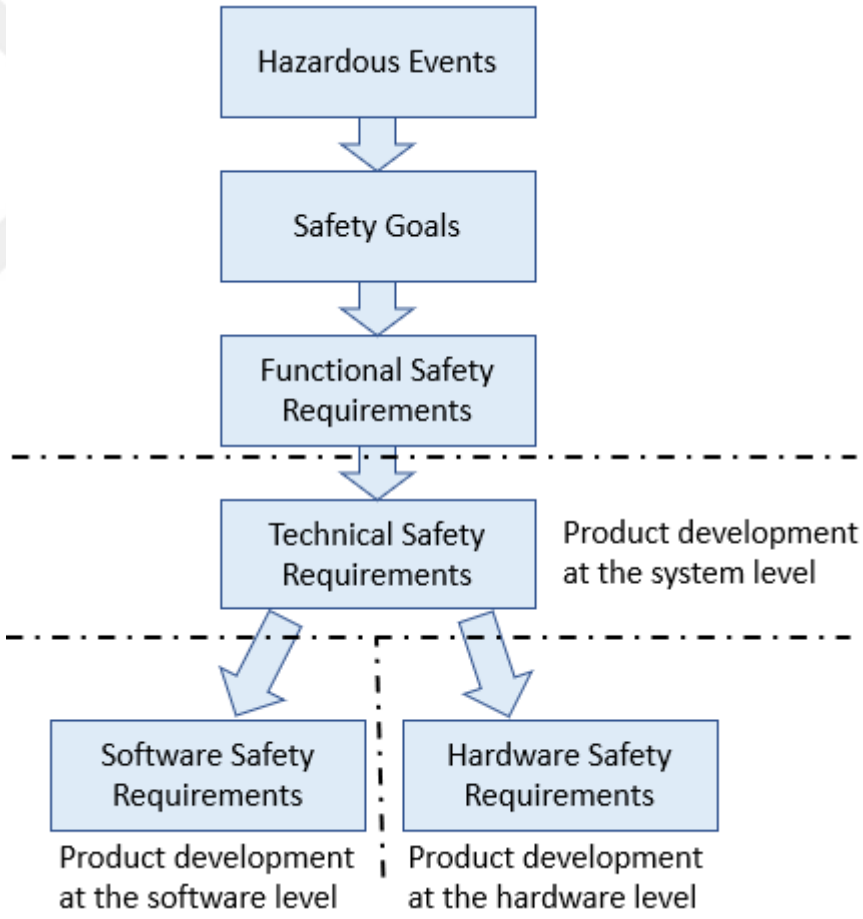


**Figure 2.2 :** Flow of safety requirements in ISO 26262.

# 3. AEBS ARCHITECTURE

## 3.1 Autosar

Software development has gained critical importance in the automotive industry in the last 20 years. The most important reason for this is the development of active and passive safety systems and the widespread use of electronic components. However, fast-growing software has begun to pose difficulties for automotive manufacturers. For these reasons, leading automotive manufacturers and suppliers have developed a software architecture that is standardized and open software with the aid of suppliers and tool developers in July 2003. That software is called Automotive Open System Architecture (AUTOSAR). Today, AUTOSAR has been a widely used and accepted software architecture. Companies such as Bosch, BMW, Continental, Daimler, Ford, General Motors, PSA, Toyota, and Volkswagen are the main partners of AUTOSAR. The control, administration, and organization of AUTOSAR are carried out by these companies [36].

Many ECU and microcontroller modules are used in cars and these read data from the sensors on the vehicle. For example, the vehicle speed is read by sensors and transmitted to the ECU. In the ECU, the software is developed to keep the vehicle at the speed desired by the driver. Finally, the speed control signals, which are the output of the ECU, are transmitted to the actuators on the vehicle.

In some vehicles, the number of ECUs used on the vehicle is around 80 and therefore the software architecture to be used in ECUs needed to be planned. The planned architecture will provide great advantages. AUTOSAR is based on partitioning ECU software with hardware-independent application software and hardware-oriented Basic Software (BSW) with the Runtime Environment (RTE), the software abstraction layer. While the software is developed for the ECU according to the AUTOSAR architecture, the software is developed according to a layered structure. The basis of the AUTOSAR software architecture is to create a standardized architecture for ECU software. Figure 3.1 shows the main architectural design of the ECU.

Furthermore, the abstraction layer makes the improvement of OEM-specific and competitive software applications possible as driver assistance systems. Also, the standardization of OEM-independent BSW can be become simple by an abstraction layer. Moreover, the abstraction layer is the precondition for the software of ECU for enabling the scaling it for different car lines and variants. Moreover, the abstraction layer is the precondition for the software of ECU for enabling the scaling it for different car lines and variants. Also, the distribution of the applications between a number of ECUs and integration of software modules from different sources can be enabled by it.

The BSW is divided into 3 distinct layers which are; “services,” “ECU abstraction,” “microcontroller abstraction”. The application layer is abstracted from the basic software by the Runtime Environment. Also, the flow of the data and information among them are arranged by this. The basis of the structure of the software modules which are component-oriented, hardware-independent on the application level, and independent units are formed by this.

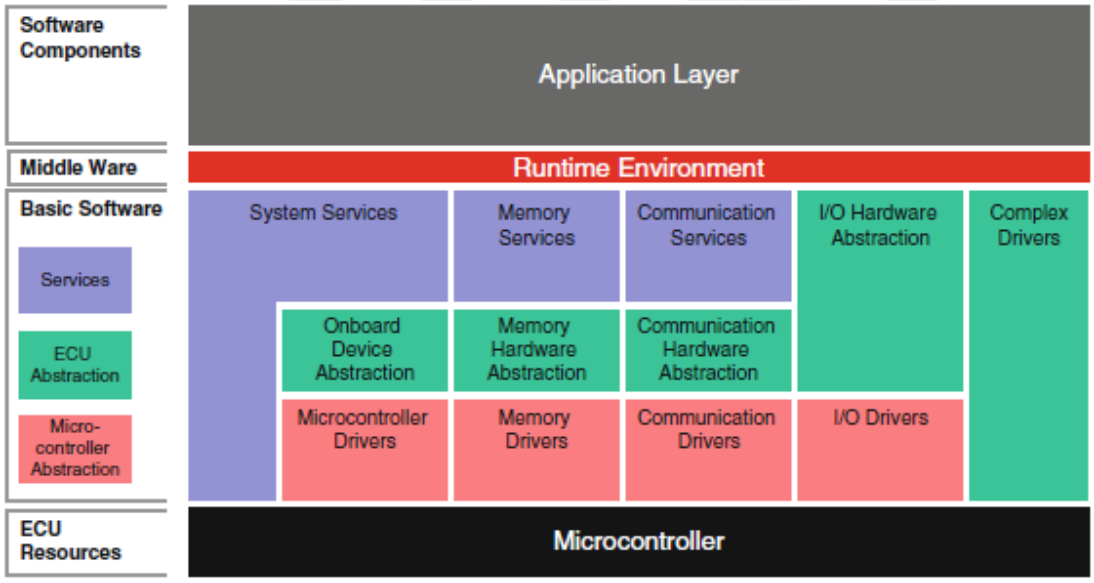


**Figure 3.1:** Software architecture of AUTOSAR [36].

For instance, software modules are responsible for conducting the functions of a driver assistance system. RTE is connected to each individual software module, and among them, there is no connection. Also, each of them communicates only with the RTE, and this enables clear communication design without taking into account of occurring within an ECU or exceeding the boundaries of ECU. Although the knowledge of used and planned hardware has not been known, this independence enables the development

of software components and the distribution of software modules existed between the ECUs.

Application layer is composed of AUTOSAR software components, which are atomic software components of sensor/actuator or application type of software components, mapped on the ECU. The information is conveyed through the AUTOSAR runtime environment between components of AUTOSAR. The software connectivity elements are guaranteed by the AUTOSTAR interface.

The communication abstraction is provided by RTE with the same services and interfaces without taking into consideration of usage of inter-ECU communication channels like CAN, LIN, FlexRay, and MOST or communication only between intra-ECU.

Basic software (BSW) is the standardized software layer. This layer is required for running the functional part of the software. Also, the services are supplied by this layer to AUTOSTAR software components. The location of BSW is under RTE and BSW does not have any functional duty. Its function is handling the communication between different ECUs.

Thanks to the standard of the AUTOSAR, vehicular system design can be done with component-based software. The application software components are used in the architecture of the AUTOSTAR. These components are connected to an abstract component that is called the virtual function bus [37].

AUTOSAR Application Software includes a lot of domains. These domains are Powertrain, Body Electronics, Occupant and Pedestrian Safety, Multimedia, Telematics and HMI, and Chassis.

### 3.1.1 Chassis Domain Architecture Overview

Figure 3.2 shows the chassis domain functions. As well as these functions, the AEBS function is developed in the chassis domain.

Chassis domain software architecture example of Cruise Control and Adaptive Cruise Control (CrsCtrlAndAcc) is given in [38] and ACC software architecture is shown in Figure 3.3 from that example. AEBS software component architecture is done by taking into account the AUTOSAR recommendations regarding the architecture of

ADAS functions in [38] and derived from example of Cruise Control and Adaptive Cruise Control (CrsCtrlAndAcc).

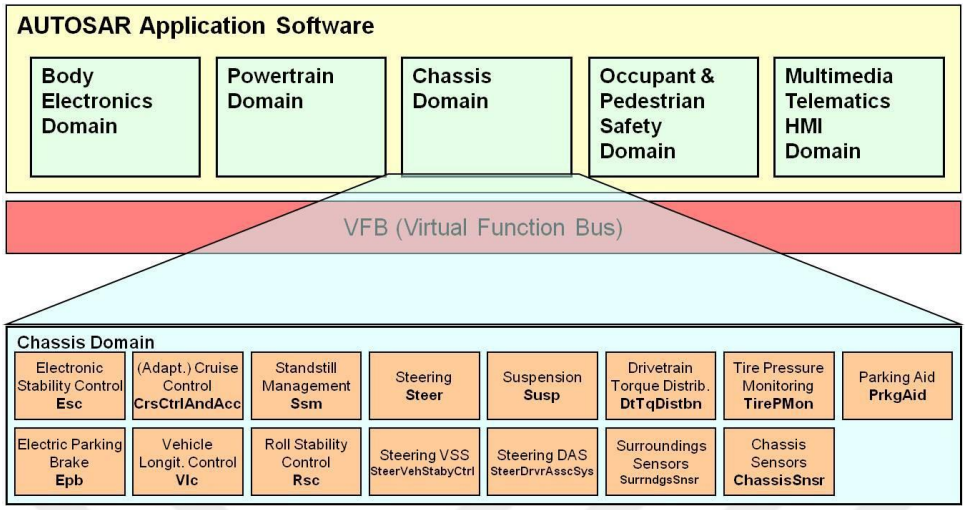


**Figure 3.2 :** Chassis Domain Overview [38].

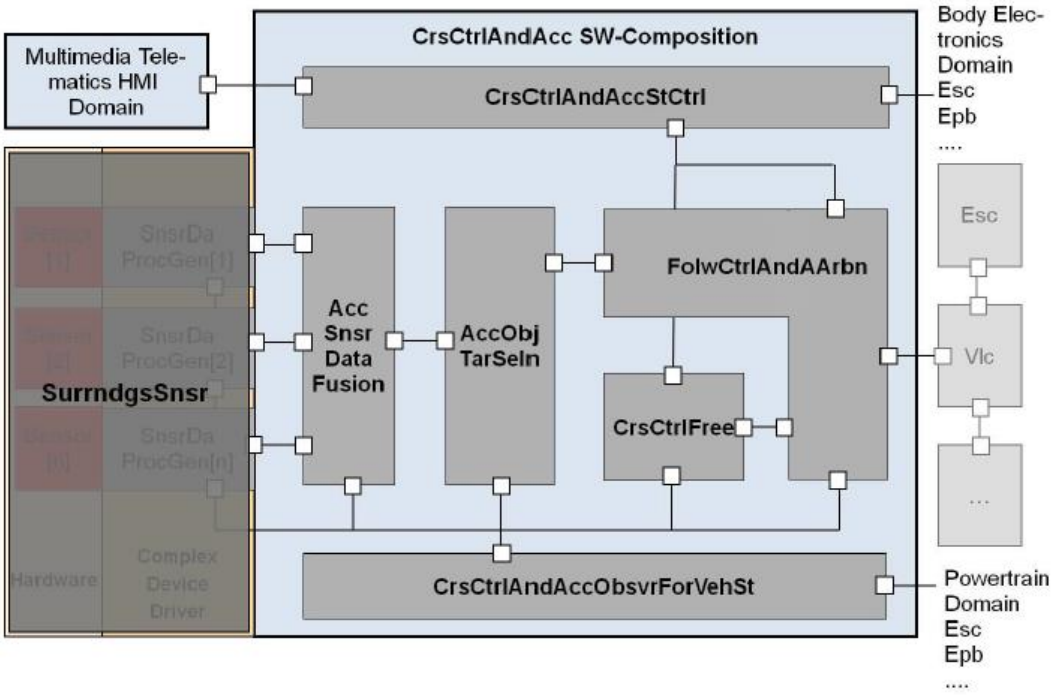


**Figure 3.3 :** Cruise Control and Adaptive Cruise Control software architectue example [38].

Figure 3.4 illustrates the main functions of the AEBS. The task of the target object selection function is to select the object as a target that is closest and in the driving path. It does these operations using data from sensor fusion and situation analysis.

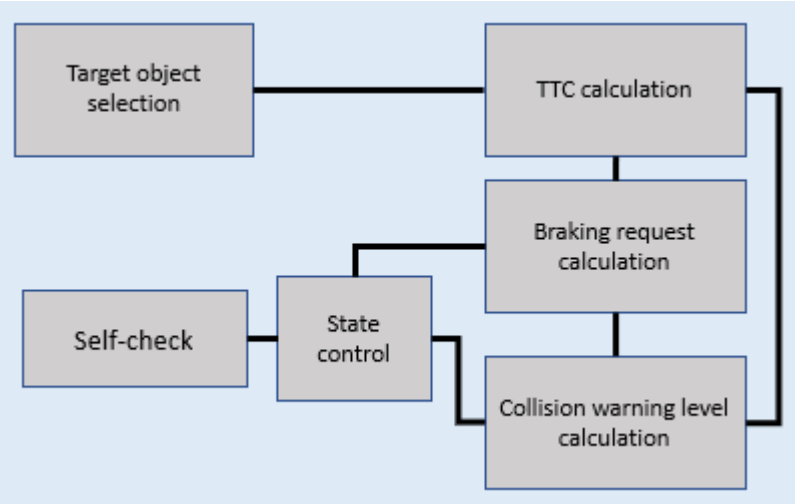


**Figure 3.4 :** Software architecture of AEBS based on AUTOSAR Chassis Domain.

The TTC calculation function is used to calculate the Time to Collision (TTC) and Enhanced Time to Collision (ETTC) values using the relative speed, relative acceleration, and distance information between the selected target and the subject vehicle. The Braking request calculation function compares the TTC values for the selected target with the Collision Judgment Curve and Collision Risk Judgment Curve values. According to this comparison, autonomous braking is initiated. Collision warnings are initiated by the collision warning level calculation function. The current state determination of the AEBS system performed by the state control function. Error messages are generated by the self-check function according to the error signals that coming from the sensors and actuators that are on the vehicle and used in AEBS.

### 3.2 Longitudinal motion

The effects of tire forces and moments are highly important for longitudinal motion of the vehicle. Mathematical models of tire forces are explained in this section. The forces of the tire that are received from the road can be decomposed along the three axes. These forces are:

- $F_x$ is longitudinal force along x-axis
- $F_y$ is lateral force along y-axis
- $F_z$ is vertical force along z-axis

Also, the moments which are received from the road can be decomposed into 3 axes. These moments are:

- $M_x$ is overturning moment along x-axis
- $M_y$ is rolling moment along y-axis
- $M_z$ is aligning moment along z-axis

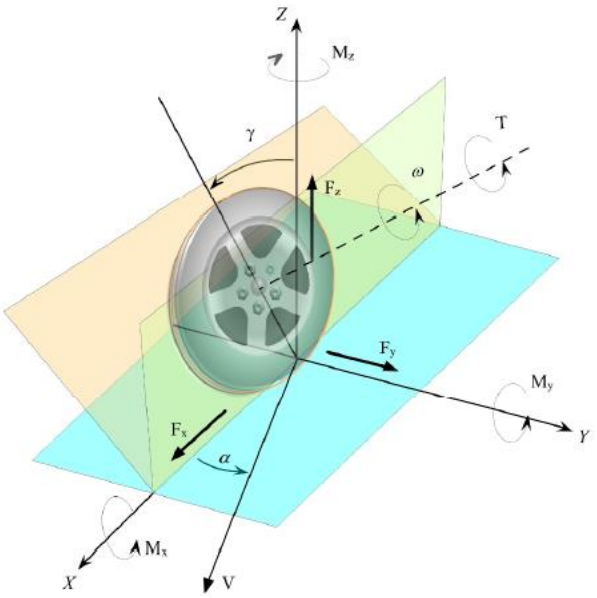


**Figure 3.5 :** Tire forces and moments [39].

The axes of forces and moments acting on the tire are displayed in Figure 3.5.

### 3.2.1 Longitudinal equation of motion

In Figure 3.6, longitudinal motion equations are shown while the vehicle is moving on the inclined road. Longitudinal tire forces, aerodynamic drag forces, rolling resistance forces and gravitational forces are longitudinal forces that affect the longitudinal movement of the vehicle. Longitudinal motion equation is:

$$m\ddot{x} = F_{xf} + F_{xr} - F_{aero} - R_{xf} - R_{xr} - mg\sin\theta \tag{3.1}$$

Variables of longitudinal motion equation are:

- $F_{xf}$ is front tires longitudinal tire force.
- $F_{xr}$ is rear tires longitudinal tire force.
- $F_{aero}$ is longitudinal aerodynamic drag force.
- $R_{xf}$ is rolling resistance force of the front tires.

- $R_{xr}$is rolling resistance force of the rear tires.
- $m$ is vehicle mass.
- $g$ is gravity.
- $\theta$ is the inclination angle of the road that the vehicle travels.

$F_{aero}$ is defined as:

$$F_{aero} = \frac{1}{2}\rho C_d A_F (V_x + V_{wind})^2 \tag{3.2}$$

In equation (3.2), $\rho$ is the air density, $C_d$ is the aerodynamic drag coefficient, $A_F$ is vehicle frontal area, $V_x$ is longitudinal velocity of the vehicle, and $V_{wind}$ is the wind velocity.

Summation of $R_{xf} + R_{xr}$ is:

$$R_{xf} + R_{xr} = C_{roll} mg \tag{3.3}$$

In equation (3.3), $C_{roll}$ is the rolling resistance coefficient.

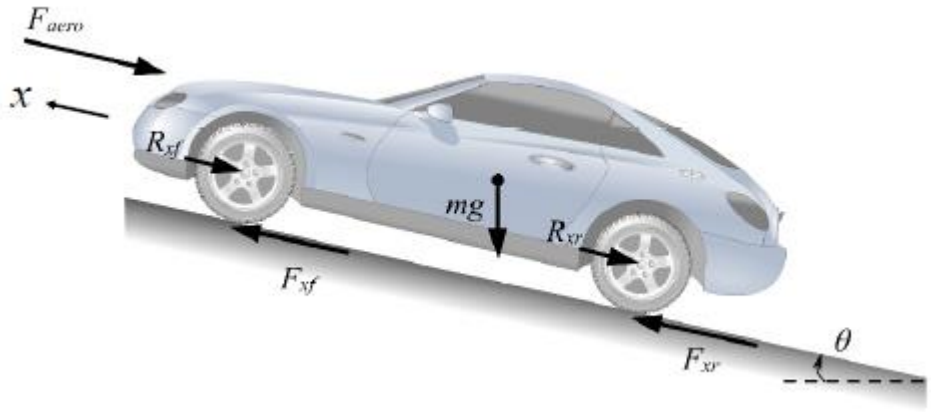


**Figure 3.6 :** Longitudinal forces acting on a vehicle [39].

### 3.2.2 Longitudinal tire force

The definition of longitudinal slip is the difference between longitudinal wheel velocity ($V_x$) and equivalent rotational wheel velocity ($\omega * r_e$). Where ω is the angular velocity of the tire and $r_e$ is the effective wheel radius. Longitudinal slip ratio is defined as the following equations:

$$\sigma_x = \frac{\omega * r_e - V_x}{V_x} \tag{3.4}$$

$$\sigma_x = \frac{\omega * r_e - V_x}{V_x} \tag{3.5}$$

The longitudinal slip ratio is determined when the vehicle is decelerating according to equation (3.4) and when the vehicle is accelerating according to equation (3.5).

According to experimental results, slip ratio, the normal (vertical) force on the tire, and the friction coefficient of the road surface effects the longitudinal tire force. Figure 3.7 shows that longitudinal tire force is how changes due to wheel slip ratio when the friction is assumed 1 and the normal force is equal to a constant value.

It is seen that from Figure 3.7, the longitudinal tire force is changing linearly when the wheel slip ratio is between -0.1 and 0.1. Also, Figure 3.7 displays that longitudinal tire force saturates when the slip ratio takes high values [39].

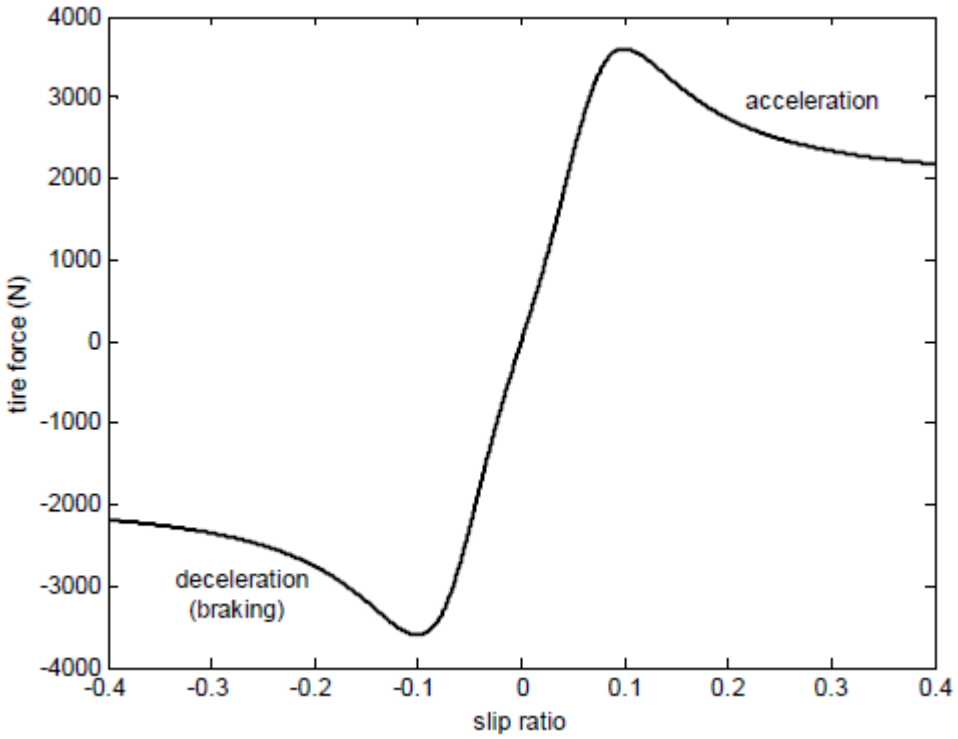


**Figure 3.7 :** Relationship of the tire longitudinal force and wheel slip ratio [39].

### 3.2.3 Pacejka's magic formula

The Pacejka tire model provides a method for calculating longitudinal, lateral tire forces and aligning moment for a wide range of operating conditions. This model is

also called Magic Tire Formula since it is based on experimental data and not on analytical formulas. Longitudinal tire force, lateral tire force, and aligning moment can be calculated by the Magic Formula in various conditions like large slip angle and slip ratios. Additionally, combined lateral and longitudinal forces can be used for that calculation.

For simple cases where only the lateral or longitudinal force is calculated, the generated force Y can be calculated as a function of the input variable X [39].

$$Y(X) = y(x) + S_v \tag{3.6}$$

In equation (3.6), $Y(X)$ is the output variable of $F_x$ or $F_y$ or $M_z$. The $S_v$ is the vertical shift value and $y(x)$ is defined in the equation (3.7).

$$y(x) = Dsin\left[C\tan^{-1}\left(Bx - E(Bx - \tan^{-1}(Bx))\right)\right] \tag{3.7}$$

In equation (3.7), $B$ is the stiffness factor, $C$ is the shape factor, $D$ is peak value, $E$ is curvature factor, and $x$ is defined as:

$$x = X - S_h \tag{3.8}$$

In equation (3.8), $S_h$ is the horizontal shift value.

The values of $B$, $C$, $D$, and $E$ are defined as following [39]:

$$C = a_0 \tag{3.9}$$

$$D = a_1 {F_z}^2 + a_2 F_z \tag{3.10}$$

$$BCD = \frac{a_3 {F_z}^2 + a_4 F_z}{e^{a_5 F_z}} \tag{3.11}$$

$$BCD = a_3 \sin\left(tan^{-1}(a_5 F_z)\right) \tag{3.12}$$

$$B = \frac{BCD}{CD} \tag{3.13}$$

$$E = a_6 {F_z}^2 + a_7 F_z + a_8 \quad (3.14)$$

Equation (3.11) and equation (3.12) shows the longitudinal force and lateral force respectively.

**Table 3.1 :** Coefficients for tire formula with load influence [40, 41]**.**

| | $a_0$ | $a_1$ | $a_2$ | $a_3$ | $a_4$ | $a_5$ | $a_6$ | $a_7$ | $a_8$ |
|---|---|---|---|---|---|---|---|---|---|
| $F_y$ | 1.30 | -22.1 | 1011 | 1078 | 1.82 | 0.208 | 0 | -0.35 | 0.707 |
| $M_z$ | 2.40 | -2.72 | -2.28 | -1.86 | -2.73 | 0.110 | -0.07 | 0.643 | -4.04 |
| $F_x$ | 1.65 | -21.3 | 1144 | 49.6 | 226 | 0.069 | -0.006 | 0.056 | 0.486 |

According to the Magic formula, the forces on the wheel are shown in Figure 3.8 and Figure 3.9, according to the Magic formula coefficients that are given in Equation (3.11) and equation (3.12) shows the longitudinal force and lateral force respectively.

Table 3.1. Figure 3.8 illustrates the longitudinal forces according to different slip rates and the lateral forces according to different slip rates are shown in Figure 3.9.

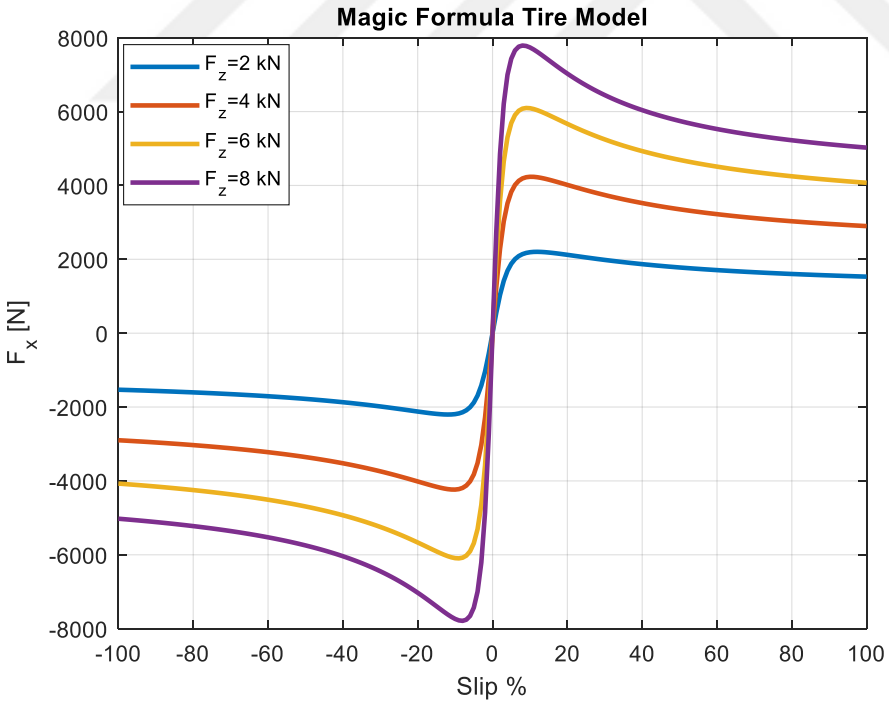


**Figure 3.8 :** According to Magic Formula Tire Model, longitudinal tire forces at different slip ratios.

### 3.3 Ackerman Steering Geometry

In Figure 3.10, the turning of the vehicle with front wheels to left is shown. According to Ackerman steering condition, if the vehicle moves at low speeds, the inner and outer wheels will turn without slipping. The formula of the Ackerman steering is displayed in equation (3.15) [42].

$$\cot \delta_o - \cot \delta_i = \frac{w}{l} \tag{3.15}$$

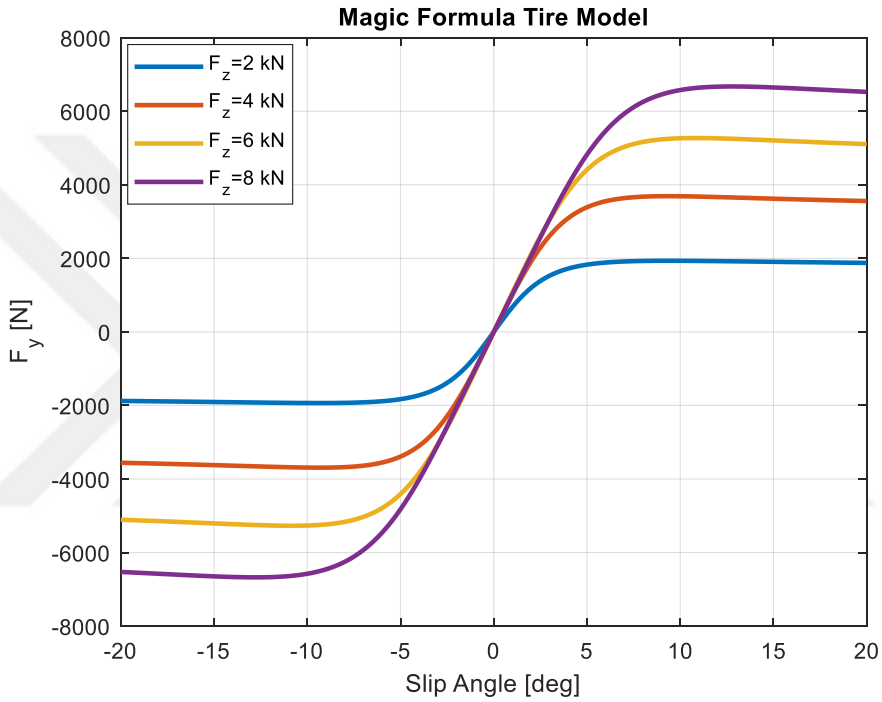


**Figure 3.9 :** According to Magic Formula Tire Model, longitudinal tire forces at different slip ratios.

In equation (3.15), $\delta_o$ is the steering angle of the front outer wheel, $\delta_i$ is the steering angle of the inner front wheel, $w$ is the distance between steering points of the front wheels and known as track, and $l$ is the distance between the front and rear axles and known as wheelbase.

Where point O is the center of rotation and the intersection point of drawn perpendicular lines to wheels. Point C is the center of gravity (cog) and $a_2$ is the distance between the center of gravity and the rear axle. The radius, R is the distance between point O and point C and it is calculated as:

$$R = \sqrt{{a_2}^2 + l^2\,(\cot\delta)^2} \tag{3.16}$$

The angle $\delta$, which is used in equation (3.16), is calculated in equation (3.17).

$$\cot\delta = \frac{\cot\delta_o + \cot\delta_i}{2} \tag{3.17}$$

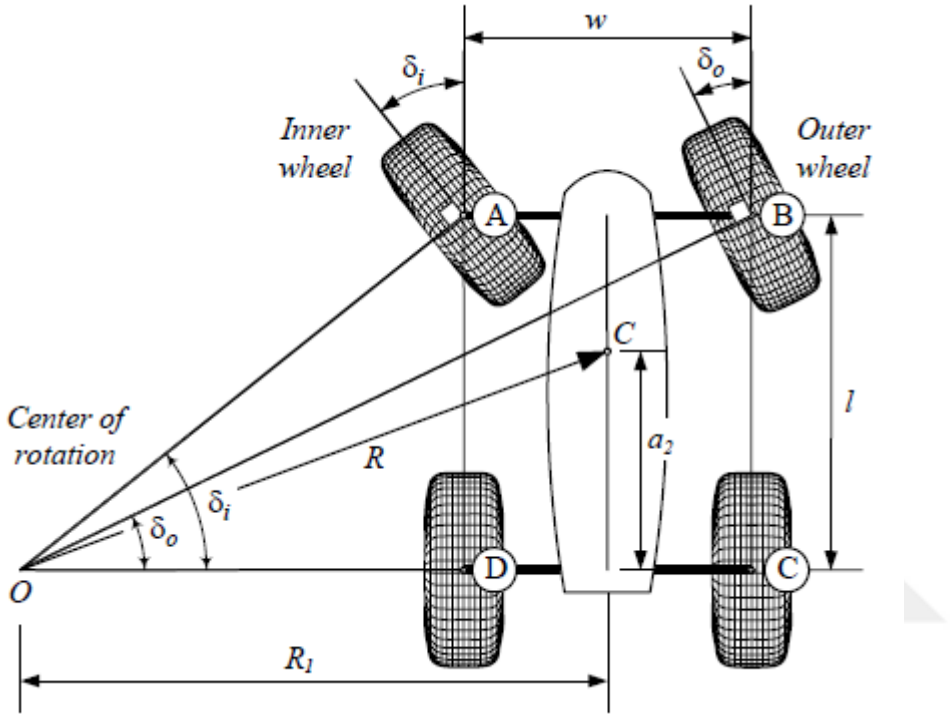


**Figure 3.10 :** Front vehicle steering and road radius [42].

### 3.4 ISO 22839:2013 Forward Vehicle Collision Mitigation System Overview

In this International Standard, the concept of operation, minimum functionality, system requirements, system interfaces, and test methods are discussed for Forward Vehicle Collision Mitigation Systems (FVCMS).

FVCMS helps reduce the extent of property damage, personal injury, or death by reducing the collision energy in rear-end collision scenarios. This standard specifies that the FVCMS is to be used on public and non-public roads. These systems are not suitable for use in land conditions.

### 3.4.1 Classifications

This part introduces different types of FVCMS system which are covered by that standard.

#### 3.4.1.1 System classification by curve radius capability

Class I systems shall be able to detect forward obstacle vehicles when road radius higher or equal to 500 meters.

Class II systems shall be able to detect forward obstacle vehicles when road radius higher or equal to 250 meters.

Class III systems shall be able to detect forward obstacle vehicles when road radius higher or equal to 125 meters.

Systems are classified in terms of their curve radius capacity as shown in Table 3.2.

**Table 3.2 :** System classifications for curve radius [3].

| Class | Horizontal curve radius capability |
|---|---|
| I | Curve radius is not lower than 500 meters |
| II | Curve radius is not lower than 250 meters |
| III | Curve radius is not lower than 125 meters |

#### 3.4.1.2 Classification by countermeasure types included

FVCMS is classified according to its countermeasure functionality.

#### 3.4.1.3 Collision warning countermeasure

Collision Warning includes audible, visual, tactile, or haptic modes according to requirements of ISO 15623.

Collision warnings shall be issued before or at the same time with speed reduction or mitigation braking.

#### 3.4.1.4 Speed reduction braking countermeasure

Speed reduction braking is part of the autonomous braking and it aims to reduce subject vehicle’s speed before mitigation braking. During the speed reduction braking, the driver can take the control with different countermeasure such as lane change or hard braking. Speed reduction braking shall not be activated if mitigation braking is active.

#### 3.4.1.5 Mitigation braking countermeasure

Mitigation braking is an autonomous braking that is activated when a collision becomes unavoidable. In case of mitigation braking is applied, the collision energy will be less than if mitigation braking is not applied. Also, in some cases, collision can be prevented completely thanks to mitigation braking.

#### 3.4.1.6 Combining countermeasures

According to this standard, there are three types of system based on countermeasure combinations. In type 1 system, speed reduction braking and collision warnings are allowed but mitigation braking is not allowed. For type 2 system, while mitigation braking and collision warnings are allowed, speed reduction braking is not allowed. In type 3 system, mitigation braking, speed reduction braking, and collision warnings are allowed. These configurations are displayed in Table 3.3.

### 3.4.2 Requirements

#### 3.4.2.1 Minimum enabling capabilities

For the light vehicles FVCMS shall be equipped with the below functions:

- Forward target vehicles shall be detected.
- Relative velocity and distance between the subject vehicle and target vehicle shall be detected.

**Table 3.3 :** Permissible system configurations [3].

| Type | Mitigation Braking | Speed Reduction Braking | Collision Warning |
|---|---|---|---|
| 1 | 0 | 1 | 1 |
| 2 | 1 | 0 | 1 |
| 3 | 1 | 1 | 1 |

- Subject vehicle velocity shall be measured.
- Countermeasures shall be able to be issued when the lateral offset of the target vehicle becomes lower than 20%.
- The system shall provide warnings to the driver considering FVCMS requirements.

- If the driver is braking but that brake is not sufficient, then the brake demand shall be increased by the system or if the driver does not issue brake and braking is necessary, then the system shall initiate braking.
- Brake lamps shall be turned on when braking is issued by FVCMS.
- The driver shall be able to increase the braking demand during speed reduction or mitigation phase.

#### 3.4.2.2 Operating model - state transition diagram

FVCMS function has following states:

- **Off State:** As long as FVCMS is in Off state, countermeasures are not issued by the system. Following requirements describes the off-state conditions:
    a) The system shall transition to off state when ignition becomes off.
    b) As soon as any failure is detected by self-test function, then the system shall transition to off state.
    c) As soon as driver demands disabling request, then the system shall transition to off state.
- **FVCMS Inactive:** FVCMS shall observe the vehicle speed and current gear to activate the system in the inactive state. Following requirements explains the transition conditions to inactive state:
    a) The system shall transition to inactive state if ignition becomes on and there is no failure. If any of the activation conditions are no longer met, for example, the selected reverse gear or vehicle speed becomes lower than the activation speed, the system state shall transition from active to inactive.
    b) If recoverable failure is detected by self-test function, then the system shall transition to inactive state from active state.
    c) If recoverable failure is detected by the self-test function, then the system shall transition to the inactive state from the active state.

- **FVCMS Active:** The system observes the countermeasure conditions in the active state and activates countermeasures conditions are satisfied. Additionally, countermeasures are not issued when the system is overridden.

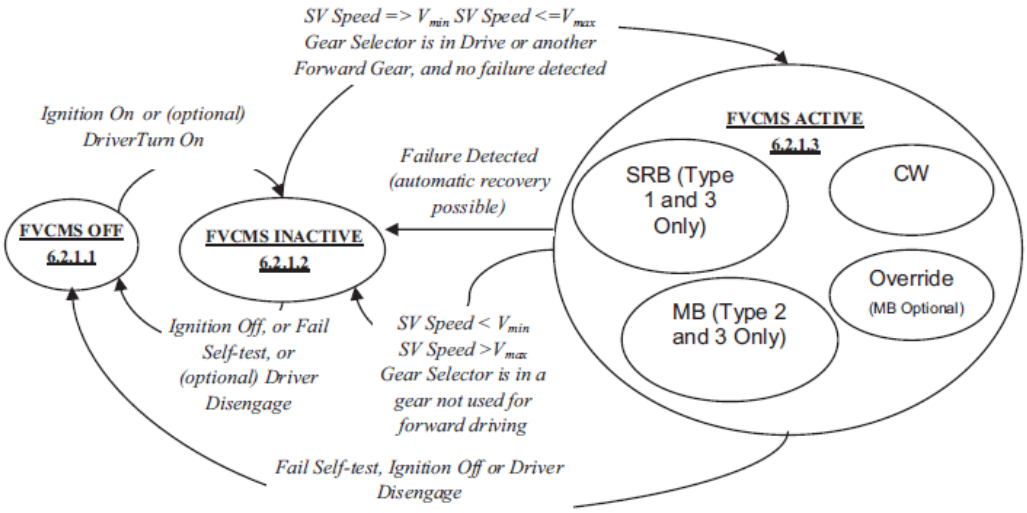


**Figure 3.11 :** State diagram of FVCMS [3].

The state diagram of FVCMS is shown in Figure 3.11.

### 3.4.3 Performance requirements

- Countermeasures shall be given for motor vehicles that are used on public roads such as motorcycles, cars, light trucks, buses, motor coaches, and other heavy vehicles by the FVCMS system.
- The system shall issue countermeasures in rear-end collision scenarios to in-lane target vehicles.
- The system shall be able to issue collision warnings, speed reduction, or mitigation braking if the vehicle speed is between $V_{min}$ and $V_{max}$. The $V_{min}$ shall be equal or lower than 8.4 $m/s$. The system shall transition to the inactive state when vehicle speed decreases below the $V_{min}$ value. However, if the vehicle speed drops below the $V_{min}$ value due to autonomous braking, then the system shall keep its state. The $V_{max}$ shall be equal to higher than 27.8 $m/s$. The system shall transition to the inactive state when the vehicle speed becomes higher than the $V_{max}$ value.
- The system shall be able to issue countermeasure for target if the relative speed is between -4.2 $m/s$ and -20 $m/s$ for that target.

- The system shall not start mitigation braking when TTC or ETTC is higher than 3 seconds.
- The system shall not start speed reduction braking when TTC or ETTC is higher than 4 seconds.
- The system shall issue at least 5 $m/s^2$ deceleration during mitigation braking phase and total speed reduction shall be higher than 2 $m/s$. If the system has both speed reduction and mitigation braking functionality (Type 3 system), then total speed reduction for speed reduction and mitigation braking phases shall be higher than 4 $m/s$.
- The system shall be overridden by driver when the system is issuing speed reduction or mitigation braking.
- If a failure is detected, then the system shall inform the driver about that failure.
- Collision warnings shall be issued before or at the same time with speed reduction or mitigation braking.
- FVCMS shall not issue any countermeasure to target vehicles that are not in rear-end collision scenarios.

## 3.5 UNECE Regulation No 152: Overview

- Passenger cars with a maximum mass of 3.5 tonnes and a maximum of 9 passengers with the driver are in the M1 category vehicles, while vehicles used for the carriage of goods and with a maximum mass not exceeding 3.5 tonnes are in the N1 category vehicles [43]. The Advanced Emergency Braking Systems (AEBS) is used in motor vehicles that are in the M1 and N1 categories. The main goal of this regulation is to make uniform provisions for those used in driving conditions in urban areas [9].
- This regulation is used in the vehicles related to an on-board system within the M1 and N1 categories. This regulation states that the vehicles in the M1 and N1 categories should prevent or reduce the effect of accidents that will occur with passenger cars and pedestrians.

- Vehicles having AEBS function shall be equipped with an Anti-lock Braking System (ABS).
- If there is a failure preventing the regulation requirements in the AEBS, there will be a warning that shall be constant yellow warning.
- The AEBS shall have self-control without causing an appreciable time interval when there is an electrically detectable failure. Also, the warning signal shall be illuminated without any delay. Additionally, if there is a non-electrical failure condition such as misalignment or blindness of the sensor, and if this has detected, the warning shall be given.
- It is important to calibrate the system after driving the vehicle for 15 seconds over 10 $km/h$. If it has not happened, the driver shall get the indication about that, and it shall not be disappeared until the successful calibration.
- If the vehicle is equipped with a tool that can deactivate the AEBS manually, there shall be a deactivation warning when the system is deactivated by the driver. The deactivation of the AEBS at a speed over 10 $km/h$ shall not be allowed and the design of the AEBS control shall not make it possible to deactivate the system manually with less than two deliberate actions. Also, at the onset of each new ignition cycle, the AEBS function shall be reinstated automatically if it was deactivated before ignition cycle.
- The design of the system shall be based on the reduction of the collision warning signal generation to a minimum and the avoidance of autonomous braking when an impending collision is not recognized by the driver.
- The collision warning shall be issued at the latest 0.8 seconds before the start of emergency braking when there is a collision probability with a preceding vehicle of Category M1 or crossing pedestrian target on the road with 5 $km/h$ speed. Nevertheless, when the collision cannot be predicted 0.8 seconds before emergency braking, the collision warning shall be issued at once after the preceding target is detected. If the conditions that are prevailing a collision do not exist anymore, the collision warning can be aborted. Additionally, the collision warning shall be provided by at least two modes. These modes can be selected from acoustic, haptic, or optical modes.

- In the case of the detection of the probability of an imminent collision by the system, a breaking of at least 5.0 $m/s^2$ shall be demanded by the system to the vehicle's service braking system. If the conditions that are prevailing a collision do not exist anymore, the emergency braking might be aborted.
- If the system is not deactivated manually, the activation of the system shall continue in the range of the speed from 10 $km/h$ to 60 $km/h$ for car-to-car scenarios and from 20 $km/h$ to 60 $km/h$ for car to pedestrian scenarios.
- The vehicles shall be provided by the AEBS for the driver to stop the collision warning and the emergency braking. The interruption can be started by any positive action indicating the awareness of the situation by the driver. For example, kick-down, running the direction indicator control.

### 3.6 AEBS Working Principle

Time to Collision (TTC) is the most common method which is used to calculate collision probability. Conventional TTC is found by dividing the distance between two vehicles by the relative velocity and that formula is displayed in equation (3.18). There is also another method that uses the relative acceleration between the vehicles to calculate the TTC value. This method is called as Enhanced Time to Collision (ETTC). While doing this calculation, it is assumed that both vehicles are moving in the same direction and the relative acceleration between them is constant. The ETTC formula is given in equation (3.21).

$$TTC = -\frac{x}{v_{rel}} \tag{3.18}$$

Where $x$ is distance value between two vehicles and the unit of $x$ is meter ($m$).

$$v_{rel} = v_{TV} - v_{SV} \tag{3.19}$$

The formula of relative velocity is shown in equation (3.19). Where $v_{TV}$ is target vehicle velocity and $v_{SV}$ is subject vehicle velocity. The units of these values are $m/s$.

$$a_{rel} = a_{TV} - a_{SV} \tag{3.20}$$

The formula of relative acceleration is provided in equation (3.20). Where $a_{TV}$ is target vehicle acceleration and $a_{SV}$ is subject vehicle acceleration. The units of these values are $m/s^2$.

$$ETTC = \frac{-(v_{TV} - v_{SV}) - \sqrt{(v_{TV} - v_{SV})^2 - 2x(a_{TV} - a_{SV})}}{a_{TV} - a_{SV}} \tag{3.21}$$

In this thesis, $TTC_{brk}$, which is shown in Table 3.4, is used in the decision-making process.

The main logic behind the AEBS algorithm is based on two TTC curves. Those curves are used to initiate autonomous braking and called the Collision Judgment Curve and Collision Risk Judgment Curve. The Collision Judgment Curve is used to initiate mitigation braking. When the $TTC_{brk}$ value becomes lower than the calculated limit value of the Collision Judgment Curve, mitigation braking is initiated. The same logic is used for speed reduction braking. Collision Risk Judgment Curve is used to initiate speed reduction braking. When the $TTC_{brk}$ value becomes lower than the calculated limit value of the Collision Risk Judgment Curve, speed reduction braking is initiated.

In rear-end collision scenarios, an accident can be avoided by the driver in two ways. These are the braking and avoidance maneuvers made by the driver. The vehicle's braking performance shall be taken into account to determine the evasion braking limit. This limit value can be calculated by considering the relative speed and the braking distance. Also, the braking distance is determined by the hard braking performance of the vehicle corresponding to the relative speed value. For this reason, these values should be determined by performing brake tests on vehicles.

**Table 3.4 :** TTC Brake Calculation [44].

| $TTC_{brk}$ | Condition |
|---|---|
| $-\frac{x}{v_{rel}}$ | $v_{rel} < 0$ and $a_{rel} = 0$ |
| $-\frac{x}{v_{rel}} - \frac{\sqrt{{v_{rel}}^2 - 2xa_{rel}}}{a_{rel}}$ | $v_{rel} < 0$ and $a_{rel} \neq 0$ |
| $-\frac{x}{v_{rel}} + \frac{\sqrt{{v_{rel}}^2 - 2xa_{rel}}}{a_{rel}}$ | $v_{rel} \geq 0$ and $a_{rel} < 0$ |
| undefined | $v_{rel} \geq 0$ and $a_{rel} \geq 0$ |
| undefined | ${v_{rel}}^2 - 2xa_{rel} < 0$ |

According to [45], evasive steering maneuver time is also considered as the predicted collision time limit. This time is the minimum time for the subject vehicle in order to travel laterally 40% overlap of its width with every relative speed. The percentage overlap ratio L is shown in equation (3.22).

$$L = 100 * \frac{B}{A} \tag{3.22}$$

In equation (3.22), L is the percentage overlap ratio, and the values of A and B are demonstrated in Figure 3.12.

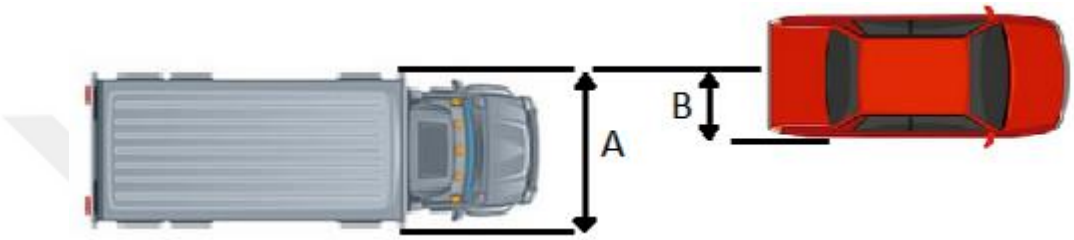


**Figure 3.12 :** Percentage Overlap Ratio [46].

Collision Judgment limit for evasive steering is defined as:

- 0.6 seconds for passenger cars. For these vehicles capacity of seating is at most 10 occupants.
- 0.8 seconds for heavy duty vehicles with a Gross Vehicle Weight (GVW) is at most 8 tonnes or maximum capacity of loading is at most 5 tonnes. Also, this time limit used for passenger cars that are higher than 10 seating capacity.

Collision Risk Judgment limit for braking is defined as:

- $T_{Lim} = 0.0167V_r + 1.0$ for passenger cars. For these vehicles capacity of seating is at most 10 occupants.
- $T_{Lim} = 0.031V_r + 1.54$ for heavy duty vehicles with a GVW is at most 8 tonnes or maximum capacity of loading is at most 5 tonnes. Also, this time limit used for passenger cars that are higher than 10 seating capacity.

Where $V_r$ is the relative speed with unit $\mathrm{km/h}$ and it has positive value when subject vehicle speed is higher than target vehicle speed.

Collision Risk Judgment limit for evasive steering is defined as:

- 1.4 seconds for passenger cars. For these vehicles capacity of seating is at most 10 occupants.
- 1.6 seconds for heavy duty vehicles with a GVW is at most 8 tonnes or maximum capacity of loading is at most 5 tonnes. Also, this time limit used for passenger cars that are higher than 10 seating capacity.

On the other hand, when the percentage overlap ratio with the target object becomes greater than 40%, the formula of evasive steering maneuver time can be evaluated as:

- $T_{Lim} = 0.0067\mathrm{L} + 1.13$ seconds for passenger cars. For these vehicles capacity of seating is at most 10 occupants.
- $T_{Lim} = 0.0142\mathrm{L} + 1.62$ seconds for heavy duty vehicles with a GVW is at most 8 tonnes or maximum capacity of loading is at most 5 tonnes. Also, this time limit is used for passenger cars that are higher than 10 seating capacity.

According to [45], the collision judgment curve shall be defined based on road test data of steering and braking of the subject vehicle because every car has different behaviour for steering and braking. In order to avoid unnecessary braking, the minimum value between collision judgment limit for evasive steering and braking collision evasion time is taken as collision judgment time. The collision risk judgment curve should be determined by taking into consideration the driver's behavior. If the system generally brakes earlier than the driver's normal behavior, the driver will be disturbed by this situation and disable AEBS. The minimum value between collision risk judgment limit for evasive steering and collision risk judgment limit for braking is taken as collision judgment time.

# 4. FUNCTIONAL SAFETY FOR AEBS

## 4.1 AEBS Related Items

### 4.1.1 Sensors

Sensors are the basis of autonomous vehicles. The surfaces of autonomous vehicles are equipped with sensors and autonomous vehicles perceives their surroundings thanks to these sensors. Sensors such as a Camera, Lidar, Radar, Sonar, a Global Positioning System (GPS), an Inertial Measurement Unit (IMU), and a wheel odometer are indispensable parts of autonomous vehicles. The data received from these sensors are processed and the braking, speed, and steering of autonomous vehicles are controlled [47]. Sensors used for autonomous vehicles are illustrated in the Figure 4. Radar, Lidar, and Camera sensors are commonly used for AEBS systems in order to detect target objects. These sensors are examined in the following part. The comparison among Radar, Camera, and Lidar is shown in Table 4.2.

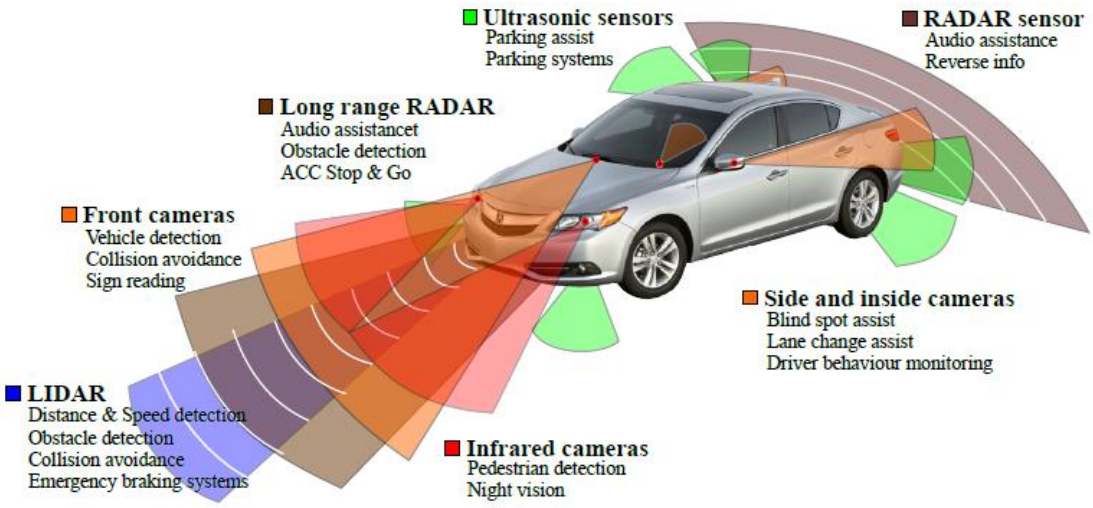


**Figure 4.1 :** Configurations of sensors on the vehicle [48].

#### 4.1.1.1 Radar

The full name of Radar is Radio Detection and Ranging. Radar systems have been already using in various working areas. Military applications are the most popular usage area of Radar sensors. These sensors have been used in the automotive industry

to increase driving safety. Radars used in that industry work at three different frequencies such as 24, 77, and 79 GHz, and they are known as millimeter-wave Radar. Currently, the 77 GHz band Radar is the most used Radar in the automotive field.

Radar calculates the distance by measuring the time between the signals which sending and receiving. Additionally, Radars are able to measure the speed of objects and their directions [50].

Radar's method of measuring speed is different from other sensors. While other sensors calculate the speed value by using the difference in the two readings, the Radar directly calculates the speed information with the Doppler Method [47].

Radars are not affected by weather conditions such as rain, snow, fog, and haze as well as darkness. Hence, Radar sensors always give good results, and especially in short-range targets are detected accurately. On the other hand, there are some disadvantages of Radars such as the lack of precision, its reduced Field of View (FOV), and wrong choices that can be made due to the jumping of the emitted signals. Table 4.1 shows the FOV, operational freuency and safety integrity level of the Radar.

**Table 4.1 :** Radar measurement data information [49].

| Radar | Field of View | Operation Frequeny | Safety Integrity Level according to ISO 26262 |
|---|---|---|---|
| Continental ARS441 | ± 9° (250 $m$)<br>± 45° (70 $m$)<br>± 75° (20 $m$) | 76…77 GHz | B |
| Continental ARS510 | ± 4° (200 $m$)<br>± 9° (120 $m$)<br>± 45° (40…70 $m$) | 76…77 GHz | B |

#### 4.1.1.2 Lidar

The full name of Lidar is Light Detection and Ranging. Lidar sensors use an infrared laser beam to measure the distance to an object. Lidar systems calculate the distance to an object by measuring the flight time of a pulsed light emitted from a laser diode until it is received by an emitter [50]. Most Lidar sensors use laser light with a wavelength of 900 $nm$ in their measurements. Lidar sensors can be classified according to 2 methods. The first method is their structure such as rotary or solid-state Lidar. The second method is the dimension of their measurements as 2D or 3D. Since

the working principle of the Lidar is the measuring of emitted and received light, it is higly affected by bad weather conditions. Because light is diffracted in weather conditions such as rain, snow, fog, or dusty environments, so accurate measurements may not be obtained. Moreover, the operating range of Lidar reduces if the reflectivity of the objects is low.

#### 4.1.1.3 Camera

Cameras have been using in the field of autonomous driving systems for many years and are now one of the most used sensors. The surrounding of the vehicle can be visualized by the Camera. The Cameras are used for different information such as lane recognition, target recognition, and target tracking. Additionally, Cameras are more successful for object classification than Lidar and Radar.

**Table 4.2 :** Comparison of different sensors and technologies [51].

| Type | Advantages | Disadvantages | Max working distance |
|---|---|---|---|
| MMW Radar | Working distance is long.<br>Radial velocity is available.<br>It works all weather conditions. | Static object performance is low.<br>Ghost object detection is possible. | 5 $m$ – 200 $m$ |
| Camera | Excellent discernibility.<br>Lateral velocity is available.<br>Color distribution suitable. | Heavy computing load.<br>Light interference.<br>Weather sensitive.<br>Radial velocity is unavailable. | 250 $m$ |
| Lidar | Field of view (FOV) is high.<br>High range resolution.<br>High angle resolution. | Unbearable for bad weather.<br>Price is high. | 200 $m$ |

### 4.1.2 Electronic control unit

The Electronic Control Unit (ECU) is widely used in vehicles today. The task of this device is to control certain functions on the vehicle. ECUs require power and data connections in order to work. Also, they contain a special chip and thanks to this chip, they can run their own software. Since each ECU has a different task on the vehicle, ECUs receive the necessary signals from the vehicle according to their tasks. For example, the Door Control Unit (DCU) receives inputs to lock the door or adjust the

vehicle windows. ECUs need to communicate with the actuators they want to control. For example, the DCU sends the signal which is generated to lock the doors to the actuator that locks the door. Thanks to the increased electronic components in vehicles, nearly 100 ECUs are used in vehicles [52]. Examples of ECUs used in vehicles are Transmission Control Module (TCM), Body Control Module (BCM), Powertrain Control Module (PCM), Vehicle Control Unit (VCU) [55]. In addition to these systems, ECUs are used to control the comfort functions such as power windows, seats, door locks, and keyless entry. ECUs also control ADAS systems such as Advanced Emergency Braking System (AEBS), Emergency Steering System (ESS), Adaptive Cruise Control (ACC), Blind Spot Detection (BSD), and Lane Departure Warning (LDW). Those ADAS functions are controlled by ADAS ECU in vehicles.

The task of the TCU is to calculate the gear shift time in automatic transmission vehicles and to increase the efficiency of fuel performance. The TCU performs its task by using signals such as vehicle speed sensor, wheel speed sensor, throttle position sensor, brake light switch received from the vehicle.

The main component of the engine management system is the electronic engine control unit. Some duties of the the electronic engine control unit are; controlling fuel supply, management of air, controlling of ignition and injection of fuel and exhaust system, and integration of functions of vehicle and transmission. There are some systems for active driving safety like TCS and ESC that can meddle the torque of the engine. This meddling is allowed by the electronic engine control unit [53].


**Figure 4.2 :** Bosch ADAS ECU [54].

Figure 4.2 displays Boch's DASy model ADAS ECU. With this ECU, data received from sensors such as Radar, Lidar, and Camera are processed and ADAS software is

realized. The DASy is a μC based ECU and it is suitable for ASIL D software development for driver assistance systems. It is also suitable for the development of partially automatic driving software up to SAE level 2 for example Highway Assist [54].

### 4.1.3 Brake systems

Today, hydraulic brake systems are generally used as brake systems in passenger cars. Hydraulic brake systems slow down the vehicle according to the braking request which is requested by the driver with the brake pedal. The wheel forces resulting from the braking of the vehicle are transferred to the road surface through the tires. During braking, the vehicle must move in the direction desired by the driver and the vehicle must be controllable.

Hydraulic systems such as ABS, ESC, and TSC are electronically controlled and used to optimize vehicle dynamics. Brake requests produced by ADAS are also transmitted to the vehicle by means of electronic hydraulic brake units and vehicle safety is increased.

The operating architecture of hydraulic brake systems is shown in Figure 4.3 and hydraulic brake systems contain components covering the following functions [56]:

- Brake force starting with foot.
- Increase braking force.
- Converting the braking force to brake pressure/volume flow.
- Pressure/volume transfer.
- The braking force on the wheels is generated from the pressure/volume.

#### 4.1.3.1 Antilock braking system

It is inevitable that each driver faces an emergency braking situation. This situation might lead to the locking of the wheels due to hard braking, as well as snowy or rainy weather. There will be a reduction in the adhesion forces between the surface of the road and the tires of the wheels due to locking. In order to overcome this problem, the antilock braking system (ABS) has developed. So, safe braking is obtained.

One of the main components of an ABS is a hydraulic unit that contains valves. The pressure of the braking is controlled by them for each wheel. Also, an ECU and a return pump are found in valves. Moreover, the speed of each wheel is measured by the sensor

that also conveys the information between the wheel and ECU. When the braking is applied heavily, the locking of the wheels can be seen. In order to prevent this, the pressure of the braking of each wheel is decreased by the ABS and reduction is not removed until finishing the risk of locking. When the risk is overcome, there will be a rise in the pressure of braking. Raising and decreasing the braking pressure depends on both the force applied to the pedal and the adhesion force between the wheel and the surface of the road. The pulsation of the pedal can happen according to specific systems [58].

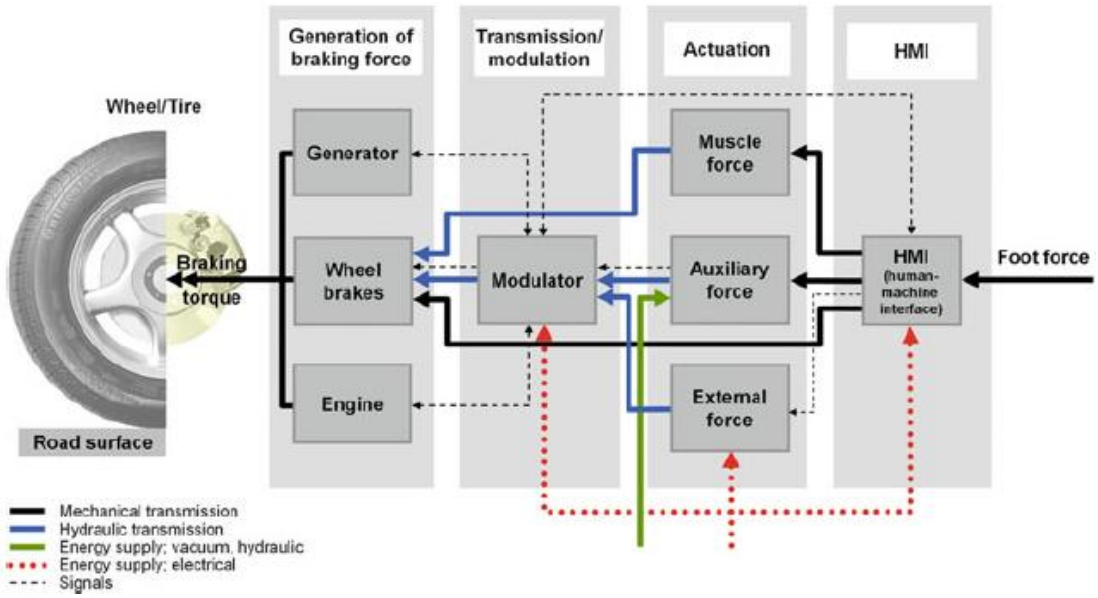


**Figure 4.3 :** The architecture of hydraulic brake systems [56].

### 4.1.3.2 Electronic stability control

The meaning of the ESC is the systems that help to driver for maintenance of the vehicle control and so providing a driving through the course intended by the driver by using computer control of brakes of each individual wheel. ESC is applied even between extreme maneuvers and reaching the road traction limit [57].

When the driver is off the route that is different from the route planned by the driver, there would be an intervention via ESC when the vehicle is closing to the road traction limit. There are a few types of deviations, and the most common ones are; understeer and oversteer. These two types are displayed in Figure 4.4. Oversteer is exceeding the deviation level planned by the driver. Technically, front wheels reach the road traction limit after rear wheels and spinning out at the rear wheels, so oversteer is seen.

Understeer is that happening less deviation from the planned one by the driver. Technically, rear wheels reach the road traction limit after front wheels [57].

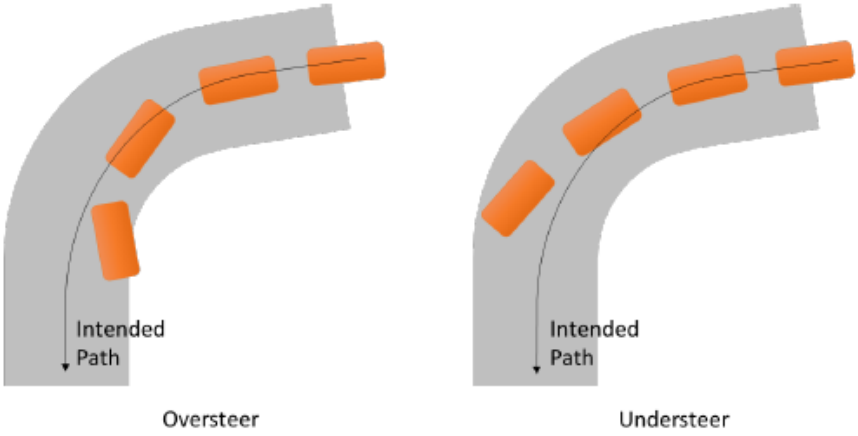


**Figure 4.4 :** Oversteer and Understeer description [57].

A differential braking force is created by braking to individual wheels by ESC in order to provide planned yaw, and the vehicle would be obtaining a corrective deviation moment. Application of the control of closed-loop is maintaining till the alignment of the headings between the driver and the vehicle. Moreover, ESC provides this by application of differential braking forces as well as modulation of the torque of the engine.

#### 4.1.3.3 Traction control system

There are a lot of similar characteristics in Traction Control System (TCS) functions and ABS. These similarities are not seen in the implementation situation of TCS. TCS is primarily enforced while the vehicle increases its speed, not while braking is applied. Moreover, the sensors that are used in ABS and TCS are similar such as the status of brake application and data of individual wheel speed. These sensors are used to notice the region of spin of the wheel. During the acceleration, if the level of the spinning is going into the unstable region, this is detected by sensors. The drive wheels have a friction coefficient. If the acceleration rate of the car is extremely higher than this value, the TCS will be triggered.

The friction coefficients of the roads can be different at different sides of the vehicle. Besides this conveying torque of drive by using the differential, they cause continuation of the spin in one of the drive wheels. If this is happening, there will be an application of brake torque to the drive wheel that is influenced without any

interference by the driver. Therefore, the vehicle will continue to be stable and the acceleration will be seen depending on the level of the available friction.

### 4.2 Item Definition For AEBS

#### 4.2.1 AEBS description

Advanced Emergency Braking System (AEBS) is a function of the Advanced Driver Assistant System (ADAS). That function aims to reduce the collision effect if the collision with forward object is not avoidable or that function aims to avoid collision with forward object. Relative velocity, longitudinal and lateral distance information and the classification of forward target are taking into account to evaluate collision risk by the AEBS system. If situation becomes critical and subject vehicle driver is not issue any countermeasure, then the AEBS system issues collision warnings and autonomous braking.

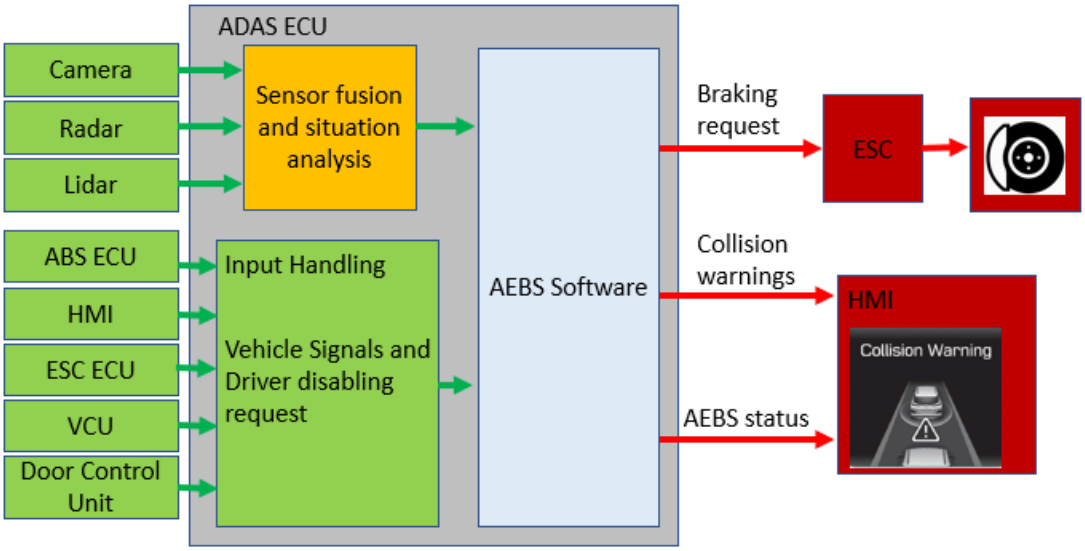


**Figure 4.5 :** AEBS structure.

Figure 4.5 shows the general operating logic of the AEBS system. The target data detected by the Radar, Camera, and Lidar sensors are fused by the sensor fusion and situation analysis block. In this way, meaningless targets are eliminated by the sensor fusion and situation analysis block. After the targets are fused and the meaningless data are eliminated, the information about the remaining targets is sent to AEBS software and used by target object selection in AEBS. Vehicle speed, yaw rate, yaw angle, steering angle, and gear status information are received from the vehicle. Gear

status and vehicle speed signals are used to decide AEBS state transitions. In addition, the override and disabling signals that AEBS receives from the driver are also used in state transitions. With vehicle speed, yaw rate, yaw angle, steering angle information, the driving path of the subject vehicle is calculated.

The deceleration request which is calculated from AEBS is sent to the ESC component. The ESC component applies the braking which is requested by AEBS to the brakes as soon as possible. It is the duty of the ESC component to apply braking according to the reference deceleration demand of AEBS. Other outputs sent by AEBS are AEBS 'state values and collision warnings. On the HMI screen, a warning is given to inform the driver that AEBS is not working when the AEBS system is turned off. In addition, visual collision warnings are shown on the HMI screen to inform the driver about the risk of collision.

AEBS only deals with the longitudinal movement of the vehicle so, it does not make any lateral movement to avoid the accident. Autonomous emergency steering (AES) system makes an evasive maneuver, by controlling the lateral movement of the vehicle with steering, to prevent collision.

#### 4.2.1.1 Operating modes

AEBS has three main modes which are AEBS off, AEBS passive and AEBS active. Additionally, active system has 4 modes which are collision warning, speed reduction braking, mitigation braking, and overridden.

- AEBS off

  AEBS does not issue any countermeasure in the off state.

- AEBS passive

  In the AEBS passive state, AEBS monitors the vehicle speed, gear status, and checks the failure signal determined by self – check function. If the conditions are satisfied for enabling the AEBS, then the system transitions to the enabled state.

- AEBS active

  In this state, the AEBS system is able to issue any collision warnings or deceleration demand.

a) Collision Warning Substate: This is the default substate of the active state. In this state, the system monitors the driving path of the subject vehicle and is able to issue collision warnings.

b) Speed Reduction Braking Substate: The system transitions to this substate when the system is issuing a speed reduction braking.

c) Mitigation Braking Substate: When mitigation braking issued, the system transitions to mitigation braking substate.

d) Overridden Substate: The driver takes control by overriding the system. It means that any countermeasures are not issued by the system when the system is in overridden substate.

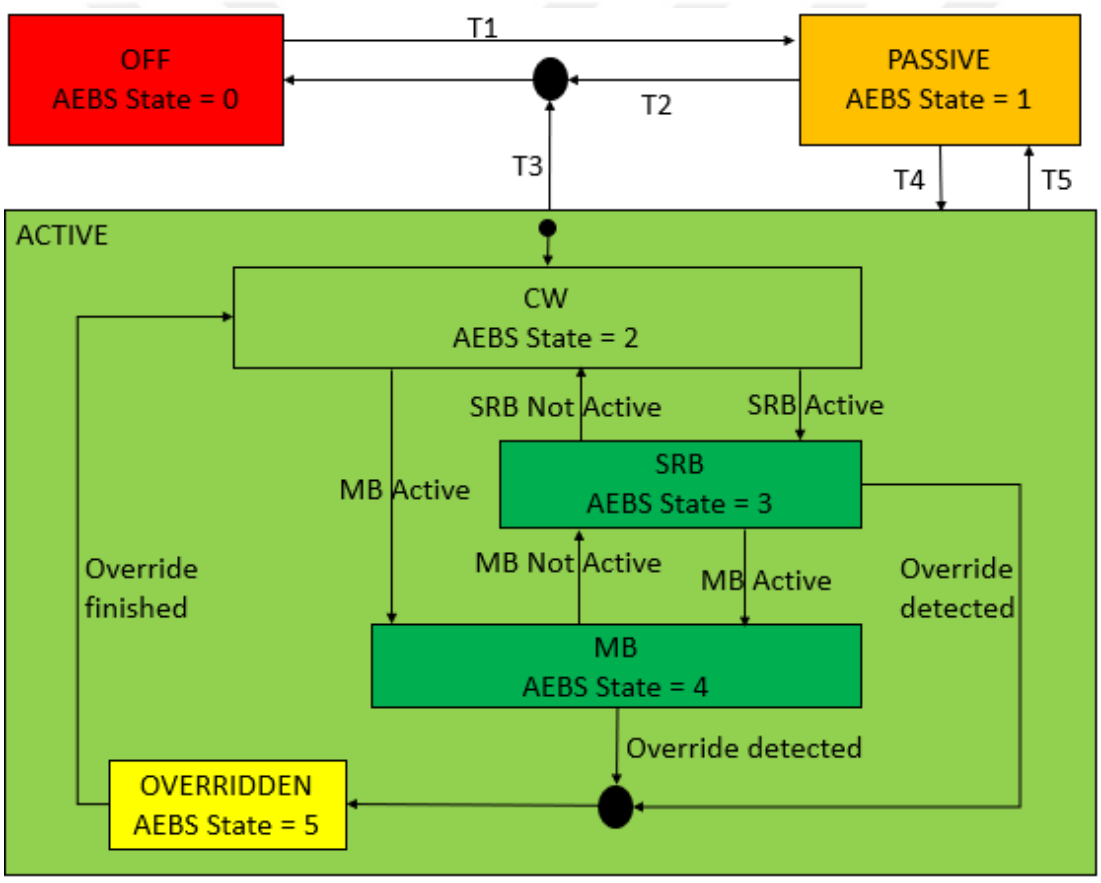


**Figure 4.6 :** AEBS state diagram.

AEBS function state transitions are explained below:

- Transition 1 (T1): If the ignition becomes on and any failure is not detected, then the system transitions from the off state to the passive state.

- Transition 2 (T2): If the ignition turns off or permanent failure is detected by self-check function or the driver disengages the AEBS system, then the system transitions from the passive state to the off state.
- Transition 3 (T3): If the ignition turns off or permanent failure is detected by self-check function or the driver disengages the AEBS system, then the system transitions from the active state to the off state.
- Transition 4 (T4): If the selected gear is any forward gear or neutral gear, the vehicle speed is greater than 10 $km/h$, and any failure is not detected, then the system transitions from the passive state to the active state.
- Transition 5 (T5): If the selected gear is reverse or the vehicle speed decreases under 10 $km/h$ or recoverable failure is detected by self-check function, then the system transitions from the active state to the passive state.

The state diagram of the AEBS system is shown in Figure 4.6.

### 4.2.2 AEBS functions

The main functions of AEBS are:

- Activation of AEBS: AEBS is activated every ignition time. Also, the driver uses on/off switch to reactivate when it was deactivated manually.
- Deactivation of AEBS: The driver uses on/off switch to deactivate AEBS manually.
- Issuing Collision warnings: AEBS gives collision warnings when the probability of collision is becoming high.
- Autonomous Braking: AEBS sends deceleration demand to reduce the collision energy or to avoid collision.
- Driver informing: Informs driver about the state of AEBS.
- TTC calculation: Determines the longitudinal distance and relative longitudinal velocity between target and subject vehicle. TTC is calculated based on that data.

### 4.2.3 Potential consequences of behavioral shortfalls

Unintended deceleration and loss of deceleration are malfunctions that are related with AEBS. The consequences of that malfunctions are rear – end or front – end collisions with other traffic objects.

### 4.2.4 Interaction with other items or elements

AEBS need to take some signals from other inputs. Following signals are necessary for AEBS:

- Vehicle speed: Vehicle speed is used to enable the system. In addition, in case of an accident that may occur at high speeds, the vehicle becomes difficult to control and the severity of the accident becomes high.
- Steering angle: Steering angle is used to determine the driving path of the vehicle. Objects which are inside the driving path selected as target. Also, the steering angle can be used to override the system.
- Current gear number: The gear number is used for state transitions.
- Ignition status: The ignition signal is used to enable the system.
- ABS: The subject vehicle shall be equipped with anti-lock brake system (ABS). As soon as ABS becomes active or ABS detects a failure, the AEBS transitions to off state. Since AEBS will be turned off when ABS is activated, we can say that ABS has priority.
- ESC: As soon as ESC becomes active or ESC detects a failure, the AEBS transitions to off state. Also, AEBS sends a deceleration request to the ESC component, then the ESC component apllies braking according to demand of AEBS.

### 4.2.5 Interaction with the environment

- Radius: Curve radius shall be higher than 125 $m$ for AEBS to work correctly.
- Weather conditions: The Camera and Lidar sensors are highly affected by bad weather conditions such as snow, fog, or rain.
- AEBS is not designed for land use according to ISO 22839.

- If the vehicle is driven on rural, highway, or city roads and in case of a possible accident, the severity of the accident in these places will be different. Therefore, when performing the HARA analysis, the places where the accident occurred are also important in determining the severity level.

### 4.2.6 Interaction with driver

- Right/left turn signal status: Those signals are used to determine the driver override request.
- Accelerator pedal position: That signal is used to determine the driver override request.

**Table 4.3 :** Input and output signals of AEBS.

| Signal Name | R/T | Source of Signal |
|---|---|---|
| ABS status | R | ABS ECU |
| Accelerator pedal kick down | R | Transmission Control Unit (TCU) |
| Accelerator pedal percentage | R | Transmission Control Unit (TCU) |
| Brake pedal percentage | R | ABS ECU |
| AEBS disabling button | R | HMI |
| Hand brake status | R | HMI |
| Gear status | R | Transmission Control Unit (TCU) |
| ESC status | R | ESC ECU |
| Turn indicator signals status | R | HMI |
| Seat belts fastened status | R | HMI |
| Doors closed status | R | Door Control Unit (DCU) |
| Steering angle | R | ESC ECU |
| Yaw angle | R | ESC ECU |
| Yaw rate | R | ESC ECU |
| Vehicle speed | R | Vehicle Control Unit (VCU) |
| Vehicle acceleration | R | Vehicle Control Unit (VCU) |
| Ignition status | R | Vehicle Control Unit (VCU) |
| ACC braking request | R | ACC Software |
| Sensor’s failure status | R | Radar/Camera/Lidar Sensors |
| Distance to target | R | Radar/Camera/Lidar Sensors |
| Relative speed | R | Radar/Camera/Lidar Sensors |
| Relative acceleration | R | Radar/Camera/Lidar Sensors |
| Target classification | R | Radar/Camera/Lidar Sensors |
| Target dynamic property | R | Radar/Camera/Lidar Sensors |
| AEBS state | T | AEBS Software |
| AEBS collision warning level | T | AEBS Software |
| AEBS deceleration demand | T | AEBS Software |
| AEBS intervention number | T | AEBS Software |
| AEBS failure status | T | AEBS Software |

- Brake pedal position: The driver can increase braking demand with the brake pedal while AEBS sends deceleration demand. Additionally, the brake pedal position is used to delay the collision warnings. If the driver applies brake before collision warnings are given, then the collision warnings are delayed.
- AEBS sends the AEBS status and collision warning level signal to HMI in order to inform the driver.
- Disabling button: AEBS can be disabled by the driver with the disabling button. Also, the system can be activated again by the driver.

The input and output signals that are required in the development of the AEBS system are displayed in Table 4.3. R means received and T means transmitted which are used in Table 4.3. AEBS software can be developed independently from other components using these signals.

## 4.3 Hazard Analysis and Risk Assessment of AEBS

Recommendations on how to perform Hazard Analysis and Risk Assessments (HARA) according to ISO 26262 have published by the German Automotive Industry Association (VDA). Specifically, the VDA 702 "Situations catalog: E-Parameter nach ISO 26262-3" is a situation catalog with methodological guidance on the allocation of exposure (E) parameters [59]. In this situation catalog, conditions based on duration and frequency of exposure parameters are mentioned. While conducting HARA analysis, the scenarios and the exposure values of these scenarios were determined according to this catalog. HARA tables are given in Appendix B.

## 4.4 Functional Safety Concept

### 4.4.1 Safety goal 1: prevent loss of collision warnings (B)

- Background of safety goal

  Collision warnings are issued before autonomous braking to warn the driver of the potential risk of collision. If collision warnings are not given by the system, the driver may be late to brake, which increases the possibility of an accident.

  The safe state of this safety goal is defined as “Collision warnings shall be given if it is necessary”. The Fault Tolerant Time Interval (FTTI) shall be

determined for each safety goal according to ISO 26262 and the definition of FTTI is done in Appendix C. The FTTI value is determined as 250 ms for safety goal 1 according to [60].

- Functional safety requirement

  FSR 1: If AEBS collision warnings are lost due to any reason, then the ADAS ECU shall detect that loss of collision warnings.

### 4.4.2 Safety goal 2: prevent unintended collision warnings (B)

- Background of safety goal

  Collision warnings are given before the autonomous braking when they are necessary. The driver can brake due to unintended collision warnings and this braking can cause accidents with rear vehicles.

  The safe state of this safety goal is defined as “Driver shall be warned only when required”. The FTTI value is determined as 250 ms for safety goal 2 by considering [60].

- Functional safety requirement

  FSR 2: As long as AEBS gives unintended collision warnings due to any reason, the ADAS ECU shall classify that warning as an unintended warning and the driver shall not be warned about AEBS status. Driver shall be warned only when required.

### 4.4.3 Safety goal 3: prevent unintended vehicle deceleration (C)

- Background of safety goal

  Unintended deceleration request of the AEBS system can cause accidents. Vehicles behind can collide with the subject vehicle due to unintended deceleration request.

  The safe state of this safety goal is defined as “Unintended deceleration shall be limited”. The FTTI value is determined as 250 ms for safety goal 3 taking into account the [60].

- Functional safety requirement

  FSR 3: If AEBS issues unintended deceleration demand due to any reason, then unintended deceleration demand shall be detected by ADAS ECU and the system shall limit the deceleration demand. Braking demand shall be given only when required.

### 4.4.4 Safety goal 4: prevent loss of vehicle deceleration (B)

- Background of safety goal

  As long as the system requests less deceleration demand or does not request deceleration demand, the accident becomes unavoidable with the front target.

  The safe state of this safety goal is defined as “The braking system shall issue the braking request of AEBS”. The FTTI value is determined 250 ms for safety goal 4 by considering [60].

- Functional safety requirement

  FSR 4: If AEBS deceleration demand losses, then loss of deceleration shall be detected by ADAS ECU.

# 5. SIMULATION RESULTS

## 5.1 TORCS Simulation Environment

Firstly, ADAS functions are first tested in simulation environments, thus it is checked whether there is any error in the related function during development phase. This test method is called Model-in-the Loop (MIL) and that tests are performed before Hardware-in-the Loop (HIL) or vehicle tests, so that money and time are saved. Therefore, simulation environments are important and widely used in ADAS testing.

For testing, simulation environment which is called The Open Racing Car Simulator (TORCS) is used. That test platform is flexible for environment and vehicle characteristic settings also simulation environment is realistic.


**Figure 5.1:** TORCS environment**.**

TORCS has a lot of advantages in terms of different simulation environments such as vehicle dynamics, collision effects, brake lights, mark of skid, and tire stiffness [61].

TORCS simulation environment is an open-source platform based on General Public License (GPL) [62]. Figure 5.1 shows a screenshot from the TORCS simulation environment.

### 5.1.1 Installation of TORCS

Downloading and installation of TORCS shall be done according to its website [62]. That website introduces the installation procedure in the following order:

- Firstly, the source package which is “torcs-1.3.7.tar.bz2” is downloaded. Download link is available on the website [62].
- The source package “torcs-1.3.7.tar.bz2” is unpacked.
- Command prompt (cmd) is opened, then “torcs-1.3.7” shall be selected as the working directory.
- The command “setup_win32.bat” is run.
- The command “setup_win32-data-from-CVS.bat” is run.
- Microsoft Visual Studio 2008 is used to open the “TORCS.sln” file.
- TORCS project and the win32-Release (win32-Debug) version is selected.
- The project is compiled without any warnings.
- The "wtorcs.exe" is run.

### 5.1.2 Matlab/Simulink interface

Matlab/Simulink is able to communicate and control the vehicles on TORCS platform. In order to communicate TORCS and Matlab/Simulink, communication interface installation shall be done from webpage [63].

Following steps shall be applied to interface setup:

- Firstly, “TORCSLink” shall be downloaded from webpage [63].
- Files is copied to under “src/drivers” folder on command window with “git clone https://github.com/VerifiableAutonomy/TORCSLink.git”.
- Project, which is “matlab.vcxproj”, is added to TORCS solution.

- In “TORCSLink.h”, TL_USE_DOUBLE_POSITION and TL_ENABLE_RESTARTS features shall be commended out by the #define lines in order to do the first initialization.
- The project is compiled without any warnings.

Thanks to this interface, up to 10 vehicles can be controlled simultaneously in the TORCS environment with Matlab/Simulink. Also, the sampling time of the interface is 0.02 seconds due to TORCS environment data sampled every 0.02 seconds. Data such as position, speed, and acceleration of all vehicles can be read, thus relative speed and distance information between two vehicles can be calculated.

As it is displayed in Figure 5.2, Matlab 1 vehicle reads its data signals from bus signal. Then in the controller subsystem, controllers are designed to control the vehicle’s steering and speed according to lateral and velocity references. Gear, throttle, brake, and steering signals are assigned with bus assigned block and sent to TORCS simulator.

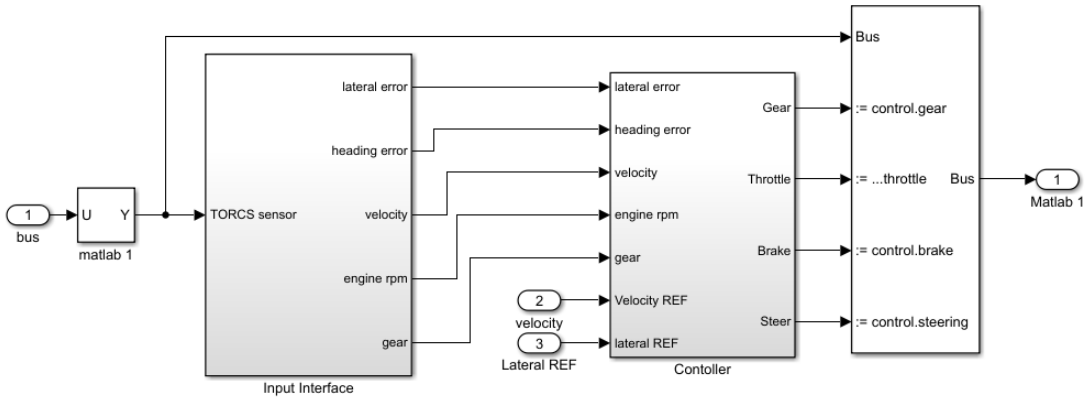


**Figure 5.2 :** TORCS Bus Assignment.

In Table 5.1, sensor signals, which are taken from TORCS environment, are shown. Controller signals, which are sent to TORCS environment, are displayed in Table 5.2.

## 5.2 Test Scenarios

UNECE Regulation No 152: 2020 [9] describes the test conditions of the AEBS function and how the test should be performed. This regulation specifies separate test scenarios and passing conditions for moving vehicle targets, stationary vehicle targets and pedestrian targets. Since pedestrian tests cannot be performed in the TORCS

simulation environment, pedestrian tests are excluded from the scope of this thesis. The tests for the moving vehicle target are described separately in the part 5.2.1

**Table 5.1 :** Sensor signals from TORCS environment.

| Name of signal | Description | Unit |
|---|---|---|
| Gear | Current gear of the vehicle | - |
| Velocity | Current velocity of the vehicle. 3 axis velocity information available. | $[m/s]$ |
| Heading error | Error between heading of vehicle and heading of track. | [rad] |
| Angle | Angle of the vehicle. Roll, Pitch, and Yaw angles are available. | [rad] |
| Position | Global position of the vehicle. Angle of the vehicle. Roll, Pitch, and Yaw angles are available. | $[m]$ |
| Lateral error | Distance error between car position and track axis position | $[m]$ |
| Acceleration | Current acceleration of the vehicle. 3 axis acceleration information available. | $[m/s^2]$ |

**Table 5.2 :** Controller signals which are sent to TORCS environment.

| Name of signal | Description | Range |
|---|---|---|
| Throttle | Throttle of the vehicle | [0,1] |
| Steering | Steering command of the vehicle. -1 means full right turn and 1 means full left turn | [-1,1] |
| Gear | Gear command of the vehicle. -1 means reverse gear, 0 means neutral gear, and 6 is maximum gear. | [-1,6] |
| Brake | Brake command of the vehicle. 0 means no brake request and 1 means full brake request. | [0,1] |

### 5.2.1 Moving target test scenarios

The moving target and the ego vehicle must move on a straight road and in the same direction. While these vehicles are moving, they should move with their midpoints aligned or with a maximum error of 0.2 $m$.

#### 5.2.1.1 Test 1: Ego vehicle velocity is 60 $km/h$

For this test scenario, the ego vehicle moves at 60±2 $km/h$ and the target vehicle is moving a velocity of 20±2 $km/h$ speed [9]. As it can be seen in Figure 5.6, the speed of the ego vehicle is around 16.65 $m/s$, in other words 60 $km/h$, before the AEBS function is activated. Since the relative speed with the target vehicle is -11.1 $m/s$, the speed of the target vehicle is 5.55 $m/s$, that is 20 $km/h$.

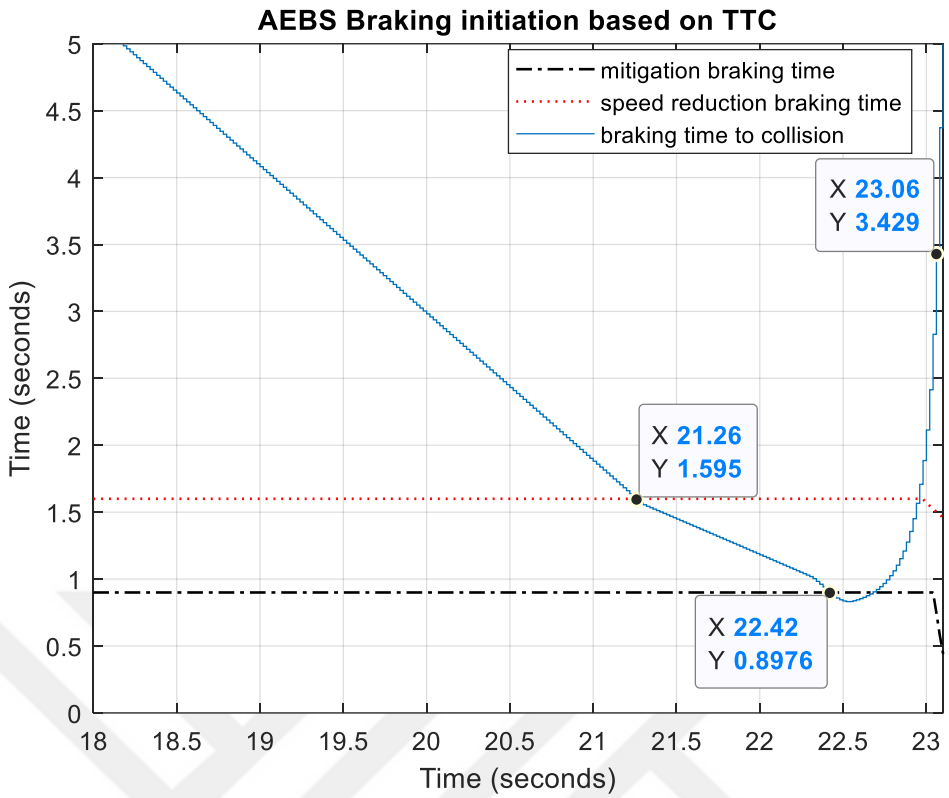


**Figure 5.3 :** Decision making for test 1 based on TTC braking time, collision risk judgment, and collision judgment values.

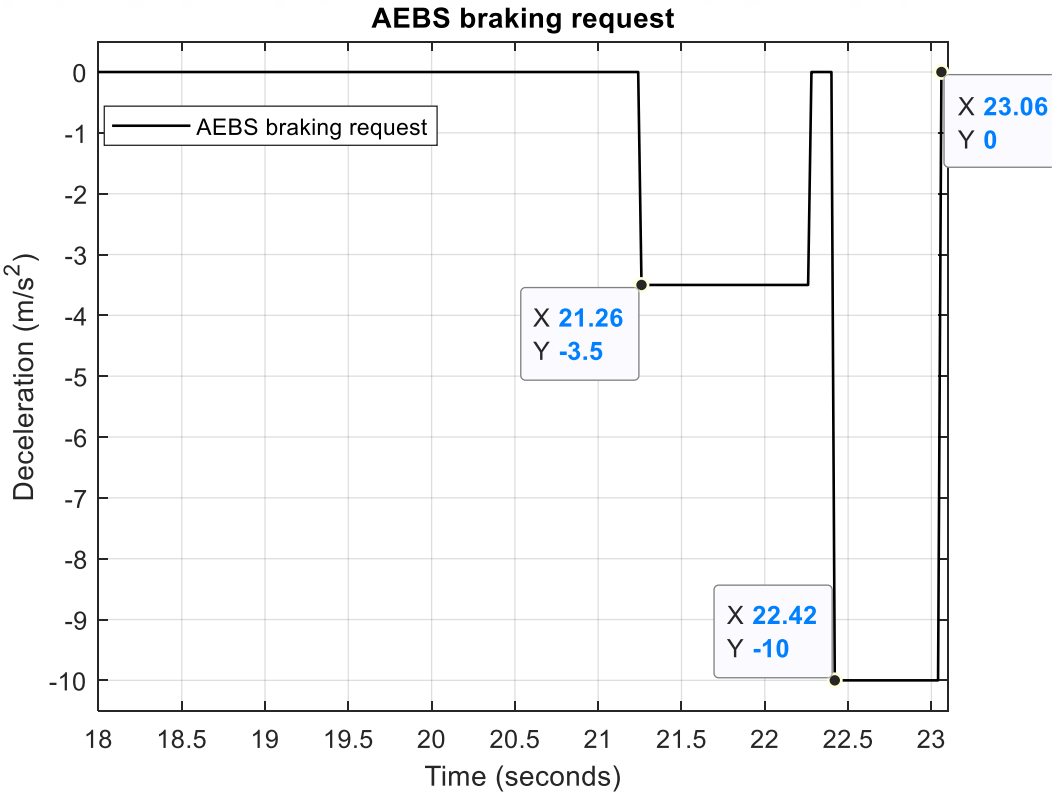


**Figure 5.4 :** Autonomous braking for test 1.

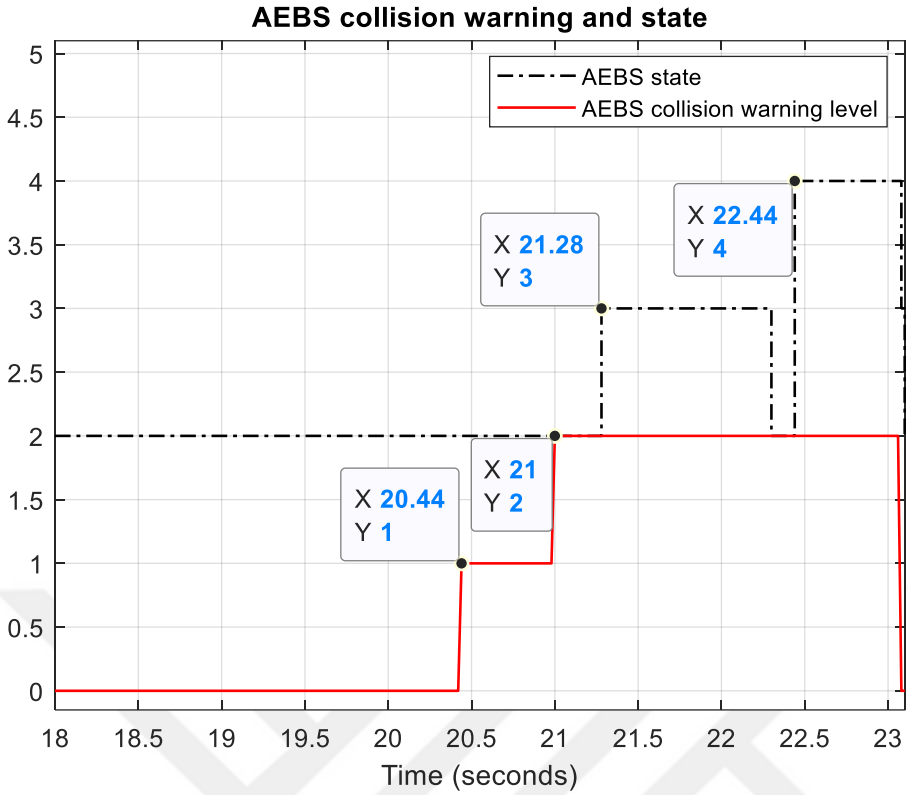


**Figure 5.5 :** AEBS state and collision warning levels for test 1.

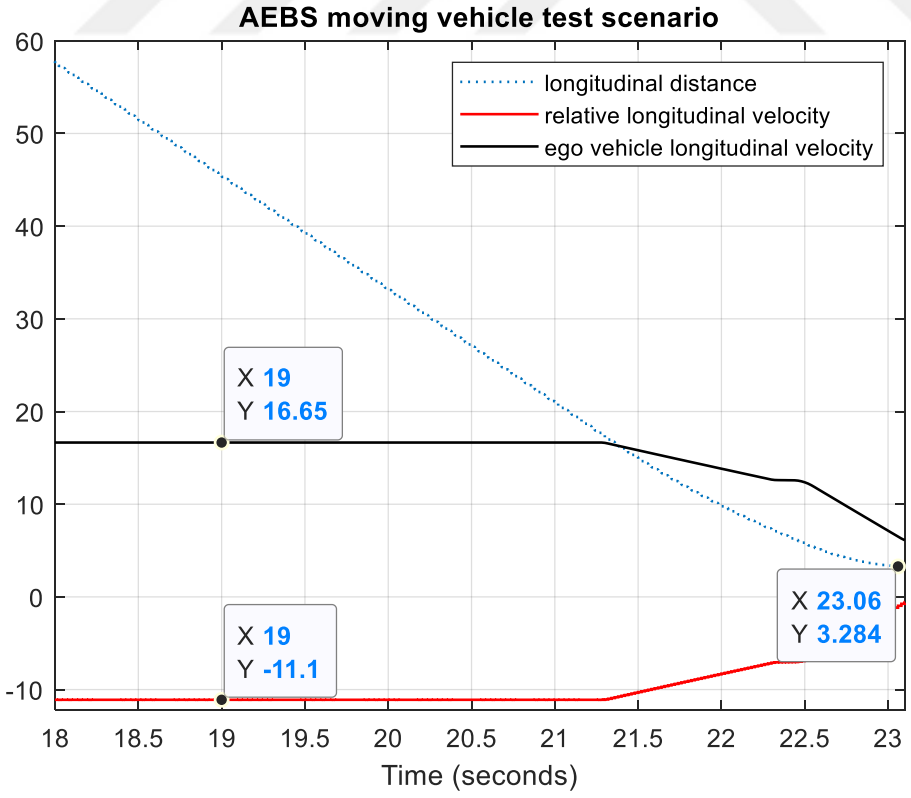


**Figure 5.6 :** Distance, relative velocity, and SV speed information for test 1.

Figure 5.4 shows the acceleration values demanded by AEBS. While the acceleration value of speed reduction braking is -3.5 $m/s^2$, the value of mitigation braking is -10 $m/s^2$. The braking Time to Collision value as well as the initiating time values of mitigation braking and speed reduction braking are displayed in Figure 5.3. In Figure 5.3, at time 21.26 seconds, the braking Time to Collision value becomes lower than the speed reduction braking time value and speed reduction braking started at the same time as shown in Figure 5.4. Moreover, in Figure 5.3, at time 22.42 seconds, the braking Time to Collision value becomes lower than the mitigation braking time value and mitigation braking started at the same time as shown in Figure 5.4.

Figure 5.5 shows the collision warning levels and AEBS state values. At 20.44 seconds, the first level of collision warning is given, and at time 21 seconds, the second level of collision warning is given. One of the conditions for passing the test is that at least 2 collision warnings shall be given 0.8 seconds before the start of mitigation braking. The satisfaction of this condition is approved by Figure 5.5. As it can be seen in Figure 5.5, since speed reduction braking starts at time 21.26 seconds, the AEBS state value becomes 3 at time 21.28 seconds. Here, state 3 indicates that AEBS is in the speed reduction braking phase. Also, since mitigation braking starts at time 22.42 seconds, the AEBS state value becomes 4 at time 22.44 seconds. Here, state 4 indicates that AEBS is in the mitigation braking phase.

As indicated in Figure 5.6, the distance between the target vehicle and the ego vehicle at the end of mitigation braking is 3.28 $m$. As a result, the accident is prevented and the test has passed.

#### 5.2.1.2 Test 2: Ego vehicle velocity is 30 $km/h$

For this test scenario, the ego vehicle is moving with speed of 30±2 $km/h$ and the target vehicle is moving with speed of 20±2 $km/h$ speed [9]. As it is shown in Figure 5.10, the speed of the ego vehicle is around 8.32 $m/s$, in other words 30 km/h, before the AEBS function is activated. Since the relative speed with the target vehicle is -2.77 $m/s$, the speed of the target vehicle is 5.55 $m/s$, that is 20 $km/h$.

Figure 5.8 shows the braking Time to Collision value as well as the initiating time values of mitigation braking and speed reduction braking. In Figure 5.7, at time 60.24 seconds, the braking Time to Collision value becomes lower than the speed reduction braking time value and speed reduction braking started at the same time as displayed

in Figure 5.8. For this scenario, AEBS does not issue mitigation braking because speed reduction braking is enough for speed reduction of the ego vehicle that as seen in Figure 5.8.

Figure 5.9 shows the collision warning levels and AEBS state values. At 59.32 seconds, the first level of collision warning is given, and at time 59.92 seconds, the second level of collision warning is given.

As it can be seen in Figure 5.9, since speed reduction braking starts at time 60.24 seconds, the AEBS state value becomes 3 at time 60.26 seconds. Here, 3 indicating that AEBS is in the speed reduction braking phase.

According to Figure 5.10, the distance between the target vehicle and the ego vehicle at the end of speed reduction braking is 3.25 $m$. As a result, the accident is prevented and the test has passed.

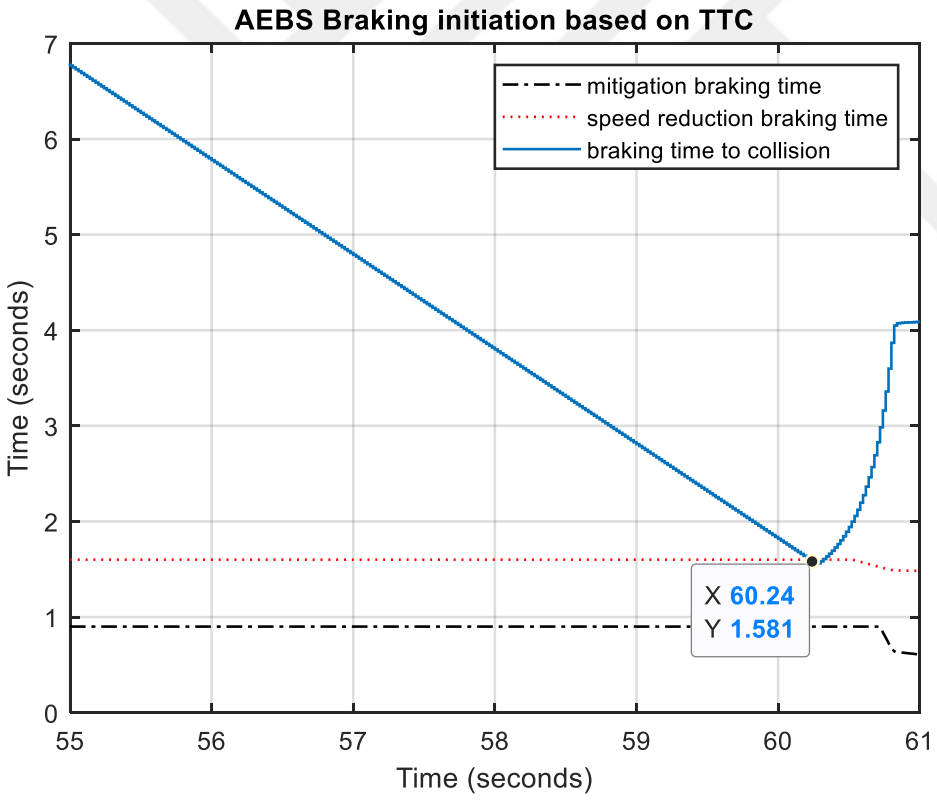


**Figure 5.7 :** Decision making for test 2 based on TTC braking time, collision risk judgment, and collision judgment values.

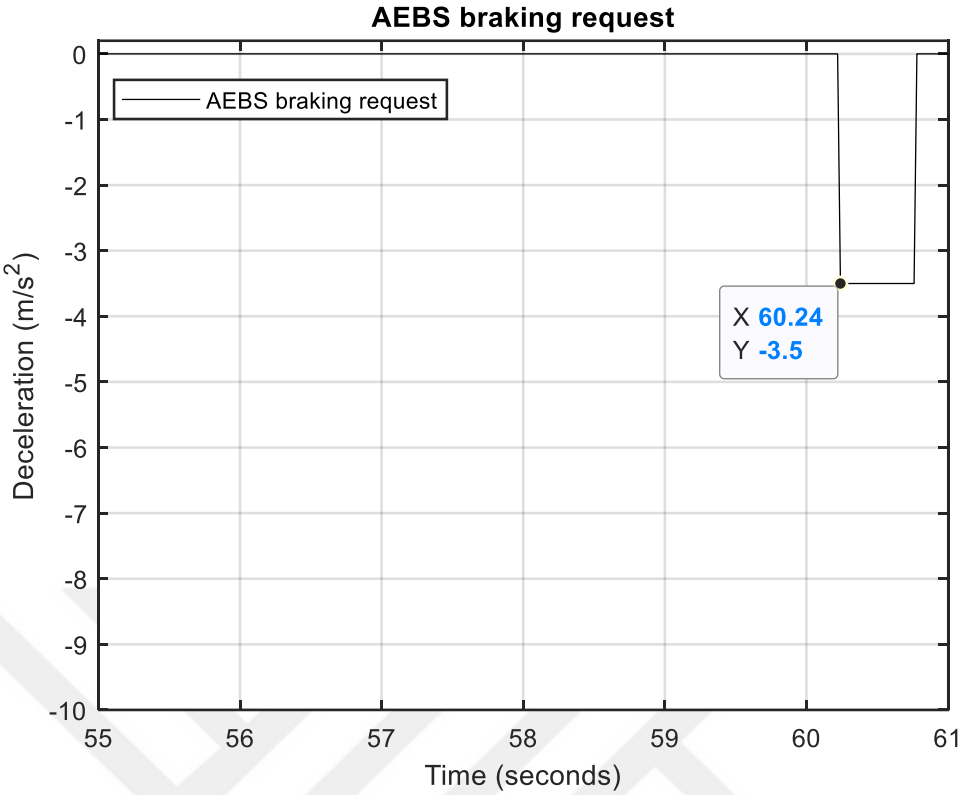


**Figure 5.8 :** Autonomous braking for test 2.

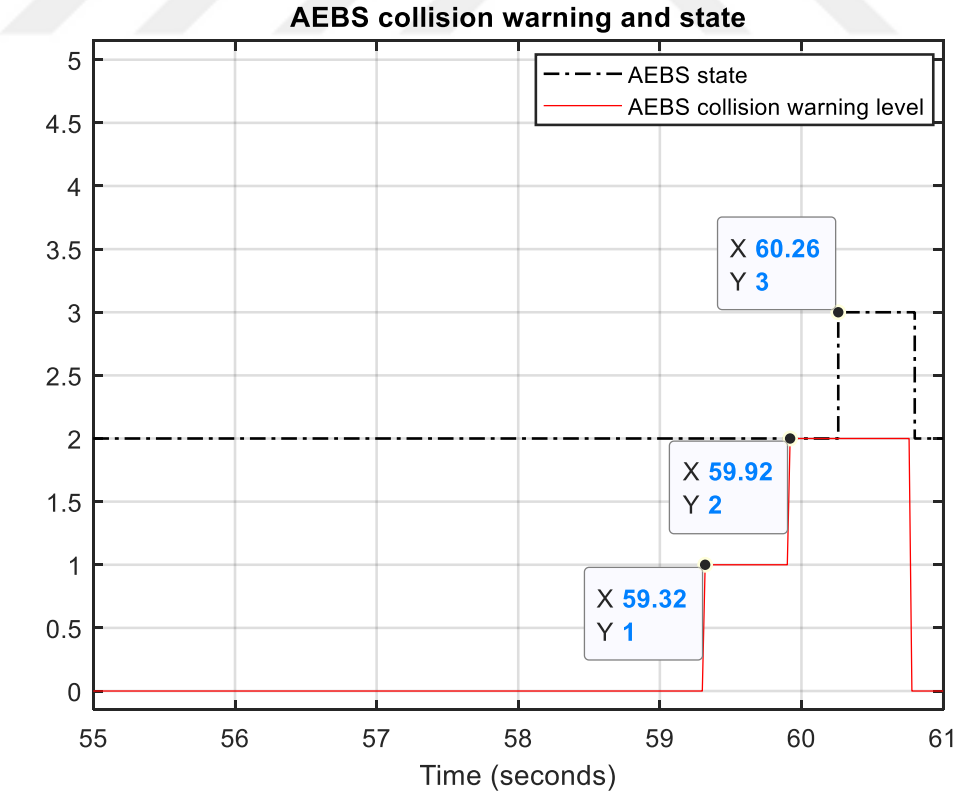


**Figure 5.9 :** AEBS state and collision warning levels for test 2.

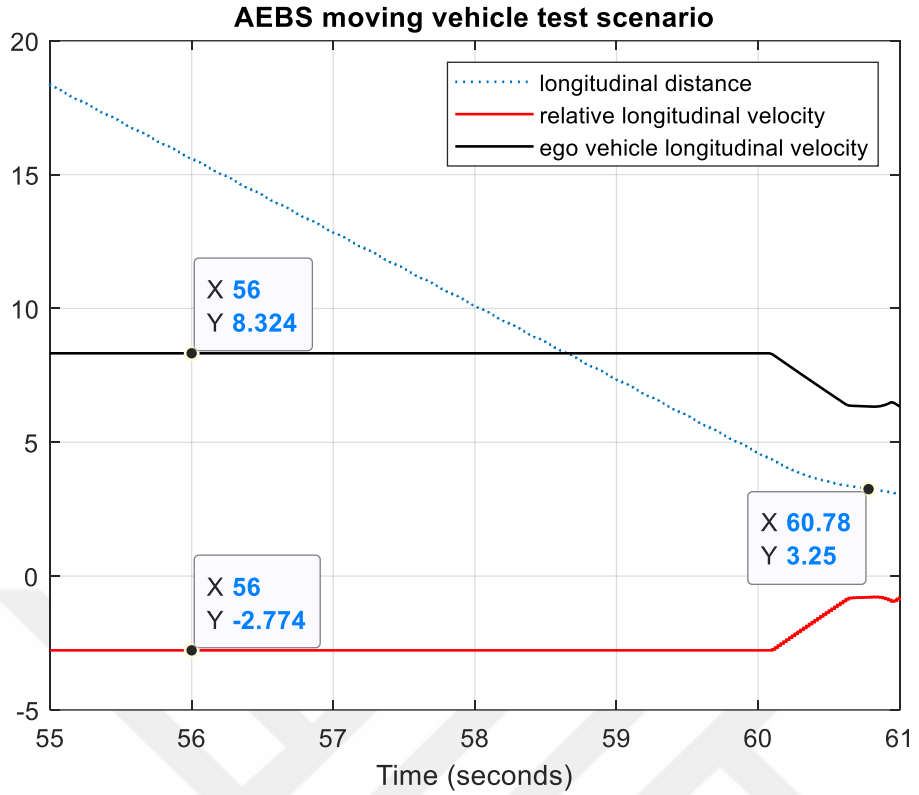


**Figure 5.10 :** Distance, relative velocity, and SV speed information for test 2.

### 5.2.2 AEBS disabling and reactivated test

According to UNECE Regulation No 152: 2020, if the AEBS system has the feature of turning off the system, the system shall be turned off at speed below 10 $km/h$. In addition, the driver shall be turn off the system with at least two deliberate movements while trying to turn off the system. These tests are carried out as seen in Figure 5.11 and Figure 5.12. In Figure 5.11, while the vehicle is moving at a speed of 8 $km/h$ (2.42 $m/s$), the disabling button is pressed in 2.02 and 2.44 seconds consecutively. As seen in Figure 5.11, when the disabling signal is true for the second time, the AEBS state becomes 0 (off). As displayed in Figure 5.11, when the AEBS state is off at time 8 seconds, by pressing the disabling button again, the AEBS system has been turned on and the state has become 1 (passive). In this case, deactivation and activation tests have successfully passed.

In Figure 5.12, while the vehicle is moving at a speed of 20 $km/h$ (5.34 $m/s$), the disabling button is pressed in 2.02 and 2.44 seconds consecutively. As illustrated in Figure 5.12, when the disabling signal is true for the second time, the AEBS state is not changed. In this case, the deactivation test has successfully passed.

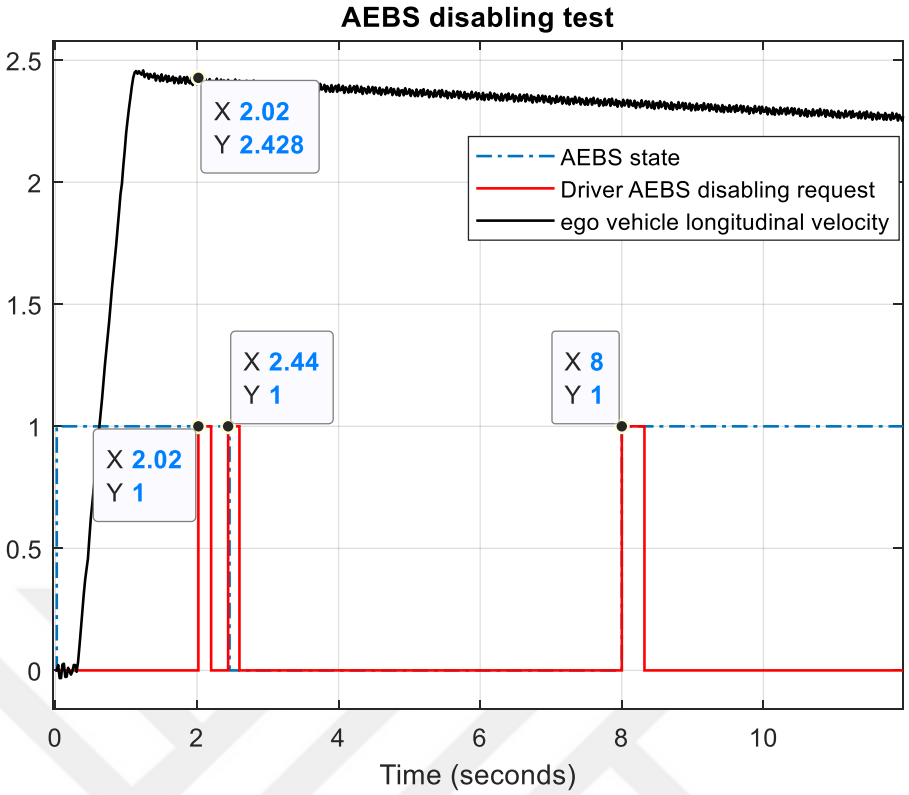


**Figure 5.11 :** AEBS deactivation test while vehicle velocity is under 10 $km/h$.

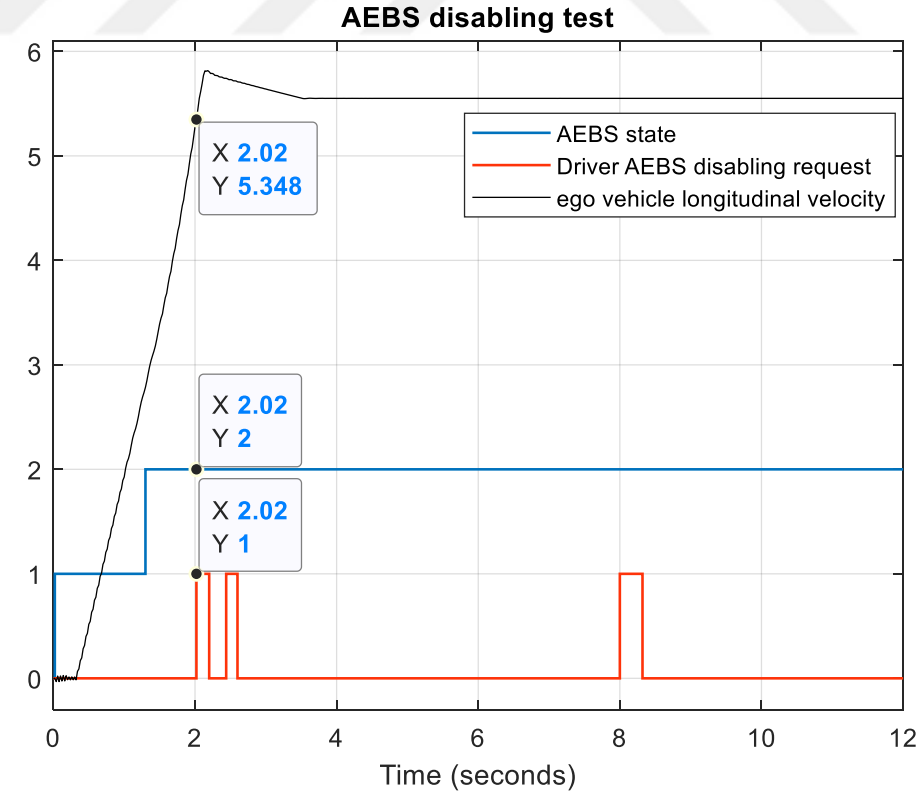


**Figure 5.12 :** AEBS deactivation test while vehicle velocity is higher than 10 $km/h$.

# 6. CONCLUSIONS AND RECOMMENDATIONS

Basically, two purposes have been achieved in this thesis. The first aim was to realize the AEBS software in accordance with the standards. The test phase of the AEBS software was carried out in the TORCS simulation environment and as seen in the results, accidents were prevented in rear-end collision scenarios. In addition, two warnings are given before mitigation braking, as specified in the standards.

The second goal was to perform functional safety analysis for AEBS according to ISO 26262 Part 3: concept phase. At this stage, the item definition of AEBS, HARA analysis, and functional safety concept phase were done.

In this thesis, no calculation has been made for FTTI, which must be determined for safety goals. FTTI values were created inspired by academic studies. The future work will be finding a method for calculating FTTI. In addition, the determination of technical safety requirements to be derived from functional safety requirements is among the future studies.

In this thesis, functional safety software was not developed, only L1 AEBS software was developed. L1 software is not functional safety-related software, it is only based on AEBS related regulations and standards. In other words, ISO 26262 is not considered in L1 software. Future work includes implementing L2 AEBS functional safety software for AEBS. At this stage, it will be considered in cases where a failure occurs, but the hardware does not generate a failure signal. Failure that occurs in this way is called dangerous undetected failure. To give an example, when a failure occurs in the ABS ECU and the failure is detected, the Level 1 AEBS software system will turn off AEBS. However, in cases where ABS has a failure and the ABS ECU does not generate a failure signal, that is, in dangerous undetected situations, L1 AEBS will think that there is no error in the system and will continue to operate normally. A dangerous undetected failure in the ABS ECU will be detected by the L2 AEBS functional safety software and the L2 AEBS functional safety software will prevent the working of AEBS. In this way, the driver will be informed that the AEBS is not working and the driver will be aware of the situation.

## REFERENCES


[1] **Url-1** < *https://unece.org/press/un-regulation-advanced-emergency-braking-systems-cars-significantly-reduce-crashes*>, date retrieved 25.02.2021.

[2] **Url-2** < *https://www.nhtsa.gov/press-releases/10-automakers-equipped-most-their-2018-vehicles-automatic-emergency-braking*>, date retrieved 20.02.2021.

[3] **International Organization for Standardization**. (2013). ISO 22839: 2013. Forward Vehicle Collision Mitigation Systems – Operation, performance, and verification requirements.

[4] **International Organization for Standardization.** (2013). ISO 15623: 2013. Intelligent transport systems—Forward vehicle collision warning systems—Performance requirements and test procedures.

[5] **International Organization for Standardization.** (2017). ISO 19237: 2017. Intelligent transport systems — Pedestrian detection and collision mitigation systems (PDCMS) — Performance requirements and test procedures.

[6] **International Organization for Standardization.** (2017). ISO 19377: 2017. Heavy commercial vehicles and buses - Emergency braking on a defined path - Test method for trajectory measurement.

[7] **International Organization for Standardization.** (2020). ISO 22078: 2020. Intelligent transport systems - Bicyclist detection and collision mitigation systems (BDCMS) - Performance requirements and test procedures.

[8] **The United Nations Economic Commission for Europe.** (2013). Addendum 130: UN Regulation No. 131. Uniform provisions concerning the approval of motor vehicles with regard to the Advanced Emergency Braking Systems (AEBS).

[9] **The United Nations Economic Commission for Europe.** (2020). Addendum 151: UN Regulation No. 152 Uniform provisions concerning the approval of motor vehicles with regard to the Advanced Emergency Braking System (AEBS) for M1 and N1 vehicles.

[10] **Commission Regulation (EU).** (2012). No 347/2012 .Implementing Regulation (EC) No 661/2009 of the European Parliament and of the Council with respect to type-approval requirements for certain categories of motor vehicles with regard to advanced emergency braking systems.

[11] **Euro, N. C. A. P.** (2019). Test Protocol - AEB Car-to-Car systems v3.0.2.

[12] **Euro, N. C. A. P.** (2020). Test Protocol - AEB VRU systems v3.0.3.

[13] **Euro, N. C. A. P.** (2020). Assessment Protocol - SAFETY ASSIST - Version 9.0.3.

[14] **Euro, N. C. A. P.** (2020). Assessment Protocol - VULNERABLE ROAD USER PROTECTION - Version 10.0.3.

[15] **AUSTRALASIAN, N. C. A. P.** (2020). Test Protocol. AEB Car-to-Car Systems v3.0.2.

[16] **AUSTRALASIAN, N. C. A. P.** (2020). Test Protocol. AEB Vulnerable Road User Systems v3.0.3.

[17] **AUSTRALASIAN, N. C. A. P.** (2020). Assessment Protocol. Safety Assist v9.0.3.

[18] **AUSTRALASIAN, N. C. A. P.** (2020). Assessment Protocol. Vulnerable Road User Protection v10.0.3.

[19] **SAE International, Standards**. (2017). SAE J3087: Automatic Emergency Braking Performance Testing.

[20] **Url-3** < *https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety#topic-road-self-driving*>, date retrieved 10.02.2021.

[21] **Url-4** < *https://global.toyota/pages/news/older/images/2003/02/17/20030217_01_en.pdf*>, date retrieved 25.05.2021.

[22] **Url-5** < *https://global.honda/newsroom/news/2003/4030520-eng.html* >, date retrieved 5.04.2021.

[23] **Url-6** < *https://www.sae.org/news/2019/01/sae-updates-j3016-automated-driving-graphic*>, date retrieved 10.01.2021.

[24] **Url-7** < *https://media.daimler.com/marsMediaSite/en/instance/ko/PRE-SAFE-brake-world-premiere-of-the-first-autonomous-braking-system-Automatic-partial-braking-before-impending-rear-end.xhtml?oid=9905452*>, date retrieved 24.03.2021.

[25] **Url-8** < *https://media.daimler.com/marsMediaSite/en/instance/ko/PRE-SAFE-brake-latest-Mercedes-innovation-for-safety-on-the-road-S-Class-brakes-automatically-when-faced-with-acute-risk-of-accident.xhtml?oid=9905229*>, date retrieved 24.03.2021.

[26] **Url-9** < *http://ophelia.sdsu.edu:8080/ford/10-21-2008/innovation/car-safety/helping-avoid-accidents/european-safety-systems/eu-vehicle-safety-350p.html*>, date retrieved 25.05.2021.

[27] **Url-10** < *https://www.media.volvocars.com/global/en-gb/media/pressreleases/12129*>, date retrieved 25.05.2021.

[28] **Url-11** < *https://media.lexus.co.uk/2006/08/lexus-ls-460-achieves-world-first-in-preventive-safety/*date retrieved 25.05.2021.

[29] **Jansson, J., Johansson, J., & Gustafsson, F. (**2002). Decision making for collision avoidance systems. SAE Transactions, 197-204.

[30] **Nitsche, B., & Schulz, R.** (2004). Automotive Applications for the ALASCA Laser Scanner. In Advanced Microsystems for Automotive Applications 2004 (pp. 119-136). Springer, Berlin, Heidelberg.

[31] **Moxey, E., Johnson, N., McCarthy, M. G., & McLundie, W. M.** (2005). Advanced protection for vulnerable road users (No. 2005-01-1870). SAE Technical Paper.

[32] **Chitnis, K., Mody, M., Swami, P., Sivaraj, R., Ghone, C., Biju, M. G., ... & Dubey, A.** (2017). Enabling functional safety ASIL compliance for autonomous driving software systems. Electronic Imaging, 2017(19), 35-40..

[33] **International Organization for Standardization.** (2018). ISO 26262-3:2018. Road vehicles — Functional safety — Part 3: Concept phase.

[34] **Sari, B.** (2020). Fail-operational Safety Architecture for ADAS/AD Systems and a Model-driven Approach for Dependent Failure Analysis. Springer Nature.

[35] **Violante, M., & Gnaniah, R.** (2019). Functional Safety Assessment for Advanced Driver Assistance System.

[36] **Fürst, S., & Bunzel, S.** (2016). AUTOSAR and Driver Assistance Systems. In H. Winner, S. Hakuli, F. Lotz, & C. Singer (Eds.), Handbook of Driver Assistance Systems: Basic Information, Components and Systems for Active Safety and Comfort (pp. 133–155). Springer International Publishing. https://doi.org/10.1007/978-3-319-12352-3_7

[37] **Url-12** < *https://automotivetechis.wordpress.com/autosar-concepts/*>, date retrieved 25.02.2021.

[38] **AUTOSAR.** (2017). Explanation of Application Interfaces of the Chassis Domain AUTOSAR CP Release 4.3.1.

[39] **Rajamani, R.** (2006). Vehicle Dynamics and Control, Springer.

[40] **Lath, U., Kakkar, S., Agarwal, A., Ashok, B., Babu, V. R., Ashok, S. D., & Kavitha, C.** (2019). Modelling and Validation of a Control Algorithm for Yaw Stability & Body Slip Control Using PID & Fuzzy Logic Based Controllers (No. 2019-28-0054). SAE Technical Paper.

[41] **Blundell, M., & Harty, D.** (2015). Chapter 5 - Tyre Characteristics and Modelling. In M. Blundell & D. Harty (Eds.), *The Multibody Systems Approach to Vehicle Dynamics (Second Edition)* (Second Edition, pp. 335–450). Butterworth-Heinemann. https://doi.org/https://doi.org/10.1016/B978-0-08-099425-3.00005-4

[42] **Jazar, R. N.** (2017). Vehicle dynamics: theory and application. Springer.

[43] **Directive 2007/46/EC of the European Parliament and of the Council** (2007) Official Journal of the European Union.

[44] **Coelingh, E., Eidehall, A., & Bengtsson, M**. (2010, September). Collision warning with full auto brake and pedestrian detection-a practical example of automatic emergency braking. In 13th International IEEE Conference on Intelligent Transportation Systems (pp. 155-160). IEEE.

[45] **Grover, C., Knight, I., Okoro, F., Simmons, I., Couper, G., Massie, P., & Smith, B.** (2008). Automated emergency brake systems: Technical requirements, costs and benefits (TRL Published Project Report PPR

227). Crowthorne: Transportation Research Library http://ec. europa. eu/enterprise/sectors/automotive/fil es/projects/report_aebs_en. pdf.

[46] **Sevil, A. O.** (2019). Adaptive Autonomous Emergency Braking System Based on Estimation of Tire/Road Friction Coefficient.

[47] **Kocić, J., Jovičić, N., & Drndarević, V. (**2018, November). Sensors and sensor fusion in autonomous vehicles. In 2018 26th Telecommunications Forum (TELFOR) (pp. 420-425). IEEE.

[48] **Rezaei, M.** (2014). Computer Vision for Road Safety: A System for Simultaneous Monitoring of Driver Behaviour and Road Hazards.

[49] **Url-13 <** *https://www.continental-automotive.com/en-gl/Passenger-Cars/Autonomous-Mobility/Enablers/Radars/Long-Range-Radar.>*, date retrieved 10.05.2021.

[50] **Rosique, F., Navarro, P. J., Fernández, C., & Padilla, A.** (2019). A systematic review of perception system and simulators for autonomous vehicles research. Sensors, 19(3), 648.

[51] **Wang, Z., Wu, Y., & Niu, Q.** (2019). Multi-sensor fusion in automated driving: A survey. IEEE Access, 8, 2847-2868.

[52] **Url-14 <** *https://www.aptiv.com/en/insights/article/what-is-an-electronic-control-unit*>, date retrieved 15.04.2021.

[53] **Url-15 <** *https://www.bosch-mobility-solutions.com/en/solutions/control-units/eengine-control-unit/*>, date retrieved 06.06.2021.

[54] **Url-16 <** *https://www.bosch-mobility-solutions.com/en/solutions/vehicle-computer/dasy-vehicle-computer/*>, date retrieved 02.06.2021.

[55] **Url-17** < *https://en.wikipedia.org/wiki/Electronic_control_unit* >, date retrieved 25.02.2021.

[56] **Remfrey, James & Gruber, Steffen & Ocvirk, Norbert. (2016**). Hydraulic Brake Systems for Passenger Vehicles. 10.1007/978-3-319-12352-3_30.

[57] **Becker, C., Arthur, D., & Brewer, J. (2018).** Functional safety assessment of a generic, conventional, hydraulic braking system with antilock brakes, traction control, and electronic stability control (No. DOT-VNTSC-NHTSA-16-08). United States. Department of Transportation. National Highway Traffic Safety Administration.

[58] **Url-18** < *https://www.bosch-mobility-solutions.com/en/solutions/driving-safety/antilock-braking-system/*>, date retrieved 06.06.2021.

[59] **VERBAND DER AUTOMOBILINDUSTRIE E. V.** (2015). VDA 702 Situationskatalog E-parameter Nach ISO 26262-3: Technical Report.

[60] **Böhlander, M.** (2018). Design and Safety Analysis ofEmergency Brake System forAutonomous Formula Car: In Reference to Functional Safety ISO 26262.

[61] **Armağan, E.** (2020). An Intelligent Overtaking Assistant For Autonommous Racing Cars.

[62] **Url-19** < *http://torcs.sourceforge.net/index.php*>, date retrieved 20.04.2021.

[63] **Url-20 <** *https://github.com/VerifiableAutonomy/TORCSLink.*>, date retrieved 20.04.2021.

[64**] International Organization for Standardization.** (2018). ISO 26262-1:2018. Road vehicles — Functional safety — Part 1: Vocabulary.

[65] **Denomme, D., Hooson, S., & Winkelman, J.** (2019). A Fault Tolerant Time Interval Process for Functional Safety Development (No. 2019-01-0110). SAE Technical Paper.

**APPENDICES**

**APPENDIX A:** AIS levels
**APPENDIX B:** HARA Tables
**APPENDIX C:** Fault Tolerant Time Interval

## APPENDIX A

The AIS classification is used for the severity description. The Association for the Advancement of Automotive Medicine (AAAM) publishes the AIS. Also, the severity of injuries classification is represented by the AIS. The guidelines make the severity comparison available internationally.

| | | | | |
|---|---|---|---|---|
| | **S0** | **S1** | **S2** | **S3** |
| Description | No injuries | Light and moderate injuries | Severe and life-threatening injuries (survival probable) | Life-threatening injuries (survival uncertain), fatal injuries |
| Reference for single injuries (from AIS scale) | AIS 0 and less than 10 % probability of AIS 1-6; or damage that cannot be classified safety-related | More than 10 % probability of AIS 1-6 (and not S2 or S3) | More than 10 % probability of AIS 3-6 (and not S3) | More than 10 % probability of AIS 5-6 |
| Examples | — Bumps with roadside infrastructure<br>— Pushing over roadside post, fence, etc.<br>— Light grazing damage<br>— Damage entering/ exiting parking space<br>— Leaving the road without collision or rollover | — Side impact with a narrow stationary object, e.g. passenger car crashing into a tree (impact to passenger cell) with very low speed<br>— Rear/front collision with another passenger car with very low speed<br>— Front collision (e.g. rear-ending another vehicle, semi-trailer, etc.) without passenger compartment deformation | — Side impact with a narrow stationary object, e.g. passenger car crashing into a tree (impact to passenger cell) with low speed<br>— Rear/front collision with another passenger car with low speed<br>— Pedestrian/ bicycle accident with low speed | — Side impact with a narrow stationary object, e.g. passenger car crashing into a tree (impact to passenger cell) with medium speed<br>— Rear/front collision with another vehicle with medium speed<br>— Front collision (e.g. rear-ending another vehicle, semi-trailer, etc.) with passenger compartment deformation |

**Figure A.1 :** Severity classification examples [33].

There are seven classes for this scale:

1) AIS 0: no injuries;
2) AIS 1: light injuries for example muscle pains, skin-deep wounds, etc.;
3) AIS 2: moderate injuries for instance deep flesh wounds, unconsciousness if it is less than 15 minutes, uncomplicated long bone fractures, uncomplicated rib fractures, etc.;
4) AIS 3: injuries that are serious but not life-threating for example skull fractures without causing brain injury, dislocations of spinal below the fourth cervical

vertebra and not harm to the spinal cord, more than one rib fractions but not leading paradoxical breathing, etc.;

5) AIS 4: severe injuries (life-threating) for example paradoxical breathing, concussion with unconsciousness for less than 12 hours and this can be accompanied with skull fractures or not;
6) AIS 5: critical injuries (life-threatening) for instance spinal fractures harming to spinal cord below the fourth cervical vertebra, intestinal tears, cardiac tears, intracranial bleeding included unconsciousness up to 12 hours;
7) AIS 6: extremely critical or fatal injuries for instance cervical vertebrae fractures above the third cervical vertebra with spinal cord damage, highly critical body cavities open wounds (abdominal and thoracic cavities), etc.

Figure Figure A.1 displays the severity classification examples.

## APPENDIX B

HARA tables are given in this section.

**Table B.1 :** AEBS is not activated when AEBS activation is demanded.

| | |
|---|---|
| Function | Activation of AEBS |
| Malfunction 1 | No AEBS activation |
| Hazard 1 | No Hazard |
| Hazard Comment | The driver is informed about AEBS status. The driver is responsible. |
| Consequence | - |
| Scenario | Following front vehicle with normal distance |
| Exposure | E4 (Based on Frequency) |
| Exposure Comment | Scenario from VDA 702 (June 2015) |
| Severity | - |
| Severity Comment | - |
| Controllability | - |
| Controllability Comment | - |
| ASIL | - |
| Safety Goal | - |
| Safe State | - |

**Table B.2 :** AEBS is deactivated unintendedly while AEBS is active.

| | |
|---|---|
| Function | Deactivation of AEBS |
| Malfunction 2 | Unintended Deactivation of AEBS |
| Hazard 1 | No Hazard |
| Hazard Comment | The driver is informed about AEBS status. The driver is responsible. |
| Consequence | - |
| Scenario | Following front vehicle with normal distance |
| Exposure | E4 (Based on Frequency) |
| Exposure Comment | Scenario from VDA 702 (June 2015) |
| Severity | - |
| Severity Comment | - |
| Controllability | - |
| Controllability Comment | - |
| ASIL | - |
| Safety Goal | - |
| Safe State | - |

**Table B.3 :** AEBS is not deactivated while AEBS is active.

| | |
|---|---|
| Function | Deactivation of AEBS |
| Malfunction 3 | No AEBS Deactivation |
| Hazard 1 | No Hazard |
| Hazard Comment | The driver is informed about AEBS status. The driver is responsible. |
| Consequence | - |
| Scenario | Following front vehicle with normal distance |
| Exposure | E4 (Based on Frequency) |
| Exposure Comment | Scenario from VDA 702 (June 2015) |
| Severity | - |
| Severity Comment | - |
| Controllability | - |
| Controllability Comment | - |
| ASIL | - |
| Safety Goal | - |
| Safe State | - |

**Table B.4 :** AEBS does not issue collision warning when it is necessary.

| | |
|---|---|
| Function | Issuing Collision Warnings |
| Malfunction 4 | No Collision Warning |
| Hazard 2 | Loss of Vehicle Deceleration |
| Hazard Comment | The driver waits for braking until collision warnings are given. |
| Consequence | Rear - end collision with other traffic objects |
| Scenario | Driving on highway |
| Exposure | E4 (Based on Duration) |
| Exposure Comment | Scenario from VDA 702 (June 2015) |
| Severity | S3 |
| Severity Comment | Life-threatening injuries (survival uncertain), fatal injuries due to high speed collision |
| Controllability | C1 |
| Controllability Comment | 99% of the drivers can control the vehicle with lane change. |
| ASIL | B |
| Safety Goal 1 | Prevent loss of collision warnings (B) |
| Safe State | Collision warnings shall be given if it is necessary |

**Table B.5 :** AEBS issues unnecessary collision warning.

| | |
|---|---|
| Function | Issuing Collision Warnings |
| Malfunction 5 | Unintended Collision Warning |
| Hazard 3 | Unintended Vehicle Deceleration |
| Hazard Comment | The driver applies brake when unnecessary collision warnings are given because the driver thinks that there is a potential collision. |
| Consequence | Front - end collision with other traffic objects |
| Scenario | Driving on highway |
| Exposure | E4 (Based on Duration) |
| Exposure Comment | Scenario from VDA 702 (June 2015) |
| Severity | S3 |
| Severity Comment | Life-threatening injuries (survival uncertain), fatal injuries due to high speed collision |
| Controllability | C1 |
| Controllability Comment | 99% of the drivers can understand that situation is not critical. |
| ASIL | B |
| Safety Goal 2 | Prevent unintended collision warnings (B) |
| Safe State | Driver shall be warned only when required |

**Table B.6 :** AEBS demands unnecessary braking on higyway road.

| | |
|---|---|
| Function | Autonomous Braking |
| Malfunction 6 | Unintended Deceleration |
| Hazard 3 | Unintended Vehicle Deceleration |
| Hazard Comment | - |
| Consequence | Front - end collision with other traffic objects |
| Scenario | Driving on highway |
| Exposure | E4 (Based on Duration) |
| Exposure Comment | Scenario from VDA 702 (June 2015) |
| Severity | S3 |
| Severity Comment | Life-threatening injuries (survival uncertain), fatal injuries due to high speed collision |
| Controllability | C2 |
| Controllability Comment | Between 90 % an 99 % of the average drivers are able to avoid harm with lane change |
| ASIL | C |
| Safety Goal 3 | Prevent unintended vehicle deceleration (C) |
| Safe State | Unintended deceleration shall be limited |

**Table B.7 :** AEBS demands unnecessary braking on city road.

| | |
|---|---|
| Function | Autonomous Braking |
| Malfunction 6 | Unintended Deceleration |
| Hazard 3 | Unintended Vehicle Deceleration |
| Hazard Comment | - |
| Consequence | Front - end collision with other traffic objects |
| Scenario | Driving in the city |
| Exposure | E4 (Based on Duration) |
| Exposure Comment | Scenario from VDA 702 (June 2015) |
| Severity | S3 |
| Severity Comment | Life-threatening injuries (survival uncertain), fatal injuries due to high speed collision |
| Controllability | C2 |
| Controllability Comment | Between 90 % an 99 % of the average drivers are able to avoid harm with lane change |
| ASIL | C |
| Safety Goal 3 | Prevent unintended vehicle deceleration (C) |
| Safe State | Unintended deceleration shall be limited |

**Table B.8 :** AEBS demands low decelaration demand on highway road.

| | |
|---|---|
| Function | Autonomous Braking |
| Malfunction 7 | Loss of Deceleration |
| Hazard 2 | Loss of Vehicle Deceleration |
| Hazard Comment | - |
| Consequence | Rear - end collision with other traffic objects |
| Scenario | Driving on highway |
| Exposure | E4 (Based on Duration) |
| Exposure Comment | Scenario from VDA 702 (June 2015) |
| Severity | S3 |
| Severity Comment | Life-threatening injuries (survival uncertain), fatal injuries due to high speed collision |
| Controllability | C1 |
| Controllability Comment | 99% of the drivers can control the vehicle with lane change. |
| ASIL | B |
| Safety Goal 4 | Prevent loss of vehicle deceleration (B) |
| Safe State | The braking system shall issue the braking request of AEBS |

**Table B.9 :** AEBS demands low decelaration demand on city road.

| | |
|---|---|
| Function | Autonomous Braking |
| Malfunction 7 | Loss of Deceleration |
| Hazard 2 | Loss of Vehicle Deceleration |
| Hazard Comment | - |
| Consequence | Rear - end collision with other traffic objects |
| Scenario | Driving in the city |
| Exposure | E4 (Based on Duration) |
| Exposure Comment | Scenario from VDA 702 (June 2015) |
| Severity | S3 |
| Severity Comment | Life-threatening injuries (survival uncertain), fatal injuries due to high speed collision |
| Controllability | C1 |
| Controllability Comment | 99% of the drivers can control the vehicle with lane change. |
| ASIL | B |
| Safety Goal 4 | Prevent loss of vehicle deceleration (B) |
| Safe State | The braking system shall issue the braking request of AEBS |

**Table B.10 :** Subject vehicle issues more deceleration than AEBS demand on highway road.

| | |
|---|---|
| Function | Autonomous Braking |
| Malfunction 8 | More deceleration than AEBS demand |
| Hazard 3 | Unintended Vehicle Deceleration |
| Hazard Comment | - |
| Consequence | Front - end collision with other traffic objects |
| Scenario | Driving on highway |
| Exposure | E4 (Based on Duration) |
| Exposure Comment | Scenario from VDA 702 (June 2015) |
| Severity | S3 |
| Severity Comment | Life-threatening injuries (survival uncertain), fatal injuries due to high speed collision |
| Controllability | C2 |
| Controllability Comment | Between 90 % an 99 % of the average drivers are able to avoid harm with lane change |
| ASIL | C |
| Safety Goal 3 | Prevent unintended vehicle deceleration (C) |
| Safe State | Unintended deceleration shall be limited |

**Table B.11 :** Subject vehicle issues more deceleration than AEBS demand on city road.

| | |
|---|---|
| Function | Autonomous Braking |
| Malfunction 8 | More deceleration than AEBS demand |
| Hazard 3 | Unintended Vehicle Deceleration |
| Hazard Comment | - |
| Consequence | Front - end collision with other traffic objects |
| Scenario | Driving in the city |
| Exposure | E4 (Based on Duration) |
| Exposure Comment | Scenario from VDA 702 (June 2015) |
| Severity | S3 |
| Severity Comment | Life-threatening injuries (survival uncertain), fatal injuries due to high speed collision |
| Controllability | C1 |
| Controllability Comment | 99% of the drivers can control the vehicle with lane change. |
| ASIL | B |
| Safety Goal 3 | Prevent unintended vehicle deceleration (C) |
| Safe State | Unintended deceleration shall be limited |

**Table B.12 :** Subject vehicle issues less deceleration than AEBS demand on highway road.

| | |
|---|---|
| Function | Autonomous Braking |
| Malfunction 9 | Less deceleration than AEBS demand |
| Hazard 2 | Loss of Vehicle Deceleration |
| Hazard Comment | - |
| Consequence | Rear - end collision with other traffic objects |
| Scenario | Driving on highway |
| Exposure | E4 (Based on Duration) |
| Exposure Comment | Scenario from VDA 702 (June 2015) |
| Severity | S3 |
| Severity Comment | Life-threatening injuries (survival uncertain), fatal injuries due to high speed collision |
| Controllability | C1 |
| Controllability Comment | 99% of the drivers can control the vehicle with lane change or hard braking. |
| ASIL | B |
| Safety Goal 4 | Prevent loss of vehicle deceleration (B) |
| Safe State | The braking system shall issue the braking request of AEBS |

**Table B.13 :** Subject vehicle issues less deceleration than AEBS demand on city road.

| | |
|---|---|
| Function | Autonomous Braking |
| Malfunction 9 | Less deceleration than AEBS demand |
| Hazard 2 | Loss of Vehicle Deceleration |
| Hazard Comment | - |
| Consequence | Rear - end collision with other traffic objects |
| Scenario | Driving in the city |
| Exposure | E4 (Based on Duration) |
| Exposure Comment | Scenario from VDA 702 (June 2015) |
| Severity | S3 |
| Severity Comment | Life-threatening injuries (survival uncertain), fatal injuries due to high speed collision |
| Controllability | C1 |
| Controllability Comment | 99% of the drivers can control the vehicle with lane change or hard braking. |
| ASIL | B |
| Safety Goal 4 | Prevent loss of vehicle deceleration (B) |
| Safe State | The braking system shall issue the braking request of AEBS |

**Table B.14 :** AEBS does not inform the driver when the system is not working on highway road.

| | |
|---|---|
| Function | Inform the driver about AEBS status |
| Malfunction 10 | No AEBS warning |
| Hazard 2 | Loss of Vehicle Deceleration |
| Hazard Comment | The driver waits for braking until collision warnings are given. |
| Consequence | Rear - end collision with other traffic objects |
| Scenario | Driving on highway |
| Exposure | E4 (Based on Duration) |
| Exposure Comment | Scenario from VDA 702 (June 2015) |
| Severity | S3 |
| Severity Comment | Life-threatening injuries (survival uncertain), fatal injuries due to high speed collision |
| Controllability | C1 |
| Controllability Comment | 99% of the drivers can control the vehicle with lane change or hard braking. |
| ASIL | B |
| Safety Goal 4 | Prevent loss of vehicle deceleration (B) |
| Safe State | The braking system shall issue the braking request of AEBS |

**Table B.15 :** AEBS does not inform the driver when the system is not working on city road.

| | |
|---|---|
| Function | Inform the driver about AEBS status |
| Malfunction 10 | No AEBS warning |
| Hazard 2 | Loss of Vehicle Deceleration |
| Hazard Comment | The driver waits for braking until collision warnings are given. |
| Consequence | Rear - end collision with other traffic objects |
| Scenario | Driving in the city |
| Exposure | E4 (Based on Duration) |
| Exposure Comment | Scenario from VDA 702 (June 2015) |
| Severity | S3 |
| Severity Comment | Life-threatening injuries (survival uncertain), fatal injuries due to high speed collision |
| Controllability | C1 |
| Controllability Comment | 99% of the drivers can control the vehicle with lane change or hard braking. |
| ASIL | B |
| Safety Goal 4 | Prevent loss of vehicle deceleration (B) |
| Safe State | The braking system shall issue the braking request of AEBS |

**Table B.16 :** The calculated relative speed between subject vehicle and target vehicle is lower than its actual value when driving on highway..

| | |
|---|---|
| Function | TTC calculation |
| Malfunction 11 | Low relative speed calculation |
| Hazard 2 | Loss of Vehicle Deceleration |
| Hazard Comment | TTC becomes higher due to wrong relative speed calculation |
| Consequence | Rear - end collision with other traffic objects |
| Scenario | Driving on highway |
| Exposure | E4 (Based on Duration) |
| Exposure Comment | Scenario from VDA 702 (June 2015) |
| Severity | S3 |
| Severity Comment | Life-threatening injuries (survival uncertain), fatal injuries due to high speed collision |
| Controllability | C1 |
| Controllability Comment | 99% of the drivers can control the vehicle with lane change or hard braking. |
| ASIL | B |
| Safety Goal 4 | Prevent loss of vehicle deceleration (B) |
| Safe State | The braking system shall issue the braking request of AEBS |

**Table B.17 :** The calculated relative speed between subject vehicle and target vehicle is higher than its actual value when driving on highway.

| | |
|---|---|
| Function | TTC calculation |
| Malfunction 12 | High relative speed calculation |
| Hazard | Unintended Vehicle Deceleration |
| Hazard Comment | TTC becomes lower due to wrong relative speed calculation |
| Consequence | Front - end collision with other traffic objects |
| Scenario | Driving on highway |
| Exposure | E4 (Based on Duration) |
| Exposure Comment | Scenario from VDA 702 (June 2015) |
| Severity | S3 |
| Severity Comment | Life-threatening injuries (survival uncertain), fatal injuries due to high speed collision |
| Controllability | C2 |
| Controllability Comment | Between 90 % an 99 % of the average drivers are able to avoid harm with lane change |
| ASIL | C |
| Safety Goal 3 | Prevent unintended vehicle deceleration (C) |
| Safe State | Unintended deceleration shall be limited |

**Table B.18 :** The calculated longitudinal distance between subject vehicle and target vehicle is higher than its actual value when driving on highway.

| | |
|---|---|
| Function | TTC calculation |
| Malfunction 13 | High longitudinal distance calculation between target and subject vehicle |
| Hazard 2 | Loss of Vehicle Deceleration |
| Hazard Comment | TTC becomes higher due to wrong longitudinal distance calculation |
| Consequence | Rear - end collision with other traffic objects |
| Scenario | Driving on highway |
| Exposure | E4 (Based on Duration) |
| Exposure Comment | Scenario from VDA 702 (June 2015) |
| Severity | S3 |
| Severity Comment | Life-threatening injuries (survival uncertain), fatal injuries due to high speed collision |
| Controllability | C1 |
| Controllability Comment | 99% of the drivers can control the vehicle with lane change or hard braking. |
| ASIL | B |
| Safety Goal 4 | Prevent loss of vehicle deceleration (B) |
| Safe State | The braking system shall issue the braking request of AEBS |

**Table B.19 :** The calculated longitudinal distance between subject vehicle and target vehicle is lower than its actual value when driving on highway.

| | |
|---|---|
| Function | TTC calculation |
| Malfunction 14 | Low longitudinal distance calculation between target and subject vehicle |
| Hazard 3 | Unintended Vehicle Deceleration |
| Hazard Comment | TTC becomes lower due to wrong longitudinal distance calculation |
| Consequence | Front - end collision with other traffic objects |
| Scenario | Driving on highway |
| Exposure | E4 (Based on Duration) |
| Exposure Comment | Scenario from VDA 702 (June 2015) |
| Severity | S3 |
| Severity Comment | Life-threatening injuries (survival uncertain), fatal injuries due to high speed collision |
| Controllability | C2 |
| Controllability Comment | Between 90 % an 99 % of the average drivers are able to avoid harm with lane change |
| ASIL | C |
| Safety Goal 3 | Prevent unintended vehicle deceleration (C) |
| Safe State | Unintended deceleration shall be limited |

## APPENDIX C

Fault Tolerant Time Interval (FTTI) - ISO 26262-1:2018, 3.61 [64]: If the activation of the safety system mechanism does not start working, minimum time-span between the fault occurrence in an item and possible occurrence of a hazardous event. This is demonstrated by Figure C.1, in which the horizontal axis is the time.

Within this time period, it is critical to activate The Safety Mechanism successfully in order to achieve safe operation of the vehicle.

According to the investigation of Figure C.1 with a higher magnification within this period of time, the FTTI can be divided into two different segments:

- The time period between the fault occurrence and the Malfunctioning Behavior manifestation at the vehicle level
- The time period between Malfunctioning Behavior manifestation and hazard/violation occurrence of a Safety Goal

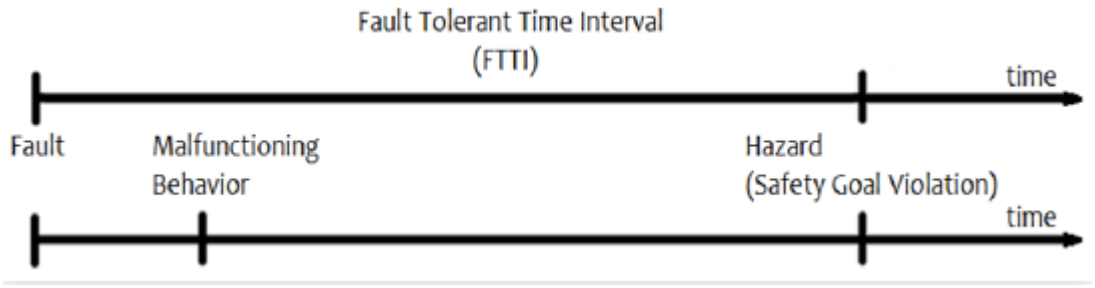


**Figure C.1 :** Fault Tolerant Time Interval [65].

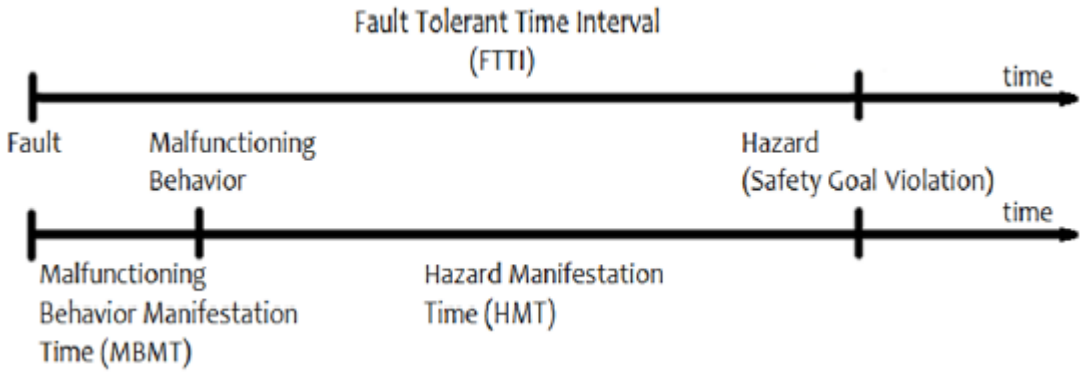


**Figure C.2 :** MBMT and HMT [65].

Below definitions are given to absorb clearly these distinct periods and to take into consideration these subintervals:

- **Malfunctioning Behavior Manifestation Time (MBMT):** The minimum time period at the vehicle level from when the fault occurs until the Malfunctioning Behavior occurs.
- **Hazard Manifestation Time (HMT):** The minimum time period from when the malfunctioning behavior starts until the safety goal violation.

Figure C.2 shows the illustrations of these time intervals. According to FTTI definition, while calculating the numeric FTTI value, any safety mechanism is not taking into account. There are some terminologies required for FTTI and these are defined below.

- **Fault Handling Time Interval (FHTI) - ISO 26262- 1:2018, 3.56** [64]: "sum of fault detection time interval and the fault reaction time interval"
- **Fault Detection Time Interval (FDTI) - ISO 26262- 1:2018, 3.55** [64]: "Time-span from the occurrence of a fault to its detection"
- **Fault Reaction Time Interval (FRTI) - ISO 26262-1:2018, 3.59** [64]: "Time-span from the detection of a fault to reaching a safe state or to reaching emergency operation."

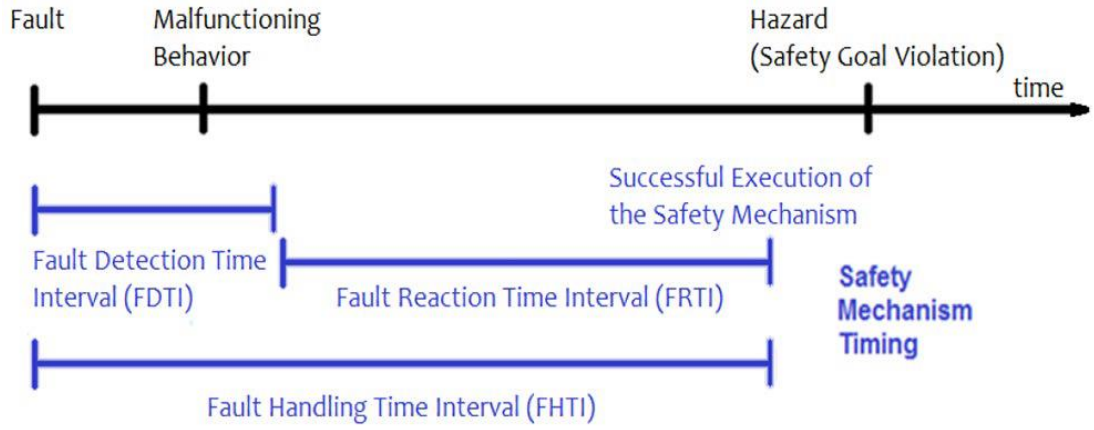


**Figure C.3 :** Illustration of FDTI and FHTI [65].

The demonstration of these time intervals is shown in Figure C.3. Based on these definitions equation (C.1), equation (C.2), and equation (C.3) are derived.

$$FTTI = MBMT + HMT \tag{C.1}$$

$$FHTI = FDTI + FRTI \tag{C.2}$$

$$FHTI \leq FTTI \tag{C.3}$$

Consequently, as shown in equation (C.3), FHTI must be less than or equal to FTTI. This relationship must be respected when developing safety systems.

**CURRICULUM VITAE**

**Name Surname** **:** Semih Uzun

**EDUCATION** **:**

- **B.Sc.** **:** 2018, Yildiz Technical University, Electrical and Electronics Engineering, Control and Automation Engineering

**PROFESSIONAL EXPERIENCE AND REWARDS:**

- 2018- Control and Software Engineer, FEV Turkey