Otto-von-Guericke-University Magdeburg
Faculty of Electrical Engineering and Information Technology
Chair for Electromagnetic Compatibility

Non Technical Project Seminar (NTPS)

Autonomous Vehicle Safety Analysis and Assessment

Submitted on: March 31, 2023

Submitted by: Arman Ahmed Khan (230601)

Advisor: Dr.-Ing. Mathias Magdowski

Examiner: Prof. Dr.-Ing. Ralf Vick

Abstract

The obstacles to creating and using autonomous cars are examined in this research. It is essential to ensure that these vehicles are built, tested, and used to minimise the danger of mishaps or malicious assaults as their use grows.

The first section of the research looks at the level of autonomy, the basic design of highly and completely autonomous cars, and the present regulatory environment for autonomous vehicles, including the function of governmental bodies and trade associations. It emphasizes the necessity of a unified regulatory strategy that strikes a balance between innovation and safety.

The report briefly discusses the importance of security and safety for autonomous cars. The main issues that must be resolved to enable the safe and secure operation of autonomous cars are then covered, such as the necessity of strong cybersecurity safeguards, efficient testing processes, ready infrastructure, liability, and insurance, among others.

Finally, the research offers several suggestions to assist assure the secure development and use of autonomous cars for policymakers, regulators, and industry stakeholders. The necessity for standardized testing procedures, redundant, diversified, cutting-edge sensor and artificial intelligence approaches, greater investment in cybersecurity research, etc., are some of these proposals.

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG | EIT | FACULTY OF ELECTRICAL ENGINEERING AND INFORMATION TECHNOLOGY

Non-Technical Project Task Assignment

for Mr. Arman Ahmed Khan (born on 10.12.1995 in Ferozepur Jhirka, India)

Topic: Autonomous Vehicle Safety Analysis and Assessment

As the world is changing at a drastic rate advancing automation and robotics, with the rise of machine learning and computational power, the dream of autonomous driving is considered a feasible goal that can be achieved in near future. But despite the promising technologies and advancements, one of the most challenging problems faced in commercializing fully autonomous vehicles in uncontrolled environments remains testing and validation. It would take a lot of autonomous vehicles driving 24/7 to demonstrate a failure rate low enough to have only a certain number of fatalities per several hundred million kilometers. Hence, the industry needs to aggressively try to simulate and analytically assess the scenarios to identify and understand the potential failures of autonomous driving systems as far as possible.

This report will try to answer what safety means in the aspect of autonomous vehicles, different types of standards defined for the safety of autonomous vehicles, different stages of autonomous safety, the limitation of currently deployed strategies in failure management of autonomous vehicles, and the start-of-the-art purposed solutions for tackling the safety problem. How can simulation play a major role in safety analysis?

The main objective of this work is literature analysis.

In detail the following things must be done:

- literature research,
- writing a report (at least 30 pages, at most 40 pages, from the introduction to the summary), and
- giving a final presentation of 15 minutes.

The report should be written in the document markup language LaTeX, which is a quasi standard for scientific publication, or using the SciFlow online editor at `https://app.sciflow.net/`.

Magdeburg, August 23, 2022

Prof. Dr.-Ing. Ralf Vick
Assignor of the task

Date of issue: 17.08.2022

Date of submit: 11.10.2022

Editing time: 8 weeks

Advisor: Dr.-Ing. Mathias Magdowski

Examiner: Prof. Dr.-Ing. Ralf Vick

Figure 1: Original Task Sheet

Declaration by the candidate

I hereby state that this report is my own creation and hasn't been filed anywhere for any distinction. Wherever additional sources of data were consulted, they were noted.

The work has not been made public or submitted to any other testing body in the same or a comparable format.

I also grant permission for the Otto von Guericke University of Magdeburg (OvGU) or any other commissioned third party, such as *iParadigms Europe Limited*, the provider of the plagiarism-detection service "Turnitin", to duplicate, save, and archive my work (free of charge, without restriction locally, and for an indefinite period of time) to check it for plagiarism and to improve the evaluation of results.

Arman Ahmed Khan

Magdeburg, March 31, 2023

Contents

Acronyms

ADAS Advanced Driver–Assistance Systems 3, 26
ADS Automated Driving System 3
AI Artificial intelligence 3
ANN Artificial Neural Network 3
ASIL Automotive safety integrity level 3, 25
AV Autonomous Vehicle 3

CAN Controller Area Network 3, 38
CNN Convolution Neural Network 3, 12

FSM Finite State Machine 3, 16

GPS Global Positioning System 3, 11, 14, 15, 18, 19

HMI Human Machine Interaction 3

ICP Iterative Closest Point 3, 15
IMU Inertial Measurement Unit 3, 11, 14, 18, 19
ISO International Organization for Standardization 3, 22, 26

LiDAR light detection and ranging 3, 12–14, 17, 19, 37

MPC Model Predictive Control 3

NDT normal distributions transform 3, 14
NIST National Institute of Standards and Technology 3, 21

ODD Operational Design Domain 3, 28

Radar radio detection And ranging 3, 12, 17, 37
RNN Recurrent Neural Network 3
ROS Robotic Operating System 3
RRT rapidly–exploring random tree 3, 17

SAE Society of Automotive Engineers 3, 8, 21, 30
SLAM Simultaneous Localization and Mapping 3, 13
SOTIF Safety of The Intended Functionality 3, 21, 26–30

TARA Threat Analysis and Risk Assessmen 3, 31

UAV Unmanned Areal vehicles 3
UGV Unmanned Ground vehicle 3
UL Underwriters Laboratories 3, 21, 32

V2V Vehicle–to–Vehicle 3
V2X Vehicle–to–Everything 3, 11

List of Figures

List of Tables

1 Introduction

Autonomous vehicles, sometimes called self-driving cars, have been fitted with cutting-edge technologies that allow them to navigate, detect, and react to their environment without human interaction. Since the early 20th century, the idea of autonomous cars has evolved, with noteworthy developments occurring in the last few decades due to a rising desire for better transportation ease, efficiency, and safety.

The general use of this technology depends on addressing serious concerns about the safety and security of autonomous cars. Autonomous cars have the potential to transform transportation since they can lower human error and increase safety. However, certain safety and security issues specific to autonomous cars must be addressed to enable this technology's safe and secure implementation.

With the creation of the first self-driving automobile, the "American Wonder" by Houdina Radio Control Corporation in 1926, autonomous cars were first introduced in the early 20th century [1]. The 1980s saw a considerable increase in interest in the idea as Carnegie Mellon University created the Navlab, the first autonomous vehicle [2]. Since then, the technology has quickly improved thanks to significant investments from both the IT sector and the car industry.

Hardware and software technologies are used by autonomous cars to navigate and react to their environment. These innovations combine a variety of sensors, including cameras, lidar, radar, and ultrasonic sensors, with machine learning and artificial intelligence algorithms that analyze and interpret the data from these sensors to make judgments and steer the vehicle.

Recent years have seen considerable advancement in autonomous cars thanks to extensive research and development investments from numerous significant automakers and technology firms. Commercially available Level 2 and Level 3 autonomous vehicles currently only offer a limited degree of automation when driving on the highway or in parking lots. However, fully autonomous Level 4 and 5 cars are still in the research and development stage and have not yet seen widespread use [3].

Many obstacles still exist in assuring the safety and security of this technology, despite

breakthroughs in the creation of autonomous cars. Ensuring the sensors and algorithms used by autonomous vehicles are accurate and reliable is one of the biggest hurdles. To guarantee safe and effective functioning, these technologies must precisely sense and react to their surroundings [4].

Keeping autonomous cars' cybersecurity up to par is a significant concern since they are susceptible to hacking and cyberattacks [5, 6]. Autonomous vehicle deployment poses moral and legal issues, such as who is responsible for mishaps or accidents [7].

Autonomous vehicle security and safety are essential for this technology's success and extensive use. However, although there has been great progress in creating autonomous cars, several issues still need to be resolved, such as assuring the accuracy and dependability of the sensors and algorithms utilized and ensuring these vehicles' cybersecurity. [8] To guarantee the safe and responsible deployment of autonomous cars, it is crucial to emphasize safety and security as research and development proceed.

2 Level of Autonomy

The Society of Automotive Engineers (SAE) has created a standard called SAE J3016 that outlines the degrees of driving automation for on-road cars. From little automation to complete automation, the standard offers a uniform vocabulary and structure for expressing the capabilities of automated vehicles [9].

From no automation to full automation, SAE J3016 [10] outlines six stages of automation:

Level 0 **No automation** - the driver completely controls the vehicle.

Level 1 **Driver Assistance** - Although the car contains certain systems that help the driver, such as adaptive cruise control or lane-keeping assistance, the driver is still in charge of most driving-related decisions.

Level 2 **Partial Automation** - The car contains two or more driver aids that simultaneously regulate steering and acceleration/deceleration. Yet the driver must always be prepared to take over at any moment.

Level 3 **Conditional Automation** - In some circumstances, the vehicle may perform all driving elements, but the driver must be prepared to take over when necessary.

Level 4 **High Automation** - Under some circumstances, the car can handle all aspects of driving. Thus, the driver is not required to take over.

Level 5 **Full Automation** - The driver does not need to take over because the vehicle can do all aspects of driving in any situation.

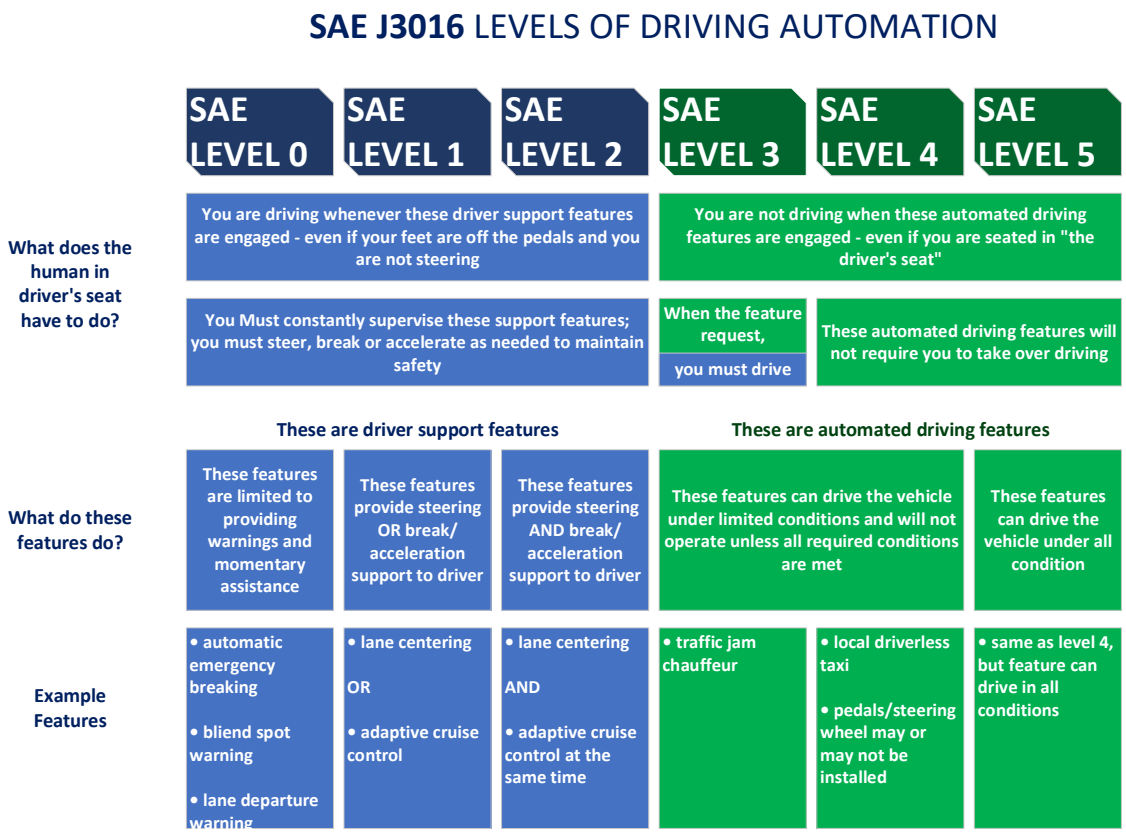

Figure 2.1: SAE J3016 Levels of Driving Autonomy [10]

Communication between industry participants, such as manufacturers, regulators, and customers, is crucial, and SAE J3016 offers a standard means of presenting the capabilities of autonomous cars. The standard offers regulators a framework for creating rules that assure the safety of automated cars and allows customers to evaluate the automation capabilities of various vehicles [9].

The SAE J3016 standard is crucial for creating and implementing autonomous vehicles. It offers a uniform vocabulary and structure for characterizing these vehicles' capabilities to assure safety and enable communication amongst stakeholders.

3 Autonomous Vehicle Architectures

Self-driving cars, sometimes called autonomous vehicles, use a mix of hardware and software technologies to navigate, recognize, and react to their environment without a driver's assistance. The underlying technology uses sensors, communication networks, and sophisticated computer tools to operate the vehicle and make choices depending on its operating environment. [11]

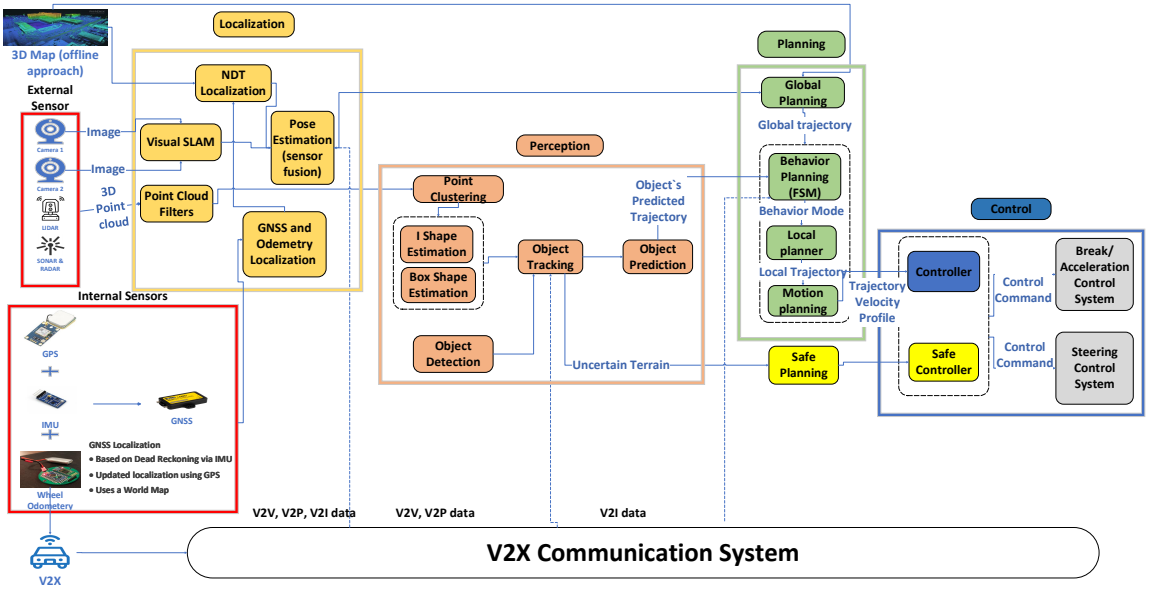

Figure 3.1: Autonomous Vehicle Architecture

Here's a more thorough breakdown of how autonomous cars operate:

Perception: The initial phase of autonomous vehicle operation uses sensors to identify and understand the surrounding environment. Cameras, lidar, radar, and ultrasonic sensors are some examples of these sensors. The information gathered by these sensors is then processed by computer vision algorithms to identify and classify objects such as other vehicles, pedestrians, and obstacles. Lidar and radar identify objects and their vicinity to the car, while cameras detect visual information such as lane lines, road signs, and barriers. Close-range sensing applications, like parking, can use ultrasonic sensors [4, 12].

Mapping: High-definition mapping is another tool used by autonomous cars to navigate their surroundings. Detailed maps of the surrounding area, including the roads,

traffic lights, and other features, must be made in order to do this. These maps are then utilized to direct the car along a predetermined route, with localization employed to establish the vehicle's position with respect to the map.

Localization: The process of localization involves locating and orienting the vehicle inside the mapped area. Many methods can accomplish this, such as Inertial Measurement Unit (IMU), Global Positioning System (GPS), ocular odometry, or laser-based localization [11, 13].

Planning: The car may start planning its course once it has observed its surroundings, produced a map and located itself on that map. In order to do this, algorithms must be used to find the best route while accounting for obstructions, traffic, and other variables. The design process may also include the passengers' preferences, such as avoiding twisting or high-speed highways [13, 14].

Control: Control requires moving the vehicle along the intended path as the last stage in autonomous vehicle operation. Actuators, such as brakes and motors, are used for acceleration, braking, and steering of the vehicle, and the onboard computer of the vehicle controls them [15, 16].

The architecture of an autonomous vehicle also includes various communication modules that enable the vehicle to communicate with other vehicles and the infrastructure around it [17]. This includes wireless communication modules such as Wi-Fi, cellular, and Vehicle–to–Everything (V2X) communication, which allows the vehicle to communicate with other vehicles, pedestrians, and infrastructure such as traffic lights and road signs [18, 19].

The vehicle continuously monitors and modifies each action as it travels through its surroundings. The onboard computer is in charge of examining the information from the numerous sensors and selecting the best course of action for real-time vehicle control. Autonomous cars rely on cutting-edge computer technology, such as artificial intelligence and machine learning algorithms, to make prompt and precise judgments, which demands a lot of processing power [11].

One of the key challenges in designing an autonomous vehicle architecture is ensuring the safety and security of the system. This includes ensuring that the sensors and processing units are reliable and accurate, that the algorithms are robust and able to handle unexpected situations, and that the communication modules are secure and protected from cyberattacks [20]. To ensure the safety and security of the system, various standards and regulations have been developed, such as ISO 26262 [21] and SAE J3061 [22], which provide guidelines for designing safe and secure autonomous vehicle architectures.

To overcome these challenges, the architecture includes various safety and security features that ensure the vehicle operates reliably and securely. These features include redundancy in critical components such as sensors and control systems [23], fail-safe mechanisms to prevent accidents in the event of a system failure [24], and encryption and authentication protocols to prevent unauthorized access or tampering.

Different autonomous vehicle architectures exist, depending on the specific requirements of the vehicle's application. For example, an autonomous car designed for city driving may have different sensor configurations and decision-making algorithms than an autonomous truck designed for highway transportation. Additionally, the architecture of an autonomous vehicle may change over time as new technologies and algorithms are developed and incorporated into the system.

The technology that underpins autonomous vehicles has the potential to revolutionize transportation by enhancing safety, reducing congestion, and raising the general effectiveness of our transportation systems. However, issues still need to be resolved, such as ensuring the dependability and accuracy of the sensors and algorithms used.

3.1 Perception Module

An autonomous vehicle's ability to perceive its environment and comprehend its circumstances is a key component of its usefulness. The perception stack in the workflow for autonomous vehicles is in charge of gathering and analyzing data from various instruments, including cameras, light detection and ranging (LiDAR), and radio detection And ranging (Radar), to produce a 3D depiction of the world around the car.

The perception stack comprises three primary modules: sensor fusion, object detection, and object tracking.

Data collection, the first stage of the awareness stack, is where the sensors gather unprocessed information about the surroundings. The data is then preprocessed to weed out unnecessary information and remove noise. Sensor integration comes after this phase. The sensor fusion module creates a unified picture of the world, which integrates input from various sensors. The program makes use of Kalman filtering [25], particle filtering [26], or Bayesian networks to merge the information and eliminate noise, outliers, and inconsistencies [27].

The object detection module uses deep learning algorithms such as Convolution Neural Network (CNN) or region-based CNNs (R-CNNs) to detect and identify objects in the

environment. The impediments that are identified by this module include road signs, people, and cars. The item's position, height, and direction are all included in the bounding box that the object recognition module creates around it [28, 29].

The object tracking module employs numerous object recognition frames to forecast the future position of the identified objects. This module tracks the object's velocity and predicts its future location using methods like the Kalman filter or particle filter. The car can make wise choices by anticipating the movements of other things in the surroundings thanks to object tracking [30].

Scene comprehension is the last step in the perception stack, where the system analyzes the input to determine the general dynamics and structure of the picture. The scene comprehension module provides important details like the location and direction of the car, the state of the roads, and the volume of traffic. The decision-making, planning, and management components of the autonomous car pipeline require this knowledge.

Overall, perception algorithms provide the vehicle with spatial awareness, which is essential for allowing autonomous cars to travel securely and effectively in challenging settings.

3.2 Mapping and Localization Module

The mapping and localization stack is crucial to the autonomous vehicle process because it enables the vehicle to comprehend and manage its surroundings correctly. It is made up of several sensors, algorithms, and pieces of software that all work together to deliver precise information about the location and environs of the car.

The creation of an in-depth model of the area in which the car will function is the first stage in the Mapping and Localization stack. This process involves using various sensors such as LiDAR, cameras, and radar to collect data about the surrounding environment. Once this information has been gathered, it is analyzed and combined to produce a high-resolution 3D model of the surroundings. This is typically done using Simultaneous Localization and Mapping (SLAM) techniques [31], which combines odometry, visual information, and sensor data to create a 3D map of the environment. This map gives the vehicle a thorough grasp of its surroundings, including where things, structures, and locations are located. The map is refreshed as the car moves along and is saved in its memory [13,14].

Localization, the following stage, entails pinpointing the vehicle's exact location and orientation within the mapped environment. This is done using the vehicle's sensors, such

as IMU, GPS, odometry and LiDAR, to compare the current surroundings to the map. By comparing the two, the car can precisely identify its location and direction within the surroundings.. Techniques like normal distributions transform (NDT) Localization [32] compares the map and localise the ego vehicles. In situations where there may be several routes to follow, this knowledge is essential for the vehicle to navigate securely. Real-time map updates are made as new sensor data comes in while the car moves through the area. As a result, the car can always correctly depict its surroundings and modify its trajectory as necessary.

Autonomous cars' secure and dependable functioning depends on the mapping and localization stack. For the car to be able to traverse complicated settings, avoid obstructions, and make crucial choices in real-time, accurate tracking and localisation are required. Additionally, since mistakes or discrepancies may have significant safety consequences, the accuracy and dependability of these components must be continuously monitored and kept. As a result, this technology is continuously developing as new instruments, software, and algorithms are created to increase its precision and dependability.

All things considered, integrating mapping, localization, and sensor fusion algorithms allow driverless cars to move around in complicated and dynamic settings securely and effectively.

3.2.1 3D Map Creation

Creating a 3D map of the environment is a key component of the perception module in autonomous vehicles [20]. Here are the general steps involved in creating a 3D map from sensor data:

Sensor data collection: The first step is to collect data from various sensors such as lidar, cameras, and GPS.

Point cloud generation: The data from LiDAR sensors are typically used to create a 3D point cloud of the environment. LiDAR sensors emit laser beams that bounce off objects in the environment and return to the sensor. The distance between the sensor and the object is calculated from the time it takes for the beam to return, enabling for the construction of a 3D point cloud.

Data filtering: The accuracy of the image can be impacted by the noise and artefacts in the original point cloud data. Voxelization, outlier elimination, and segmentation are examples of data filtering methods that are used to eliminate noise and enhance the clarity of the point cloud.

Registration: To produce a unified 3D image after the point cloud data has been filtered, it is frequently required to record data from various instruments. This involves aligning the point clouds from different sensors using Iterative Closest Point (ICP) techniques [33].

Map creation: Once the point clouds are registered, a 3D map of the environment can be created using voxel-based or mesh-based techniques [34]. These methods involve dividing the point cloud into distinct areas and using those regions to depict the world.

Map refinement: The map can be refined further by incorporating data from other sensors such as cameras and GPS. This can help increase the map's accuracy and ensure it accurately depicts the condition of the surroundings.

Overall, producing a 3D model from sensor data is a challenging process that calls for advanced algorithms and methods. However, autonomous cars can travel securely and effectively in complicated and dynamic settings thanks to a high-quality 3D map.

3.2.2 Localization

The process of locating an autonomous car in a predetermined location and direction is known as localization. It is a crucial part of autonomous vehicles' sensing and control algorithms. The general steps involved in localization for autonomous vehicles are:

Localization algorithms: After combining data from various instruments to generate a 3D map, localization is accomplished in driverless cars using a variety of algorithms, such as the Kalman filter, Particle filter, and Monte Carlo Localization [35]. These algorithms determine the location and orientation of the car within the surroundings using the sensor data and the map.

Map matching: By comparing the sensor data with the map, the "map matching" method increases localization precision. The vehicle's location is predicted by the localization algorithm using the map, which then contrasts with sensing data. If there is a difference, the algorithm modifies the predicted location based on the sensor data.

In general, localization is a difficult process requiring advanced methods and algorithms. It is necessary for automated cars to travel securely and effectively in complicated and dynamic settings.

3.3 Planning Module

An essential part of an automated vehicle pipeline, the planning module creates a viable and secure route for the vehicle. The module analyzes the vehicle's present condition, reads sensor data, and projects future conditions to choose the best course of action.

The planning module creates a high-level path plan using data from the perception and mapping/localization modules. This plan is then modified using the vehicle's kinematics, dynamics, and control inputs to produce a lower-level plan. The scheduler must consider limitations like speed limits, lane markers, and other road users to produce a viable and secure trajectory.

Several planning strategies for driverless vehicles include rule-based systems, model predictive control, and optimization-based techniques. Rule-based systems produce a trajectory using a collection of preset principles. In comparison, model predictive control creates a route that meets a set of conditions using a model of the vehicle's dynamics. Numerical optimization is used in optimization-based techniques to produce an ideal trajectory that meets constraints and reduces a cost function [15].

The planning module is essential for maintaining the dependability and safety of a driverless car. A well-designed planner must be able to manage complicated and dynamic settings while producing a car trajectory that is both secure and effective. The manager must also have the flexibility to adjust to environmental changes like the presence of building sites, walkers, or other unforeseen circumstances.

The Planning Module comes at the end of the chain for driverless vehicles. The planning module utilizes the information from the perception and mapping modules to decide how the car should act in relation to its surroundings.

The primary goal of the planning module is to produce a path that navigates the vehicle from its present position to its target securely and effectively. To produce the best route, the module considers several variables, such as the vehicle's speed, acceleration, braking, and turning radius. It also takes into account the physical restrictions of the car as well as regional traffic rules and regulations.

The mobility and behaviour planning modules are common divisions of the planning module. The motion planning module aims to create a viable and secure route for the car. The behaviour planning algorithm, in comparison, decides on high-level driving behaviours like merging, passing and turning. Behaviour planner usually uses Finite State Machine

(FSM) [36] to decide the behaviour or state [37].

The motion planning module creates a route that avoids obstructions and follows the road layout using the information produced by the perception and localization modules. This route must also consider the vehicle's characteristics, such as its top speed and rate of acceleration. The motion planning module considers the environment's uncertainties, such as the existence of other cars, people, and unpredictable items.

The behaviour planning module decides the high-level driving behaviour necessary to follow the route generated by the motion planning module. It decides, for instance, whether the car should turn, decelerate down, or shift directions. In addition, the behaviour planning module considers the car's location, the driver's desires, and the traffic flow.

Here are the general steps involved in motion planning for autonomous vehicles:

Perception: As explained in the previous section, the first step is to perceive the environment using various sensors such as LiDAR, cameras, and Radar. Perception algorithms are used to analyze the sensor data to find the location and direction of the car, track down obstructions, and identify and monitor them.

Map creation: As explained in the previous section, a 3D environment map is created using sensor data. The map represents the location of obstacles and the vehicle's position.

Route planning: A route manager chooses the car's intended course. Typically, the route planner considers variables like the location, road conditions, speed limits, and any other pertinent restrictions.

Path planning: The car can travel from its present location to the target while avoiding obstructions thanks to the path planner's creation of a precise path. The path planner typically uses techniques such as A$*$ search [38] or rapidly–exploring random tree (RRT) to generate a path [39].

Trajectory generation: The path planner's route is used by the trajectory generator to create a precise trajectory that includes the vehicle's speed, acceleration, and steering angle at each location. To ensure the route is viable, the trajectory generator considers the car's kinematic and dynamic limitations.

Control: The trajectory produced by the trajectory generator is used by the automated vehicle's control system to calculate the inputs required to direct the vehicle's speed, including the throttle, stop, and steering angle. The control system adjusts

the motion of the car based on sensor data and ensures it stays on the planner's route by employing feedback control methods.

Overall, the planning module allows autonomous cars to move around in complicated and dynamic settings securely and effectively. To achieve secure and dependable automated driving, it must be able to create flexible plans that consider the environment's uncertainties and the vehicle's physical constraints.

3.4 Control Module

The planning module's results are translated into real vehicle motion by the control module, which is the last step in the process for driverless vehicles. It comprises processors that decide how the car ought to behave in real-time based on sensor data. The management module also ensures the car operates safely and complies with all applicable laws and regulations.

The throttle, stop, and steering systems are just a few of the actuators that receive the proper control impulses from the control module. It receives input from various sources, including the vehicle's perception and planning modules and other external data sources such as IMU, wheel odometry, GPS and maps.

Feedback control methods are frequently used in constructing the control module, where the control signals are modified in response to input from instruments and other data sources. In various travelling situations and settings, these control strategies aid in keeping the car steady and responsive.

The control module creates control impulses, keeps track of the vehicle's performance, and can start corrective actions if required. For instance, the control module may autonomously apply the brakes if the vehicle senses a possible collision to avoid or lessen the impact.

The control module uses the planning module's output to issue instructions to the actuators on the vehicle to carry out the intended route. To guarantee the safe and effective functioning of the vehicle, the control module employs model-based and learning-based control methods known as data-driven control.

Using statistical models, model-based control predicts the car's behaviour and then modifies the controls to match. These models might consider the vehicle's characteristics, the state of the road, and other elements that influence the efficiency of the vehicle. The control module can also use machine learning techniques to refine its control strategies by

learning from previous driving encounters.

The control module keeps track of the vehicle's instruments and ensures it operates within secure parameters. For instance, if the sensors identify one in the path, the control module will alter the vehicle's trajectory to escape an obstruction. If the car deviates from the intended trajectory or the control module notices unsafe behaviour, it can overrule the planning module.

The control module can improve the vehicle's performance based on fuel economy and passenger comfort and ensure secure vehicle operation. For instance, the control module can modify the speed and acceleration of the car to meet the intended degree of comfort and reduce gasoline usage.

Here are the general steps involved in the control module of an autonomous vehicle:

Motion planning: The motion planning module creates a trajectory for the car to follow that contains details about the intended pace, direction, and additional restrictions.

Vehicle state estimation: The control module estimates the vehicle's state (e.g., position, velocity, orientation, etc.) using various sensor data, such as GPS, IMU, LiDAR, and cameras.

Control signal generation: Based on the intended trajectory and the car's present condition, the control module produces control signals. These control signs frequently include instructions for steering, throttle and stopping.

Feedback control: To ensure that the vehicle stays on the intended course, the control module employs feedback control methods to modify the motion of the vehicle based on sensor data. For instance, the control module may change the steering angle to rectify the vehicle's path if it departs from the intended direction.

Actuation: The vehicle's actuators receive the control impulses used to direct the vehicle's movements. The car's steering, throttle, and stop mechanisms can serve as actuators.

Overall, the control module is essential to the infrastructure for driverless vehicles because it guarantees reliable and effective operation. The control module is an essential part of the pipeline for driverless vehicles because it has the ability to watch the vehicle's sensors, modify the controls, and improve performance.

4 Standards Related to Autonomous Vehicle Safety and Security

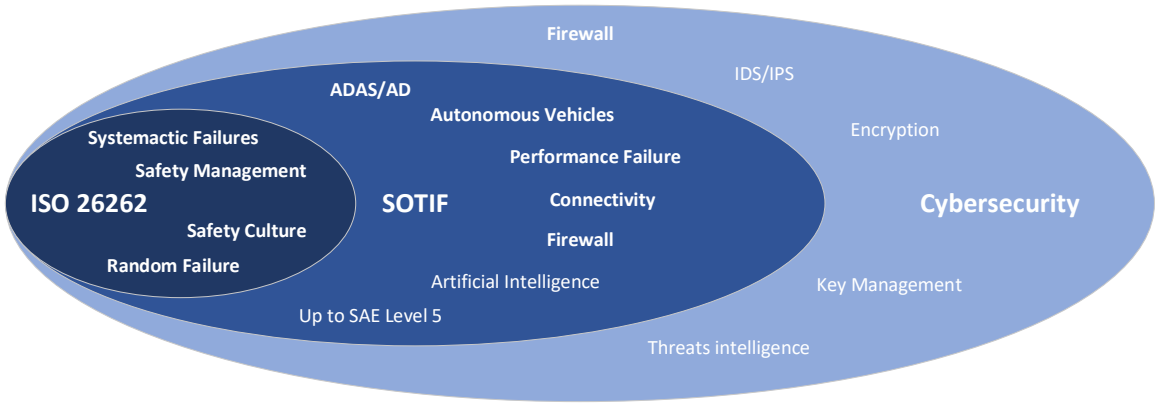

Figure 4.1: Autonomous Vehicle Safety and Security Standard [40]

Standards for autonomous car security and safety are necessary to guarantee these vehicles' security, reliability, and safety. Some of the essential standards related to safety and security for autonomous vehicles are mentioned in 4.1

Standard	Title	Organization
ISO 21448	Road Vehicles - Safety of the Intended Functionality (SOTIF)	International Organization for Standardization (ISO)
ISO 26262	Road Vehicles - Functional Safety	International Organization for Standardization (ISO)
SAE J3016	Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles	Society of Automotive Engineers (SAE)
SAE J3061	Cybersecurity Guidebook for Cyber-Physical Vehicle Systems	Society of Automotive Engineers (SAE)
UL 4600	Standard for Safety for the Evaluation of Autonomous Products	Underwriters Laboratories (UL)
IEEE 2846	Standard for Safety and Testing Requirements for Highly Automated Vehicles	Institute of Electrical and Electronics Engineers (IEEE)
EN 303 645	Cyber Security for Consumer Internet of Things	European Committee for Standardization (CEN)

Table 4.1: Key standards related to safety and security for autonomous vehicles

A more detailed explanation of the most significant guidelines for autonomous cars is listed here:

ISO 26262: The ISO 26262 standard offers a foundation for the practical safety of road cars. It outlines requirements for making components that must be secure, like those found in driverless vehicles. This specification includes all phases of a vehicle's existence, including design, production, use, and maintenance [23].

ISO 21448: This is a standard for the Safety of The Intended Functionality (SOTIF). It offers recommendations for spotting and mitigating potential risks and dangers resulting from automated cars' planned usefulness, like incorrect mapping or misinterpretation of sensor data [41].

SAE J3016: The SAE produced the SAE J3016 standard, which offers a standardized taxonomy and terminology for automated driving systems (ADS). There are five levels of mechanization in vehicles, from Level 0 (no automation) to Level 5. (full automation). This standard enables straightforward communication between engineers, decision-makers, and other concerned parties in creating autonomous vehicles [9].

SAE J3061: A standard developed by the SAE provides a structure for creating cybersecurity engineering standards for car systems, including driverless vehicles. It offers advice on controlling and reducing these risks throughout the development process and is created to handle the new risks presented by cybercrime attacks in the car industry. The standard's primary goal is to protect both people's and vehicle systems' safety, security, and privacy [22].

UL 4600: Underwriters Laboratories (UL) created the UL 4600 standard, which provides a base for the safety of driverless vehicles. It outlines the requirements for developing, testing, and approving automated car systems and the hardware, software, and other components that make up these systems. To ensure the security of autonomous vehicles, this guideline is addressed to manufacturers, suppliers, and officials [42].

NIST Cybersecurity Framework: The National Institute of Standards and Technology (NIST) Cybersecurity Framework offers recommendations and best practices for protecting information systems, including those utilized in autonomous cars. This approach identifies five key activities—identify, defend, monitor, react, and recover—that can help businesses manage and lessen cyber risks related to autonomous cars [43].

IEEE 2846: IEEE 2846 is a guideline offering advice on the ethical concerns of developing automated systems. In order to create autonomous vehicles responsibly, issues like responsibility, transparency, and the preservation of human rights must be considered [44].

ISO 21434: This is a standard published by the International Organization for Standardization (ISO) for the cybersecurity of road vehicles. It offers a structure for creating, putting into practice, and sustaining road car cybersecurity [45].

These requirements ensure the security, reliability, and safety of autonomous cars. They provide a structure for developing, assessing, and validating autonomous vehicle systems, which can help ensure that these vehicles are ready for use on our roadways. To keep up with new developments and issues, these guidelines must be revised as driverless vehicle technology develops.

4.1 ISO 26262: Functional Safety Standard

Road vehicle functional safety standard ISO 26262 was originally released in 2011 [21]. The ISO created the standard in response to modern automobiles' increasingly complicated electrical and software systems. It provides a foundation for guaranteeing the security of safety-critical components and systems, such as those used in autonomous cars.

The requirement is applicable from the time of creation until the dismantling of a car. It contains guidelines for developing, implementing, and managing hardware, software, automobiles, and safety-critical systems. ISO 26262 specifies four major parts.:

Management of Functional Safety: This part of the standard provides instructions for managing practical safety throughout the vehicle's lifetime. The safety administration, planning, assessment, verification, and validation requirements are described in detail.

Development at the System Level: This part of the standard provides guidelines for developing safety-critical systems at the system level. It includes system engineering criteria, hardware and program specs, and architectural design.

Development at the Hardware Level: This standard component gives guidelines for building safety-critical components. The requirements, testing, and proof for electronics design and development are covered.

Development at the Software Level: This standard part offers guidelines for developing safety-critical software. In addition to the requirements for creating software, it also involves testing and verification.

In order to determine the degree of effective safety required for each component or system, the standard adopts a risk-based methodology. With this approach, hazards are identified, their risks are assessed, and the necessary safety measures are determined.

ISO 26262 is a critical guideline for ensuring the practical safety of autonomous vehicles. To ensure the dependability and safety of these cars, it provides a structure for developing and analyzing safety-critical systems and components. As a consequence, the standard has been extensively adopted by the automotive industry and is now considered the industry standard for functional safety.

A worldwide guideline for the operational safety of motor vehicles is ISO 26262. It offers a foundation for guaranteeing the security of electrical and computer systems in all types of road vehicles, including motorcycles, trucks, buses, and passenger automobiles.

The standard was first released in 2011, and since then, it has undergone several updates to consider advancements in technology and business procedures. In the automobile sector, it is frequently used to guarantee the security of intricate systems, such as those found in highly automated and autonomous cars.

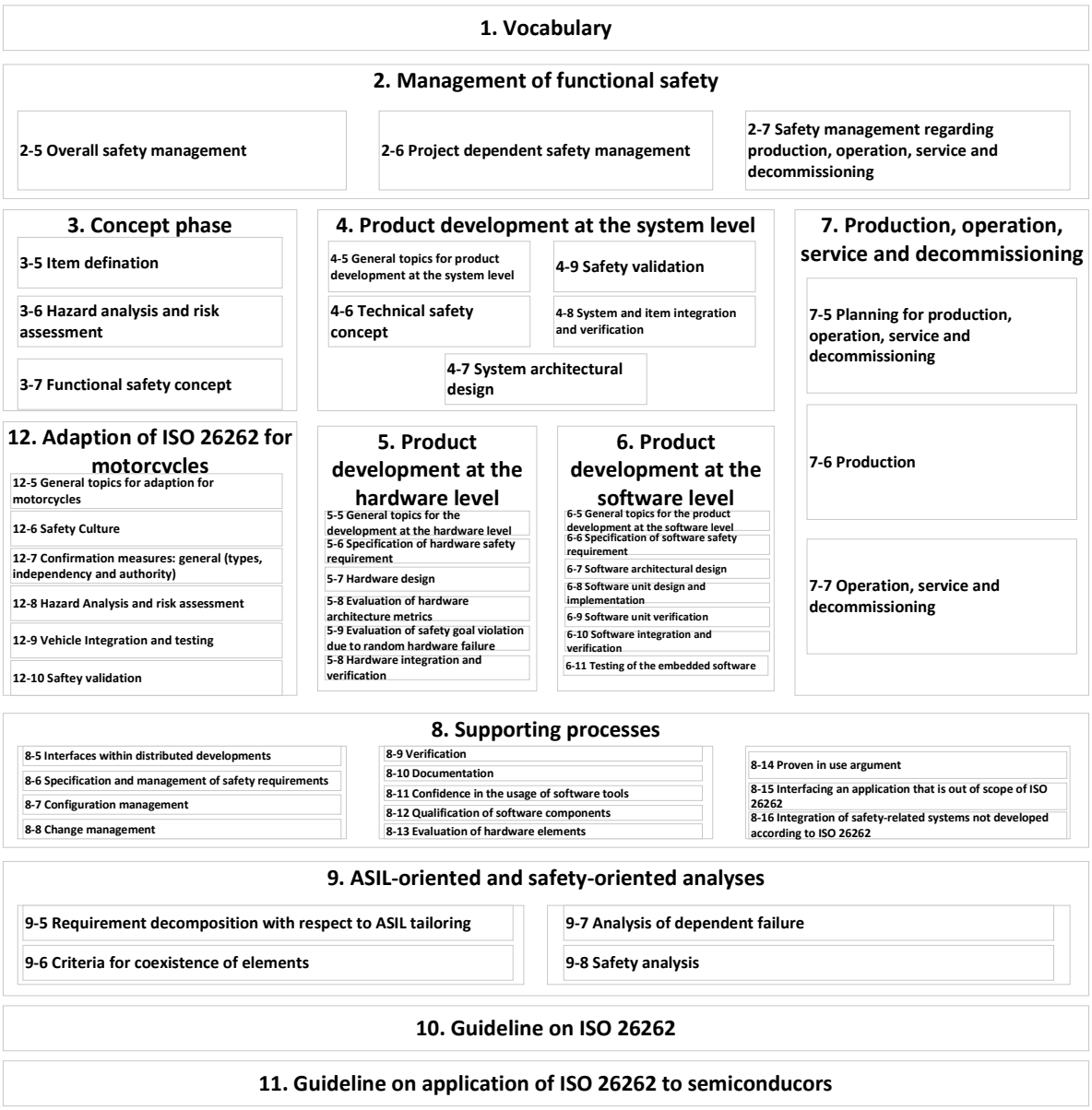

Figure 4.2: ISO 26262 Functional Safety Standard [21]

ISO 26262 is organized into ten parts, each covering a specific aspect of functional safety for road vehicles. These include:

Scope, definitions, and general requirements: The standard's purview is established, important words are defined, and basic functional safety standards are outlined in this section.

Management of functional safety: The administration of functional safety during the development process is covered in this section, along with planning, risk analysis, and safety verification and confirmation.

Concept phase: This section offers suggestions for creating road car system safety ideas.

Product development at the system level: The creation of safety standards, system design, and system integration for road car systems are covered in this section.

Product development at the hardware level: This section offers advice on creating design and verification specifications that are secure for hardware components of road car systems.

Product development at the software level: The creation of safety standards, as well as the design and verification of software for road car systems, are all covered in this section.

Production and operation: This section offers instructions on how to make sure that road vehicle systems are created and used in a trustworthy and secure way.

Supporting processes: The development of functional safety-enabling processes, such as configuration management, change management, and safety analysis, is covered in this section.

Automotive safety integrity level (ASIL)-oriented and safety-oriented analysis: This section offers instructions on assessing road car systems' safety using safety- and ASIL-oriented analysis methods.

Guidelines on ISO 26262: This part provides additional guidance on using and applying ISO 26262.

One of the key features of ISO 26262 is the ASIL) concept. A system's degree of safety risk is determined by this classification system based on the seriousness of its possible failures and the probability that they will occur. The ASIL levels range from A (lowest) to D (highest) and are used to determine the level of safety requirements that must be met in the design and development of a system.

The significance of a methodical strategy for functional safety is also emphasized by ISO 26262. It calls for safety requirements to be created and checked at each step of development, the definition of safety goals, and their tracking throughout the development process. Additionally, it necessitates using suitable techniques and instruments for risk evaluation, verification, confirmation and hazard analysis.

In addition to the ASIL classification system, the standard provides specific guidance on developing systems for autonomous driving.

The requirement for intricate hardware and software systems that must operate in perfect harmony presents one of the main obstacles in developing autonomous cars. The

guidelines in ISO 26262 for creating these systems cover functional safety standards, system architecture, and software development.

The standard also offers instructions on creating safety scenarios for automated cars. A safety case is a well-organized justification for why a system is secure to use. The assertion that the system satisfies its safety objectives and was planned and developed in accordance with pertinent standards and best practices is supported by evidence and reasoning in the document.

Developing safety cases for driverless cars can be difficult because it requires proving that the system is secure under various working circumstances. To assess the system's performance in various situations, including those that are challenging to reproduce in the real world, modelling and testing are required.

Overall, ISO 26262 is a vital standard for creating driverless cars because it offers a thorough framework for guaranteeing their dependability and safety. Manufacturers can help ensure that their autonomous cars satisfy the most significant safety and functional integrity standards by adhering to the advice given in the standard.

4.2 ISO 21448: Safety of Intended Functionality

A new road vehicle safety standard called ISO 21448 [41, 46], sometimes called "Road Vehicles - Safety of the Intended Functionality (SOTIF)" was released in 2019. In response to the growing complexity of Advanced Driver–Assistance Systems (ADAS) and driverless cars, the ISO created it. The standard is distinct from ISO 26262's functional safety, focusing on the safety of a vehicle's intended functioning.

SOTIF describes how a vehicle will act safely when its intended functionality is used under typical operating circumstances. This standard deals with situations that ISO 26262 does not cover, such as those that result from complex relationships between a car and its environs, unexpected sensor or algorithmic behaviour, and other dangerously unpredictable situations.

The comprehensive structure provided by ISO 21448 allows the identification, analysis, and mitigation of safety risks related to the planned use of a vehicle. The guideline lists three essential elements.:

Knowing the Expected Functionality's Safety-Related Performance: This standard part outlines the requirements for identifying safety threats and assessing how well a car performs its intended functions in terms of safety. It involves

locating circumstances that could pose safety risks, assessing the seriousness and propensity of those risks, and assessing the overall safety of the desired usefulness.

Safety Requirements and Specification of the Intended Functionality: This part of the standard specifies the requirements for creating safety criteria and safety requirements for the intended working of a vehicle. It describes safety-critical components, safety goals, and safety standards.

Validation and Confirmation of the Intended Functionality: In this part of the standard, the requirements for validating and confirming the intended functionality of a car are outlined. It involves verifying the safety-related performance of the intended features and that the safety standards and specifications have been met.

ISO 21448 is a critical standard for the security of autonomous vehicles and other cutting-edge driving aid technologies. It addresses safety risks not covered by ISO 26262 and provides a comprehensive approach for identifying, assessing, and lowering such risks. This standard is expected to become more important as the technology underpinning autonomous vehicles evolves to ensure their protection.

The safety hazards connected to a system or component's intended usefulness, including those unconnected to malfunctions or failures, can be assessed and managed using the recommendations in this standard.

The guideline applies especially to highly automated systems. Autonomous cars, where safety is greatly influenced by the system's intended usefulness. SOTIF is concerned with the safety risks that can arise from the interactions between the automated system and the environment, as well as the safety risks that can arise from the system's limitations.

SOTIF is intended to complement existing safety standards such as ISO 26262, which focus on the functional safety of systems and components. While functional safety ensures that a system or component performs its intended function safely and reliably, SOTIF is concerned with the unintended safety risks arising from its functionality.

The SOTIF standard provides a framework for identifying and managing safety risks associated with the intended functionality of a system or component. This includes an emphasis on spotting possible risks and investigating their causes and effects. Additionally, the guideline offers advice on evaluating and managing safety risks using techniques like scenario-based analysis and probability risk assessment.

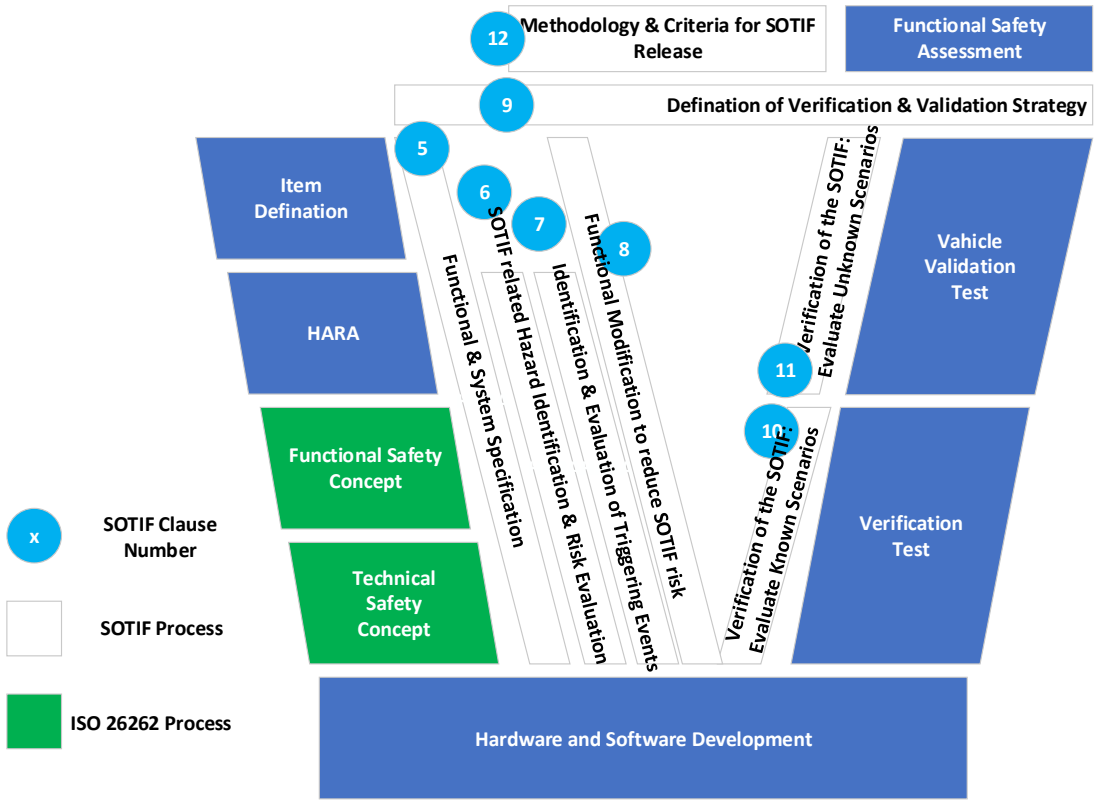

Figure 4.3: ISO 21448: Safety of Intended Functionality [41, 46]

One key aspect of the SOTIF standard is the Operational Design Domain (ODD) concept. The ODD is the set of operating conditions in which a system or component is intended to operate safely and reliably [47]. It includes factors such as road type, weather conditions, and traffic density. The SOTIF standard emphasizes the importance of defining the ODD for a system or component, which is critical for assessing and managing safety risks.

Another key aspect of the SOTIF standard is the importance of considering the "known unknowns" - the safety risks that are not yet fully understood or quantified. This necessitates a proactive strategy for safety, which includes continuous monitoring, research, and development of risk management strategies.

Overall, the standards provide the SOTIF An essential foundation for controlling safety threats related to the intended use of automatic and autonomous systems. It highlights the significance of adopting a proactive attitude toward safety and considering a wide variety of possible safety risks. As a result, it is crucial to ensure the dependability and safety of highly automated and driverless cars.

ISO 21448 provides guidelines and recommendations for achieving the SOTIF. SOTIF refers to the hazards that can arise from the system's functional limitations or unexpected behaviours that do not fall within the scope of traditional functional safety standards like ISO 26262.

ISO 21448 outlines a risk-based approach to identifying and addressing SOTIF hazards that are not covered by existing functional safety standards. It suggests using a methodical approach to finding and evaluating potential hazards, taking into account the system's intricacy, probability, and seriousness of potential hazards, as well as the intended practical design area of the vehicle.

The standard provides guidance on hazard identification, risk assessment, and risk management techniques. It also recommends methods for validating and verifying the SOTIF of autonomous vehicles, such as scenario-based testing and simulation. The guideline also stresses how crucial it is to consider human aspects in developing and using autonomous cars, such as designing user interfaces and driver monitoring systems.

ISO 21448 is a relatively new standard, first published in 2019, and is not yet widely adopted by the automotive industry. However, as autonomous vehicle technology continues to evolve, the need for guidance on SOTIF will become increasingly important.

By tackling the risks related to system constraints and unforeseen behaviours that are outside the purview of conventional functional safety standards, ISO 21448 marks a significant advancement in the development of autonomous vehicles. However, it has its restrictions and difficulties, just like any other norm.

The difficulty of finding and handling SOTIF hazards is one of the major issues with ISO 21448. SOTIF dangers, in contrast to conventional functional safety risks, may be challenging to pinpoint because they aren't always connected to a particular system function or component. Therefore, in order to handle these hazards, risk assessment and management methods may need to be modified or expanded.

Another challenge is the lack of a common understanding of SOTIF across the industry. As a relatively new concept, SOTIF is not yet well-defined, and different organizations may have different interpretations of what it entails. This might restrict ISO 21448's ability to increase the safety of autonomous cars and cause execution inconsistencies.

Last but not least, some parties who worry about the possible effects on growth and

development may oppose the adoption of ISO 21448. Implementing SOTIF requirements could increase the cost and complexity of development, leading to slower innovation and adoption of autonomous vehicle technology.

Despite these challenges, ISO 21448 represents an important step forward in ensuring the safety of autonomous vehicles. As the industry continues to develop, it is likely that further research and refinement of SOTIF concepts will be necessary to address new challenges and emerging technologies.

There are numerous ongoing initiatives to create complementary standards and rules that can aid in ensuring the safety of autonomous cars in order to resolve some of the issues with ISO 21448. One such initiative is the creation of ISO/SAE 21434, a new standard concentrating on cybersecurity threats related to linked and autonomous cars.

ISO/SAE 21434 [45] is intended to provide guidance on identifying, assessing, and managing cybersecurity risks throughout the lifecycle of autonomous and connected vehicles. It contains specifications for risk modelling, testing, validation and standards for secure development methods.

Several other standards and rules are being created in addition to ISO/SAE 21434 to ensure autonomous car safety. These cover functional safety, risk evaluation, and human factors engineering requirements.

In terms of guaranteeing the security and safety of autonomous vehicles, creating these norms and rules is a major advancement. By offering a uniform structure and set of criteria for creating these systems, these standards can help ensure that autonomous vehicles are created and implemented securely and responsibly.

4.3 SAE J3061: Cybersecurity for Autonomous Vehicles

The SAE released SAE J3061 [22], a cybersecurity manual for automotive systems, in 2016. It provides a comprehensive approach for identifying, assessing, and mitigating cybersecurity threats to automotive systems, including autonomous autos [22].

The standard was created in response to hacking, illegal access, harmful assaults, and other cybersecurity threats to cars. The manual offers guidance on protecting against different threats, including communication networks, hardware, software in vehicles, and systems linked to them.

SAE J3061 outlines a planned and methodical strategy to cybersecurity risk management for car systems. The standard defines the following key parts:

Cybersecurity Management Plan (CSMP): This is a thorough strategy for handling cybersecurity throughout a system's or vehicle's development lifetime. It contains guidelines, policies, and methods for finding, evaluating, and reducing cybersecurity threats.

Cybersecurity Risk Assessment: This method finds and evaluates a vehicle or system's cybersecurity threats. The system's components, design, and possible threats are all carefully examined.

Threat Analysis and Risk Assessmen (TARA): This is a methodical procedure for locating and evaluating possible cybersecurity risks and dangers. It thoroughly examines the design, parts, and possible weaknesses of the system [48].

Cybersecurity Validation and Verification: This procedure confirms that a car or system satisfies the CSMP's safety standards. It thoroughly examines the system's design, parts, and possible weaknesses.

Incident Response Plan (IRP): This is a strategy for handling cybersecurity mishaps that might happen while a car or system is being developed or used. It consists of steps for identifying, notifying, and minimizing occurrences.

Security Controls: Several security measures and best practices should be implemented to reduce cybersecurity threats. These measures are intended to stop or identify cybercrime events and lessen their effects when they do.

SAE J3061 offers a uniform language and structure for cybersecurity in the car business is one of the standard's main advantages. In order to handle cybersecurity risk effectively, cooperation and information exchange among stakeholders can be encouraged.

The guideline also promotes a proactive strategy to cybersecurity, which is a bonus. Stakeholders can identify and handle potential cybersecurity risks early in the development process before they become more challenging and costly to prevent by adhering to the cybersecurity lifecycle strategy described in the standard.

Implementing SAE J3061, however, also comes with some difficulties. For instance, the standard may be complicated and challenging for stakeholders unfamiliar with cybersecurity concepts. In addition, there may be variations in how different organizations interpret and implement the standard, leading to inconsistencies in cybersecurity approaches across

the industry.

It is crucial for businesses to spend money on staff safety education and training to deal with these issues. They should also collaborate closely with other industry players to encourage the uniform and efficient application of the standard.

SAE J3061 is an important standard for developing safe and secure autonomous and connected vehicles [22]. It provides a framework for effective cybersecurity risk management and promotes a proactive approach to cybersecurity. To guarantee the safety and security of cars and their occupants, stakeholders must continue to be diligent and adhere to the principles and rules outlined in this standard as the industry develops.

4.4 UL 4600 Standard

UL 4600 [42, 49, 50] is a new safety standard by UL) developed for autonomous vehicle technology. It is a collection of recommendations for evaluating the security of autonomous car systems. It was made to help ensure these systems are secure before being used on open roads.

The standard was created in reaction to the quickly changing autonomous car technology landscape and the requirement to create a uniform and open set of safety standards that can be used throughout the sector. Regardless of the unique technology or strategy various businesses use, UL 4600 seeks to provide a unified framework for the safety evaluation of autonomous car systems.

The standard comprises several standards and best practices that address different facets of the safety evaluation process, such as finding safety hazards, analyzing the risks involved, and creating and validating safety measures To mitigate those risks.

A risk-based strategy to safety evaluation is used by UL 4600, and it aims to find and reduce the risks that are most likely to endanger people, property, or the environment. The requirement also stresses the significance of openness and documentation throughout the safety evaluation process to guarantee that all parties know the safety risks and precautions related to autonomous car technology.

The fact that UL 4600 is flexible and adaptable to various automated car systems and technologies is one of its main characteristics. This means that various autonomous vehicle companies, including those building completely self-driving cars, drones, and other vehicles, can use the standard.

The standard includes several key elements regarding the requirements and processes outlined in UL 4600 [42, 49, 50]. These include:

Safety Case: A thorough description of the autonomous car system's safety-related features, including details on the system's creation, testing, and design.

Safety Requirements: System must comply with criteria in order to be deemed secure. Usually, these requirements are drawn from best practices, business standards, and other sources.

Safety Analysis: An in-depth examination of the risks and hazards that could be connected to the automated car system, as well as an evaluation of the system's capacity to identify and reduce these risks.

Verification and Validation: A process of putting the automated car system through testing and validation to make sure it complies with safety standards and operates as anticipated under different circumstances.

Functional Safety Management: Throughout the creation and lifecycle of the automated car system, functional safety is managed in a systematic way using functional safety management.

Companies must adhere to these requirements and conduct a comprehensive safety evaluation of their autonomous vehicle systems in order to be in compliance with UL 4600. Competent people with knowledge of practical safety and autonomous vehicle technology must perform this evaluation.

As of early 2023, UL 4600 has not yet been extensively accepted by the driverless car industry because it is still a comparatively new standard. However, a few businesses have begun utilizing UL 4600 as a foundation for their safety evaluations, and it is anticipated that more businesses will do the same in the upcoming years.

One of UL 4600's main advantages is that it offers a standardized method of safety evaluation, which can aid in fostering customer, governmental, and other stakeholders' faith in the technology of autonomous vehicles. Additionally, it can lessen the possibility of mishaps and other safety occurrences, which might hasten the acceptance of autonomous cars in the future.

The application of UL 4600, however, also comes with some difficulties. The complexity of the safety assessment procedure, which can take substantial resources and expertise to finish successfully, is one of the major challenges. Additionally, different standard readings

have the potential to result in discrepancies in the safety evaluations carried out by various businesses.

While the adoption of UL 4600 is still in its early stages, there is a growing recognition of the need for standardized safety frameworks for autonomous vehicles [42, 49, 50]. As the market develops, more businesses will probably implement UL 4600 or comparable standards to guarantee the responsible and secure deployment of autonomous cars on public roadways.

5 Challenges in Achieving Safety and Security

For highly and fully autonomous vehicles to be safe and secure, several crucial barriers must be removed before they can be extensively used. Among the significant challenges are the following:

Cybersecurity: A complex set of sensors, computers, and communication networks are required for the functioning of completely automated and highly autonomous vehicles. As a result, hacking may endanger the vehicle's and its passengers' safety and security. As a result, it is difficult to ensure trustworthy cybersecurity practices that protect against breaches [6].

Complex software and hardware: Due to their complexity, hardware and software for autonomous vehicles are difficult to evaluate and verify. It is challenging to guarantee that these systems are reliable, precise, and private [8, 29].

Human-machine interaction: Autonomous cars must be built to coexist peacefully with other vehicles, pedestrians, and human pilots. Advanced sensing, networking, and decision-making skills are needed for this [51, 52].

Environmental conditions: The ability to function securely in various weather situations, such as rain, snow, and fog, is a requirement for autonomous vehicles. Advanced detecting and navigational skills are needed for this [17, 23].

Ethical considerations and dilemmas: Autonomous vehicles must make decisions in real-time that are morally solid. This can be difficult when goals are in dispute, or the outcomes of many actions are uncertain. In some circumstances, such as when choosing between striking a person or colliding with another car, autonomous vehicles may confront moral conundrums. Making an ethical decision-making structure is a basic issue [53].

Data privacy: Large quantities of data are produced by autonomous cars, including data on the position, speed, and driving habits of the vehicle. It is crucial to guarantee the security of this data and the observance of users' private rights.

Safety certification and Regulatory hurdles: A complex set of laws that may vary by region and country are in effect for driverless vehicles. Creating rules that ensure these vehicles' security and safety while encouraging invention and development is difficult.

Public trust and acceptance: Because they are still a relatively new technology, many people are concerned about the reliability and safety of autonomous cars. Consistent effort is needed to build public acceptance and confidence, such as more public education and awareness of these issues from all stakeholders engaged in the auto industry [54, 55].

Infrastructure readiness: Infrastructure, such as communication networks, recharge facilities, and other enabling technologies, will need to receive substantial investment if driverless cars are to be adopted widely. The advanced infrastructure that highly and fully automated vehicles depend on includes elements like high-speed data networks and complex tracking systems. A significant challenge is ensuring that this infrastructure is developed and ready for extensive implementation [56].

Liability and insurance: Who is at fault in collisions involving highly and fully autonomous cars is frequently unclear. Creating a responsibility and insurance framework that protects passengers and other drivers is difficult.

Limited testing environments: Autonomous vehicle testing is frequently carried out in constrained settings, such as test towns or closed circuits. Because of this, testing the cars in various real-world situations is challenging, which may cause problems with safety and security when the vehicles are used on public roadways [57, 58].

Cost: Autonomous car deployment and research are expensive, which may restrict the general public's access to them. It might be challenging to make driverless cars accessible to all due to the high expense of the required infrastructure, such as superior communication and sensing systems [59].

Furthermore, it is extremely difficult to integrate driverless cars into current transit and infrastructure networks. To guarantee effective and secure transit, interoperability with other cars and systems, as well as communication and data-sharing methods, must be created [60].

Overall, creating and implementing highly and fully automated vehicles presents significant challenges; ensuring the safety and security of highly and fully autonomous vehicles is a challenging and multifaceted job that necessitates partner collaboration across the automotive industry. But with ongoing study, creation, and coordination between sectors and regulatory agencies, these difficulties can be surmounted. To fully realize the benefits and potential of this technology, however, it will be imperative to resolve these problems.

6 The State-of-the-Art Purposed Solution in Achieving Safety and Security

Modern solutions employing technological development are required for highly and fully autonomous vehicles to be safe and secure. The following are some suggestions made to make these vehicles safe and secure:

Redundancy and Diversity: One solution to address the challenge of hardware and software failures is to incorporate redundancy and diversity into the system [27]. This involves having multiple sensors, control systems, and communication networks to ensure backup systems are in place if one fails [12]. In case of a system failure, redundant steering, braking, and acceleration systems, for instance, can offer a backup. These solutions are also recommended by ISO 26262 for functional safety [23] and ISO 21448 for intended functionality.

Advanced sensors: A car may be able to make better decisions and prevent potential dangers with the help of improved sensors, which may give it a complete knowledge of its surroundings. Examples include LiDAR and Radar, which can help improve the accuracy and reliability of the vehicle's perception and decision-making systems [56]. These sensors can detect objects and obstacles from long distances. Under different weather conditions, providing a complete picture of the vehicle's surroundings [14]. These solutions are also recommended by ISO 26262 for functional safety and ISO 21448 for intended functionality.

Machine Learning and Artificial Intelligence: Autonomous cars may use machine learning algorithms to gain experience, make better decisions over time, and learn from their mistakes [15]. These algorithms can better forecast how to navigate the road safely by evaluating data from sensors and other sources to find trends [29]. For the safety of the intended functionality in scenarios where the decision-making module encounters an unforeseen circumstance and produces unpredictable results despite the sensors functioning accurately, ISO 21448 provides instructions on how to implement them [61]. The machine learning stack must identify, incorporate, and learn these critical situations [62].

Blockchain technology: Through the use of blockchain technology, a secure and open account of the data generated by driverless vehicles may be made available. This

can help other interested parties make wiser choices and improve the security and safety of the vehicle.

Communication Standards (V2X): In order for autonomous cars to interact successfully with other vehicles, infrastructure, and people, communication protocols are essential. For the transit system's various organizations to communicate securely and reliably, a standardized communication mechanism must be created [17, 18, 63].

Secure Intra-Communication Network: To avoid hacking and cyberattacks, the communication networks used in driverless cars must be trustworthy and safe. The communication lines of the car can be shielded from unauthorized access with the aid of sophisticated encryption algorithms and other security measures. The communication protocol used in vehicles today is Controller Area Network (CAN)-Bus, which is highly susceptible to hacking and overload. [5] provided a brilliant way to overcome this by using Software Defined In-VehicleNetworking (SDIVN) that does not add overhead compared to Legacy In-Vehicle Networks (LIVNs).

Cybersecurity solutions: Autonomous cars can benefit from advanced cybersecurity technologies to defend against cyberattacks. Solutions like firewalls, encryption, authentication, intrusion detection and response, and continuous monitoring of the vehicle's systems fall under this category [8, 64].

Test and validation frameworks: Developing test and evaluation systems can help to guarantee the dependability and safety of autonomous cars.. This includes creating testing protocols, simulation tools, [59] and other tools to evaluate the vehicle's performance under different conditions, identify potential failure modes [62], and ensure that it meets all safety and security requirements [24, 57]. Simulation and testing can help identify potential safety and security issues in autonomous vehicles before they are deployed on public roads [65, 66]. This includes testing the vehicle's hardware and software components, as well as its decision-making capabilities, under different scenarios and conditions [67].

Standards and regulations: Creating guidelines and rules for autonomous cars can aid in ensuring their security and safety [60, 68]. Creating technological standards, safety standards, and regulatory frameworks that support innovation and growth while maintaining the safety of travellers and other road users are all included in this [6, 7].

Human Factors: Human variables are essential for autonomous cars to be safe and secure. This entails creating user interfaces and encounters that are clear, simple

to use and encourage secure operation. It also entails creating systems that can recognize, address, and inform users of human mistakes [30, 53]. Human-Machine Interaction can further solve the problem of lack of trust and dependability on AVs and widespread acceptance [55]. Being able to interact with AVs gives a feeling of assurance to the user and hence helps in the cause of widespread acceptance of AVs [52, 69].

For highly and completely autonomous cars to be safe and secure, cutting-edge solutions utilizing technology developments are needed [37]. The players in the automobile industry can work together by putting these ideas into practice to ensure that autonomous vehicles are reliable, safe, and ready for widespread use.

7 Conclusion

In conclusion, developing highly and fully autonomous automobiles presents a number of security and safety issues. To ensure the safety and protection of passengers, pedestrians, and other road users, these automobiles require cutting-edge technologies. The foundation for ensuring the safety and security of autonomous vehicles is provided by a number of standards and guidelines, including ISO 26262, ISO 21448, SAE J3061, and SAE J3016. Moreover, technical advancements like blockchain, cybersecurity, and AI-based testing provide potential answers for ensuring the safety and security of autonomous automobiles. Nonetheless, challenges remain, such as addressing cybersecurity threats, ensuring the dependability of AI-based systems, developing a V2X network, and developing a comprehensive regulatory framework. In general, collaboration and continual innovation across several industries, such as the automobile, technology, and governmental regulation, are required to achieve safety and security for highly and fully autonomous vehicles.

Bibliography

[1] The Man Who Tested The First Driverless Car In 1925 Had A Bizarre Feud With Harry Houdini.

[2] Charles Thorpe, Martial H. Hebert, Takeo Kanade, and Steven A. Shafer. Vision and Navigation for the Carnegie-Mellon Navlab. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 10(3):362–373, 1988.

[3] Jean Paul Skeete. Level 5 autonomy: The new face of disruption in road transport. *Technological Forecasting and Social Change*, 134:22–34, 9 2018.

[4] Andrzej Wardziński. The role of situation awareness in assuring safety of autonomous vehicles. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 4166 LNCS:205–218, 2006.

[5] Khalid Halba, Charif Mahmoudi, and Edward Griffor. Robust Safety for Autonomous Vehicles through Reconfigurable Networking. 4 2018.

[6] Caleb Kennedy. New Threats To Vehicle Safety: How Cybersecurity Policy Will Shape the Future of Autonomous Vehicles. *Michigan Telecommunications & Technology Law Review*, 2017.

[7] Araz Taeihagh and Hazel Si Min Lim. Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks. *Transport Reviews*, 2019.

[8] Jin Cui, Giedre Sabaliauskaite, Lin Shen Liew, Fengjun Zhou, and Biao Zhang. Collaborative Analysis Framework of Safety and Security for Autonomous Vehicles. *IEEE Access*, 2019.

[9] Lorenz Steckhan, Wolfgang Spiessl, Nils Quetschlich, and Klaus Bengler. Beyond SAE J3016: New Design Spaces for Human-Centered Driving Automation. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 13335 LNCS:416–434, 2022.

[10] J3016_202104: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles - SAE International.

[11] Alexandru Constantin Serban, Erik Poll, and Joost Visser. A Standard Driven Software Architecture for Fully Autonomous Vehicles. *Proceedings - 2018 IEEE 15th International Conference on Software Architecture Companion, ICSA-C 2018*, pages 120–127, 8 2018.

[12] Sagar Behere and Martin Törngren. A functional reference architecture for autonomous driving. *Information and Software Technology*, 73:136–150, 5 2016.

[13] Farzeen Munir, Shoaib Azam, Muhammad Ishfaq Hussain, Ahmed Muqeem Sheri, and Moongu Jeon. Autonomous vehicle: The architecture aspect of self driving car. *ACM International Conference Proceeding Series*, pages 1–5, 10 2018.

[14] Wenhao Zong, Changzhu Zhang, Zhuping Wang, Jin Zhu, and Qijun Chen. Architecture design and implementation of an autonomous vehicle. *IEEE Access*, 6:21956–21970, 4 2018.

[15] Khan Muhammad, Amin Ullah, Jaime Lloret, Javier Del Ser, and Victor Hugo C. De Albuquerque. Deep Learning for Safe Autonomous Driving: Current Challenges and Future Directions. *IEEE Transactions on Intelligent Transportation Systems*, 22(7):4316–4336, 7 2021.

[16] Kai Gao, Di Yan, Fan Yang, Jin Xie, Li Liu, Ronghua Du, and Naixue Xiong. Conditional Artificial Potential Field-Based Autonomous Vehicle Safety Control with Interference of Lane Changing in Mixed Traffic Scenario. *Sensors (Basel, Switzerland)*, 19(19), 10 2019.

[17] Furqan Jameel, Zheng Chang, Jun Huang, and Tapani Ristaniemi. Internet of Autonomous Vehicles: Architecture, Features, and Socio-Technological Challenges. *IEEE Wireless Communications*, 26(4):21–29, 8 2019.

[18] Swaminathan Gopalswamy and Sivakumar Rathinam. Infrastructure Enabled Autonomy: A Distributed Intelligence Architecture for Autonomous Vehicles. *IEEE Intelligent Vehicles Symposium, Proceedings*, 2018-June:986–992, 10 2018.

[19] Miguel Ángel de Miguel, Francisco Miguel Moreno, Fernando García, Jose María Armingol, and Rodrigo Encinar Martin. Autonomous Vehicle Architecture for High Automation. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 12014 LNCS:145–152, 2020.

[20] Shoaib Azam, Farzeen Munir, Ahmad Muqeem Sheri, Joonmo Kim, and Moongu Jeon. System, Design and Experimental Validation of Autonomous Vehicle in an Unconstrained Environment. *Sensors 2020, Vol. 20, Page 5999*, 20(21):5999, 10 2020.

[21] ISO/DIS 26262-2(en), Road vehicles — Functional safety — Part 2: Management of functional safety.

[22] J3061_202112: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems - SAE International.

[23] Mukul Anil Gosavi, Benjamin B. Rhoades, and James M. Conrad. Application of Functional Safety in Autonomous Vehicles Using ISO 26262 Standard: A Survey. *Conference Proceedings - IEEE SOUTHEASTCON*, 2018-April, 10 2018.

[24] Manuel Seet, Andrei Dragomir, Jonathan Harvy, Nitish V. Thakor, and Anastasios Bezerianos. Objective assessment of trait attentional control predicts driver response to emergency failures of vehicular automation. *Accident Analysis & Prevention*, 168:106588, 4 2022.

[25] Richard J. Meinhold and Nozer D. Singpurwalla. Understanding the kalman filter. *American Statistician*, 37(2):123–127, 1983.

[26] J. Carpenter and P. Clifford. Improved particle filter for nonlinear problems. *IEE Proceedings: Radar, Sonar and Navigation*, 146(1):2–7, 1999.

[27] Sanjay Seshan. Horus: Using Sensor Fusion to Combine Infrastructure and On-board Sensing to Improve Autonomous Vehicle Safety. 9 2020.

[28] Aditya Dixit, Ramesh Kumar Chidambaram, and Zaheer Allam. Safety and Risk Analysis of Autonomous Vehicles Using Computer Vision and Neural Networks. *Vehicles*, 3(3):595–617, 9 2021.

[29] Rowan McAllister, Yarin Gal, Alex Kendall, Mark Van Der Wilk, Amar Shah, Roberto Cipolla, and Adrian Weller. Concrete problems for autonomous vehicle safety: Advantages of Bayesian deep learning. In *IJCAI International Joint Conference on Artificial Intelligence*, 2017.

[30] Adithya Ranga, Filippo Giruzzi, Jagdish Bhanushali, Emilie Wirbel, Patrick Pérez, Tuan-Hung Vu, and Xavier Perrotton. VRUNet: Multi-Task Learning Model for Intent Prediction of Vulnerable Road Users. 7 2020.

[31] Giorgio Grisetti, Rainer Kummerle, Cyrill Stachniss, and Wolfram Burgard. A tutorial on graph-based SLAM. *IEEE Intelligent Transportation Systems Magazine*, 2(4):31–43, 12 2010.

[32] Peter Biber. The Normal Distributions Transform: A New Approach to Laser Scan Matching. *IEEE International Conference on Intelligent Robots and Systems*, 3:2743–2748, 2003.

[33] Juyong Zhang, Yuxin Yao, and Bailin Deng. Fast and Robust Iterative Closest Point. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 44(7):3450–3466, 7 2022.

[34] Jiajun Deng, Shaoshuai Shi, Peiwei Li, Wengang Zhou, Yanyong Zhang, and Houqiang Li. Voxel R-CNN: Towards High Performance Voxel-based 3D Object Detection. *Proceedings of the AAAI Conference on Artificial Intelligence*, 35(2):1201–1209, 5 2021.

[35] Frank Dellaert, Dieter Fox, Wolfram Burgard, and Sebastian Thrun. Monte Carlo localization for mobile robots. *Proceedings - IEEE International Conference on Robotics and Automation*, 2:1322–1328, 1999.

[36] Pavel Gladyshev and Ahmed Patel. Finite state machine approach to digital event reconstruction. *Digital Investigation*, 1(2):130–149, 6 2004.

[37] Karen Leung, Sushant Veer, Edward Schmerling, and Marco Pavone. Learning Autonomous Vehicle Safety Concepts from Demonstrations. 10 2022.

[38] František Duchon, Andrej Babinec, Martin Kajan, Peter Beno, Martin Florek, Tomáš Fico, and Ladislav Jurišica. Path Planning with Modified a Star Algorithm for a Mobile Robot. *Procedia Engineering*, 96:59–69, 1 2014.

[39] Kourosh Naderi, Joose Rajamaki, and Perttu Hamalainen. RT-RRT: A real-time path planning algorithm based on RRT. *Proceedings of the 8th ACM SIGGRAPH Conference on Motion in Games, MIG 2015*, pages 113–118, 11 2015.

[40] CertX | We ensure your innovation.

[41] ISO - ISO 21448:2022 - Road vehicles — Safety of the intended functionality.

[42] UL 4600: Standard for Safety for the Evaluation of Autonomous Products.

[43] Cybersecurity Framework | NIST. 4 2018.

[44] IEEE SA - IEEE 2846-2022.

[45] ISO - ISO/SAE 21434:2021 - Road vehicles — Cybersecurity engineering.

[46] ISO/FDIS 21448 - Consulting and Implementation | SOTIF EV-AV.

[47] Andrew Smart, Chess Stetson, and Kiran Jesudesan. Autonomous Vehicle Safety Assessment with Fully Quantified ODDs. *SAE Technical Papers*, (2021), 2021.

[48] Georg Macher, Eric Armengaud, Eugen Brenner, and Christian Kreiner. A review of threat analysis and risk assessment methods in the automotive context. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9922 LNCS:130–141, 2016.

[49] An Overview of Draft UL 4600: "Standard for Safety for the Evaluation of Autonomous Products" | by Edge Case Research | Medium.

[50] About 1 — Edge Case Research.

[51] Tang Xiaofeng. Ecological driving on multiphase trajectories and multiobjective optimization for autonomous electric vehicle platoon. *Scientific reports*, 12(1), 12 2022.

[52] Zijiang Zhu, Zhenlong Hu, Weihuang Dai, Hang Chen, and Zhihan Lv. Deep learning for autonomous vehicle and pedestrian interaction safety. *Safety Science*, 145:105479, 1 2022.

[53] Yineng Xiao. Application of Machine Learning in Ethical Design of Autonomous Driving Crash Algorithms. *Computational intelligence and neuroscience*, 2022, 2022.

[54] Alysson G. Oliveira, Yuzo Iano, Diego Pajuelo, Ana Carolina Borges Monteiro, Reinaldo Padilha França, and Gabriel Gomes de Oliveira. A Look at the Evolution of Autonomous Cars and Its Impact on Society Along with Their Perspective on Future Mobility. *Smart Innovation, Systems and Technologies*, 201:583–594, 2021.

[55] Joanna Moody, Nathaniel Bailey, and Jinhua Zhao. Public perceptions of autonomous vehicle safety: An international comparison. *Safety Science*, 2020.

[56] Akhil Shetty, Mengqiao Yu, Alex Kurzhanskiy, Offer Grembek, Hamidreza Tavafoghi, and Pravin Varaiya. Safety Challenges for Autonomous Vehicles in the Absence of Connectivity. 6 2020.

[57] Philip Koopman and Michael Wagner. Challenges in Autonomous Vehicle Testing and Validation. *SAE International Journal of Transportation Safety*, 4(1):15–24, 4 2016.

[58] Nidhi Kalra. Challenges and Approaches to Realizing Autonomous Vehicle Safety. *Challenges and Approaches to Realizing Autonomous Vehicle Safety*, 3 2017.

[59] Mark Mario Morando, Qingyun Tian, Long T. Truong, and Hai L. Vu. Studying the Safety Impact of Autonomous Vehicles Using Simulation-Based Surrogate Safety Measures. *Journal of Advanced Transportation*, 2018.

[60] Gopindra S. Nair and Chandra R. Bhat. Sharing the road with autonomous vehicles: Perceived safety and regulatory preferences. *Transportation Research Part C: Emerging Technologies*, 2021.

[61] Alexandre Moreira Nascimento, Lucio Flavio Vismari, Caroline Bianca Santos Tancredi Molina, Paulo Sergio Cugnasca, João Batista Camargo, Jorge Rady De Almeida, Rafia Inam, Elena Fersman, Maria Valeria Marquezini, and Alberto Yukinobu Hata. A Systematic Literature Review about the Impact of Artificial Intelligence on Autonomous Vehicle Safety, 2020.

[62] Xingyu Xing, Tong Jia, Junyi Chen, Lu Xiong, and Zhuoping Yu. An Ontology-based Method to Identify Triggering Conditions for Perception Insufficiency of Autonomous Vehicles. 10 2022.

[63] Yanqiu Cheng, Chenxi Chen, Xianbiao Hu, Kuanmin Chen, Qing Tang, and Yang Song. Enhancing Mixed Traffic Flow Safety via Connected and Autonomous Vehicle Trajectory Planning with a Reinforcement Learning Approach. *Journal of Advanced Transportation*, 2021.

[64] Christoph Schmittner, Zhendong Ma, Carolina Reyes, Oliver Dillinger, and Peter Puschner. Using SAE J3061 for automotive security requirement engineering. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9923 LNCS:157–170, 2016.

[65] Alexandre M. Nascimento, Anna Carolina M. Queiroz, Lucio F. Vismari, Jeremy N. Bailenson, Paulo S. Cugnasca, Joao B. Camargo, and Jorge R. De Almeida. The role of virtual reality in autonomous vehicles' safety. In *Proceedings - 2019 IEEE International Conference on Artificial Intelligence and Virtual Reality, AIVR 2019*, 2019.

[66] Mohsen Malayjerdi, Barış Cem Baykara, Raivo Sell, and Ehsan Malayjerdi. Autonomous vehicle safety evaluation through a high-fidelity simulation approach. *Proceedings of the Estonian Academy of Sciences*, 2021.

[67] Lanhang Ye and Toshiyuki Yamamoto. Evaluating the impact of connected and autonomous vehicles on traffic safety. *Physica A: Statistical Mechanics and its Applications*, 2019.

[68] Stephen Thomas and Katrina M. Groth. Toward a hybrid causal framework for autonomous vehicle safety analysis. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 2021.

[69] Subasish Das. Autonomous vehicle safety: Understanding perceptions of pedestrians and bicyclists. *Transportation Research Part F: Traffic Psychology and Behaviour*, 2021.