REPUBLIC OF TÜRKİYE

YILDIZ TECHNICAL UNIVERSITY

GRADUATE SCHOOL OF SCIENCE AND ENGINEERING

SAFETY OF THE INTENDED FUNCTIONALITY BASED ON SYSTEM THEORETIC PROCESS ANALYSIS FOR AUTOMATED LANE CENTERING AND CYBERSECURITY CONCEPT FOR STEER BY WIRE SYSTEM

Okan ÖZÇETİN

MASTER OF SCIENCE THESIS

Department of Control and Automation Engineering

Program of Control and Automation Engineering

Supervisor

Asst. Prof. Dr. Mumin Tolga EMİRLER

July, 2024

REPUBLIC OF TÜRKİYE

YILDIZ TECHNICAL UNIVERSITY

GRADUATE SCHOOL OF SCIENCE AND ENGINEERING

SAFETY OF THE INTENDED FUNCTIONALITY BASED ON SYSTEM THEORETIC PROCESS ANALYSIS FOR AUTOMATED LANE CENTERING AND CYBERSECURITY CONCEPT FOR STEER BY WIRE SYSTEM

A thesis submitted by Okan ÖZÇETİN in partial fulfillment of the requirements for the degree of **MASTER OF SCIENCE** is approved by the committee on 02.07.2024 in Department of Control and Automation Engineering, Program of Control and Automation Engineering.

Asst. Prof. Dr. Mumin Tolga EMİRLER
Yıldız Technical University
Supervisor

Approved By the Examining Committee

Asst. Prof. Dr. Mumin Tolga EMİRLER, Supervisor
Yildiz Technical University _____

Assoc. Prof. Dr. Erkin DİNÇMEN, Member
İsik University _____

Asst. Prof. Dr. Muharrem MERCİMEK, Member
Yildiz Technical University _____

I hereby declare that I have obtained the required legal permissions during data collection and exploitation procedures, that I have made the in-text citations and cited the references properly, that I haven't falsified and/or fabricated research data and results of the study and that I have abided by the principles of the scientific research and ethics during my Thesis Study under the title of "SAFETY OF THE INTENDED FUNCTIONALITY BASED ON SYSTEM THEORETIC PROCESS ANALYSIS FOR AUTOMATED LANE CENTERING AND CYBERSECURITY CONCEPT FOR STEER BY WIRE SYSTEM" supervised by my supervisor, Asst. Prof. Dr. Mumin Tolga EMİRLER. In the case of a discovery of false statement, I am to acknowledge any legal consequence.

Okan ÖZÇETİN

Signature

Dedicated to my wife

ACKNOWLEDGEMENTS

I would like to many thanks to Asst. Prof. Dr. Mumin Tolga EMİRLER who provided his knowledge, experience and help throughout my thesis work.

I would like to express my gratitude to my precious mother Kader ÖZÇETİN and father Orhan ÖZÇETİN who have been with me all my life and have never spared their financial and moral support to reach this day and extend my warmest regards to my brothers.

Finally, I would like to express my sincere gratitude and love to Elif KÜTÜKLÜ ÖZÇETİN, my biggest supporter, companion, and beloved wife of 7 years.

Okan ÖZÇETİN

TABLE OF CONTENTS

LIST OF SYMBOLS

l_f	Distance from centre of gravity to the front axles
ϑ_f	Far visual angle
ψ_l	Heading error
y_l	Lateral deviation error
l_s	Look ahead distance
ϑ_n	Near visual angle

LIST OF ABBREVIATIONS

AEB	Automatic Emergency Braking
AI	Artificial Intelligence
ACC	Adaptive Cruise Control
ALC	Automated Lane Centering
CAL	Cybersecurity Assurance Level
CVSS	Common Vulnerability Scoring System
DDT	Dynamic Driving Task
ECU	Electronic Control Unit
FMECA	Failure Mode and Effect Critically Analysis
FTA	Fault Tree Analysis
E/E	Electric/Electronic
ECU	Electronic Control Unit
EHPS	Electrohydraulic Power-Assisted Steering
EPS	Electronic Control Unit
ESC	Electronic Stability Control
ETA	Event Tree Analysis
HAZOP	Hazard and Operational Analysis
HMI	Human Machine Interface
HPS	Hydraulic Power-Assisted System
ISO	International Organization of Standardization
LIDAR	Laser Imaging Detection and Ranging
OBD	On-board diagnostic
ODD	Operational Design Domain
OTA	Over-the-air update
SAE	Society of Automotive Engineers
SbW	Steer-by-Wire
SOTIF	Safety of the Intended Functionality
STAMP	System Theoretic Accident Model and Process
STPA	System Theoretic Process Analysis
STRIDE	Spoofing, Tampering, Repudation, Information Disclosure, Denial of Service, Elevation of Privilege
TARA	Threat Analysis and Risk Assessment

UCA Unsafe Control Action

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Safety Of The Intended Functionality Based On System Theoretic Process Analysis For Automated Lane Centering And Cybersecurity Concept For Steer By Wire System

Okan ÖZÇETİN

Department of Control and Automation Engineering
Master of Science Thesis

Supervisor: Asst. Prof. Dr. Mumin Tolga EMİRLER

Within the increasing automated vehicles and their associated functionalities have led to a corresponding increase in complexity and many risks emerge. This thesis, within the scope of ISO 21448:2022, presents functional insufficiencies, performance limitations in the implementation of the E/E system, and reasonably foreseeable driver misuse which to led to hazards and also outlines the improvement measures. This thesis examines SOTIF based on system theoretic process analysis (STPA) for automated lane centering (ALC). The STPA for ALC, which falls under the SOTIF scope, identifies the purpose and scope of the analysis, the modelling of the control structure, unsafe control actions, and causal scenarios (triggering conditions). Subsequently, the severity and controllability of the identified hazardous behaviour are determined based on the triggering conditions. As a consequence of the risk evaluation, it is determined whether the hazardous behaviours resulting from the triggering conditions are SOTIF related. As final step, improvement measures are identified for SOTIF related triggering conditions.

Furthermore, enabled by the advancement of sophisticated technology, the proliferation of automated vehicles has facilitated the emergence of intelligent and interconnected vehicle functions. One illustrative example is the evolution of the

steering system. With the advent of the steer-by-wire (SbW) system, the traditional hydraulic steering mechanism has been transformed into a more sophisticated electronic system. Furthermore, steer-by-wire systems are networked to communicate with other connected components and systems outside the vehicle, which introduces a multitude of cybersecurity risks. This thesis is also focused on the cybersecurity perspective of SbW based on ISO/SAE 21434:2021. Firstly, boundaries of the SbW item are demonstrated in the thesis. Subsequently, threat analysis and risk assessment (TARA) and cybersecurity concept are represented. As output of TARA, cybersecurity goals are determined. Finally, cybersecurity concept is demonstrated based on determined cybersecurity goals. In this concept, cybersecurity architecture and cybersecurity requirements are developed.

Keywords: Automated lane centering, cybersecurity, SbW, SOTIF, STPA

ÖZET

Otomatik Şerit Merkezleme İçin Sistem Teorik Süreç Analizi Bazlı Amaçlanan İşlevselliğin Güvenliği Ve Kablo Yönlendirmeli Direksiyon Sistemi İçin Siber Güvenlik Konsepti

Okan ÖZÇETİN

Kontrol ve Otomasyon Mühendisliği Anabilim Dalı
Yüksek Lisans Tezi

Danışman: Dr. Öğr. Üyesi Mumin Tolga EMİRLER

Otomatikleştirilmiş araçların ve bunlarla ilgili işlevselliklerin artması, karmaşıklığın da artmasına yol açmış ve birçok risk ortaya çıkmıştır. Bu tez, ISO 21448:2022 kapsamında, E/E sisteminin uygulanmasındaki fonksiyonel yetersizlikleri, performans sınırlamalarını ve tehlikelere yol açabilecek makul şekilde öngörülebilir sürücü hatalı kullanımlarını sunmakta ve ayrıca iyileştirme tedbirlerinin ana hatlarını çizmektedir. Bu tez, otomatik şerit ortalama için sistem teorik süreç analizine (STSA) dayalı olarak amaçlanan işlevselliğin güvenliğini incelemektedir. Amaçlanan işlevselliğin güvenliği kapsamına giren otomatik şerit merkezleme için STSA, analizin amacını ve kapsamını, kontrol yapısının modellenmesini, güvenli olmayan kontrol eylemlerini ve nedensel senaryoları (tetikleyici koşullar) tanımlar. Daha sonra belirlenen tehlikeli davranışın şiddeti ve kontrol edilebilirliği, tetikleyici koşullara göre belirlenir. Risk değerlendirmesi sonucunda tetikleyici koşullardan kaynaklanan tehlikeli davranışların amaçlanan işlevselliğin güvenliği ile ilişkili olup olmadığı belirlenir. Son adım olarak amaçlanan işlevselliğin güvenliği ile ilgili tetikleyici koşullar için iyileştirme tedbirleri belirlenir.

Ayrıca, gelişmiş teknolojinin ilerlemesiyle otomatikleştirilmiş araçların yaygınlaşması, akıllı ve birbirine bağlı araç fonksiyonlarının ortaya çıkmasını kolaylaştırdı. Açıklayıcı bir örnek direksiyon sisteminin evrimidir. Kablo yönlendirmeli direksiyon sisteminin ortaya çıkmasıyla birlikte, geleneksel hidrolik direksiyon mekanizması, araç dışındaki diğer bağlı bileşenler ve sistemlerle iletişim kurmak için ağ bağlantılı daha karmaşık bir elektronik sisteme dönüştürüldü ve bu da çok sayıda siber güvenlik riski doğurmaktadır. Bu tez aynı zamanda SbW'nin ISO/SAE 21434:2021'i temel alan siber güvenlik perspektifine odaklanmıştır. Tezde öncelikle kablo yönlendirmeli direksiyon sisteminin sınırları gösterilmiştir. Daha sonra tehdit analizi ve risk değerlendirmesi (TARD) ve siber güvenlik konsepti anlatılmaktadır. TARD çıktısı olarak siber güvenlik hedefleri belirlenir. Son olarak belirlenen siber güvenlik hedeflerine dayalı olarak siber güvenlik konsepti ortaya konulmaktadır. Bu konseptte siber güvenlik mimarisi ve siber güvenlik gereksinimleri geliştirilmektedir.

Anahtar Kelimeler: amaçlanan işlevselliğin güvenliği, cybersecurity, sistem teorik süreç analizi, otomatik şerit merkezleme, kablolu yönlendirme sistemi,

1
INTRODUCTION

1.1 Literature Review

With the vehicles becoming more intelligent and connected, the automotive system is also becoming increasingly complex [1-4]. With the increase in complexity in electric-electronic systems and the development of automotive communication networks, wireless access to vehicles is possible. According to Upstream Security [5], by 2025 the totality of new cars will be shipped connected, intending as connected not only the possibility of leveraging Internet or localisation services but the adoption of the V2X (Vehicle-to-*X*) paradigm. This term refers to the capability of the car to communicate and exchange data with other vehicles (V2V, Vehicle-to-Vehicle), with a generic infrastructure (V2I) or with pedestrians (V2P) [6]. Increment of feature sets, connectivity, and complexity can lead to a large number of interactions in data, thus causing vulnerabilities that may be exploited by hackers, criminals, terrorists, and spies [7]. The dynamic, diversified, and high-level attacks faced by intelligent vehicles may lead to issues involving personal privacy and safety, and even national security [8-9]. The Steer-by-wire (SbW) system is the next main technology development in the steering section of the automotive industry [10]. The main function of the steer-by-wire system can be specified as steering vehicle. Instead of mechanical linkage from the steering wheel to the steering rack and the use of hydraulics as power steering, the SbW system without the linkage uses electric motors at both the steering wheel and steering rack [10]. Instead of the mechanical linkage used in the traditional steering system, in the steer-by wire system; electronic control unit, steering actuator, steering angle sensor and feedback actuator are used as electronic components. The electronic control unit receives the information from the sensors and driver. After evaluation of the information, electronic control unit transmits the information about how the steering wheel should take action to the steering actuator. The electronic control unit sends this information to other control units in the vehicle via CAN communication when necessary. Thus, with the increasing complexity and communication structure, the steer-by wire system becomes that can leaked by

cyber attackers with security vulnerabilities if measures are not taken. In this thesis, threat analysis and risk assessment and based on determined cybersecurity goals, developed cybersecurity concept are represented for steer-by wire system under the scope of ISO/SAE 21434:2021.

Furthermore, testing and verifying autonomous vehicles' safety is one of the main challenges when developing self-driving functions. These functions are realized by integrating sensors, controllers, actuators, and algorithms. The complexities of autonomous vehicles bring on more safety issues than traditional vehicles, including the functional safety and Safety of The Intended Functionality (SOTIF) [11]. ISO 26262:2018 and ISO 21448:2022 are two standards that address different aspects of risk in the development of E/E systems. ISO 26262 focuses on mitigating unreasonable risk caused by malfunctioning behavior, while ISO 21448:2022 focuses on mitigating unreasonable risk caused by functional insufficiencies that differ from those addresses by ISO 26262:2018. This thesis also concentrates on the SOTIF-related issues of ALC. The ALC system ensures that the vehicle maintains in the centered within the lane on reference trajectory. ALC system evaluates the sensor information such as lane marking, road curvature and lane width to determine the reference trajectory and vehicle location. If the ALC control module determines that an adjustment is needed to return the vehicle to the reference trajectory, the ALC control module commands a steering [12]. In this thesis, STPA method is used to solve SOTIF issue for ALC. STPA has proven to be a valuable tool for addressing functional insufficiencies, human misuse, and other factors beyond hardware or software failures in the context of SOTIF analysis, particularly in scenarios involving unsafe interactions among components [13]. Its applications in the automotive domain include safety analyses of various systems such as the drive-by-wire shift system, electronic control system, and adaptive cruise control (ACC) [14–17]. Even if existence of certain limitations, the use of STPA has increased in recent years, particularly in the context of ADAS and automated driving systems (ADS) such as Lane Keeping Assistance (LKA) system and ACC.

1.2 Purpose

The development of automotive technology has led to an increase in the number of electronic and electrical (E/E) components in vehicles, accompanied by a corresponding increase in the complexity of the systems. This leads to in a number of risks. In the context of vehicles with advanced driving functions and connectivity capabilities, there is a growing need to evaluate the cybersecurity and safety of the intended functionality (SOTIF), including insufficiencies of the intended functionality at the vehicle level and insufficiencies or performance insufficiencies of E/E elements in the system.

In the context of vehicles with advanced functions and connectivity capabilities, there is a growing need to evaluate the cybersecurity and safety of the intended functionality of E/E systems. The purpose of this thesis was to conduct a SOTIF study utilising the STPA method for the automated lane centering system and cybersecurity concept study for SbW system that subsystem of ALC system.

One of the thesis aspects is to examine the functional insufficiencies and performance limitations of the intended functionality in the context of the ALC system. It is necessary to evaluate SOTIF using systematic safety methods. The system theoretic process analysis (STPA) is a system theory-based approach proposed by Nancy Leveson that emphasises a comprehensive system analysis. This section of the thesis presents the results of the progress operation for a specific control action within the scope of the ALC system. It also identifies risk evaluation and improvement measures based on the outputs of the STPA.

The other part of the thesis examines cybersecurity activities for SbW that subsystem of the ALC system. In parallel with the increasing complexity of vehicle systems, functionalities have also evolved. One of the innovations brought about by the development of technology in the steering system is the SbW system. Furthermore, vehicles have also become more vulnerable to cyber threats. For instance, the signal can be spoofed, malicious firmware and software can be injected into a vehicle via OTA, a large number of messages can be sent and interfaces such as OBD and memory cards can be accessed to ECUs. Mainly, this part of thesis focuses on the assets, damage, threat that could lead to damage, as well as the cybersecurity concept that could be employed of SbW system.

1.3 Hypothesis

The existing literature contains studies of the ALC system utilising the STPA method in the context of ISO 26262. However, there is a paucity of studies in the SOTIF field employing the STPA method. In contrast to other studies in the literature, one of the parts of this thesis examines the ALC system using the STPA method in terms of SOTIF in accordance with ISO 21448:2022. As initial step, Purpose and scope of the analysis is identified, and control structure is modelled in this study. Subsequently, specific control action is determined based on control structure under the scope of ALC system. According to related malfunctional behavior of control action, unsafe control actions are defined. In the last step of STPA, causal scenarios, triggering conditions are specified for ALC system. After completion of STPA methods, risk evaluation is performed for triggering conditions based on unsafe control actions to determine whether SOTIF related or not. As result of risk evaluation, measures are defined for SOTIF related risk as determined.

Furthermore, there is a dearth of studies evaluating the steer-by-wire system in terms of cybersecurity. A review of the literature reveals that there is no academic study that addresses the cybersecurity of SbW. Other part of this thesis, cybersecurity concept study is conducted for the SbW system in accordance with ISO/SAE 21434:2021. The initial step in the cybersecurity concept for SbW, creation of the item definition architecture and determine functions of item. Subsequently, asset is identified based on boundary of item architecture. After that, damage scenarios are identified that compromised cybersecurity properties of assets and impact rating are defined. Threat scenarios are defined to determine in order to realize damage scenarios based on STRIDE methods. Risk value and Cybersecurity Assurance Level (CAL) is determined combination of attack feasibility rating, an attribute of an attack path that describes the ease with which an attack, and impact rating. According to compromised cybersecurity properties of assets and CAL value, cybersecurity goals are determined. In conclusion, the cybersecurity requirements, including those pertaining to the allocation of item elements and the detailed cybersecurity architecture with associated measures, are represented in the cybersecurity concept phase.

2
AUTOMATED VEHICLE TECHNOLOGY

2.1 Automated Lane Centering

In recent years, vehicle technology has improved, resulting in intelligent vehicles with advanced driver assistance systems, including lane centering assist.

The automated lane centering (ALC) system offers continuous lateral control to maintain the vehicle on a reference trajectory. The ALC system receives the information regarding lane such as road curvature, lane marking, lane width, lateral position. In addition to lane detection sensors, map and global positioning system (GPS) information are used for ALC system. The ALC system adjusts the vehicle to the reference trajectory via steering command based on the received information.

Figure 2.1 Automated lane centering [18]

Once the position of the lane boundaries has been determined, the subsequent step is to extract the precise position and heading of the vehicle within the lane. In order to determine the position of the vehicle, it is necessary to estimate the coordinates of the lane boundaries and the target path in the world coordinate system. This necessitates an accurate camera calibration, as the optical characteristics of the camera, in addition to its relative position and orientation in the world, result in pixels having a distinct meaning depending on the location of the pixel in the image plane.

The camera is typically installed on the vehicle in such a way that its optical axis is aligned with the symmetry plane of the vehicle. The heading angle of the car is then compared with the heading of the target path.

A representation of the automated lane centering is shown in Figure 2.2.

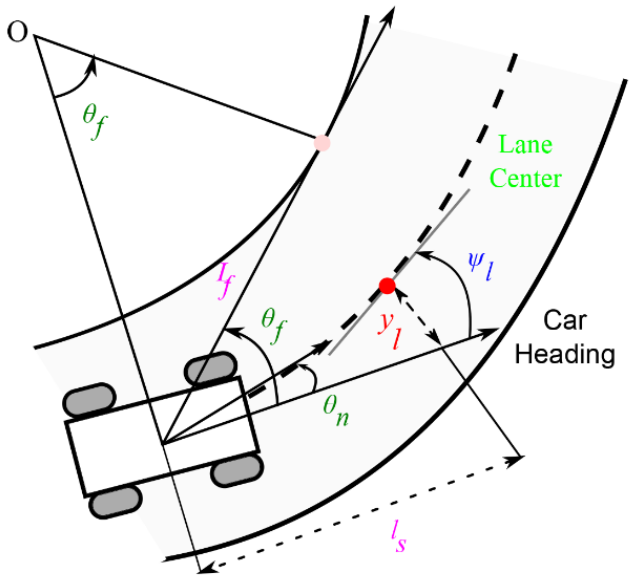

Figure 2.2 Lane keeping task for a vehicle at a look-ahead distance [19]

2.2 Levels of Automation

The level of driving automation is determined by the functionality of the driving automation system feature. The Society of Automotive Engineers (SAE) defines levels of automation for driving, ranging from 0 (no driving automation) to 5 (fully autonomous), in J3016. These levels are explained in the below:

Level 0: No automation. Driver assistance. The driver is capable of steering, braking and accelerating without the use of automated or advanced driver assistance systems. At this level, the driver is responsible for the performance of all tasks.

Level 1: The driver is accountable for all aspects of driving, including steering, braking, acceleration, and other driving tasks. In this level, the driving assistance system is capable of providing support in the areas of braking, steering, and acceleration. Level 1 encompasses features such as adaptive cruise control (ACC)

and lane keeping assist (LKA). The driver is able to activate or deactivate the assistance system via the on/off button.

Level 2: Partial automation. In this level, Advance driving assistance system can take over the driving task at the same time but in limited operational constraints. Advance driving assistance systems can be combined such as lane keeping assist and adaptive cruise control to one system.

Level 3: Conditional automation. In this level of operation, the automated system is capable of assuming control of the vehicle from the driver in accordance with a set of predefined conditions. Within certain limits, the human driver is permitted to engage in other activities without having to continuously monitor the system. In the event that the system reaches the limits of its capabilities, a warning period must elapse before the driver is required to intervene.

Level 4: High Automation. Nevertheless, the degree of autonomy afforded to the vehicle at Level 4 is contingent upon the satisfaction of certain conditions, including the existence of a defined route, the vehicle's operation on a highway or in a parking garage.

Level 5: Full automation. In Level 5, the vehicle's autonomy is no longer subject to conditions. In contrast to Level 4, a Level 5 vehicle is capable of acting completely autonomously. The vehicle is capable of navigating any road traffic situation and operating in any weather or road condition without the input of a human operator. Consequently, these vehicles are devoid of the requisite steering wheel, gas and brake pedals. At this juncture, the role of the human driver is no longer necessary. The vehicle is becoming a mere passenger.

Driving automation levels in SAE J3016 [20] are shown in Figure 2.3.

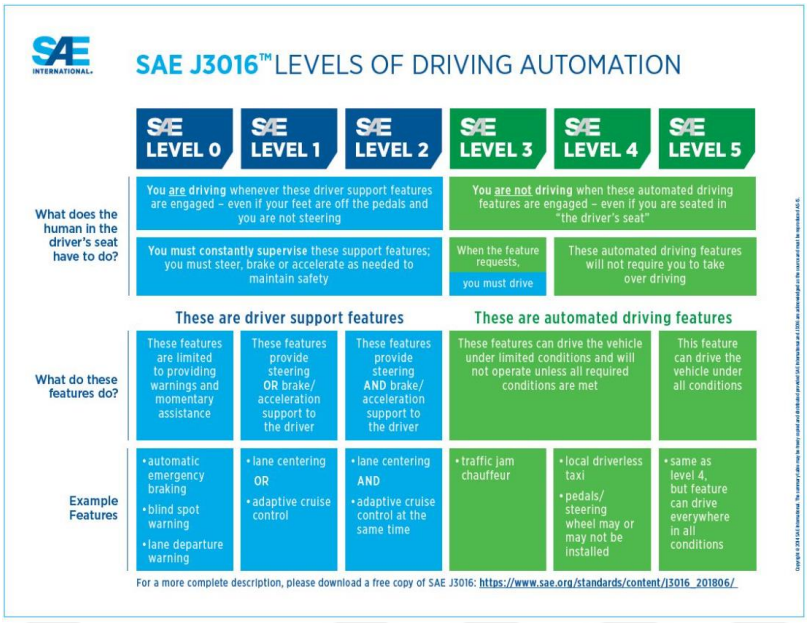

Figure 2.3 SAE level [20]

The vehicle is capable of performing all driving functions under all conditions. The driver may have the option to control the vehicle [20].

2.3 Advancement of Steering System

Vehicle steering system has an evolution history started from pure mechanical generation upgraded with, hydraulic power-assisted system (HPS), electrohydraulic power-assisted steering (EHPS), electric power-assisted steering (EPS), and moves toward steer-by-wire (SBW) system [21]. Traditional steering systems consist of the main components of steering wheel, column, gear, rack, and pinion. The system must transfer the driver's commands to vehicle tires and enforce them to follow the desired path determined by the driver [22].

The SbW is the next generation of steering technology that employs an electrical connection between the steering wheel and the vehicle, as opposed to the traditional steering column. The majority of road imperfections are not directly transmitted to the steering wheel, which results in a more comfortable driving experience due to the lack of a mechanical link between the steering wheel and the tyres. SbW system architecture is represented in figure 2.4.

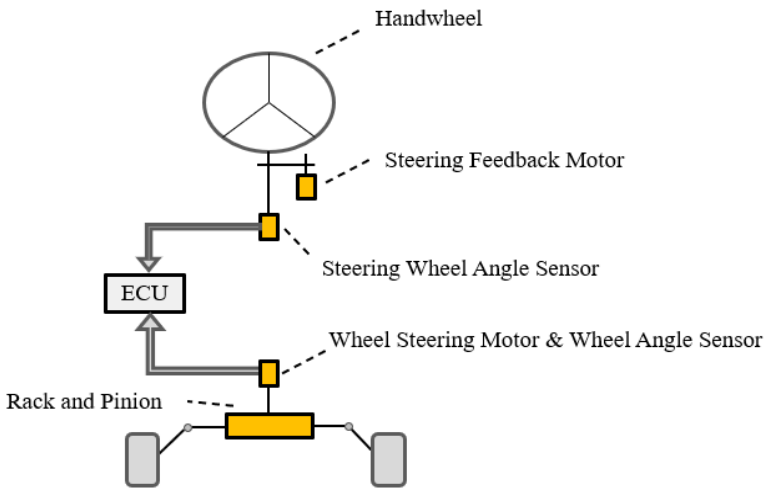

Figure 2.4 Steer-by-wire system architecture [10]

The system can be divided into two distinct parts, namely the upper and lower sections. In addition, Upper part can be specified as handwheel module part, lower part can be specified as road-wheel part. The main duty of steering handwheel module is to receive the driver commands and to convert the demanded angle or torque to an electronic signal using appropriate sensors located on steering handwheel motor shaft. The electronic signal is transmitted via connection wires to road wheel electronic control unit (ECU) in order to determine a relevant command for the vehicle wheels motor drive [23]. The lower part (road wheel) receives information regarding speed, yaw rate, and steering angle, which is used to determine the corresponding steering command to be sent to the steering feedback actuator. The wheel steering motor also receives command from main ECU and changes the road wheel angle in response to these commands. In order to notify driver about vehicle wheel conditions and forces applied on tires in various road situations, sensors should be used in wheels and a feedback system from the road wheel module to the handwheel module is to be established [23].

3
RELATED STANDARDS

3.1 ISO 21434:2021 - CYBERSECURITY ACTIVITIES

The advent of sophisticated technology has led to the development of numerous intelligent and interconnected vehicle functions. The increased complexity and interconnectivity of modern vehicles renders them susceptible to cyber attacks. ISO/SAE 21434:2021 is a standard that addresses the cybersecurity aspects of E/E systems for road vehicles. This thesis examines the cybersecurity concept part of the ISO/SAE 21434:2021 standard, with a particular focus on the ALC system.

3.1.1 Item Definition

In the item definition; the item boundary, item functions and preliminary architecture are identified. The item boundary may include interfaces between items and other items within the vehicle, as well as interfaces between items and E/E systems in the external to the vehicle.

The item describes the intended behaviour of the item during the lifecycle phases and includes the vehicle functionality that is realized by the item [24]. The preliminary architecture describes the components of the item and their interactions, as well as the external interfaces of the item.

3.1.2 Threat Analysis and Risk Assessment

TARA is the output that describes methods for determining the extent to which a road user may be affected by a threat scenario. TARA is flowed based on that represented in Figure 3.1.

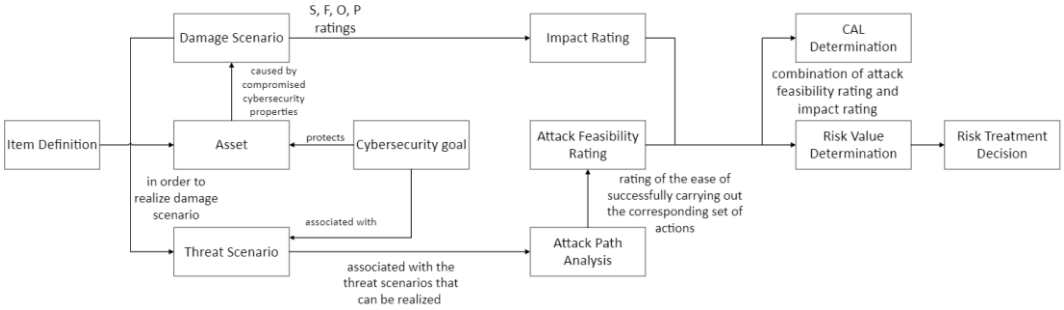

Figure 3.1 TARA flow

3.1.3 Cybersecurity Concept

Cybersecurity concept contains of cybersecurity requirements of the item and requirements on the operational environment that derived from cybersecurity goals. Technical and operational cybersecurity controls and their interactions should be described that consider cybersecurity claims and dependencies between the item functions to achieve the cybersecurity goals. Cybersecurity requirements should be allocated to item.

3.2 ISO 21448:2022 – ROAD VEHICLES – SOTIF

The safety of road vehicles is a matter of utmost importance for the road vehicle industry. The quantity of automated driving features integrated into vehicles on the rise. These systems rely on sensing, processing of complex algorithms, and actuation implemented by electrical and/or electronic (E/E) systems. ISO 26262:2018 and ISO 21448:2022 are two standards that address different aspects of risk in the development of E/E systems. ISO 26262 focuses on mitigating unreasonable risk caused by malfunctioning behavior, while ISO 21448:2022 focuses on mitigating unreasonable risk caused by functional insufficiencies that differ from those addresses by ISO 26262:2018.

Intended functionality and its implementation can cause hazardous behavior in E/E systems. These are:

- Failure of ability sensing elements to perceiving the environment correctly
- The lack of robustness of the function, system, or algorithm
- Failure of the decision making and control algorithms
- Driver expectations/misuse

3.2.1 Overview of the SOTIF Activities

The term “hazardous scenario” is used to describe a situation that could potentially lead to hazardous behavior. The scenarios included in the relevant use cases have been classified into four areas:

- Area 1 represents the known, not hazardous scenarios.
- Area 2 represents known, hazardous scenarios.
- Area 3 represents unknown, hazardous scenarios.
- Area 4 represents unknown, not hazardous scenarios.

The ultimate goal of the SOTIF activities is to evaluate the potentially hazardous behavior present in areas 2 and 3 and to provide an argument that the residual risk caused by these scenarios is sufficiently low [26].

Area 2, probability of known hazardous scenarios, is reduced to acceptable level through functional modification with improving measures. Area 3 is reduced, the probability of the unknown scenarios, to acceptable level through verification and validation strategies. These are system verification through real vehicle testing technology, hardware-in-the-loop testing technology, and virtual simulation technology [25]. Hazardous event categories before SOTIF implementation and after SOTIF activities implementation are shown in Figure 3.2.

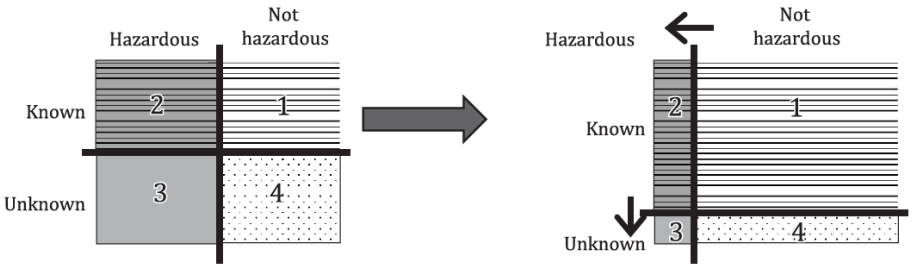

Figure 3.2 Example of initial starting point of development and goal for SOTIF release [26]

3.2.2 Identification and Evaluation of Hazards

3.2.2.1 Hazard Identification

The hazards resulting from functional insufficiencies are determined systematically at the vehicle level. This systematic identification is primarily based on knowledge about the function and its possible deviations resulting from functional insufficiencies [26].

3.2.2.2 Risk Evaluation

The objective of the risk evaluation is to assess the risk associated with hazardous behaviour in specific scenarios. This enables the determination of the criteria for the acceptance of a SOTIF-related risk based on controllability (C) and severity (S) parameters. In accordance with the ISO 26262:2018 standard, the severity and controllability parameters are classified into one of four categories, ranging from 0 to 3. If the controllability rating is determined to be 0 (C=0) or the severity rating

is determined to be 0 (S=0), then the absence of unreasonable risk is found. In all cases except for S=0 or C=0, a hazardous event is considered to be related to SOTIF.

Example regarding evaluation of a potential consequence of a SOTIF-related hazardous event for an AEB system is given in Table 3.1.

Table 3.1 Risk evaluation example [26]

Hazardous behaviour	**Potential consequence**	**S rating**	**Note**	**C rating**	**Note**
Unintended AEB activation at $x\ m/s^2$ for y seconds while opeating on a highway	Rear collision with following vehicle	S>0	Effective impact $v \geq x\ km/h$	C>0	The following vehicle might not be able to brake to avoid collision

3.2.3 Potential Functional Insufficiencies and Potential Triggering Conditions

Potential insufficiencies of specification, potential performance insufficiencies and potential triggering conditions including reasonably foreseeable direct misuse that led to hazardous events are defined.

3.2.3.1 Analysis of Potential Functional Insufficiencies and Triggering Conditions

The potential functional insufficiencies and triggering conditions are subjected to a systematic analysis. There are a number of analysis methods that can be employed. These include deductive methods, inductive methods such as system-based analysis and scenario-based analysis and exploratory methods such as STPA. Specified type analysis methods may be conducted qualitative or quantitatively, or a combination of both.

The following subclauses present the functional insufficiencies and triggering conditions for planning algorithms, sensors and actuators.

3.2.3.2 Potential Functional Insufficiencies and Triggering Conditions Related to Planning Algorithms

A number of potential insufficiencies and trigger conditions may arise from the implementation of planned algorithms. These are generally related to machine

learning, road infrastructure and the environment. In the following points, it is given the potential insufficiencies and triggering conditions regarding planning algorithm The behavior of drivers and other road users, including foreseeable misuse, can lead to the triggering of conditions and potential functional insufficiencies. These include scenarios such as construction sites, accidents, traffic jams with emergency corridors, and vehicles driving in the wrong direction. It is possible that these triggering conditions and potential functional insufficiencies may also be caused by road infrastructure, including highways, urban and rural infrastructure. It is important to note that there are certain limitations associated with machine learning, particularly in the context of planned algorithms. These limitations include the inability to handle potential scenarios or non-deterministic behaviour, as well as the lack of clarity in the specification of machine learning, the quality of the measurement data for machine learning, and the lack of functional improvements.

3.2.3.3 Potential Functional Insufficiencies and Triggering Conditions Related to Sensors and Actuators

A number of potential insufficiencies and trigger conditions may arise from the also sensors and actuators. The performance of sensors, including the presence of dirt on sensors, accuracy, range, acoustic disturbance, response time, glare, and poor-quality reflection regarding sensors and actuators, may have resulted in potential insufficiencies and triggering conditions. Furthermore, disturbances and interference can influence sensor performance. For instance, mechanical disturbances may be caused by noisy sensor output, which can result from vibration due to the location of the sensor on the vehicle. Additionally, electromagnetic interference (EMI) and interference from other vehicles or other sources regarding radar or lidar may also affect sensor performance. There are also related with weather conditions. For example, the presence of fog, snow, and other atmospheric conditions that result in reduced visibility may impact the performance of the sensors. Other factors relating to sensors and actuators for potential insufficiencies and triggering conditions can be extended with operational the Operational Design Domain (ODD), performance impact due to durability, wear, ageing and authority capability such as the maximum applicable braking pressure for a hydraulic braking system by the intended functionality, multi-sensor data fusion and alignment and installation of sensors.

3.2.3.4 Analysis of Reasonably Foreseeable Direct or Indirect Misuse

It is possible that a reasonably foreseeable direct or indirect misuse of the intended functionality could contribute to an unreasonable level of risk. The following are examples of causes of direct or indirect misuse that can be reasonably foreseen:

- Lack of understanding of the system by the users
- Wrong user expectations of the system
- Loss of concentration
- Overreliance on the system
- Incorrect assumption of user interaction [26]

3.2.4 System Modification

The objective of the proposed modifications to the system is to ensure that its intended functionality is preserved to the greatest extent possible. Such measures may include, but are not limited to, the following:

1) Improvement sensor performance and/or accuracy through:
    - Improved sensor technology;
    - Improved sensor disturbance detection that triggers an appropriate warning and degradation strategy;
    - Diverse sensor types;
    - Improved sensor calibration and installation;
    - Sensor blockage detection and cleaning methods [26];
2) Increased actuator performance and/or accuracy by improving actuator technology, such as increasing accuracy, extending or limiting output range, reducing response time, repeatability, arbitration capability, using other functions to assist, or adding a new actuator to assist.increased performance and/or accuracy of the recognition and decision algortihms by algorithmic modifications;
3) Increasing the conspicuity of the ego vehicle to improve the controllability of other participants in case of dangerous behaviour of the ego vehicle.

3.2.4.1 Functional Restriction

Functional limitation measures aim to maintain partial functionality by reducing or limiting the intended functionality. These measures may include:

1) Restriction of the intended functionality for specific use cases;
2) Removal of authority for the intended functionality for specific use cases [26]

3.2.4.2 Handing Over Authority

Measures for handing over authority from a system to driver are aimed at increasing controllability at lower levels of driving automation [26]. These measures can be included in the following:

1) Modifying the Human-Machine Interface (HMI);
2) Modifying the user notification and dynamic driving task (DDT) fallback strategy [26].

3.2.4.3 Addressing Reasonably Foreseeable Misuse

Measures of addressing reasonably foreseeable misuse can include in the following:

1) Customer education through training and information
2) Enhancing the HMI properties and implementation of a driver warning/monitoring system
3) Measures implementation to avoid prevent misuse [26]

4
SYSTEM DEFINITON

4.1 System Description

In this master thesis is focused to ALC system and SbW that subsystem of ALC system. ALC system receives the information such as lane marking, location of the vehicle, longitudinal and lateral acceleration, steering request and this system determines the trajectory by processing all receiving information.

4.2 System Architecture

System architecture is demonstrated below that interaction between the ALC system elements.

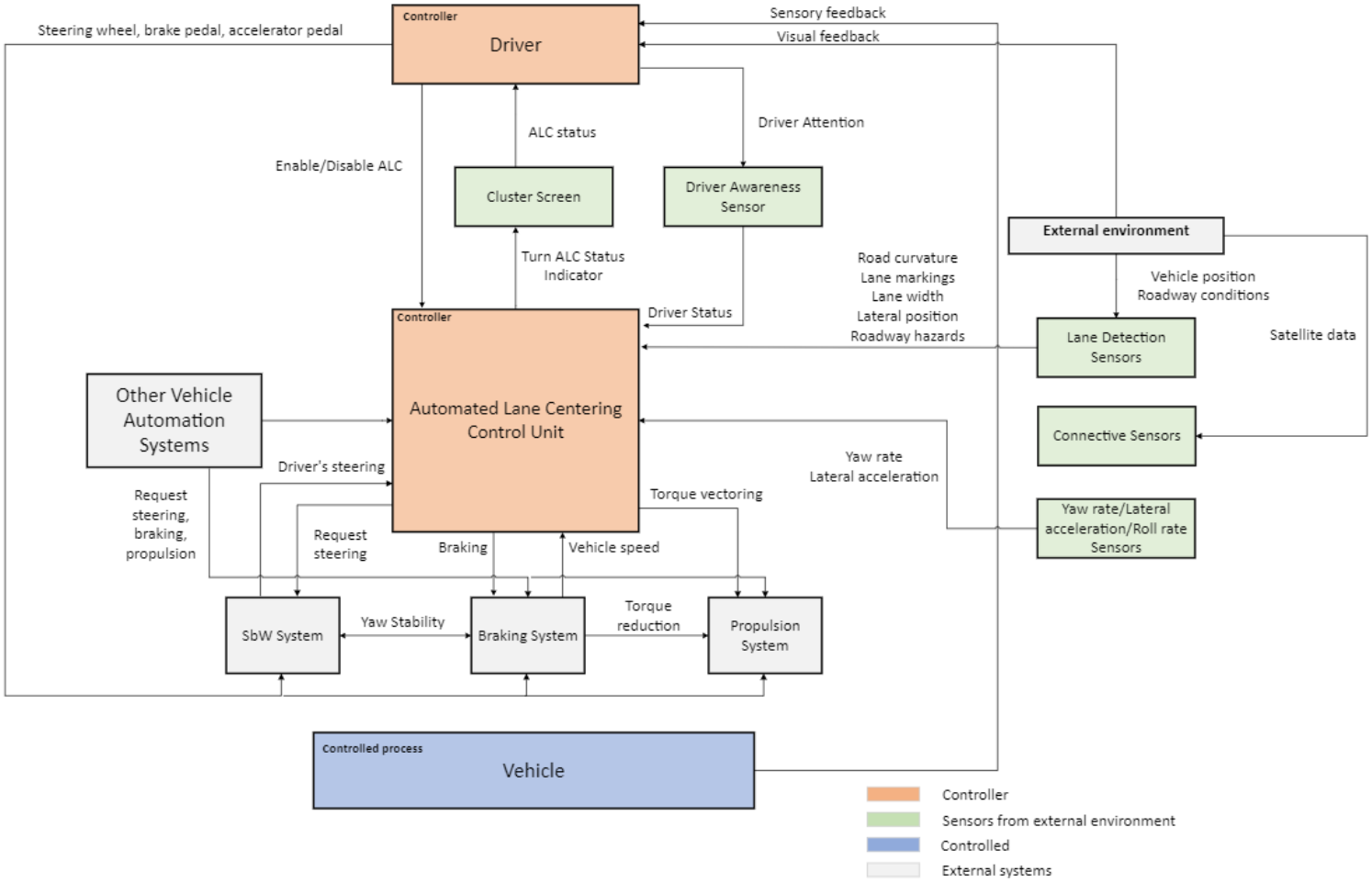

Figure 4.1 ALC system architecture [24]

4.3 System Elements

ALC system comprises for interaction of many elements. The fundamental elements of the pertinent ALC system are represented below.

4.3.1 Lane Centering Control Unit

The ALC control module utilize the information received by the integrated sensors in the vehicle regarding lane marking, lane width, road curvature, GPS location and other connected sensors to determine whether vehicle in the center of lane or not. The ALC control module computes the vehicle's heading and the vehicle's offset relative to the reference trajectory. The error between the vehicle's actual position and heading, and the reference trajectory allows the ALC control module to determine the lateral adjustment required to return the vehicle to the reference trajectory [12]. In the event that the vehicle departs from the lane, the ALC control module transmits the requisite torque command information to the related SbW system, thereby enabling lateral adjustments to the vehicle's position within the reference trajectory.

4.3.2 Lane Detection Sensors

The lane detection sensors are used to ascertain the lane markings through the utilisation of cameras, radar, and LIDAR technologies. In addition to detecting the lane markings, these sensors are utilised to detect roadway boundaries, roadway obstacles, roadway curvature, and lane width. The information received from the lane detection sensors becomes more meaningful when combined with GPS data, vehicle-to-vehicle (V2V) data, and vehicle-to-infrastructure (V2I) data. This information is then transmitted to the ALC control unit for processing. The also utilisation of sensory feedback facilitates an understanding of the relationship between the vehicle and the road.

4.3.3 Vehicle Dynamic Sensors

The ALC control unit is processed the vehicle dynamic information such as yaw rate, lateral acceleration, vehicle speed and roll rate in order to determine any necessary adjustments to ensure the vehicle remains within the lane.

4.3.4 Steer-by-Wire System

The SbW system receives the handwheel steering input and torque to the handwheel from the driver and processes it. It then determines the required steering forces from the steering motor to adjust the heading of the road wheels. Since there is no mechanical connection between the steering wheel and the road wheels, the SbW system also simulates all feedback to the driver via a separate feedback motor [27].

4.3.5 Cluster Screen

The cluster screen displays notifications from the ALC system to the driver. These notifications:

- The instrument panel and other displays may also be used to display visual information.
- The term "audible notifications" is used to describe any auditory alerts, such as chimes or voice prompts.
- Haptic feedback may be provided in the form of seat or steering wheel vibrations, among other possibilities.

The cluster screen provides the driver with information regarding the status of the ALC, including whether it is active, available, and whether the driver is required to regain control of the vehicle in specific circumstances.

4.3.6 Driver Awareness Sensor

Driver awareness sensor monitor the driver and relay the status of driver to the ALC system.

4.3.7 Braking System

The ALC system provides the lateral control adjustment on the reference trajectory with the support of the braking system. The brake/stability control system arbitrates the yaw request from the ALC system with other braking needs, such as ESC or deceleration requests from ACC [12].

4.3.8 Propulsion System

The propulsion system is responsible for providing the torque required for torque vectoring to be applied to the driven wheels of the vehicle.

5
METHODS

5.1 System Theoretic Process Analysis (STPA)

STPA is an analyses method based on system theory, which was recommended by Professor Nancy Leveson from MIT for the purpose of addressing problems that arise from interactions between system components. STPA (System-Theoretic Process Analysis) is a relatively new hazard analysis technique based on an extended model of accident causation. In addition to component failures, STPA assumes that accidents can also be caused by unsafe interactions of system components, none of which may have failed [28]. There are a plethora of advantages associated with the use of STPA over conventional hazard/risk analysis techniques. Firstly, it is of the utmost importance that complex systems can be analysed using STPA. In STPA, in addition to scenarios that have been known, unknown scenarios that could previously only be detected in operations can be identified and eliminated or reduced. In addition to intended functionality of a system, STPA can also address unintended functionality. In contrast to the conventional hazard analysis techniques, STPA can be initiated at the preliminary stage of concept analysis in order to facilitate the identification of safety requirements and constraints. Such measures can then be integrated into the system architecture and design to enhance its overall safety and security. As the design is developed and becomes more specific, it is possible to refine and enhance the STPA analysis in a more detailed manner. Given that STPA is a systematic process, it is relatively straightforward to trace the refined process. The STPA methodology encompasses the analysis of software and human operators, thereby ensuring that the hazard analysis encompasses all potential causal factors that could lead to losses. The STPA provides a comprehensive documentation of the system functionality. This is frequently absent or challenging to identify within expansive, intricate systems. The integration of STPA into the system engineering process and model-based system engineering is straightforward.

The utilization of appropriate safety analysis tools is of paramount importance in order to ensure that SOTIF issues are analyzed in a comprehensive and logical manner. A plethora of safety analysis methodologies are recommended in ISO 21448:2022 including fault tree analysis (FTA), failure mode and effect analysis (FMEA), hazard and operational analysis (HAZOP) and STPA.

The STPA methodology identified all of the causal scenarios identified by the more traditional analyses, in addition to numerous other scenarios, many of which were software-related and non-failure scenarios that the traditional methods had not identified. Furthermore, the results demonstrated that STPA was considerably more cost-effective in terms of time and resources than the traditional methods. STPA, an analytical tool derived from STAMP, employs a top-down risk analysis approach that involves four steps.

The fundamental steps of the STPA methodology are represented in Figure 5.1 [28].

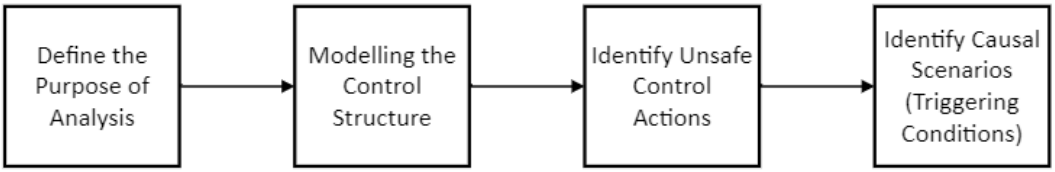

Figure 5.1 STPA methodology

In STPA, the first step is to define the purpose of the analysis. The second step is to construct a model of the system, which is referred to as a control structure. The third step is to analyze the control actions within the control structure in order to examine how they could lead to the losses that were defined in the first step. The fourth step is to identify the reasons, triggering conditions, why unsafe control might occur in the system.

5.1.1 Defining the Purpose and Scope of the Analysis

This initial step in STPA method is to define the purpose of the analysis. This entails identifying the types of losses that analysis is designed to prevent and determining the system to be analyzed and the system boundary. After identifying of losses, vehicle-level hazards are determined. These are vehicle-level states or conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss. The definition of the purpose of the analysis comprises four parts:

- Identifying losses
- Identifying vehicle-level hazards
- Identifying vehicle-level safety constraints
- Refining hazards (optional)

5.1.1.1 Identifying Losses

A loss involves something of value to stakeholders [28]. Prior to the commencement of any analysis, it is imperative that the stakeholders identify the specific losses that they wish to be the focus of the analysis. The STPA methodology can be employed to identify and address any loss that is deemed unacceptable by the relevant stakeholders. In the event that more than one loss is included, it is possible to rank and prioritise them. Some examples of losses:

- Loss of customer satisfaction
- Loss of reputation
- Loss of life
- Loss of property
- Loss of mission

5.1.1.2 Identifying vehicle-level hazards

The subsequent stage is to delineate the system- and vehicle-level hazards that are likely to result in a deterioration of the worst-case environmental conditions. The potential for losses to be incurred can be identified by examining the combination of system/vehicle and the associated unsafe condition.

5.1.1.3 Identifying vehicle-level safety constraints

A system/vehicle level constraint specifies system conditions or behaviours that need to be satisfied to prevent hazards [28]. Each constraint can be traced to one or more hazards, and each hazard can be traced to one or more losses. The constraint can be identified by the combination of system/vehicle and the associated condition to enforce.

In addition, constraints can be employed to define the manner in which the system must endeavour to minimise losses in the event that the aforementioned hazards materialise.

Vehicle level safety constraint that linked with hazards can be also specified as "If the hazard occurs what needs to be done to prevent or minimize a loss" [28].

5.1.2 Modelling of the Control Structure

The process of control structure modelling commences with the conceptualisation of a control structure, which is then developed through an iterative process of adding detail. In many instances, the control structure and the control loops within the system may be readily apparent. The hierarchical control structure is comprised of control loops. A hierarchical control structure comprise for at least five types of elements. These are; controllers, control actions, feedback, other inputs to and outputs from components, controlled process [28]. Control loops are generally implemented by the controller to perform control actions. The term “controlled process” encompasses any process that is subject to control. The control algorithm is responsible for determining the control actions to be provided. Additionally, controllers poss process models that symbolize the controller’s internal beliefs, which are employed in the decision-making process. A hierarchical control structure can be employed to model the interactions between multiple control loops 5.2.

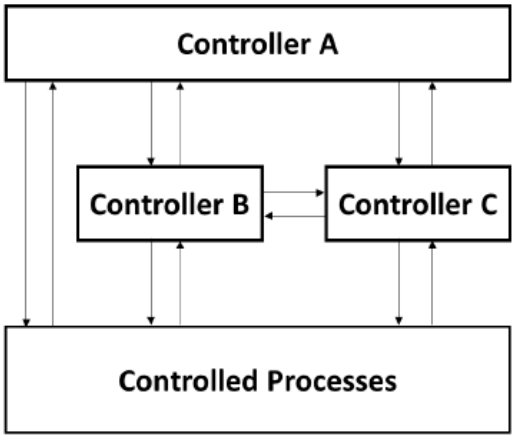

Figure 5.2 Hierarchical control structure [28]

5.1.3 Identification of the Unsafe Control Actions

The Unsafe Control Actions (UCAs) is defined as a control action that, in a specific context and under the worst-case environment, will lead to a hazard. Once the UCAs have been identified, it is necessary to specify the corresponding vehicle-level safety constraints in order to prevent the UCAs. A UCA contains five elements such as "Source", "Type Identifier", "Control Action", "UCA Context", "Link to

Hazard". A control action can be unsafe in many distinct ways. These are listed in the Table 5.1.

Table 5.1 Malfunctional behaviour example

Malfunctional behaviour					
Not providing	Unintended providing	Too late providing	Stopped providing	Excessively/ insufficiently	Locked providing

5.1.4 Identification of Causal Scenarios

The identification of causal scenarios (triggering conditions) that may lead to the unsafe control actions. In this step, the triggering conditions that can lead to the UCA under consideration are identified. These conditions may be deficiencies other elements or in the elements of the system controller itself. Triggering conditions are defined based on planning algorithm, sensors, actuators, reasonably foreseeable direct or indirect misuse.

5.2 Threat Analysis and Risk Assessment (TARA)

The following sections present a detailed account of the stages that collectively give rise to the formation of TARA, respectively.

5.2.1 Asset Identification

According to ISO/SAE 21434:2021 - Road Vehicles - Cybersecurity Engineering, asset is object that has value, or contributes to value. Assets should be defined for damage scenarios and cybersecurity properties in asset identification.

5.2.2 Damage Scenario and Impact Rating

Identify assets with cybersecurity properties, confidentiality (C), integrity (I), availability (A), authentication (Au), that, if compromised, could lead to a scenario of damage. The evaluation of damage scenarios should consider their potential adverse consequences for road users in the impact categories of safety (S), financial (F), operational (O) and privacy (P). The impact rating of a damage scenario needs to be determined for each impact category. These are severe, major, moderate and negligible.

5.2.3 Threat Scenario

A potential threat scenario may result in the compromise of the cybersecurity properties of one or more assets, thereby enabling the realisation of a damage scenario. Threat scenarios include targeted asset, compromised cybersecurity property of the asset and cause of compromise of the cybersecurity property.

5.2.4 Attack Path Analysis

Threat scenarios should be analyzed to identify path of attack. A threat scenario shall be associated with each attack path, indicating the potential for that scenario to be realised by the attack path.

5.2.5 Attack Feasibility Rating

The attack feasibility rating is determined based on one of the methods Common Vulnerability Scoring System (CVSS), attack potential-based approach, and attack vector-based approach. In this paper, an attack feasibility rating was obtained using an attack vector-based approach. Attack vector-based approach presents the context in which exploitation of the attack vector is possible. The attack feasibility is inversely proportional to the distance between the attacker and the target, both in terms of logical and physical proximity. According to ISO/SAE 21434:2021, attack vector-based approach is represented in Table 5.2.

Table 5.2 Attack vector-based approach [24]

Attack feasibility rating	**Criteria**
High	Network: Potential attack path is bound to network stack without any limitation. Example 1: Cellular network connection making the ECU directly connected and accessible on the internet.
Medium	Adjacent: Potential attack path is bound to network stack; however, the connection is limited physically or logically. Example 2: Bluetooth interface, virtual private network connection.

Table 5.2 Attack vector-based approach [24] (more)

Low	Local: Potential attack path is not bound to network stack and threat agents require direct access to the item for realizing the attack path. Example 3: Universal serial bus mass storage device, memory card.
Very Low	Physical: Threat agents require physical access to realize the attack path.

5.2.6 Cybersecurity Assurance Level and Cybersecurity Goals

A cybersecurity assruance level (CAL) is indirectly related to risk; however, it cannot be directly determined from a risk value. This is because the risk value is dynamic, varying over time depending on the evolving specification, design, implementation and operational environment of the item or component, whereas the CAL expresses a level of assurance that is to remain fixed over time [24]. CAL can be assigned to cybersecurity goals as an attribute. Cybersecurity goal is a top-level cybersecurity requirement to protect assets against a threat scenario. The CALs, which are determined by a combination of impact rating and attack feasibility rating based on attack vector-based approach, are represented in Table 5.3, which is defined in ISO/SAE 21434:2021.

Table 5.3 Example CAL determination [24]

Impact rating	**Attack vector (b)**			
	Physical	Local	Adjacent	Network
Severe	CAL2	CAL3	CAL4	CAL4
Major	CAL1	CAL2	CAL3	CAL4
Moderate	CAL1	CAL1	CAL2	CAL3
Negligible	--a	--a	--a	--a

--a: For threat scenarios of risk value 1 that are determined from an analysis in accordance with risk value determination, conformity with cybersecurity concept, product development and cybersecurity validation may be omitted.

b: Attack vector is a static parameter of attack feasibility [24].

5.2.7 Risk Value Determination

In order to determine the risk value associated with each threat scenario, it is necessary to consider the impact of the damage scenarios and the attack feasibility of the attack paths. Example risk matrix is represented in Table 5.4.

Table 5.4 Risk matrix example [24]

		Attack feasibility rating			
		Very Low	Low	Medium	High
Impact rating	Severe	2	3	4	5
	Major	1	2	3	4
	Moderate	1	2	2	3
	Negligible	1	1	1	1

5.2.8 Risk Treatment Decision

For each threat scenario, considering its risk values, one or more of the following risk treatment option(s) shall be determined [24]:

- Avoiding the risk
- Reducing the risk
- Sharing the risk
- Retaining the risk

6
CONCEPT STUDY

6.1 SOTIF Based On STPA For ALC

The STPA is performed for SOTIF analysis under the ALC scope. First step for STPA, scope and purpose are identified for ALC system. Losses and vehicle level hazards that linked with losses and vehicle level safety constraints are defined that linked with vehicle level hazards are defined as sub step of first step. Subsequently, control structure is modelled in the context of ALC system and specific control action is determined based on modelled control structure. Unsafe control actions are determined that caused by malfunctional behavior of control action as subsequent step. In final stage of STPA for ALC system, Causal scenarios that triggered to unsafe control actions are identified in the context of SOTIF perspective.

6.1.1 Defining the Purpose and Scope of the Analysis

Losses, vehicle-level hazards with linked losses and vehicle-level safety constraints based on vehicle-level hazards are given in the Table 6.1, Table 6.2 and Table 6.3, respectively.

6.1.1.1 Identifying the losses

The specific losses that should be addressed in relation to the ALC system are outlined below in Table 6.1.

Table 6.1 Potential loss for ALC

Potential loss ID	Potential Loss
L01	Loss of human life
L02	Loss of or damage property
L03	Loss of company repudation
L04	Loss of customer satisfaction
L05	Damage to the vehicle or objects situated outside the vehicle

6.1.1.2 Identification of Vehicle-Level Hazards

Vehicle-level hazards that are linked with losses is determined based on the operational situations presented below in Table 6.2.

Table 6.2 Vehicle-level hazards for ALC

Hazard ID	Vehicle-level hazards	Potential consequence
H01	The vehicle deviates from the lane in which it is travelling due to losses of steering control. [L01, L02, L03, L04, L05]	Side collision with following vehicle or run-off road.
H02	The vehicle deviates from the lane in which it is travelling due to too late steering activation. [L01, L02, L03, L04, L05]	Side collision with following vehicle or run-off road.
H03	The vehicle deviates from the lane in which it is travelling due to insufficiently steering activation. [L01, L02, L03, L04, L05]	Side collision with following vehicle or run-off road.
H04	The vehicle deviates from the lane in which it is travelling due to unintended steering activation. [L01, L02, L03, L04, L05]	Side collision with following vehicle or run-off road.
H05	The vehicle deviates from the lane in which it is travelling due to excessively steering activation. [L01, L02, L03, L04, L05]	Side collision with following vehicle or run-off road.
H06	The vehicle deviates from the lane in which it is travelling due to steering activation to wrong reference trajectory. [L01, L02, L03, L04, L05]	Side collision with following vehicle or run-off road.

6.1.1.3 Identification of Vehicle-Level Safety Constraints

Vehicle-level safety constraints based on vehicle level hazards are represented below in Table 6.3.

Table 6.3 Vehicle-level safety constraints for ALC

Vehicle-level hazards	Vehicle-level safety constraints
H01: The vehicle deviates from the lane in which it is travelling due to losses of steering control. [L01, L02, L03, L04, L05]	SC01: In the event that the vehicle deviates from the lane, the ALC system shall perform the control of the steering [H01].
H02: The vehicle deviates from the lane in which it is travelling due to too late steering activation. [L01, L02, L03, L04, L05]	SC02: In the event that the vehicle deviates from the lane, the ALC system shall perform the control of the steering timely manner [H02].
H03: The vehicle deviates from the lane in which it is travelling due to insufficiently steering activation. [L01, L02, L03, L04, L05]	SC03: In the event that the vehicle deviates from the lane, the ALC system shall perform the control of the steering [H03].
H04: The vehicle deviates from the lane in which it is travelling due to unintended steering activation. [L01, L02, L03, L04, L05]	SC04: In the event that the vehicle deviates from the lane, the ALC system shall perform the control of the steering and ensure the vehicle stability [H04].
H05: The vehicle deviates from the lane in which it is travelling due to excessively steering activation. [L01, L02, L03, L04, L05]	SC05: In the event that the vehicle deviates from the lane, the ALC system shall perform the control of the steering and ensure the vehicle stability [H05].
H06: The vehicle deviates from the lane in which it is travelling due to steering activation to wrong reference trajectory. [L01, L02, L03, L04, L05]	SC06: Driver shall take over the steering control [H06].

6.1.2 Modelling of the Control Structure

Figure 6.1 represents the control structure that used in the STPA to shows the ALC system and interfacing systems and components.

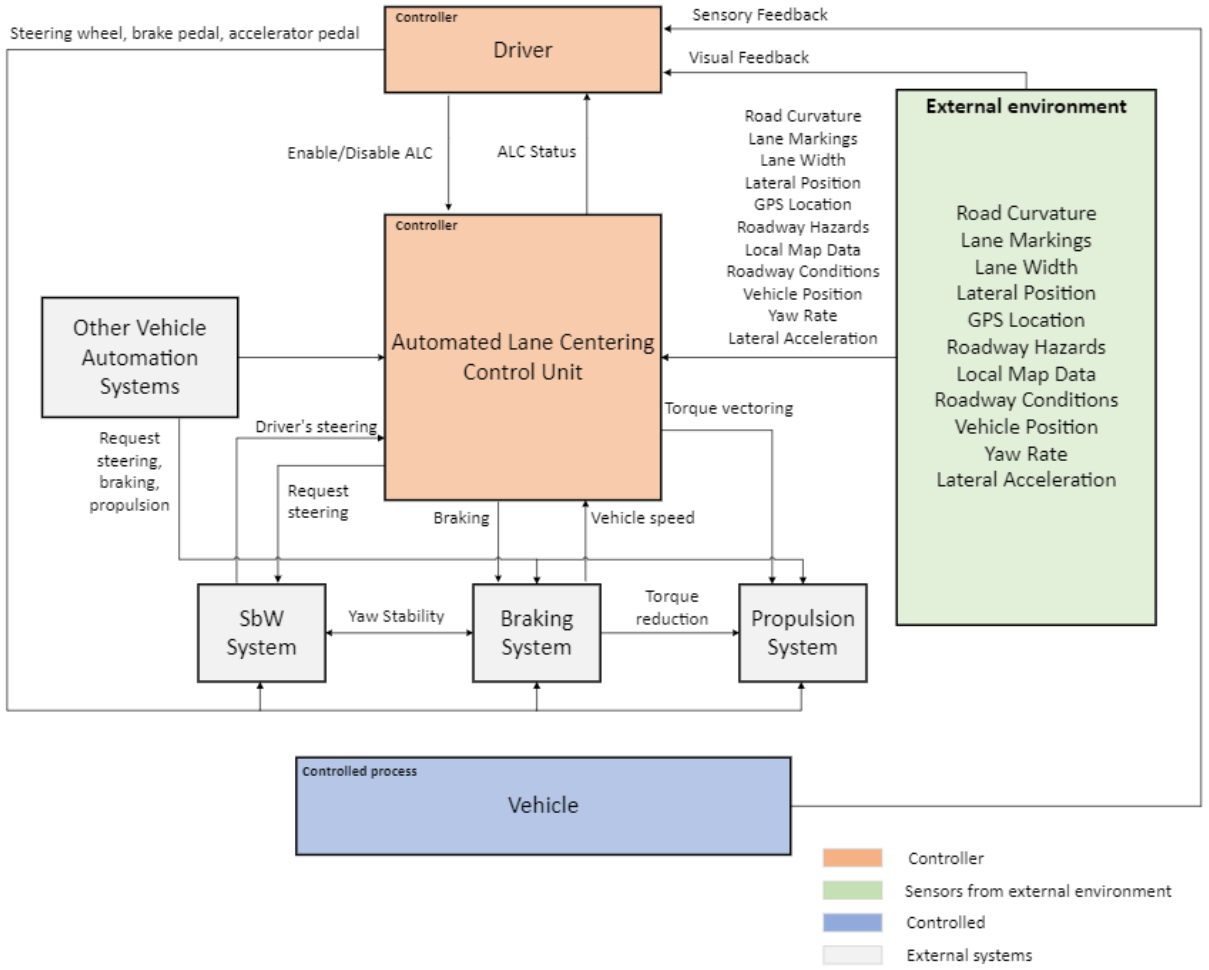

Figure 6.1 Control structure for ALC

A multitude of control actions can be derived from control structures. Regarding Figure 6.1, this thesis is concentrated on the "Adjustment Vehicle's Steering Control" as control action.

6.1.3 Identification of the Unsafe Control Actions

Unsafe control actions that determined for “Adjustment Vehicle’s Steering Control” control action under the scope of ALC system are represented in Table 6.4.

Table 6.4 Unsafe control actions for ALC

Control Actions	**Unsafe Control Actions**	
Adjustment Vehicle’s Steering Control	Not providing	UCA1: The ALC system does not provide the requisite command to adjust the vehicle's lane centering on the determined trajectory. [H01]
	Providing too late	UCA2: The ALC system provides a lateral command that adjusts the vehicle's lane centering on the determined trajectory, but too late. [H02]
	Providing too short	UCA3: The ALC system provides a lateral command that adjusts the vehicle's lane centering on the determined trajectory, but insufficiently. [H03]
	Providing but not required	UCA4: The ALC system provides a lateral command that adjusts the vehicle's lane centering on the determined trajectory, but unexpectedly. [H04]
	Providing excessively	UCA5: The ALC system provides an excessive lateral command that adjusts the vehicle's lane centering on the determined trajectory. [H05]
	Provided but wrong	UCA6: The ALC system provides a lateral command that adjusts the vehicle's lane centering on the wrong reference trajectory. [H06]

6.1.4 Identification of Causal Scenarios

In this phase, triggering conditions and functional insufficiencies are performed that triggered to unsafe control actions. Functional insufficiencies, misuse and corresponding triggering conditions that derived from UCAs are represented in the below Table 6.5.

Table 6.5 Triggering conditions for ALC

UCA	Functional Insufficiencies or Misuse	Triggering Conditions
UCA1	The ALC system does not provide steering control due to driver misuse.	TC01: The driver may not know which conditions to can be able to operate the ALC system
		TC02: The driver may not know when the system is active.
	The ALC system does not provide steering control due to incorrect lane detection.	TC03: The lane detection sensor is not correctly in place and in alignment.
		TC04: Fog, snow, and other effects that led to low quality of visibility may affect the lane detection sensor to perceive the lane marking.
	The ALC system does not provide the requisite steering control due to inadequate AI/control algorithm.	TC05: Control and machine learning algorithms may process lane marking data incorrectly due to poor quality algorithm.
		TC06: Incomplete training sets or insufficient verification of the trained parameters.

Table 6.5 Triggering conditions for ALC (more)

UCA2	The ALC system enables lateral adjustments to the vehicle's position within the reference trajectory but too late due to incorrect lane detection.	TC07: The steering torque is determined by the response time of the sensors, which is currently delayed.
UCA2	The ALC system enables lateral adjustments to the vehicle's position within the reference trajectory but too late due to inadequate control algorithm.	TC08: The steering torque is processed too late by the control algorithm, despite receiving information from both the steering wheel angle and the steering wheel torque sensor.
UCA3	The ALC system enables lateral adjustments to the vehicle's position within the reference trajectory but insufficiently due to road/lane shape.	TC09: When vehicle arrives to toll booth, the ALC system may not be able to activate sufficient steering on time.
		TC10: When vehicle arrives the diamond road shape, the ALC system may not be able to activate sufficient steering on time.
	The ALC system enables lateral adjustments to the vehicle's position within the reference trajectory but insufficiently due to road condition.	TC11: The ALC system may not be able to activate sufficient steering on time due to existence of water trough in the road.

Table 6.5 Triggering conditions for ALC (more)

UCA4	The ALC system provides unexpectedly lateral command that adjust the centering the lane of the vehicle in the determined trajectory due to driver misuse.	TC12: The driver may inadvertently disengage the ALC system by operating certain controls, such as sharp steering.
	The ALC system provides unexpectedly lateral command that adjust the centering the lane of the vehicle in the determined trajectory due to inadequate AI/control algorithm.	TC13: The vehicle's steering wheel may unintentionally change position due to incorrect determination of its lane position resulting from a deficient AI/control algorithm.
UCA5	The ALC system provides excessive lateral command that adjust the centering the lane of the vehicle in the determined trajectory due to incorrect lane detection.	TC14: The ALC system detects lane markings on the left or right side that are not actually present.
	The ALC system provides excessive lateral command that adjust the centering the lane of the vehicle in the determined trajectory due to incorrect AI/control algorithm.	TC15: The ALC system detects roadway references detected on opposite side of the vehicle.
UCA6	The ALC system does not provide steering control due to inadequate AI/control algorithm.	TC16: The ALC system may not decide to reference correct trajectory due to rubbish, tyre tread on the road.

Table 6.5 Triggering conditions for ALC (more)

UCA6	The ALC system does not provide steering control due to inadequate AI/control algorithm.	TC17: The ALC system may not decide to reference correct trajectory due to existence of kerb in the road.

6.1.5 Risk Evaluation

The risk evaluation aims to evaluate the risk due to hazardous behavior in given scenarios; this helps to specify the acceptance criteria of a SOTIF-related risk [1]. Controllability and severity parameters are considered to determine whether SOTIF related or not.

If controllability (C) rating of C=0 or a severity (S) rating of S=0 is considered as an absence of unreasonable risk. Otherwise, related hazardous events are SOTIF-related. The following table presents the results of the risk evaluation for ALC.

Table 6.6 Risk evaluation for ALC

Triggering Condition ID	**Hazardous Behaviour**	**Potential Consequence**	**S**	**C**
TC01	The vehicle is unable to adjust the lane centering and alerts the driver to take control.	Side collision with other vehicle. Run-off the road.	S>0	C>0
TC02	The vehicle is unable to adjust the lane centering and alerts the driver to take control.	Side collision with other vehicle. Run-off the road.	S>0	C>0

Table 6.6 Risk evaluation for ALC (more)

TC03	ALC system has been discontinued. Vehicle cannot adjust the lane centering.	Side collision with other vehicle. Run-off the road.	S>0	C>0
TC04			S>0	C>0
TC05			S>0	C>0
TC06			S>0	C>0
TC07	The vehicle is unable to adjust the lane centering in a timely manner and may drift out of the lane.	Side collision with other vehicle. Run-off the road.	S>0	C>0
TC08			S>0	C>0
TC09	The vehicle is unable to adjust the lane centering and may drift out of the lane.	Side collision with other vehicle. Run-off the road.	S>0	C>0
TC10			S>0	C>0
TC11			S>0	C>0
TC12	The vehicle is unable to adjust the lane centering and alerts the driver to take control.	Side collision with other vehicle. Run-off the road.	S>0	C>0
TC13	Unintended steering activation that led to out of the lane.	Side collision with other vehicle. Run-off the road.	S>0	C>0
TC14	The vehicle is unable to adjust the lane centering and may drift out of the lane.	Side collision with other vehicle. Run-off the road.	S>0	C>0
TC15			S>0	C>0
TC16			S>0	C>0
TC17			S>0	C>0

6.1.6 Improvement Measures

After risk evaluation, improvement measures should be defined for triggering conditions with S>0 and C>0 as a result of risk evaluation. Table 6.7 shows the improvement measures corresponding to related triggering conditions.

Table 6.7 Improvement measures

Triggering Condition ID	Improvement Measures
TC01	The driver requires training courses and user manual regarding usage of ALC system.
TC02	
TC03	Improving sensor installation. Positioning sensors to provide better coverage for specific corner cases that may result in performance insufficiency.
TC04	Restriction of the ALC system for fog, snow etc. automated lane centering system cannot handle the in these weather conditions. Driver needs to take over the steering control.
TC05	Algorithmic modifications have led to an increase in the performance and accuracy of the recognition and decision algorithms.
TC06	
TC07	Improved sensor attributes or change to new with improved sensor.
TC08	Algorithmic modifications have led to an increase in the performance and accuracy of the recognition and decision algorithms.
TC09	Restriction of the ALC system for toll booth. Automated lane centering system cannot handle the toll booth road feature. Driver needs to take over the steering control.

Table 6.7 Improvement measures (more)

TC10	Enhanced sensor recognition algorithm: A feature descriptor has been improved to detect objects in camera images. Refine the algorithm to enhance its robustness and precision.
TC11	Restriction of the ALC system for fog, snow etc. Automated lane centering system cannot handle the in these weather conditions. The driver is required to assume control of the steering control.
TC12	The driver requires training courses and user manual regarding usage of ALC system.
TC13	Enhanced sensor recognition algorithm: A feature descriptor has been improved to detect objects in camera images. Refine the algorithm to enhance its robustness and precision.
TC14	Enhanced sensor recognition algorithm: A feature descriptor has been improved to detect objects in camera images. Refine the algorithm to enhance its robustness and precision.
TC15	Algorithmic modifications have led to an increase in the performance and accuracy of the recognition and decision algorithms.
TC16	Enhanced sensor recognition algorithm: A feature descriptor has been improved to detect objects in camera images. Refine the algorithm to enhance its robustness and precision.
TC17	

6.2 Cybersecurity Concept for Steer-By Wire System

The main objective of the cybersecurity concept is to identify item and its operational environment, drawing item boundary, their interactions in the context of cybersecurity.

In the TARA phase, cybersecurity goals are determined which are top-level cybersecurity requirements. In order to achieve safety goal, cybersecurity risks are assessed by using TARA method.

In the cybersecurity concept, cybersecurity requirements and requirements on the operational environment are derived from cybersecurity goals based on item. Architecture is represented with specified measures to prevent the cybersecurity related risk and to achieve the cybersecurity goals.

6.2.1 Item Definition

In this phase, the item boundary is represented in the preliminary architecture. The item boundary is defined as the item and its operational environment. Preliminary architecture is demonstrated boundary of the item, interfaces between item element and other E/E systems in the external to the vehicle in the context of SbW system and the item describes the functional behaviour of the item. Main function of the SbW system is steering control.

Preliminary architecture that defined item elements, its operational environment and other E/E systems from the item in the external is represented in Figure 6.2.

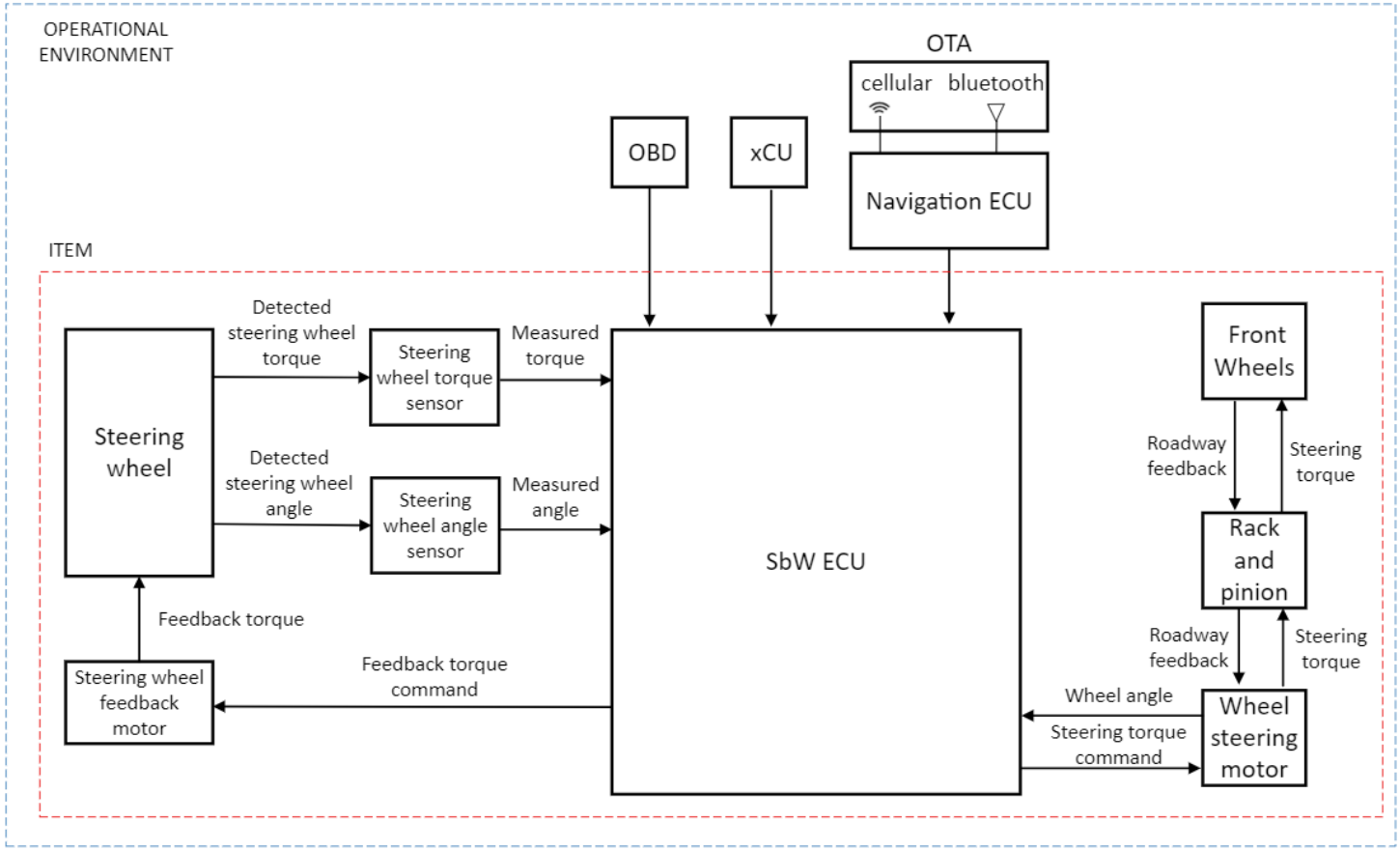

Figure 6.2 Item architecture for SbW

6.2.2 Threat Analysis and Risk Assessment (TARA)

6.2.2.1 Asset Identification

Determined assets are represented in Table 6.8 for steer-by-wire system.

Table 6.8 Assets for item

Asset ID	Assets
AS01	SbW ECU
AS02	Steering wheel angle sensor
AS03	Steering wheel feedback motor
AS04	Steering wheel torque sensor
AS05	Wheel steering motor

6.2.2.2 Damage Scenarios and Impact Ratings

Determined damage scenarios that compromised cybersecurity properties of asset for steer-by wire system and damage categories with impact ratings of damage scenarios are represented respectively in Table 6.9 and Table 6.10.

Table 6.9 Damage scenarios for SbW system

	Security Property				
Damage ID	**C**	**I**	**A**	**Au**	**Damage Scenario**
D01		x		x	Vehicle deviates from the lane in which it was travelling since steering can be locked due to loss of integrity and authentication of SbW ECU. [AS01]
D02		x	x		Vehicle deviates from the lane in which it was travelling steering can be activated unintentedly due to loss of integrity and availability of SbW ECU. [AS01]

Table 6.9 Damage scenarios for SbW system (more)

D03			x		Vehicle deviates from the lane in which it was travelling since loss of steering control may occur due to permanent loss of availability of the steering wheel angle sensor. [AS02]
D04		x			Vehicle deviates from the lane in which it was travelling since steering can be activated unintentedly due to loss of integrity of steering wheel angle sensor. [AS02]
D05		x			Driver cannot realize the road condition since less or more steering torque feedback due to loss of integrity steering wheel feedback motor. [AS03]
D06			x		Driver cannot realize the road condition since less or more steering torque feedback due to loss of availability steering wheel feedback motor. [AS03]
D07		x			Vehicle deviates from the lane in which it was travelling since loss of steering control may occur due to loss of integrity of steering wheel torque sensor. [AS04]
D08			x		Vehicle deviates from the lane in which it was travelling since loss of steering control may occur due to loss of availability of steering wheel torque sensor. [AS04]
D09		x			Vehicle deviates from the lane in which it was travelling since steering can be locked due to loss of integrity of wheel steering motor. [AS05]

Table 6.9 Damage scenarios for SbW system (more)

D10		x			Vehicle deviates from the lane in which it was travelling steering can be activated unintentedly due to loss of integrity of wheel steering motor. [AS05]
D11		x		x	Vehicle deviates from the lane in which it was travelling since loss of steering control may occur due to loss of integrity and authentication of SbW ECU. [AS01]

According to identified damage scenarios, impact ratings that include that safety, financial, operational and privacy are determined. This thesis is focused on safety impact category that is more critical than other impact category.

Table 6.10 Impact ratings for determined damage scenarios

	Damage Category					
Damage ID	**S**	**F**	**O**	**P**	**Impact Description**	**Impact Rating**
D01	x	x	x		Fatal injury to road users	Severe
D02	x	x	x		Fatal injury to road users	Severe
D03	x	x	x		Fatal injury to road users	Severe
D04	x	x	x		Fatal injury to road users	Severe
D05		x	x		Partial degradation of a steering function.	Moderate
D06		x	x		Partial degradation of a steering function.	Moderate
D07	x	x	x		Fatal injury to road users	Severe

Table 6.10 Impact ratings for determined damage scenarios (more)

D08	x	x	x		Fatal injury to road users	Severe
D09	x	x	x		Fatal injury to road users	Severe
D10	x	x	x		Fatal injury to road users	Severe
D11	x	x	x		Fatal injury to road users	Severe

6.2.2.3 Threat Scenarios

Determined threat scenarios in order to realize damage scenarios are represented in Table 6.11 for SbW system.

Table 6.11 Threat scenarios for SbW system

Threat Scenario ID	Threat Scenario	Threat Type	Damage Scenario ID
TS01	An attacker might be able to send a malicious software update package to SbW ECU using the OTA that led to lock of steering due to loss of SbW ECU integrity and authentication.	Spoofing	D01
TS02	An attacker might be able to manipulate the contents of messages being sent over the communication channel that led to unintended steering due to loss of integrity and availability of SbW ECU.	Denial of service	D02
TS03	An attacker might send malicious signal from OBD connector to SbW ECU that led to locked of steering due to loss of SbW ECU integrity and authentication.	Spoofing	D01

Table 6.11 Threat scenarios for SbW system (more)

TS04	An attacker physically cuts or damages the steering wheel angle sensor wiring connection to the SbW ECU which lead to loss of steering due to loss of steering wheel torque sensor availability.	Tampering	D03
TS05	An attacker renders the communication channel on the CAN bus unusable preventing the SbW ECU from getting the appropriate value from the steering wheel angle sensor which lead to unintended steering wheel activation due to loss of steering wheel angle sensor integrity.	Denial of service	D04
TS06	An attacker can send a malicious input that exploit a vulnerability that will be affected the driver realization with steering feedback torque on the handwheel from on board diagnostic (OBD) connector due to loss of steering wheel feedback motor integrity.	Spoofing	D05
TS07	An attacker can send a malicious input that exploit a vulnerability that will be affected the driver with steering feedback torque on the handwheel.	Spoofing	D06
TS08	An attacker physically cuts or damages the steering wheel feedback motor wiring connection to the SbW ECU that will be affected the driver with steering feedback torque on the handwheel.	Tampering	D06

Table 6.11 Threat scenarios for SbW system (more)

TS09	An attacker physically cuts or damages the steering wheel torque sensor wiring connection to the SbW ECU which lead to loss of steering due to loss of steering wheel torque sensor availability.	Tampering	D07
TS10	An attacker can potentially alter the wheel steering motor properties by interfering with communication between components within the steer-by wire system that led to locking of steering due to loss of integrity of wheel steering motor..	Denial of service	D09
TS11	An attacker might send malicious signals from SbW ECU to wheel steering motor that that led to unintended steering wheel activation due to loss of integrity of wheel steering motor.	Spoofing	D10
TS12	In the event of OTA update, an attacker might send message via smartphone and Bluetooth dongle that led to lock of steering due to loss of SbW ECU integrity and authentication.	Spoofing	D01
TS13	An attacker might be able to manipulate navigation ECU from bluetooth interface that led to lock of steering due to loss of SbW ECU integrity and authentication.	Spoofing	D01

Table 6.11 Threat scenarios for SbW system (more)

TS14	An attacker might be able to compromises xCU from cellular interface that led to unintended activation of steering due to loss of integrity and authentication of SbW ECU	Spoofing	D11

6.2.2.4 Attack Feasibility Rating

Attack feasibility rating is represented in Table 6.12 that determined attack vector-based approach for steer-by wire system.

Table 6.12 Attack feasiblity rating for SbW system

Threat Scenario ID	**Threat type**	**Attack vector**	**Attack feasiblity rating**
TS01	Spoofing	Network	High
TS02	Denial of service	Network	High
TS03	Spoofing	Local	Low
TS04	Tampering	Physical	Very Low
TS05	Denial of service	Local	Low
TS06	Spoofing	Local	Low
TS07	Spoofing	Network	High
TS08	Tampering	Physical	Very Low
TS09	Tampering	Physical	Very Low
TS10	Denial of service	Network	High
TS11	Spoofing	Network	High
TS12	Spoofing	Adjacent	Medium

Table 6.12 Attack feasiblity rating for SbW system (more)

TS13	Spoofing	Adjacent	Medium
TS14	Spoofing	Network	High

6.2.2.5 Risk Value Determination

Risk value is determined from the combination of impact rating and attack feasibility rating. Determined risk values are represented in Table 6.13 for SbW system.

Table 6.13 Risk value for SbW system

Threat Scenario ID	Impact rating	Attack feasibility rating	Risk value
TS01	Severe	High	5
TS02	Severe	High	5
TS03	Severe	Low	3
TS04	Severe	Very low	2
TS05	Severe	Low	3
TS06	Moderate	Low	2
TS07	Moderate	High	3
TS08	Moderate	Very low	1
TS09	Severe	Very low	2
TS10	Severe	High	5
TS11	Severe	High	5
TS12	Severe	Medium	4
TS13	Severe	Medium	4

Table 6.13 Risk value for SbW system (more)

TS14	Severe	High	5

6.2.2.6 Cybersecurity Assurance Level and Cybersecurity Goals

For the SbW system, The CALs, which are determined by a combination of impact rating and attack feasibility rating based on attack vector-based approach, are represented in Table 6.14 and determined cybersecurity goals to protect assests against threat scenarios are presented in Table 6.15.

Table 6.14 CAL determination

Threat Scenario ID	**Impact rating**	**Attack feasibility rating**	**CAL**
TS01	Severe	High	CAL4
TS02	Severe	High	CAL4
TS03	Severe	Low	CAL3
TS04	Severe	Very low	CAL2
TS05	Severe	Low	CAL3
TS06	Moderate	Low	CAL1
TS07	Moderate	High	CAL3
TS08	Moderate	Very low	CAL1
TS09	Severe	Very low	CAL2
TS10	Severe	High	CAL4
TS11	Severe	High	CAL4
TS12	Severe	Medium	CAL4
TS13	Severe	Medium	CAL4

Table 6.14 CAL determination (more)

TS14	Severe	High	CAL4

Based on compromised asset properties, cybersecurity goals are identified against threat scenarios.

Table 6.15 Cybersecurity goals

CySe goal ID	**CAL**	**Related threat scenario**	**Cybersecurity goals**
CSG01	CAL4	TSR01 TSR02 TSR03 TSR12 TSR13 TSR14	The integrity, availability and authentication/authorization of SbW ECU shall be ensured.
CSG02	CAL3	TSR04 TSR05	The integrity and availability of steering wheel angle sensor shall be ensured.
CSG03	CAL3	TSR06 TSR07 TSR08	The integrity and availability of steering wheel feedback motor shall be ensured.
CSG04	CAL2	TSR09	The integrity and availability of steering wheel torque sensor shall be ensured.
CSG05	CAL4	TSR10 TSR11	The integrity and availability of wheel steering motor shall be ensured.

6.2.3 Cybersecurity Concept

The cybersecurity concept is comprised of cybersecurity requirements of the item and the operational environment that are derived from the cybersecurity goals in conjunction with the cybersecurity architecture.

6.2.3.1 Cybersecurity Architecture

Cybersecurity concept architecture for SbW is refined from preliminary architecture in the item definition. In this architecture, measures are represented regarding that identified cybersecurity goals in the TARA.

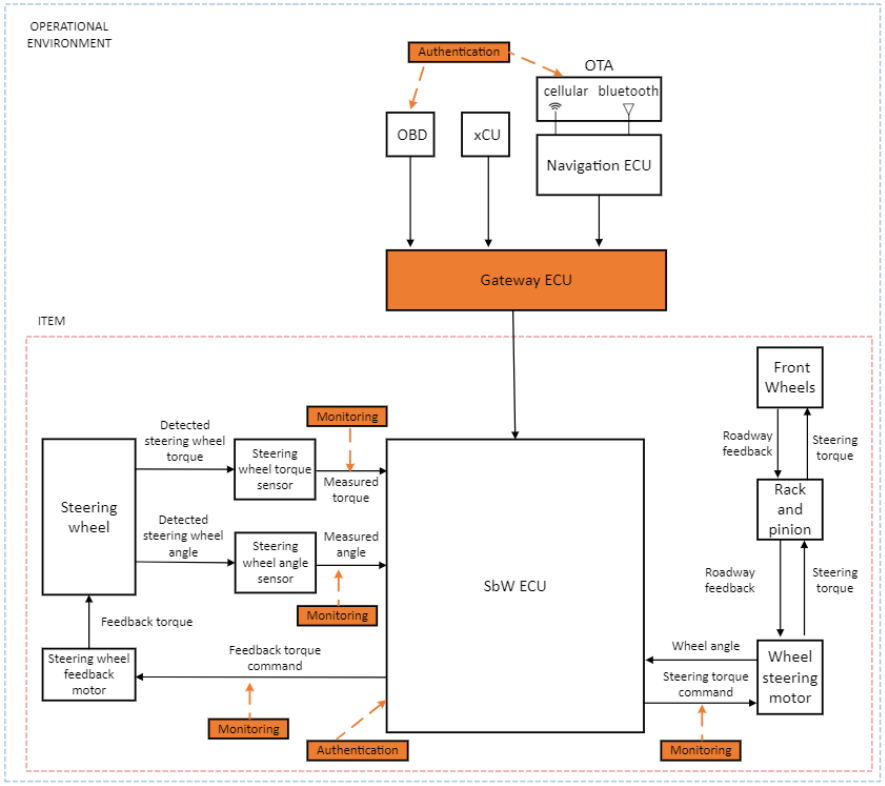

Figure 6.3 Cybersecurity concept architecture

6.2.3.2 Cybersecurity Requirements

Cybersecurity requirements that derived from cybersecurity goals of the item and operational environment in the below.

Table 6.16 Requirement 001

Requirement ID	Req001
Requirement	OTA updates shall be encrypted via using secure communication channel.
Cybersecurity claim	Over the air (OTA) authentication shall be provided against network attacks via secure OTA update
Derived cybersecurity goal(s)	CSG01: The integrity, availability and authentication/authorization of SbW ECU shall be ensured
Allocation	OTA, SbW ECU

Table 6.17 Requirement 002

Requirement ID	Req002
Requirement	OTA authentication shall be provided via implemented the key/password to software.
Cybersecurity claim	OTA authentication shall be provided against physical and local attacks via secure OTA update
Derived cybersecurity goal(s)	CSG01: The integrity, availability and authentication/authorization of SbW ECU shall be ensured
Allocation	OTA, SbW ECU

Table 6.18 Requirement 003

Requirement ID	Req003
Requirement	SbW ECU shall be authenticated via using digital signature that employing trust authority.
Cybersecurity claim	OTA authentication shall be provided against physical and local attacks via secure OTA update
Derived cybersecurity goal(s)	CSG01: The integrity, availability and authentication/authorization of SbW ECU shall be ensured CSG02: The integrity and availability between SbW ECU and xCU shall be ensured.
Allocation	OTA, SbW ECU

Table 6.19 Requirement 004

Requirement ID	Req004
Requirement	SbW ECU shall be authenticated for integrity in case of replacement.
Cybersecurity claim	OTA authentication shall be provided against physical and local attacks via secure OTA update
Derived cybersecurity goal(s)	CSG01: The integrity, availability and authentication/authorization of SbW ECU shall be ensured
Allocation	OTA, SbW ECU

Table 6.20 Requirement 005

Requirement ID	Req005
Requirement	Gateway ECU shall be implemented between SbW ECU and xCU.
Cybersecurity claim	The integrity and authentication between SbW ECU and xCU shall be ensured.
Derived cybersecurity goal(s)	CSG01: The integrity, availability and authentication/authorization of SbW ECU shall be ensured
Allocation	SbW ECU, xCU

Table 6.21 Requirement 006

Requirement ID	Req006
Requirement	Gateway ECU shall be implemented between SbW ECU and Navigation ECU.
Cybersecurity claim	The integrity and authentication between SbW ECU and Navigation ECU shall be ensured.
Derived cybersecurity goal(s)	CSG01: The integrity, availability and authentication/authorization of SbW ECU shall be ensured
Allocation	SbW ECU, Navigation ECU

Table 6.22 Requirement 007

Requirement ID	Req007
Requirement	Bluetooth communication shall be encrypted to all broadcast transmission with maximum encryption key size.
Cybersecurity claim	The SbW ECU authentication shall be provided for bluetooth interface.
Derived cybersecurity goal(s)	CSG01: The integrity, availability and authentication/authorization of SbW ECU shall be ensured
Allocation	SbW ECU, Bluetooth interface

Table 6.23 Requirement 008

Requirement ID	Req008
Requirement	Authentication shall be ensured that implement the unique key/password may protect against unauthorized access to OBD.
Cybersecurity claim	OBD authentication shall be provided against local attacks
Derived cybersecurity goal(s)	CSG01: The integrity, availability and authentication/authorization of SbW ECU shall be ensured
Allocation	SbW ECU, OBD

Table 6.24 Requirement 009

Requirement ID	Req009
Requirement	CAN bus monitoring interfaces based on intrusion detection system shall be integrated between steering wheel angle sensor and SbW ECU.
Cybersecurity claim	Steering wheel angle sensor authentication shall be monitored/authenticated against physical and local attacks
Derived cybersecurity goal(s)	CSG02: The integrity and availability of steering wheel angle sensor shall be ensured.
Allocation	SbW ECU, Steering wheel angle sensor

Table 6.25 Requirement 010

Requirement ID	Req010
Requirement	In the event of replacement, the steering wheel angle sensor be authenticated for integrity.
Cybersecurity claim	Steering wheel angle sensor authentication shall be monitored/authenticated against physical and local attacks
Derived cybersecurity goal(s)	CSG02: The integrity and availability of steering wheel angle sensor shall be ensured.
Allocation	SbW ECU, Steering wheel angle sensor

Table 6.26 Requirement 011

Requirement ID	Req011
Requirement	Monitoring interfaces shall be integrated between steering feedback actuator and SbW ECU.
Cybersecurity claim	Steering feedback actuator authentication shall be provided against physical and local attacks.
Derived cybersecurity goal(s)	CSG03: The integrity and availability of steering wheel feedback motor shall be ensured.
Allocation	SbW ECU, Steering feedback actuator

Table 6.27 Requirement 012

Requirement ID	Req012
Requirement	In the event of replacement, the steering wheel angle sensor shall be authenticated for integrity.
Cybersecurity claim	Handwheel angle sensor authentication shall be monitored/authenticated against physical and local attacks.
Derived cybersecurity goal(s)	CSG03: The integrity and availability of steering wheel feedback motor shall be ensured.
Allocation	SbW ECU, Steering feedback actuator

Table 6.28 Requirement 013

Requirement ID	Req013
Requirement	Monitoring interfaces shall be integrated between steering wheel torque sensor and SbW ECU.
Cybersecurity claim	Steering wheel torque sensor authentication shall be monitored/authenticated against physical and local attacks.
Derived cybersecurity goal(s)	CSG04: The integrity and availability of steering wheel torque sensor shall be ensured.
Allocation	SbW ECU, Steering wheel torque sensor

Table 6.29 Requirement 014

Requirement ID	Req014
Requirement	In the event of replacement, the steering wheel torque sensor be authenticated for integrity.
Cybersecurity claim	Steering wheel torque sensor authentication shall be monitored/authenticated against physical and local attacks.
Derived cybersecurity goal(s)	CSG04: The integrity and availability of steering wheel torque sensor shall be ensured.
Allocation	SbW ECU, Steering wheel torque sensor

Table 6.30 Requirement 015

Requirement ID	Req015
Requirement	Intrusion detection system based on CAN bus monitoring shall be integrated between steering wheel torque sensor and SbW ECU.
Cybersecurity claim	Steering wheel torque sensor authentication shall be monitored/authenticated against physical and local attacks.
Derived cybersecurity goal(s)	CSG04: The integrity and availability of steering wheel torque sensor shall be ensured.
Allocation	SbW ECU, Steering wheel torque sensor

Table 6.31 Requirement 016

Requirement ID	Req016
Requirement	Redundancy for steering wheel torque sensor shall be integrated.
Cybersecurity claim	Steering wheel torque sensor authentication shall be monitored/authenticated against physical and local attacks.
Derived cybersecurity goal(s)	CSG04: The integrity and availability of steering wheel torque sensor shall be ensured.
Allocation	SbW ECU, Steering wheel torque sensor

Table 6.32 Requirement 017

Requirement ID	Req017
Requirement	Monitoring interfaces shall be integrated between wheel steering motor and SbW ECU.
Cybersecurity claim	Steering feedback actuator authentication shall be monitored/authenticated against physical and local attacks.
Derived cybersecurity goal(s)	CSG05: The integrity and availability of wheel steering motor shall be ensured.
Allocation	SbW ECU, Wheel steering motor

Table 6.33 Requirement 018

Requirement ID	Req018
Requirement	In the event of replacement, the wheel steering motor be authenticated for integrity.
Cybersecurity claim	Steering feedback actuator authentication shall be monitored/authenticated against physical and local attacks.
Derived cybersecurity goal(s)	CSG05: The integrity and availability of wheel steering motor shall be ensured.
Allocation	SbW ECU, Wheel steering motor

7
CONCLUSION

In this thesis, STPA method is used for SOTIF-related activities under the automated lane centering automated driving function scope. Purpose and scope of the analysis is identified as initial step of STPA. Losses, vehicle-level hazards and vehicle-level safety constraints are identified as sub step of first step. Once the vehicle-level hazards have been identified, unsafe control actions, that will lead to hazards, are derived from control action that has been determined based on the modelling of the structure. As third step; causal scenarios, triggering conditions and potential insufficiencies and driver misuse, which are identified will lead to unsafe control actions. Following step is in this paper except for STPA methodology, risk evaluation. ISO 21448:2022 is specified that risk evaluation should be performed for identified triggering conditions to take measure or not regarding based on S and C ratings. As final step, improvement measures which determines risk evaluation of triggering conditions are identified. In the future, SOTIF for ALC system based on the STPA study can be extended to encompass additional control actions, in addition to the "Adjustment Vehicle's Steering Control" control action that has been determined.

This study is concentrated on the TARA and the cybersecurity concept including cybersecurity requirements that derived from cybersecurity goals and cybersecurity architecture. In this thesis, TARA have been performed for steer-by wire system. Prior to conducting the TARA, the boundaries, and functions of the item were identified. Subsequently, assets that attackers could use to gain access to the steer-by-wire system, were identified. Damage scenarios and impact of damage scenarios regarding compromising cybersecurity properties of assets are determined. In order to realize damage scenarios, threats were defined as actions taken by attackers who gain access to these assets. CAL and risk values have been derived based on impact rating and attack feasibility rating. Risk treatment decisions were specified considering risk values of threat scenarios. In this TARA, cybersecurity goals were determined that are the top-level cybersecurity requirements according to compromised cybersecurity properties. Within this determination, cybersecurity requirements were developed based on determined cybersecurity goals and

cybersecurity architecture was created regarding preliminary architecture from item definition. In addition, penetration testing, and other validation activities can be performed to demonstrate achievement of cybersecurity goals.

REFERENCES

[1] Steger, M., Karner, M., Hillebrand, J., Rom, W., & Römer, K. (2016, April). A security metric for structured security analysis of cyber-physical systems supporting SAE J3061. In *2016 2nd International Workshop on Modelling, Analysis, and Control of Complex CPS (CPS Data)* (pp. 1-6). IEEE.

[2] Xie, G., Zeng, G., Li, Z., Li, R., & Li, K. (2017). Adaptive dynamic scheduling on multifunctional mixed-criticality automotive cyber-physical systems. *IEEE Transactions on Vehicular Technology*, *66*(8), 6676-6692.

[3] Xie, G., Peng, H., Li, Z., Song, J., Xie, Y., Li, R., & Li, K. (2018). Reliability enhancement toward functional safety goal assurance in energy-aware automotive cyber-physical systems. *IEEE Transactions on Industrial Informatics*, *14*(12), 5447-5462.

[4] Xie, G., Peng, H., Huang, J., Li, R., & Li, K. (2019). Energy-efficient functional safety design methodology using ASIL decomposition for automotive cyber-physical systems. *IEEE Transactions on Reliability*.

[5] "Global Automotive Cybersecurity Report," Upstream Security, Technical Report 2018, 2019.

[6] Scalas, M., & Giacinto, G. (2019, October). Automotive cybersecurity: Foundations for next-generation vehicles. In *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS)* (pp. 1-6). IEEE.

[7] Wang, Y., Wang, Y., Qin, H., Ji, H., Zhang, Y., & Wang, J. (2021). A systematic risk assessment framework of automotive cybersecurity. *Automotive Innovation*, *4*, 253-261.

[8] Miller, C., & Valasek, C. (2015). Remote exploitation of an unaltered passenger vehicle. *Black Hat USA*, *2015*(S 91), 1-91.

[9] Petit, J., Stottelaar, B., Feiri, M., & Kargl, F. (2015). Remote attacks on automated vehicles sensors: Experiments on camera and lidar. *Black Hat Europe*, *11*(2015), 995.

[10] Fritzell Westlund, M., & Song, X. (2022). Steer-by-wire system safety aspects.

[11] Tokody, D., Mezei, I. J., & Schuster, G. (2017). An overview of autonomous intelligent vehicle systems. *Vehicle and Automotive Engineering: Proceedings of the JK2016, Miskolc, Hungary*, 287-307.

[12] Becker, C., Yount, L., Rozen-Levy, S., & Brewer, J. (2018). *Functional safety assessment of an automated lane centering system* (No. DOT-VNTSC-NHTSA-17-01). United States. Department of Transportation. National Highway Traffic Safety Administration.

[13] Leveson, N. G. (2016). *Engineering a safer world: Systems thinking applied to safety* (p. 560). The MIT Press.

[14] Sundaram, P., Vernacchia, M., Wagner, M. S., Thomas, J., & Placke, S. (2014, March). Application of STPA to an automotive shift-by-wire system. In *STAMP Workshop: Cambridge, MA, USA*.

[15] Hommes, Q. V. E. (2015, January). Safety analysis approaches for automotive electronic control systems. In *Society of Automotive Engineers' Meeting* (pp. 1-16).

[16] Van Eikema Hommes, Q. (2016). *Assessment of safety standards for automotive electronic control systems* (No. DOT-VNTSC-NHTSA-13-03). United States. Department of Transportation. National Highway Traffic Safety Administration.

[17] Abdulkhaleq, A., Wagner, S., & Leveson, N. (2015). A comprehensive safety engineering approach for software-intensive systems based on STPA. *Procedia Engineering*, *128*, 2-11.

[18] Ismail, R. (2017). Next-generation lane centering assist system: design and implementation of a lane centering assist system, using NXP-Bluebox.

[19] Rath, J. J., Senouth, C., & Popieul, J. C. (2019). Personalised lane keeping assist strategy: Adaptation to driving style. *IET Control Theory & Applications*, *13*(1), 106-115.

[20] Taxonomy, S. (2016). Definitions for terms related to driving automation systems for on-road motor vehicles (j3016). *Soc. Automot. Eng., Warrendale, PA, USA, Tech. Rep. J3016_201806*.

[21] Arogeti, S. A., Wang, D., Low, C. B., & Yu, M. (2012). Fault detection isolation and estimation in a vehicle steering system. *IEEE Transactions on Industrial Electronics*, *59*(12), 4810-4820.

[22] Mortazavizadeh, S. A., Ghaderi, A., Ebrahimi, M., & Hajian, M. (2020). Recent developments in the vehicle steer-by-wire system. *IEEE Transactions on Transportation Electrification*, *6*(3), 1226-1235.

[23] Fritzell Westlund, M., & Song, X. (2022). Steer-by-wire system safety aspects.

[24] International Organization for Standardization. (2021). *ISO/SAE 21434: 2021: Road Vehicles: Cybersecurity Engineering*. ISO.

[25] Xu, S., Ding, H., Du, A., Chu, C., Han, Y., Li, H., & Zhu, Z. (2022, October). A review of SOTIF research for human-machine driving mode switch of intelligent vehicles. In *2022 6th CAA International Conference on Vehicular Control and Intelligence (CVCI)* (pp. 1-6). IEEE.

[26] No, I. S. (2022). 21448: 2022; Road Vehicles—Safety of the Intended Functionality. *International Organization for Standardization: Geneva, Switzerland*.

[27] Brewer, J., Becker, C., Pollard, J., & Yount, L. (2018). *Functional safety assessment of a generic automated lane centering system and related foundational vehicle systems* (No. DOT-VNTSC-NHTSA-17-01). United States. Department of Transportation. National Highway Traffic Safety Administration.

[28] Leveson, N. G., & Thomas, J. P. STPA HANDBOOK, March 2018. Massachusetts Institute of Technology. лектронное издание.

PUBLICATIONS FROM THE THESIS

Conference Papers

1. O.Ozcetin, M.T.Emirler, “Elektrikli Araçlardaki Kablo Yönlendirmeli Direksiyon Sistemleri için Tehlike Analizi ve Risk Değerlendirmesi” TOK 2023 Turkish Annual Meeting on Automatic Control; İstanbul Technical University, İstanbul