

Cyber-physical Security Analysis of Teleoperated Autonomous Road Vehicles

by

Subhadip Ghosh

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Engineering
(Automotive Systems and Mobility)
in the University of Michigan-Dearborn
2024

Doctoral Committee:

Associate Professor Junho Hong, Chair
Assistant Professor Jaerock Kwon
Associate Professor Youngki Kim
Dr. Hyojong Lee, DTE Energy

Subhadip Ghosh
subhagh@umich.edu
ORCID iD: 0000-0001-5668-565X

© Subhadip Ghosh 2024

DEDICATION

To my Parents, my Wife and my Son Gogol.

ACKNOWLEDGEMENTS

I would like to convey my heartfelt gratitude toward my esteemed advisor Prof. Junho Hong, for his guidance throughout the doctoral program. Prof. Hong has been my research mentor for the last three years, starting from organizing my research procedure to publishing the outcomes in suitable manner, his prudence guidance has been instrumental in shaping my academic journey. I wholeheartedly wish to thank my committee member, Prof. Jaerock Kwon for his counsel in AI-ML part of my research, and the other members of the committee, Prof. Youngki Kim and Dr. Hyojong Lee, for their insightful comments and suggestions throughout the program and serving in my dissertation committee. Also, my sincere gratitude to my lab mates and other research colleagues at the university.

I would like to thank Ford Motor Co. for sponsoring my study and supporting my research. I also want to thank my manager and colleagues at Ford Motor Co. for their continued support and invaluable insight throughout my academic endeavor. I am fortunate to have such amazing cooperating colleagues during my entire doctoral study.

Additionally, I express my gratitude to all faculty and staff of the College of Engineering and Computer Science and the mechanical engineering department at the University of Michigan-Dearborn for providing me the platform and support for pursuing a Doctorate of Engineering in Automotive Systems and Mobility.

Finally, I am deeply grateful to my family for their unconditional love, engagement and understanding during the pursuit of my doctoral journey. I am forever indebted to them for their unwavering support and contributions to my success.

TABLE OF CONTENTS

DEDICATION	ii
ACKNOWLEDGEMENTS	iii
LIST OF FIGURES	vi
LIST OF TABLES	viii
ABSTRACT	x
CHAPTER	
1 Introduction	1
1.1 Problem Definition	2
1.2 Purpose and Significance of the Study	3
1.3 Research Hypothesis	4
1.4 Limitations	4
1.5 Research Methodology and Procedure	5
2 Literature Survey	9
2.1 Evolution of Road Vehicles and Mobility Solutions	9
2.2 Road Vehicle Fundamentals	11
2.2.1 Vehicle Motion	11
2.2.2 Vehicle Powertrain	18
2.2.3 Vehicle E/E and N/W Architecture	19
2.3 Road Safety and Vehicle Crash	22
2.4 Autonomous Vehicle: Purpose, Taxonomy, Operational Domain and Driving System	22
2.5 ToD Concept for Smart Mobility	26
2.5.1 Driving Context	29
2.6 Cybersecurity Practices in Automotive	31
2.7 ML Review	35
2.8 Cyber-physical Challenges of AV and ToD	40
2.9 Anomaly Detection in CPS	47
3 Threat Modeling of Automated and Teleoperated Vehicles	50
3.1 Threat Modeling for AV Perception System	50

3.1.1	Assumptions and Scope	51
3.1.2	Problem Formulation	51
3.1.3	ISO/SAE 21434 Approach	52
3.1.4	STPA-SEC Approach	60
3.1.5	Comparison Between Two Threat Models	66
3.1.6	Proposed Method: An Integrated Approach of Threat Analysis for AV	67
3.1.7	Framework	67
3.1.8	Mathematical Model	69
3.2	Threat Model and Attack Model for ToD	70
3.2.1	Attack Model for LMD	74
4	Anomaly Detection for Teleoperated LMD	78
4.1	Problem Statement	78
4.1.1	Assumption and Scope	80
4.2	Methodology	81
4.2.1	Stage 1: PCADS-Context-aware Anomaly Detection	82
4.2.2	Stage 2: PCADS-Physics-based Anomaly Detection	85
5	Experiments and Result	90
5.1	Case Study: Integrated Approach of Threat Analysis for AV	90
5.1.1	Attack Feasibility Assessment with AI Robustness Factor	92
5.2	Case Study: PCADS for Detecting FDI Attacks on Steering Command in LMD Application	95
5.2.1	Original Dataset for Driving Maneuver	95
5.2.2	Context-aware Anomaly Detection	96
5.2.3	Physics-based Anomaly Detection	97
6	Conclusions and Future Work Recommendation	108
	APPENDIX	112
	BIBLIOGRAPHY	114

LIST OF FIGURES

FIGURE

1.1	Research Methodology	6
2.1	Vehicle Motion with 6-DOF	13
2.2	Longitudinal Force on Vehicle	14
2.3	Vehicle Yaw Rate and Angular Velocity	15
2.4	Vehicle Lateral Motion as Bicycle Model	16
2.5	Electric Vehicle Architecture	21
2.6	NSC Motor-vehicle Fatality Trends	23
2.7	Vehicle Crash Point Direction of Force	23
2.8	Comparison Between SAE Automation Levels	27
2.9	Vehicle Teleoperation High-level Concept	29
2.10	Vehicle Teleoperation Types (Example)	30
2.11	Driving Context Concept	31
2.12	ANN Generic Architecture	37
2.13	Common Activation Function in ANN	37
2.14	CNN Generic Architecture	38
2.15	LSTM Vanilla Architecture	39
2.16	Automotive Attack Vectors 2010-2020	41
2.17	TARA Steps of ISO/SAE 21434 Standard	46
3.1	A Detailed Representation of ISO/SAE 21434 TARA Steps Considering the Work Products	52
3.2	An OC Concept Level Block Diagram with Different Objects	53
3.3	A STPA-Sec TARA for an AV Perception System Regarding the Loss, Hazards, and CFs	60
3.4	A Sample Vehicle Autonomy SOA Architecture	63
3.5	Evaluation of Attack Potential in Compliance with ISO/IEC 18045 Parameters	70
3.6	An Attack Tree for a ToD Event	72
3.7	A Teleoperated Vehicle Attack Likelihood vs Impact	74
3.8	An FDI Attack on Communication Between Remote Operator and the Vehicle	75
3.9	A Traffic Light Intersection Attack Scenario	76
3.10	A System Model for the Vehicle’s Steering Angle Under Attacks	76
3.11	An FDI in the Steering Wheel Angle	77
4.1	Cyber-physical Anomaly Detection of ToD at High-level	79

4.2	Example of Vehicle Physical Parameter Variation with Left Turn (LT), Right Turn (RT), U Turn (UT)	80
4.3	An LMD ToD Anomaly Detection Framework	82
4.4	A Vehicle Physics-based Anomaly Detection Framework	85
5.1	Evaluation of Attack Potential in Compliance with ISO/IEC 18045 Parameters	93
5.2	A Comprehensive Risk Assessment Based on the AI Robustness Factor for AV Perception Datasets	93
5.3	A Comparative Example of an AI Robustness Factor Evaluation Considering Case Studies from Table II for Normal, Abnormal, and Adversarial Scenarios	95
5.4	Context-aware Anomaly Detection - Incorrect Turn	97
5.5	Context-aware Anomaly Detection - Incorrect Time	98
5.6	Context-aware Anomaly Detection - Filtering Dynamic Alert	98
5.7	An Example of Attack on Steering Wheel Command by Noise Injection	100
6.1	Key Observations from Results with Proposed Threat Analysis	109
6.2	An Illustration of Resource Consumption for AV Security	110

LIST OF TABLES

TABLE

2.1	DOF with Example Usecase	13
2.2	Expected Results of the ISO/SAE 21434 TARA Approach Based on Different Steps	33
2.3	A Literature Survey on ML Algorithms for an AV Perception System	43
2.4	A Literature Survey on Anomaly Detection in CPS	48
2.5	Parametric Variations of SAE J3016 Automation Level	49
3.1	An OC Asset Identification along with Damage Scenarios due to Attacks Considering the CIA Characteristics	54
3.2	OC Impact Categories and Rating Levels with Consequences for Different Scenarios	55
3.3	OC Threat Scenarios Identified by Different Classes of Attacks Including Spoofing, Tampering, Information Disclosure, and DoS	57
3.4	Attack Feasibility Rating Considering the Parameters Defined in Accordance with ISO/IEC 18045 Standard	58
3.5	A Risk Value Determination for Different Attacks on Camera Vision	59
3.6	An OC System Description with a STPA-Sec Format for an AV Perception System	61
3.7	Different OC Unacceptable Losses Identified for the Mission (Example)	61
3.8	Sample OC Hazards Description with Relevant Losses (Example)	62
3.9	An Identification of Unsecure Element Guide Words Based on the CIA Characteristic	64
3.10	A Chart for CF Identification Guide Words	64
3.11	An Identification of CFs Based on What-How (WH) Method (Examples)	65
3.12	Functions and Dataflows for Various ToD	71
3.13	Potential Attack Types for ToD System	73
5.1	Impact Rating Parameters for Different Objects on the Road Based on Real Traffic Crash Data	91
5.2	Attack Feasibility Calculations for Different AI Algorithms' Robustness for Perception Systems	94
5.3	A Comparison of ML Algorithms for Good Dataset with Entire Sequence	101
5.4	A Comparison of ML Algorithms for Good Dataset with Sequence Focused at Maneuvering Duration	102
5.5	Example of Prediction Probability Score with Softmax Function	103
5.6	Anomaly Detection in Real Data with Noise	104
5.7	A Comparison of ML Algorithms for Virtual Vehicle Good Dataset with Sequence Focused at Maneuvering Duration	105

5.8 Anomaly Detection in Virtual Vehicle Data with Noise 106

ABSTRACT

Automated road vehicles, commonly known as autonomous vehicles (AV) is a revolutionary step for next generation mobility services on public roads. The primary mission of AV is to improve safety and convenience in road transportation by deploying automated technology for the vehicle-driving tasks. Such automated technology comprises of various sensors, software, and hardware to receive vehicle's mission, perceive the surrounding road environment, localize the vehicle's position, plan the route, make decision on driving maneuvers and finally performing the driving actions. Teleoperated driving (ToD) for road vehicles, also known as remotely operated road vehicles (RORV) has originated to handle the corner case of AV with a driver-in-loop from a remote operating station. For such a system, the teleoperator can remotely control the steering, acceleration, and braking action of the vehicle. To perform these tasks, teleoperated vehicles require interaction with the operating environment using perception sensors, localization sensors and cellular communication. Though AV and ToD are considered promising technologies to reshape the mobility landscape for public roads, they also transform the road vehicles from physical systems to cyber-physical systems and introduce new categories of challenges. Cyber-physical threats of AV and ToD is one of the critical areas as it can compromise safety and operational capability of future mobility. Therefore, research on methods for security analysis specific to AV and ToD is necessary. This dissertation conducts the research focusing on this area by analyzing threat models, attack model and detection model by following systems theory approach, knowledge of the context and physical system and machine learning (ML) algorithm.

- First, threat modeling of AV perception system is created using two approaches. First approach follows the standard 21434, jointly developed by International Organization for Standardization (ISO) and Society of Automotive Engineers (SAE). The second approach follows the method of systems theoretic process analysis for security known as STPA-Sec. Next, a comparative study is done between the output of aforementioned ISO/SAE 21434 and STPA-Sec based threat models. In the final step, an integrated approach is proposed for object-focused impact rating and feasibility analysis of artificial intelligence (AI) based perception system for AV.
- Second, a threat model for ToD is created with the attack-tree based approach. Based

on high-risk attacks, an attack model with false data injection on steering control command is created.

- Third, to detect such attack Physics-based Context-aware Anomaly Detection System (PCADS) is proposed and presented with results.

The outcome of this research highlights the importance of developing a cyber-physical security framework for teleoperated AVs. Moreover, with thorough analysis of the experimental results, this dissertation recommends potential future steps to assist in fostering research direction for cyber-physical security of such systems.

CHAPTER 1

Introduction

In recent years, rapid advancement in the tech sector has reshaped our daily life with automated and internet-of-things (IoT) devices. This triggered a paradigm shift in the auto industry to impart intelligence to cars and integrate them with the smart ecosystems of modern society. Roadmap for Automotive Technology Advancement by Center for Automotive Research projects partial deployment of connectivity and automation by 2025 and its worldwide adoption by 2040 [1]. This vision has presented automotive engineers with some unfamiliar problems to solve, among which cyberattack and its impact on safety is a critical one. Studies show that in recent years cyberattacks on cars have grown significantly [2]. Governments across the globe have responded to this situation with strict regulations for automotive original equipment manufacturers (OEM) regarding cybersecurity. As per a 2019 survey of global automotive manufacturers and suppliers (published by SAE International), 84% of respondents believed cybersecurity practices are lagging in the auto industry and 60% of the respondents indicated that insufficient knowledge on secure coding practices makes the software vulnerable [3].

One of the revolutionary steps in smart mobility is autonomous vehicle. Autonomous vehicles has the goal of providing a safe and convenient riding experience while keeping the human-driving task minimal to none [4]. Therefore, these intelligent vehicles are equipped with sophisticated perception sensors (e.g., cameras and radars), high-performance computers, artificial intelligence (AI)-driven algorithms, and connectivity with other IoT devices. ToD originated from autonomous vehicle technology is a driving system where remote operator controls the steering, acceleration, and braking action of the vehicle remotely [5]. In case of cyberattacks, malicious actors may inject false data in communication channels to manipulate the teledriver's driving command to cause harm. Hence, protection of teledriver's command is necessary. However, as per National Institute of Standards and Technology (NIST) cybersecurity framework [6] protection alone is not enough and detection of the attack is necessary. This makes teleoperated AVs a special kind of cyber-physical system (CPS) that is moving at speed in highly interactive and dynamic environments (e.g., public

roads). Thus, these systems are potential target for cyber attackers to weaponize, compromising safety and mobility on the road. Currently cybersecurity practices in automotive are primarily based on information technology (IT) driven approach. However, research on cyber-physical security of teleoperated autonomous vehicles is in its early stage and needs to be investigated in detail. Researchers from other CPS areas have shown systems approach of threat modeling for CPS techniques. Also, research in other CPS demonstrates that the mitigation of threat can go beyond traditional cyber-security approach to boost defense-in-depth [7, 8]. One of the potential approaches is understanding the behavior of physical system and using the information to improve the security of CPS. This dissertation conducts a research to assess cyber-physical threats, attacks and mitigation techniques of teleoperated autonomous driving using the knowledge about the application and system.

1.1 Problem Definition

The problem definition for this dissertation originates from the following questions:

- Q.1. What is considered as a threat for teleoperated autonomous driving?
- Q.2. What is the risk when such a threat occurs?
- Q.3. How cyber-physical attacks can cause such threats?
- Q.4. What can be done to mitigate such threats?

In search for the answers, a thorough literature review was conducted in the relevant areas involving these questions and the following gaps were identified as problem definition:

- Current cyber-security standard and practices for automotive cyber security is primarily driven by ISO/SAE 21434 standard which provides the threat analysis and risk assessment (TARA) guideline for electrical and electronic (E/E) systems within road vehicles. However, autonomous driving and ToD systems have more complex and dynamic cyber-physical interactions than conventional road vehicles in their operating environment.
- Following an unsuitable method may provide incorrect metrics of cyber-assurance and cause safety hazards or disruption of mobility services in reality. Hence, it is critical to analyze the effectiveness of these threat models for AV cyber-physical attacks with a holistic approach.
- Further, for teleoperated vehicles there are no human driver physically present inside the vehicle to monitor and control the car in case of a cyberattack. Hence, defense-in-depth principle of cyber-security is crucial for

safety. As per NIST security framework, detection is an important step for security architecture. UN R155 compliance requires securing vehicles by design and reporting security incidents specially for vehicle fleets.

- Currently, cyberattack detection methods in automotive cybersecurity primarily focus on traditional cybersecurity approach and anomaly detection which monitors on network behavior of vehicle communication and limited consideration of the physical behavior of the vehicle. Hence, exploring anomaly detection technique using the knowledge of ToD system's application and physical behavior is necessary to improve cyber-physical security and safety of such system.

1.2 Purpose and Significance of the Study

Although cyber-attacks are common in the software and IT industries [9] and there are many instances of severe business and financial loss, they are relatively new in the automotive domain. One of the early demonstrations of an automotive cyber attack was in 2015 by security researchers Charlie Miller and Chris Valasek who remotely hacked a conventional car driving at 70 miles per hour [10]. But unlike conventional cars, AVs are highly dependent on perception sensors, localization sensors, AI-based algorithms, and vehicle-to-everything (V2X) communication for driving capability without a driver [11, 12]. All of these areas affect the attack surface, software vulnerabilities, and the severity of the impact. In [13], researchers were successful in manipulating Tesla's autopilot system by using split-second light projections on roads. Sensor jamming, blinding, spoofing, distributed denial-of-service (DDoS) attacks, manipulation of communication devices, and adversarial ML techniques on AI-driven algorithms are some of these attack methods demonstrated by researchers in this area [14, 15, 16, 17, 18, 19]. These types of cyber-physical attacks are specifically targeted, posing potential threats to AVs and objects in ODD. As AVs are still in the early stages of delivering base functionality and real-life testing, cyber-physical threats to AVs are slowly emerging. But with more AVs on the road in the future, threats will also be increased. Hence, it is critical to have a robust threat modeling framework to identify the evolving cyber-physical threats for AV-specific designs and applications.

Teleoperated driver monitors, controls or provides guidance to the driving function from a remote operating station [20, 5]. Typically, the perception information is sent by the vehicle to operating station via cloud and fog infrastructure using wireless or cellular network. Similarly, control commands coming from operating station are sent to the vehicle. This poses

a potential exposure of perception data and control commands outside vehicle boundary which makes the ToD systems vulnerable against cyber-attacks. Attackers can target ToD system with denial-of-service (DoS) attacks, false data injection attacks, man-in-the-middle attacks and other attack methods similar to the attacks detected in various cyber-physical system [21, 22]. A malicious control of ToD may result in vehicle crash, disruption in teleoperation service, legal consequences and financial loss. Hence, a robust cyber-security strategy to prevent, detect and mitigate such attacks are critical for a safe ToD.

1.3 Research Hypothesis

The guiding philosophy for this dissertation is to view ToD as a cyber-physical system and understand what are the cyber-physical challenges of such system? If and how an attacker can exploit the cyber-physical challenges of this system to cause harm. Are there existing methods to address this problem? Is there any gap that can be solved using the application and system specific knowledge of the system. There are three main hypothesis for this dissertation:

- Security should not be an after-thought for teleoperated autonomous driving system. As this system is emerging to improve road safety, mobility services security research must happen in parallel as one of the key contributor of security-by-design principle.
- Cyber-physical threats of ToD need to be viewed from a holistic approach that encompasses the cyber-physical interaction of the system with other actors in its operating domain.
- Defense-in-depth strategy for teleoperated autonomous driving should not be restricted to cyber-security domain. Application and system specific knowledge should be utilized for designing security strategy of such system.

1.4 Limitations

Throughout there were some limitations.

- AI/ML algorithms for AV perception in literature either focus on normal, abnormal or adversarial scenarios. Performance of an AI/ML algorithm with all three types of scenarios are not available. This brought some limitations

to compare risk assessment with AI robustness factor for all three scenarios together.

- AVs are still emerging, hence crash data from road accidents is very limited with respect to a variety of object types. For object-focused impact assessment a simulation of AV test data with various types of objects and crash is missing in research.
- As ToD system for public roads is in its early stage of evaluation, literature survey for such system specifically from security aspect is very limited.
- A set of good data and corresponding attack dataset with various type of false data injection in ToD command is not available in research.

1.5 Research Methodology and Procedure

This study began with literature review of the evolution of automotive systems and mobility for public roads and the future road-map. Further, the following areas are reviewed in detail:

- Road vehicle fundamentals.
- Road vehicle safety.
- Autonomous driving.
- ToD.
- Cybersecurity practices in automotive.
- ML algorithms.
- Cyber-physical challenges of AV and ToD.
- Anomaly detection in CPS.

After the extensive literature review, the problem statement for this dissertation is defined. The problem definition is provided in section 1.1. In general, this dissertation aims to investigate the methods to identify cyber-physical threats of AV and ToD on public roads and to provide a security framework that extends to vehicle's physical domain. An overview of the research methodology followed for this work is presented in Fig. 1.1. The general framework for the research methodology is inspired by red team/ blue team approach in cybersecurity and cybersecurity framework of NIST [6]. The research methodology and contributions of this dissertation are described in three primary steps, as follows:

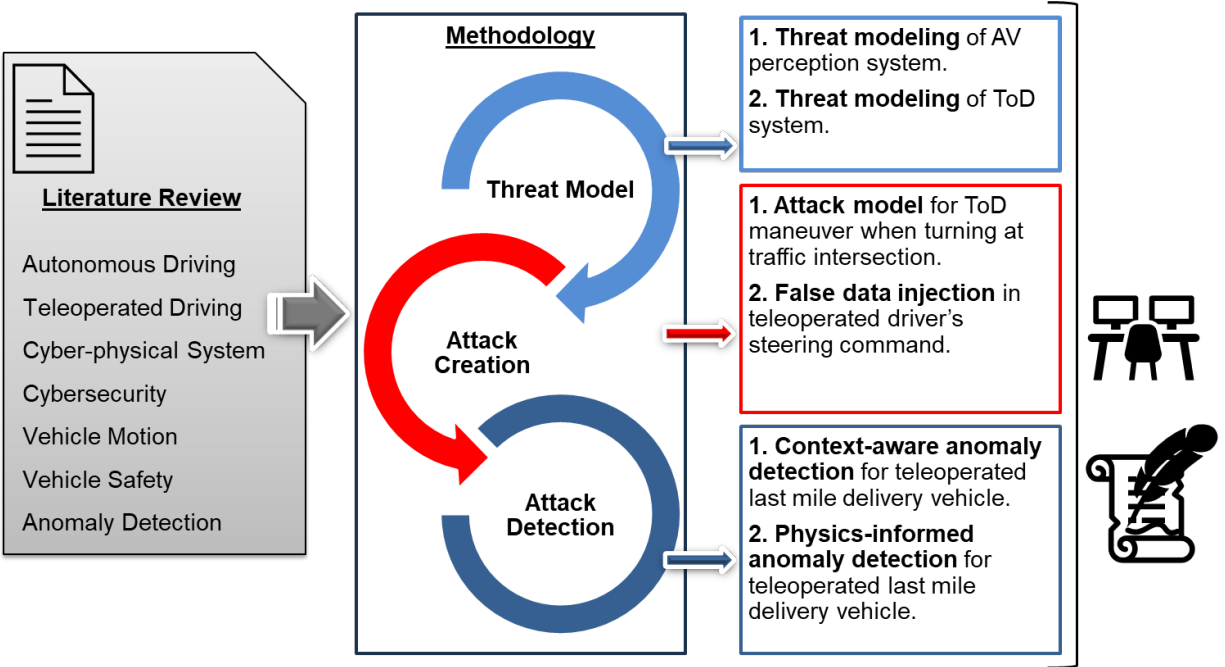


Figure 1.1: Research Methodology

- **Threat modeling:** As per NIST cybersecurity framework, identifying threats is the most critical step to develop a secure system. As shown in Fig. 1.1, threat modeling falls under the scope of blue team. For threat modeling of AV perception system cyber-physical threats are analyzed with ISO/SAE 21434 [23] approach and STAP-Sec [24] method. Based on the comparative analysis, an integrated TARA approach is proposed. The proposed method enhances the threat analysis with an object-centric approach in the AV operational domain and embed AI robustness factor for a holistic risk assessment of AI algorithms against normal, abnormal and adversarial scenarios for AV perception system. The application of the proposed method is presented in section 5. The second threat modeling is conducted for ToD system on public road with an attack-centric approach. For this purpose, the ToD system is primarily divided in three target areas: 1) vehicle, 2) IoT infrastructure, and 3) operator station. Attack types are referenced from literature review and MITRE ATT&CK matrices [25].
- **Attack creation:** As shown in Fig. 1.1, Attack creation is one of the key focus of red team in common cybersecurity practices. Attack model is created based on the result from attack-centric threat analysis of ToD in previous step. The attack model targets the ToD maneuver when turning at a traffic intersection. The attack is formulated as exploitation of the window of opportunity to inject false data on steering wheel control input from teleoperated driver. The attack dataset is created by injecting noise on

driving dataset from real vehicle. A detailed description of attack creation is provided in section 3.2.1 and attack dataset is described in section 5.2.3.1.

- **Attack detection:** Detection of the cyberattack is a crucial task for a cyber-defense mechanism. When security protection mechanism fails, detection of the attack aids in taking mitigation action and incident analysis. Blue team is responsible for this task. The proposed detection method in this dissertation is aimed at predicting an anomaly in driving maneuver based on the context of ToD and physical information of the teleoperated vehicle. This method is proposed, after detailed review of automotive IDS, potential applications and security methods of ToD, anomaly detection techniques in other CPS, ML algorithms, vehicle motion fundamentals and vehicle architecture. For this work, the detection method is experimented with the attack created in previous step with a specific application of ToD. This case study focuses on the last-mile delivery (LMD) vehicle making left turn, right turn or u-turn at a traffic intersection. The method described in section 4 and experimental results are presented in section 5.

The research work presented in this dissertation is organized in six chapters as described below:

- Chapter 1 is an introductory chapter which provides a general overview, problem definition, purpose of this study, research hypothesis, limitations, and research methodologies followed in this dissertation.
- Chapter 2 provides a literature review on evolution of road vehicles and mobility from physical system to CPS with emerging technologies including SDV, AV, and teleoperated road vehicles, evolving cyber-physical challenges of such systems, cyber-defense of other CPS, automotive cybersecurity, vehicle motion and safety, anomaly detection in IDS, and ML algorithms.
- Chapter 3 presents TARA of AV perception system, threat modeling of ToD system and attack model of false data injection on ToD input.
- Chapter 4 proposes a context-aware and physics-based anomaly detection method against the FDI attack on steering wheel angle during left, right or u-turn turning maneuver of teleoperated vehicle.
- Chapter 5 is focused on case study, experiments and results with the threat modeling techniques, attack creation and detection method described in Chapter 3 and Chapter 4.

- Chapter 6 summarizes the work done in this research in the view of cyber-physical security framework for teleoperated autonomous vehicles, underscores the main contributions and discusses the potential areas of future work.

CHAPTER 2

Literature Survey

This chapter is on the literature survey for this dissertation. It starts with section 2.1 to introduce the evolution of road vehicles and mobility solutions in today's world. In Section 2.2, underlying working principle of vehicle motion, vehicle powertrain and vehicle E/E architecture for modern road vehicles are reviewed. Section 2.3 highlights the impact of road vehicle crash and importance of road safety. In section 2.4 and 2.5, the state-of-art concept of autonomous driving and ToD are reviewed in detail. This covers purpose, taxonomy, and operational domain of such systems. Section 2.6 reviews cybersecurity practices in Automotive. As ML approach is heavily used in AV and other IoT applications, section 2.7 attempts to capture some of the fundamental concept and background of ML. Section 2.8, highlights the cyber-physical challenges of AV and ToD. The last section 2.9 discusses the approach of anomaly detection for cyber-physical system.

2.1 Evolution of Road Vehicles and Mobility Solutions

Motor vehicles for roads have a more than a century of enriched history of inventions and innovations. The journey started at the end of 1800 with gasoline powered combustion engine to provide enough power to propel a vehicle. During the first few decades of 1900, primary inventions contributed mostly towards mechanical design and electrical features to improve engine efficiency and build a feasible modern automobile for public roads. Some of the notable enhancements include electric ignition, steering wheel, headlamp, and windshield wiper. During the third industrial revolution, advent of digital electronics and computers transformed the automobiles to automotive. This started with improving the performance, emission and safety of cars with sensors, actuators and electronic control units (ECU). However, in the past few decades cars have been upgraded with comfort, convenience and driver assistance technology. Currently as part of fourth industrial revolution automotive is going through a revolutionary transformation to integrate with a smart society ecosystem. Con-

nectivity, electrification, vehicle autonomy, and shared mobility are the four main areas of innovation for this transformation [26, 27] which are expected to capture the majority of global auto markets by 2035 [28]. Moreover, future vehicles are expected to support advanced IoT concepts including software define vehicle (SDV), digital twin which is realistic virtual models of physical vehicle with bidirectional communication with the components of the vehicle and evolving service model of shared mobility such as mobility-as-a-service (MaaS) [29, 30, 31, 32]. Connectivity for vehicle is categorized in three areas which are infotainment, telematics and vehicle connectivity to environment. Infotainment provides direct interaction of vehicle features and entertainment system with drivers and passengers. Vehicle telematics exchange the vehicle data with back-end and cloud system for vehicle prognosis and better experience of vehicle users. Vehicle connectivity to environment(V2X) may include vehicle-to-vehicle (V2V), vehicle-to-pedestrian (V2P), vehicle-to-infrastructure (V2I), vehicle-to-grid (V2G) and may extend to some other types. V2X is one of the promising technologies of cooperative intelligent transport systems(C-ITS). Vehicle electrification aims to reduce the dependency on fossil fuels for vehicle powertrain and reduce tailpipe emissions by introducing battery as energy storage system (ESS) and electric motor to deliver the power and torque for propulsion. For hybrid electric vehicle (HEV) and plug-in HEV (PHEV) electrification components are added to drive-train in series or parallel to engine, whereas for battery electric vehicle (BEV) engine is completely replaced with electric drive-train. Vehicle autonomy has the primary responsibility of improving vehicle safety and mobility efficiency by removing the need for a human driver, resulting human errors in driving. In the journey towards full autonomy in road-vehicles, numerous innovations and cutting-edge technologies have emerged. Vehicle teleoperation is one of such technologies that originated to provide emergency assistance to AVs in an unusual or difficult driving scenarios [5, 33]. However, this technology is also being targeted for teleoperated taxis and teleoperated delivery services. In US NIST vehicle teleoperation forum and in Europe 5G blueprint project are leading the research in this area [34, 35]. Several start-up companies including Zoox, Ottopia, Faction, DriveU.auto have started testing their prototype of teleoperated vehicles for mobility services for some specific use cases [36, 37, 38, 39]. Shared mobility is not a specific vehicular technology like connectivity, electrification and autonomy. Shared mobility in automotive can be viewed as a service or business model that enables mobility-on-demand including car sharing, ride sharing and flexible goods delivery by commercial delivery vehicles.

2.2 Road Vehicle Fundamentals

The primary purpose of road vehicles is transportation. Hence, it is important to understand the basic principles of automotive systems and components that enable driving. For this reason, vehicle motion, vehicle powertrain and in-vehicle electrical and communication architectures are reviewed in this section.

2.2.1 Vehicle Motion

Vehicle kinematics and vehicle dynamics are two fundamental concepts to understand the motion of a vehicle and the cause of it. Kinematics information includes position, velocity and acceleration of a vehicle in an inertial coordinate frame whereas vehicle dynamics is the motion of a vehicle as a rigid body with respect to a fixed global coordinate frame when [40]. In simple terms, vehicle dynamics can be viewed as the motion of a vehicle depending on its physical characteristics when driving actions (steering, braking, and acceleration) are applied to it [41]. Vehicle dynamics provides a more realistic insight of vehicle motion as compared to simple kinematics equation. For many years, modeling of vehicle dynamics is being studied by research community, starting from classical models of tire model and finite degree of freedom model (DOF) to modern approaches of trajectory or path planning model for AV in recent years [42]. These models have helped to improve safety, comfort and efficiency for cars over the past few decades. One of the widely used vehicle models used in both kinematics modeling and vehicle dynamics modeling is known as bicycle model [43]. In this approach a four wheeled car is represented as two wheeled model by combining the two front wheels and two rear wheels respectively at the center of each wheel axis. However, with the growth of electric vehicles and drive motor architecture in the wheel, four-wheel vehicle models are also getting attention from automotive researchers to properly model the non-linearity in drive-motor at wheel [44, 45].

2.2.1.1 Basic Equations of Motion

Translational motion: A vehicle motion can be described in multiple ways. One way is to consider the whole car as a single body which moves from point to A to point B. This is known as translational motion and can be expressed by the equation:

$$v = u + at \tag{2.1}$$

where, u is initial velocity, v is final velocity, a is acceleration and t time of travel.

If, s is the travel distance, the equation can be expressed as:

$$s = ut + \frac{1}{2}at^2 \quad (2.2)$$

Further, assuming the M as the mass of the vehicle, required force to move the vehicle to distance s ,

$$F = M \cdot a \quad (2.3)$$

Rotational motion: Vehicle motion happens when wheels of the vehicle rotate, this rotational motion can be expressed as relationship between torque provide at wheel, moment of Inertia and angular acceleration of the wheel:

$$T = I \cdot \alpha \quad (2.4)$$

I is derived from the radius of wheel and mass.

In actual driving scenario, vehicle motion involves more complexity than the simple equations of force and torque mentioned above. Road load, steering angle, tire slip, vehicle degree of freedom (DOF) are some of the critical factors for vehicle dynamics while the car is moving. These areas are covered in the sections below. Another important part is to understand the power flow from the energy source to the wheel via gear and transmission. For this research, teleoperated drivetrain is explained with HV battery, electric motor.

2.2.1.2 Vehicle Coordinate System

Vehicle's position from start to destination can be viewed as a moving object in XY plan, however while moving there is also vertical component of the motion. In automotive engineering, there are two conventions followed for depicting a vehicle's movement in a coordinate system: 1) SAE convention [46] and 2) ISO convention [47]. In Fig. 2.1, both conventions are shown. Vehicles movement around each of the 3 coordinates shown in the diagram contribute to overall vehicle dynamics. Study of vehicle dynamics is important to achieve vehicle stability during its motion. In the next section DOF for vehicle is discussed followed by vehicle dynamics and its mathematical representation.

2.2.1.3 Vehicle Degree of Freedom

In the study of vehicle dynamics, DOF is used to denote the number of independent motions. DOF is widely used in mathematical modeling of the vehicle dynamics and stability for various driving conditions. Depending on the objective of the analysis DOF can be a two

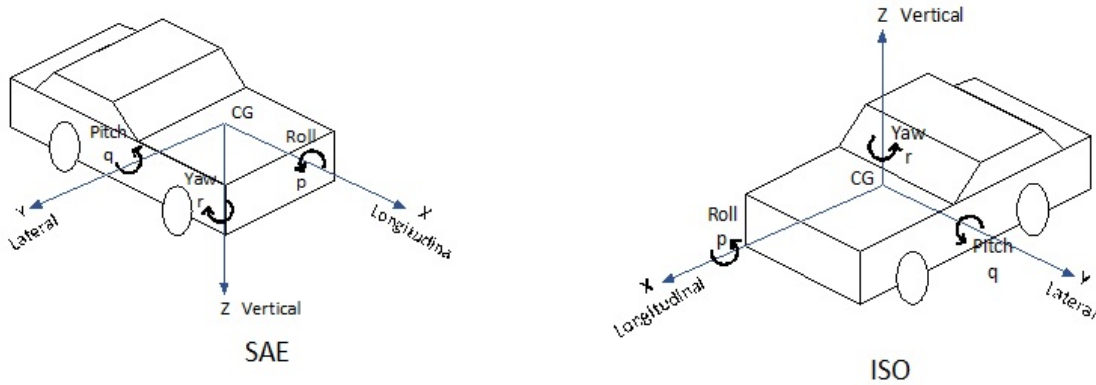


Figure 2.1: Vehicle Motion with 6-DOF

DOF model or it can be an 18-DOF model [42]. A commonly used 2-DOF model in vehicle stability research focuses on vehicle's linear displacement along the lateral axis and rotational movement along the vertical axis (yaw). 3-DOF model adds includes the movement along the longitudinal direction. A 3-DOF gets extended to a 6-DOF model by considering the linear and rotational movement along the 3-axis to the model. In Fig. 2.1, pictorial representation of a 6-DOF for SAE and ISO vehicle coordinate system is provided. The higher dynamics model such as 7, 14, 18 augments the analysis by considering the forces on tire and suspension of the vehicle. In Table 2.1, few examples are given for use of DOF for vehicle dynamics and control.

Table 2.1: DOF with Example Usecase

Degree of Freedom	Example of Analysis Type
2 DOF	Steering controller design [48]
3 DOF	Vehicle maneuver, trajectory planning [49, 50]
6 DOF	Aerodynamic and Vehicle Handling Crosswind Simulation [51]
8 DOF	Active suspension system [52]

2.2.1.4 Longitudinal Dynamics

Longitudinal vehicle dynamics is the result of various longitudinal forces acting on the vehicle when it is moving [53]. This is represented in Fig. 2.2. When a vehicle moves there is road load ($F_{roadload}$) due to aerodynamic drag (F_{aero}), rolling friction at tires (F_{roll}). If it is going uphill, then a component of gravitational force (F_g) also adds to the road load. To move the vehicle, applied force at the tire needs to be larger than road load. Acceleration (a) of the

vehicle depends on this applied force and vehicle mass. However, the maximum force that can be applied to the tire depends on the coefficient of friction between the tire and road surface. Consideration of this factor is very critical to get the traction without wheel slip (s).

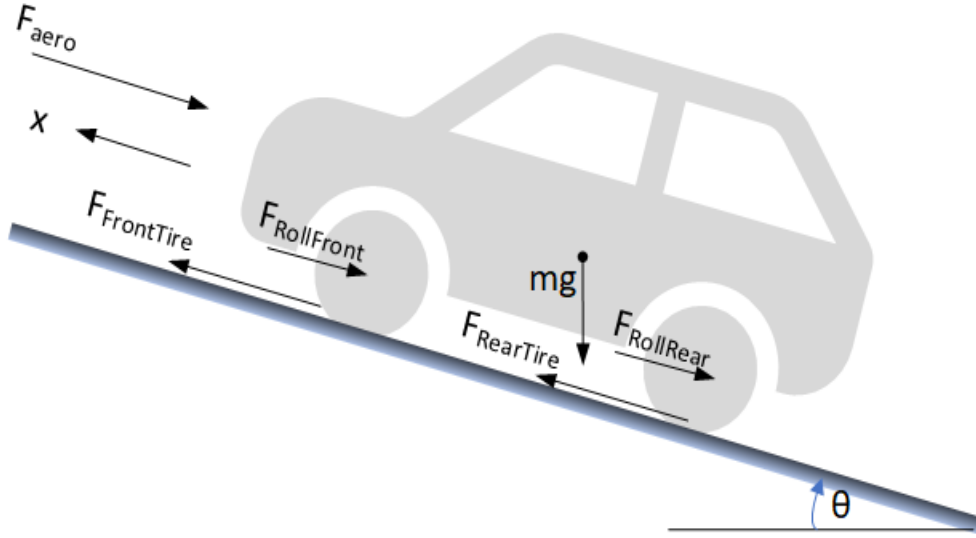


Figure 2.2: Longitudinal Force on Vehicle

Longitudinal force acting on the vehicle can be represented by the following equations:

$$F_{\text{roadload}} = F_{\text{roll}} + F_{\text{aero}} + F_g \quad (2.5)$$

Note: $F_g = mg \sin \theta$, where g is gravitational constant and θ is inclination angle of the slope.

$$F_{\text{tires}} - F_{\text{roadload}} = ma \quad (2.6)$$

where, F_{tires} is combined force for all tires, m is mass of the vehicle.

$$F_{\text{traction}} \times \eta = F_{\text{tires}} \quad (2.7)$$

where, η is coefficient of friction between tire and road surface.

Note: During braking, vehicle is decelerated by using the friction force between tire and road surface. In conventional vehicle, most of the mechanical energy during braking gets converted into heat and partially sound. Material of the tire, brake pads influence

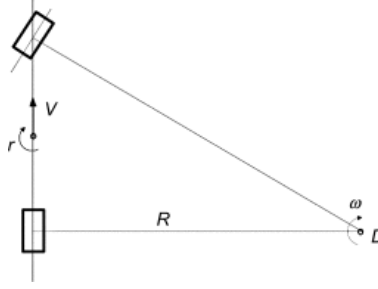


Figure 2.3: Vehicle Yaw Rate and Angular Velocity [55]

the braking performance. In modern vehicles, brake controllers are designed to optimize the braking action depending on criticality to allow maneuver control and provide rider's comfort. For electric vehicle, regenerative braking is used to recover some of the electrical energy from the mechanical energy.

2.2.1.5 Lateral Dynamics

During lane change, turning or maneuvering a vehicle, lateral force is applied to the vehicle. Vehicle response to this force impacts the stability of the vehicle. When the vehicle steers there is a change in vehicle yaw. It should be noted, there are various vehicle models to study lateral and yaw motion of a vehicle. Bicycle model is a widely used simplified representation of a car to study lateral vehicle dynamics. In this model, front wheels are assumed in the middle of the front axle and rear wheels are assumed in the middle of rear axle, like a bicycle. In this subsection, vehicle lateral dynamics is explained with a bicycle model for cornering scenario at four different speed level: 1) very low, 2) low, 3) medium and 4) high speed [54].

As shown in Fig. 2.3, if the vehicle has a velocity V and the angular velocity during the turn is ω , based on the radius of curvature R , then yaw rate (r) can be expressed as followed:

$$V = R\omega \quad (2.8)$$

$$r = V/R \quad (2.9)$$

$$r = \omega \quad (2.10)$$

For an extremely low *speed* scenario, front tires and rear wheel angle is very close, hence assuming slip angle is negligible and considering distance between the two axle is l , the

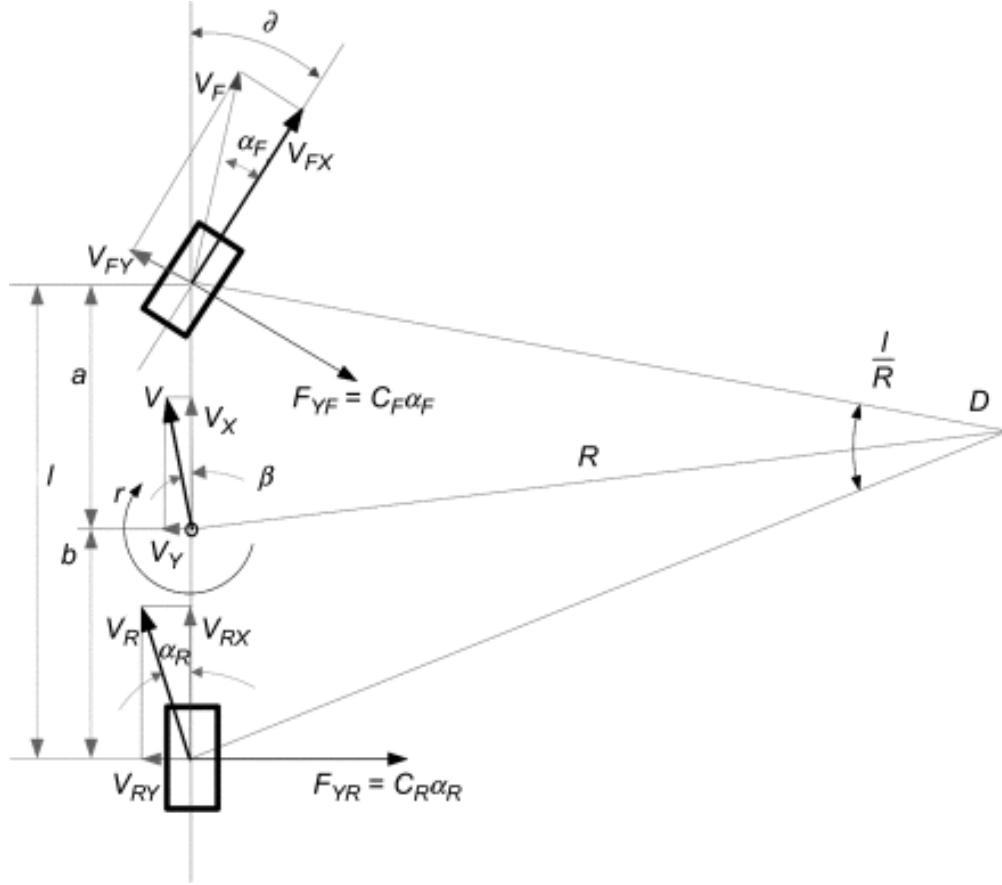


Figure 2.4: Vehicle Lateral Motion as Bicycle Model [55]

steering angle can be approximated as:

$$\delta = \frac{l}{R} \quad (2.11)$$

In 2.4, a bicycle model is shown for vehicle's lateral motion in a *low-speed* scenario. In this diagram, distance between the two axle is l , distance of front axle and rear axle from the center of vehicle's center of gravity are a , b respectively. δ is front wheel average turn angle, α is wheel side-slip angle and β slip angle of the vehicle. From this diagram it can be derived:

$$\alpha_R + \delta = \frac{l}{R} + \alpha_F \quad (2.12)$$

R and F in subscripts denote Rear and Front.

or,

$$\delta = \frac{l}{R} + \alpha_F - \alpha_R \quad (2.13)$$

The lateral force on front tires (F_{YF}) and rear tires (F_{YR}) depend on the wheel side slip angle and cornering stiffness of the tire. This is given by:

$$F_{YF} = C_F \alpha_F \quad (2.14)$$

$$F_{YR} = C_R \alpha_R \quad (2.15)$$

Further, lateral force on front tires (F_{YF}) and rear tires (F_{YR}) can be derived from centripetal force F which can be written as:

$$F = \frac{mV^2}{R} \quad (2.16)$$

Considering the distance of front wheelbase and rear wheelbase from center of gravity lateral forces can be written as:

$$F_{YF} = \frac{mV^2}{R} \times \frac{b}{l} \quad (2.17)$$

$$F_{YR} = \frac{mV^2}{R} \times \frac{a}{l} \quad (2.18)$$

2.2.1.6 Vertical Dynamics

Vertical dynamics refers to vehicles motion in vertical direction. The vehicle responds to the forces applied to the vehicle due to acceleration, braking and irregularities of road surface [53]. This results in pitch and heave movement along the vertical axis [56]. For conventional road vehicles, vertical dynamics is an important study for the suspension system of a vehicle which dampens these movements to protect the components of vehicle and provide a stable, comfortable ride. A passive suspension system is a conventional method that uses springs and dampers to provide the intended functionality, whereas an active suspension system uses controllers and actuators to dynamically change the chassis height for each wheel [56]. However, with the advent of AV and EV, study of vertical dynamics is extended to emerging topics including accurate target estimation, vehicle motion control, suspension control with BEV architectures [57, 58, 59].

2.2.2 Vehicle Powertrain

Vehicle powertrain involves the study of the process and components for generating, distributing, and delivering power to drive the vehicle. In case of internal combustion engine (ICE) vehicle, power is generated by engine and delivered to wheel via transmission, drive-shaft, differential and axle. For, EVs power comes from the high voltage (HV) battery to electric motor via power electronics components and the motor provides the torque to transmission to deliver at wheel. For HEVs, various series and parallel architectures have evolved over last three decades to optimize the power flow from engine and motor using automotive control unit [60]. As this research focus on future vehicle, battery electric vehicle (BEV) architecture is shown in Fig. 2.5. As it can be noted from the diagram, for powertrain two primary components are HV battery as ESS and the electric traction motor which transfer the electrical energy as mechanical energy to vehicle wheels. HV batteries for BEVs need to satisfy various requirements amongst which ability to deliver power for traction motor and energy density are the primary ones as they determine the acceleration time and range of the vehicle [61, 62]. Some of the other major criteria that are used to evaluate EV batteries are battery chemistry, efficiency, weight, size, pack architecture and thermal hazard. Basic mathematical equation for battery power is given by equation 2.19.

$$P = V \times I \quad (2.19)$$

where, P available from the battery,

V is voltage across positive and negative terminal of the battery and I is current flow.

In this context, range indicates the distance the vehicle can go with the total energy capacity of HV battery for EV [63]. This is typically calculated in Kilowatt hours (kWh) which can be derived from power over time. For the electric traction motor in BEV, the fundamental torque equation can be expressed as equation [64]:

$$T - T_l = \frac{d}{dt} (J\omega_m) = J \frac{d\omega_m}{dt} + \omega_m \frac{dJ}{dt} \quad (2.20)$$

It should be noted that, for BEVs some energy can be recovered during braking by using the motor as generator. This method is known as regenerative braking [65].

2.2.3 Vehicle E/E and N/W Architecture

Features offered by modern vehicles comprise of many functional areas including vehicle control, body and security, comfort, convenience, infotainment, active safety, passive safety and driver assistance. Vehicle E/E and network (N/W) architecture drives the engineering design and development of electrical components, hardware, software and communication methods between them to deliver these features. Over the years vehicle E/E and N/W architectures have evolved to satisfy the requirement for a safer, reliable and enhanced vehicle features. This includes real-time sensing and actuation, efficient use of energy, faster data processing, optimal use of computation power, functionally safe design and reliable communication [66, 67]. In Fig 2.5, a conceptual diagram of vehicle architecture is shown. Lower part of the diagram is shown for powertrain and top part is shown for E/E architecture. E/E architecture consists of various electronic control units (ECU) that are connected in a vehicle network topology to exchange information with each other. ECUs were introduced in vehicle architecture for precise control of fuel injection in engine to get optimized performance [68]. Later ECUs became widely used in other real time applications in automotive including fuel efficiency, minimize emissions, safety, body domain. Initially ECUs were built with micro-controllers, limited embedded resources, however to reduce the number control units and electrical wiring domain controller approach was introduced which combined the ECUs under few domains known as power train, body, chassis and infotainment [69]. To exchange the information across the ECUs, automotive engineers and researchers have developed several in-vehicle network protocols over past two decades [70]. One of the earliest and dominant protocol is known as control area network (CAN) which was introduced by SAE to ensure the reliable and real-time communication between automotive ECUs. Later this protocol was revised and standardized as ISO 11898. Original CAN protocol was limited to 1 Mbps and 11 bytes data per frame which was sufficient for the intended applications. However, to support higher data exchange in today's vehicles CAN with flexible data-rate (CAN-FD) which can support up to 5 Mbps speed and 64 bytes of data per frame [71, 72, 69]. Another protocol known as FLeXRay was developed to support fault tolerant with higher data rate primarily for steer-by-wire application. FlexRay has maximum data rate or 10 Mbps and its use is not limited steer-by-wire only [69]. For low speed communication between ECU to smart sensors and actuators local interconnect network (LIN) protocol is commonly used which can support maximum speed of 19.2 kpbs with low power consumption [69]. In addition to this, there are other application specific protocols in automotive. For example, infotainment application does not have a hard real-time requirement for data exchange, rather data bandwidth is more important. To support this type of application, Media Oriented Systems Transport (MOST) is a common practice which can support up to

150 Mbps data transfer speed [69]. Automotive audio bus (A2B) is another example which is used for audio data exchange in automotive with 50 Mbps of maximum speed [73]. Other than in-vehicle communication protocol, modern vehicles also use wireless protocols for various applications. One of the widely used wireless communication by passenger cars are remote keyless system (RKS) which enables unlocking, locking and starting car with keyfob. In the USA and Japan, RKS use 315MHz and in the Europe 433.92MHz and 868MHz band are used for remote entry operation from a distance of 10 meter to 100 meter and relies on LF band from 120 kHz to 130 kHz to start the vehicle remotely [74, 75]. More advanced keyless entry and keyless start commonly termed as passive entry and passive start use UHF band and can function from 1 meter to 2 meter distance without any manual activation on the keyfob [74]. However, the E/E and software architecture of conventional automotive cannot support the future landscape of automotive transforming from conventional vehicle to CAV [67]. This has necessitated the automotive industry to redesign the automotive E/E, n/w topology and software architecture. With significant advancement of high-tech industry in past decade, automotive companies are integrating high-power compute device, system on chip (SoC), larger memory and high-bandwidth communication channels for next generation architecture [76, 77, 78]. Traditional Automotive software architectures were primarily dominated by monolithic architecture and majority of the software architecture is guided by the AUTOSAR standard. However, to address the growing complexity of automotive features, future automotive design is embracing software-defined-vehicle (SDV) where features and capability of the vehicle is controlled by software. Hence, software design paradigm has shifted to distributed and service-oriented architecture to manage the dynamic demand of computation, power and faster deployment of new features [79]. To support the increasing volume of data exchange in vehicle network, specially for ADAS and AV applications, automotive ethernet technology is considered as a potential solution. Automotive ethernet can provide a maximum speed of 100 Gbps of data transfer rate to exchange perception data between sensors and high-performance compute devices that runs the AI/ML algorithms [80]. For high-speed image transmission, Low-voltage differential signaling (LVDS) bus is widely used for vehicle autonomy. [81] Some of the advantages of LVDS include low power consumption, no protocol overhead and high tolerance against interference. AVs also use global position system (GPS) technology to locate the position of the car and navigate through the route. For this purpose, GPS tracker in the vehicle communicates with Global Navigation Satellite Systems (GNSS) [82]. A pivotal design consideration for newer architectures in automotive is vehicle connectivity. Over-the-air (OTA) software upgrade, traffic management, fleet management, infrastructure assisted driving, shared mobility and vehicle prognosis are some of important connected features targeted for initial deployment [83, 84]. A modern car is

already capable of connecting with phones and other portable electronic devices (PED) using Wi-Fi, which use communication protocol defined by IEEE 802.11 and bluetooth that follows IEEE 802.15.1 standard [85, 86]. However, unlike previous architectures, connected vehicles need to extend the communication outside the vehicle to support these features. Further, communication technology for V2X communication needs to support high-speed, high bandwidth and reliable communication with growing demand of connected features for passenger vehicles and commercial vehicles on public roads. Two primary protocols which were designed for V2X communications in last decade. In US, Dedicated Short-Range Communications (DSRC) protocol and in Europe Intelligent Transportation System (ITS)-G5 protocol were developed based on 5.9 GHz band [87]. Both of these protocol use the IEEE 802.11p standard for physical (PHY) and medium access (MAC) layers of vehicular wireless communication stack. However, DSRC and (ITS)-G5 were developed for short range communication and not suitable for V2X communication longer than than 1 km. In recent years, 3GPP Long-term Evolution (LTE) has developed Cellular V2-X (C-V2X) standard based on mobile cellular connectivity. The goal of this standard is to meet the connectivity demand of larger density of vehicles and other users on the road with low latency, high speed. C-V2X uses 4G LTE or 5G for cellular communication [88].

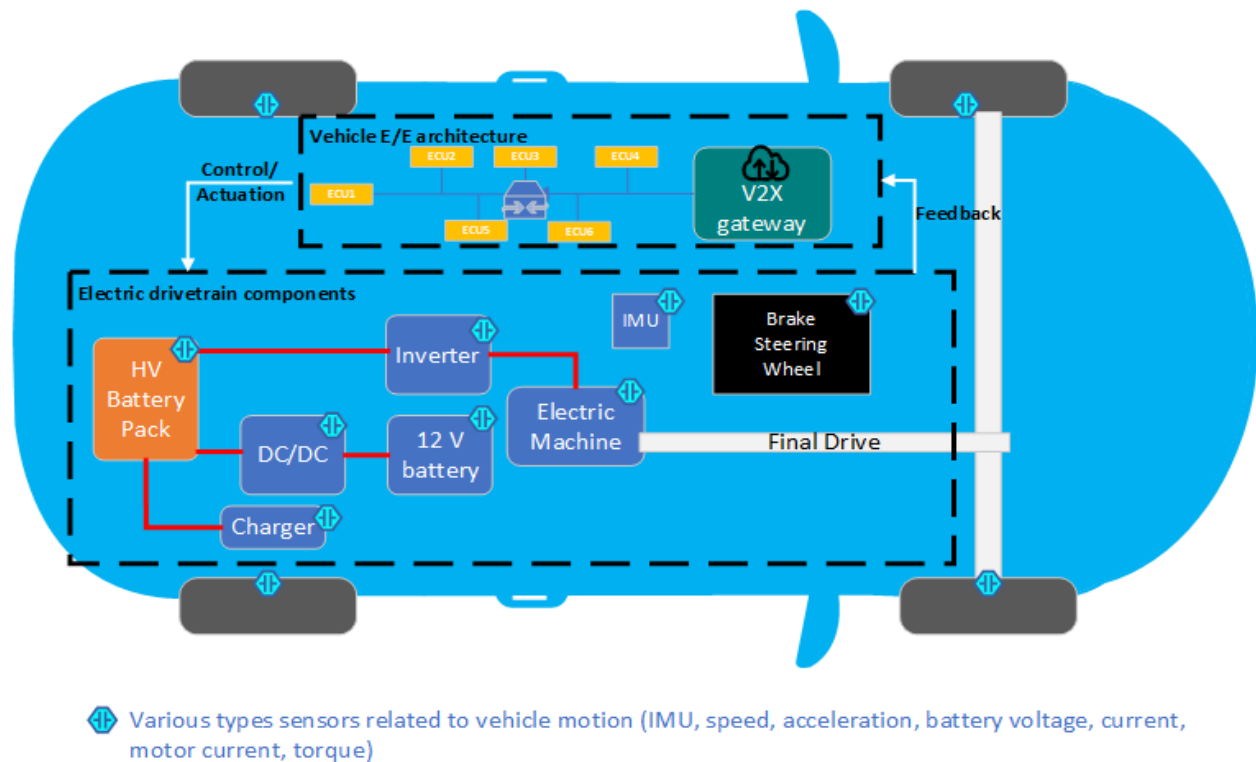


Figure 2.5: Electric Vehicle Architecture

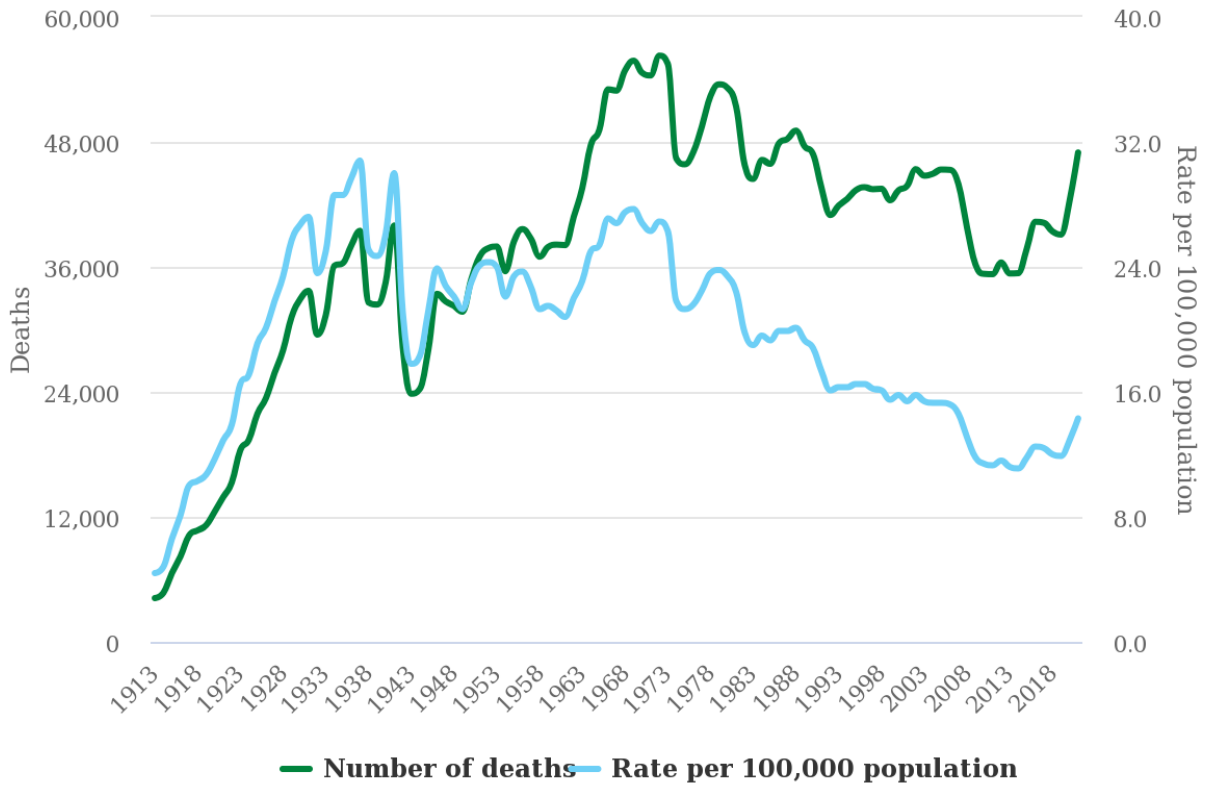
2.3 Road Safety and Vehicle Crash

Road safety in modern transportation involves various measures to avoid motor vehicle crashes, road accidents and minimize potential physical injuries due to an accident. From a holistic view, road fatalities also disrupts public health, socio-economic balance and GDP of a nation [89, 90, 91]. Hence, WHO, PAHO, UN bodies and other global forums are actively taking initiatives to raise awareness, create legislation and collaborate with vehicle safety regulatory bodies of various countries including NHTSA, METI, KMVSS, CMVSS, CCC and UNECE WP.29 to develop the capability for improved road safety around the world [92, 93, 94]. Road safety annual report from IRTAD indicates that road crashes in motorways, urban road and rural road cause even death [95]. Even with emergency assist and advanced driver assist features in many of road vehicles, every year almost 2 million people are impacted physically due to road traffic accidents [94]. For example, as shown in Fig. 2.6 from US National Safety Council data, though the death rates caused by vehicle crash has decreased over the past few decades but total number of deaths has an upward trend specially in recent years [96]. Data also shows that these fatalities impact occupants inside the car and other road users outside the vehicle. Further, fatalities to people outside the vehicle specifically pedestrians have increased in the rural and urban roads in recent years [90, 97]. For statistical analysis, road collisions can be grouped by in various ways. Some of the common methods are based on driving scenario (e.g., lane departure, turn in intersection), direction or point of the impact (e.g., head-on, angled, sideswipe, rear end) and parties involved (e.g., two vehicle, vehicle-pedestrian, vehicle-animal) [98]. Based on US NSC data 2020, angled collision and head on collision are the top two reasons for deaths and fatal crash in US [99]. In Fig. 2.7, analysis of damaged pattern and severity of impact for passenger cars presented from [98] by Kurebwa et. al. In this figure, the diagram on the left shows that authors divided the vehicle surface in 12 zones similar to a clock. On the right side authors have presented the frequency distribution by direction of force in these 12 zones for the crash dataset used in their study. It can be noted that front and front-corner zones have higher occurrence of impact as compare to other zones.

2.4 Autonomous Vehicle: Purpose, Taxonomy, Operational Domain and Driving System

One of the strong motivations for AVs is to improve road safety by reducing accidents caused by human drivers, however reduced congestion, efficient fleet management, improved fuel economy and reduction in harmful vehicle emissions are some of the other benefits ex-

Deaths and population rates, 1913-2021



© 2023 National Safety Council. All rights reserved.

Figure 2.6: NSC Motor-vehicle Fatality Trends [96]

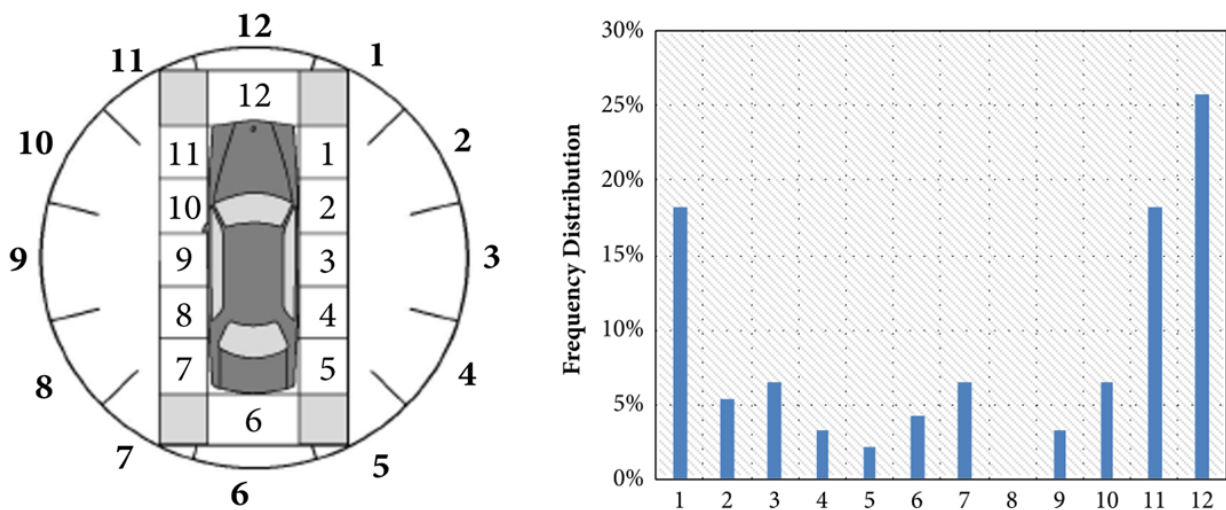


Figure 2.7: Vehicle Crash Point Direction of Force [98]

pected from AVs when complemented with connectivity [4]. In 2014, SAE published the J3016 standard that classifies six levels of ADS, which was updated significantly in collaboration with the ISO in 2021 [100]. This standard is accepted by regulatory bodies like UNECE WP.29/GRVA [101], NHTSA, US DOT [102], and California DMV [103] as well as by the key players of AV standardization like ISO/PAS 21448-SOTIF [104], ISO 34501 [105], ISO 34502 [106], ISO 34503 [107], UL4600 [108], IAMTS, and ASAM [109] to create other standards, laws and guidelines for AVs. It is stated that the driving system is described by the word “automation.” However, several complex terms such as “Automation System,” “Automated Driving,” and “Driving Automation” are used in SAE J3016 and presented differently such as “Automated Driving System” (NHTSA, 2016) and “Autonomous Driving System” [110]. Therefore, before developing the research process, this study intends to define “autonomy” and “automation.” The dictionary definition of “automation” is “made to be written by a machine or computer in order to reduce the work done by humans” (Cambridge Dictionary). “Automated systems” in vehicles cannot yet drive reliably and safely in all traffic scenarios and situations that occur on the road, and the driver does not need to monitor the system and driving environment but the driving ability of the automated systems. It states that when this is limited or when the system fails, the driver should take control of the vehicle [111, 112]. “Autonomy” is defined as “having the power to be independent and make decisions for yourself” (Cambridge Dictionary). In other words, an AI-based AV has the ability to recognize the surrounding environment and drive itself without human intervention [110, 113]. To simplify, an automated system cannot drive safely and steadily in all traffic scenarios and situations on the road. For example, when the road is blocked, it is difficult for an automated car to return to the normal driving state without driver intervention to search for another route. However, an AV can drive itself using AI technology without human input in all traffic scenarios and situations.

Operational Domain(ODD): At a high level, the first three levels (L0, L1, and L2) of J3016 are excerpted as “Driver Support Systems,” while L3, L4, and L5 are exercised for actual ADS [114]. It is important to note that these automation levels do not classify the automation level of the whole vehicle but rather define the level of automation of a feature when it is engaged [114]. For example, a vehicle capable of traffic jam chauffeur as an L3 ADS feature will have a specific operational design domain (ODD) and relevant dynamic driving task (DDT) to perform the feature, whereas exiting from the highway can still be manually operated by a human driver without involving DAS. In Table 2.5, we have summarized six levels of driving automation along with the applicability and scope of the associated key terminologies used in J3016 to define them, e.g., ODD, DDT, DDT fallback, minimal risk condition (MRC) and a few more. As per our interpretation of J3016, ODD is arguably the

most critical parameter, as other parameters are highly dependent on it. We also note that the definition of ODD in J3016 is very high level and does not give enough clarity on how ODD can be parameterized. To address this limitation, European standards have created a taxonomy document, PAS 1883 [115], which classifies ODD parameters into three main categories, (1) scenery, (2) environmental conditions, and (3) dynamic element, but this standard does not provide boundary conditions for each automated level. SAE has recently started an initiative to create J3259 for ODD taxonomy and definition, but this standard is not available for use yet. In our study, we have analyzed the ODD from a perception and connectivity perspective.

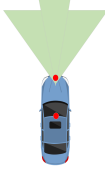




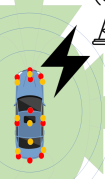



Automated Driving System (ADS): As shown in Fig. 2.8, for perception coverage in L0, only frontal coverage is required, but in L1 and L2, coverage in the rear and four corners is required as well. Perception coverage for L3 should be augmented with a surround-view in the nearby zone of the vehicle, and for L4 and L5, the surround-view coverage needs to be extended like a human driver. Connectivity is recommended starting from L4 to communicate with V2X, and for L5, the connectivity range needs to be extended to communicate with V2X from remote areas. For DDT, in L3 and above, the expectation is to have complete and continuous DDT by the system, whereas in L1 and L2, it is limited to a sustained basis. DDT fallback and MRC are significant distinguishing factors between L3 and the levels above L3, as the driver is responsible for DDT fallback and MRC for L3 features, and MRC is not mandatory. In contrast, the system must handle the DDT fallback for L4 and L5.

Architecture Requirement: The primary objective of vehicle automation is to improve safety by eliminating or at least significantly reducing the accidents caused by human error. Hence, ADS must perform better than a human driver. J3016 divides the act of driving into three main categories, (1) strategic (trip planning), (2) tactical (motion planning), and (3) operational, which can be lateral (steering) and/or longitudinal (acceleration/deceleration) control. Tactical and operational efforts and object and event detection and response (OEDR) are sub-tasks of DDT in DASs, determined by feature and associated automation level. A typical automated architecture includes five main building blocks: perception, localization, sensor fusion, planning, and control subsystems. This architecture is composed of various components such as camera, radar, lidar, and ultrasonic sensors for perception; IMU and GPS sensors for localization; high-bandwidth in-vehicle communication, V2X connectivity, and a sophisticated AI/ML algorithm for sensor processing; and sensor fusion, scene creation, motion planning, a combination of real-time and high-computing energy-efficient processor, memory with more bandwidth and bus width and ample data storage. Furthermore, depending on the scope of ODD and DDT, these components may need to follow a

higher category of specific standards such as ISO 26262 (functional safety) and ISO/PAS 21448 (safety of the intended functionality) to ensure safety-driven design. This means that a highly automated driving (L4) feature in which DAS is expected to operate independently in complex driving scenarios will require more capable and reliable hardware (sensors, processor, memory), V2X connectivity, faster as well as broader communication bandwidth, and a significant increase in lines of code and data storage as compared to conditional automation (L3) where the human driver can act as a complementary driver in complex driving condition. A typical safety-critical system like AV should also be capable of responding to failures in fail-operational, fail-safe, and fail-secure ways, which may need redundancy in some of the critical hardware and software. In Table 2.5, a plausible comparison is captured for some of the systems requirements based on our understanding of variations in driving automation tasks at each level, technology trends, and observations from some of the key players in the industry. For example, DDT sensors for perception in L3 will be more numerous than in L1 and L2 to cover the surrounding view in addition to frontal, rear, and corner coverage. In L4 and L5, the surround-view sensors need a more extended range to cover the area like a human driver. Further, redundant perception and localization sensors and computing devices will be required for DDT in L4 and L5 to replace the human driver as a complementary driver and fallback element. The enormous amount of data generated from the sensors augmented by connectivity increases the demand for communication bandwidth and data storage in L3 and above, at least five times more than in L1 and L2. For computation needs, software lines of code and processor throughput can increase at a very high rate from each level to the next one, increasing the memory requirement 10 to 20 times more in L3 and above. Also, energy utilization and heat management should be done efficiently to maintain the optimal performance from this high-computing hardware. Some of the data reported from L3 test vehicles showed that 13 to 20 percent of the total energy consumed during the drive cycle was used by the computing devices in the car. If this trend is observed more persistently, we expect this power requirement to go beyond 40% or even 50% considering the complete DDT fallback responsibility in L4 and L5, as it may require double or triple redundancy in computing and control devices.

2.5 ToD Concept for Smart Mobility

Teleoperation technology enables the ability to operate a device from a remote location by utilizing digital platform and high speed data transmission ability of modern telecommunication. Many applications including remote surgery, precision manufacturing, hazardous industrial machinery have extended this ability to operate machines by integrating teleop-

Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Perception & connectivity: 	Perception & connectivity: 	Perception & connectivity: 	Perception & connectivity: 	Perception & connectivity: 	Perception & connectivity: 
1. Perception: <ul style="list-style-type: none"> Frontal coverage 2. Connectivity is not required	1. Perception: <ul style="list-style-type: none"> In addition to frontal coverage, nearby coverage in four corners and the rear of the vehicle is required 2. Connectivity is not required	1. Perception: <ul style="list-style-type: none"> Same as L1 2. Connectivity is not required	1. Perception: <ul style="list-style-type: none"> Increase in corner coverage from L1 and L2 Nearby surround view is required 2. Connectivity is not required	1. Perception: <ul style="list-style-type: none"> Increase in surround view similar like a human driver Redundant sensors are recommended 2. Connectivity is recommended to communicate with V2X	1. Perception coverage is similar to L4 2. Increase in connectivity from L4 is recommended to connect from remote areas
ODD: Not applicable	ODD: Not applicable	ODD: Limited	ODD: Limited	ODD: Limited	ODD: Full
Automated: Not applicable	Automated: Yes	Automated: Yes	Automated: Yes	Automated: Yes	Automated: Yes
Autonomous: Not applicable	Autonomous: Not applicable	Autonomous: Not applicable	Autonomous: Not applicable	Autonomous: Yes	Autonomous: Yes
DDT motion control: Not applicable	DDT motion control: Latitudinal or longitudinal control at a time	DDT motion control: Latitudinal and longitudinal control at the same time	DDT motion control: Latitudinal and longitudinal control at the same time	DDT motion control: Latitudinal and longitudinal control at the same time	DDT motion control: Latitudinal and longitudinal control at the same time
DDT fallback: Not applicable	DDT fallback: 	DDT fallback: 	DDT fallback: 	DDT fallback: DAS	DDT fallback: DAS


• Perception sensor	• Redundant perception sensor	■ Sensor coverage	 Connectivity range. Larger circle represents longer and more connectivity.
 Human driver	DAS Driving automated system		

Figure 2.8: Comparison Between SAE Automation Levels [116]

eration with advanced robotics in their ecosystem. Teleoperation is also used in deep ocean exploration, managing radioactive debris and controlling unmanned aerial vehicle (UAV) for military and surveillance. ToD of road vehicles have emerged in recent years to enhance the capability of connected and autonomous vehicles as an assistance in situations where automated driving system (ADS) is incapable to take driving decision [117, 33, 5]. In 2020, National Policy Agency in Japan released road use demonstration of autonomous vehicle that covers testing remotely-controlled ADS [118]. In 2021, German government published a regulation which authorized a technical supervisor to steer and drive the vehicle from outside the vehicle within vicinity [119]. In US, for state of California a remote operator is allowed to command ADS to execute minimal risk condition where as Arizona state allows directing vehicle remotely for its movement [120]. In UK, as per Code of practice automated vehicle trialling, safety operators located remotely are allowed to override the autonomous vehicle if required [121]. However, interpretation of these regulatory codes varies in terms monitoring,

guidance vs direct control. In recent years, several vehicle manufacturers and mobility service providers across the globe along with their industry partners are working together to develop solutions for vehicle teleoperation from concept to deployment [5]. In Europe, 5gblueprint project was initiated in 2020 to design and validate 5G based technical architecture for connected and automated mobility. Though primary focus of this project is on cross-border teleoperated transport, however outcome of this project will be used as a foundation for 5G based teleoperated transport solutions across pan-European region [122]. Same year, NIST in US conducted a virtual conference for vehicle teleoperation forum which discussed roles of teleoperation in automated driving, key challenges in vehicle teleoperation, plausible benefit from technologies including AI, 5G, cloud computing and areas of teleoperation for standardization. In the following year, formation of teleoperation consortium in US was announced to facilitate the communication, collaboration and consensus between academia, industry partners and government organizations involved in teleoperation ecosystem [123]. In December 2021, 5G-Blueprint project organized a forum with active participation from NIST and Teleoperation Consortium which discussed various topics including taxonomy, safety, ODD, vehicle interface and passenger interaction of vehicle teleoperation [124]. During this consortium, Vehicle teleoperation technology was viewed as a primary solution to improve the safety and performance of autonomous driving on the public road. In transportation and logistics industry, the last leg of the shipping is LMD. Planning and managing a cost-efficient LMD with high fidelity is a challenging task. For this reason, vehicle teleoperation is getting strong attention for improving the operational flexibility and cost efficiency of the LMD of goods [125, 126, 127, 128]. In many countries vehicle teleoperation is being evaluated as an potential solution to provide mobility service for elderly and disabled persons [129, 130].

As per Teleoperation Consortium, remote driving or assisting ability to a piloted or self driving car is ToD [134]. NIST view teleoperation as a crucial part of AV ecosystem and also can serve transportation services including teleoperated taxis and teleoperated delivery [135]. 5G-blueprint project defines vehicle teleoperation as a technology that enables remote operator to passively control autonomous and semi-autonomous vehicles and when required allows full control of the vehicle [136]. In Fig. 2.9, a simplified diagram of dataflow involved in ToD is shown. As illustrated in this diagram, a basic teleoperated vehicle requires sensors to collect the data required for ToD. Such data primarily include perception data from the vehicle's current operating environment, information about the vehicle's location. Both perception and localization information are then transmitted to operator terminal using wireless communication. At operator terminal, the received information is process and transformed to create a remote digital perception of the vehicle for the human operator at terminal. Based on this digital perception, the human operator takes the action at the terminal which can

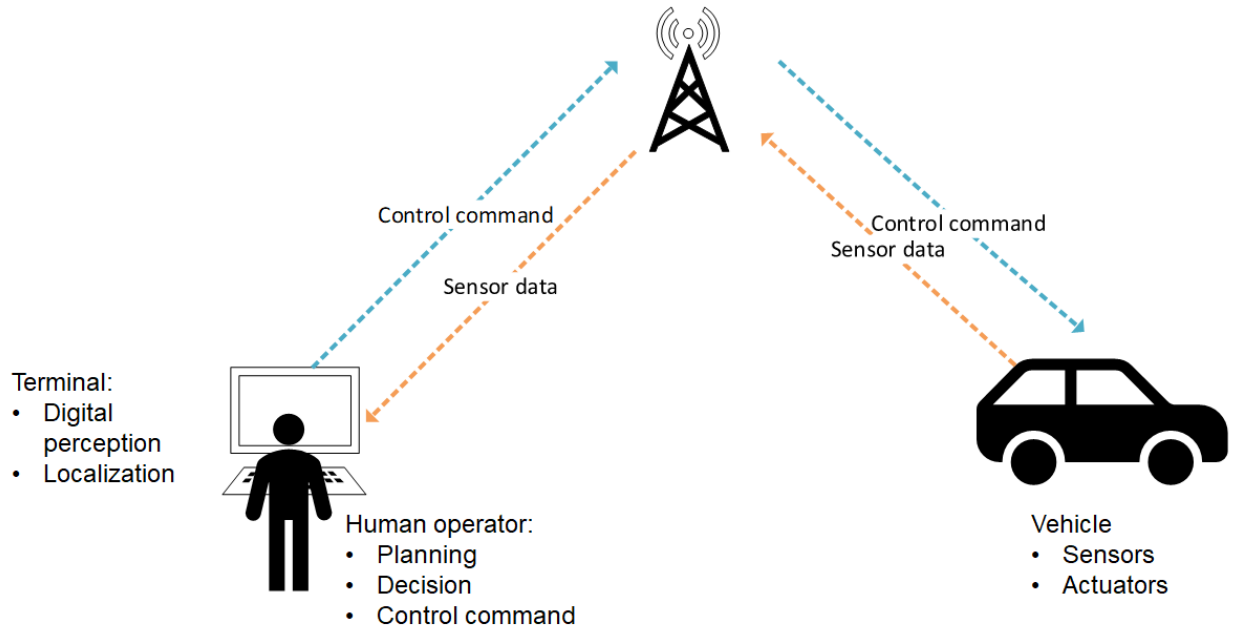


Figure 2.9: Vehicle Teleoperation High-level Concept

be guidance or control of the vehicle. Operator’s action is then transmitted back to vehicle using the wireless communication. On the vehicle side these action is received as operator’s command to determine the control logic of vehicle motion actuators. Based on the current solutions from various partners in automotive industry, ToD can be of three types: a) direct control, b) indirect control and c) teleguidance / teleassist. Example of these three types are shown in in Fig. 2.10. As shown in this figure, in case of direct ToD most of the driving tasks including planning, decision and vehicle control are performed by the remote operator. For an indirect control of ToD, the remote operator can provide guidance by providing or selecting a trajectory or way-points. With these waypoints as inputs to trained AI/ML models for trajectory and motion planning the driving control actions are deduced. Teleguidance is a type also caonsidered a shared control type of ToD, where the decision and control of the is shared between ADS and the remote driver [137, 120].

2.5.1 Driving Context

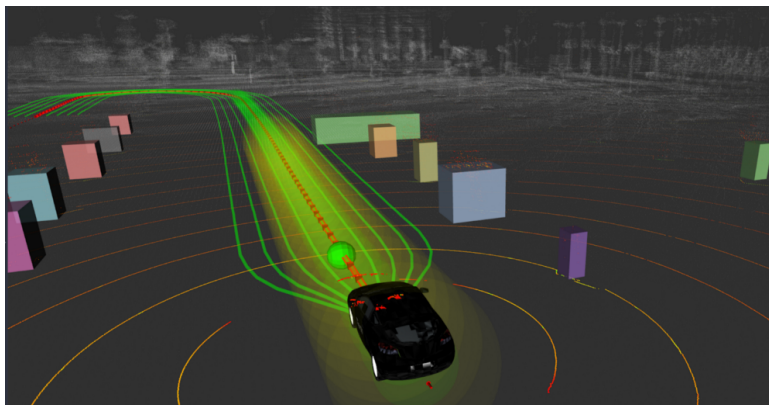
In previous section, vehicle motion and powertrain are discussed from physical perspective, however various other factors can influence driving behavior. For example, traffic situation can vary based on the road condition, weather, location, and time of the day [138]. Teleoperated vehicle might be in a time critical mission. What is teleoperated driver’s next intended



(a) Direct ToD: Human is driving remotely based on digital perception [131]



(b) Indirect ToD: AI recommends plausible paths for teleoperators to choose from [132]



(c) Teleguidance for ToD: Human is providing waypoints [133]

Figure 2.10: Vehicle Teleoperation Types

maneuvers. Also, there can be variation in driving style depending on the driver. These types of contextual and human factors influence the driving pattern [139]. In Fig. 2.11, a conceptual diagram is presented to illustrate the relation between driving context (DC) and driver’s command to vehicle. The flow is shown with three blocks, on the left block the factors defining the driving context are shown. Driver’s intended maneuver to drive straight, left turn, right turn and u-turn can be dependent several factors. Firstly, the route from source to destination determines in which location the road structures, traffic signs and traffic signals require the driver to go straight and make turns. Next, depending on time of the day traffic density impacts the driving pattern. Further, weather can impact the driver’s visibility, road surface and hence the driving behavior. Also, dynamic alert such as road congestion, detours, behaviors of other actors such as cars, motorcyclists and pedestrians require the driver to make some run-time decision. Combination of all these factors together determine driver’s intended maneuver. Based on the intended maneuver, driver controls the steering, accelerator pedal or brake pedal of the vehicle which is shown on the right most block.

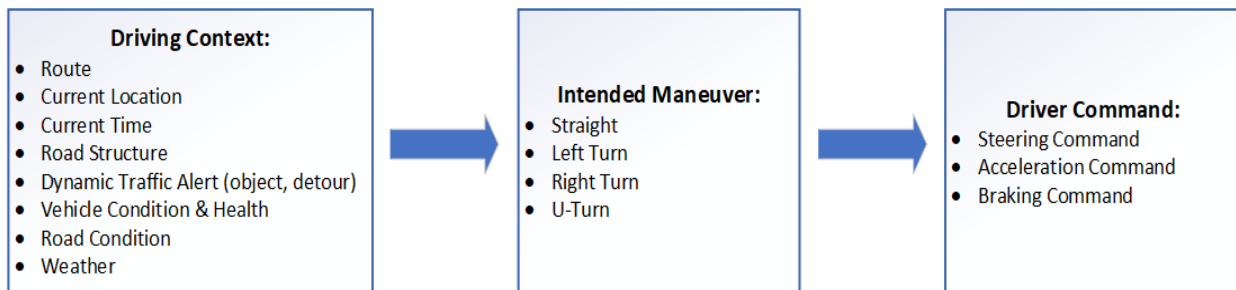


Figure 2.11: Driving Context Concept

2.6 Cybersecurity Practices in Automotive

Although cyberattacks are common in the software and IT industries [9] and there are many instances of severe business and financial loss, they are relatively new in the automotive domain. One of the early demonstrations of a publicized automotive cyber attack was in 2015 by security researchers Charlie Miller and Chris Valasek who remotely hacked a conventional car driving at 70 miles per hour [10]. In 2016, vulnerabilities were reported in remote keyless entry (RKE) for Volkswagen (VW) vehicles which was a potential attack opportunity to unlock VW vehicles [140]. In same year, Keen Security Lab demonstrated remote hijacking into brake system of a Tesla Model S vehicle which initiated major upgrade in Tesla vehicle with security mechanism [141]. With increased connectivity for cars and other IoT devices,

OTA programming for ECUs, need for charging in electric vehicle and heavy use of sensors and AI algorithms in ADAS and AV features the potential attack vectors have also increased. In [142], Sayed et. al have demonstrated impact on power grid via attack on electric vehicle. Hasrouny et al has provided a comprehensive analysis of GPS spoofing for connected vehicle in HASROUNY20177. Potential attacks on Wi-Fi, bluetooth, DSRC and cellular for V2X connectivity are shown by researchers in [143, 144, 145, 146, 147]. Recent momentum in automotive cyber security was driven by UN announcement of Reg 155 and 156 in 2020 to mandate automotive cybersecurity for vehicle type approval by 2024 and release of ISO 21434 in 2021 as guideline for automotive cybersecurity policies, framework and culture. In US, Auto-ISAC, NIST Automotive Cybersecurity Community of Interest (COI) and NHTSA vehicle cybersecurity research group are popular communities to share best practices of automotive cybersecurity across industry partners, researchers and government agencies. A wide range of critical topics including security in product development process, technical recommendation, serviceability, after market responsibility, information sharing, incident logging and reporting are discussed in these communities and published as a report [148]. In this section the literature review for automotive cybersecurity practices is presented for threat identification, protection techniques, test methods and detection systems.

Threat Identification: Threat models for the previous generation of the automotive industry are targeted for automotive E/E architecture, which are either adapted from IT and software industry (e.g., Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege (STRIDE) [149], confidentiality, integrity, and availability (CIA) [150] threat, vulnerability and risk assessment (TVRA) [151], E-safety vehicle intrusion protected applications (EVITA) [152], and healing vulnerabilities to enhance software security and safety (HEAVENS) [153] or heavily influenced by safety analysis models such as fault tree analysis, Hazard Analysis and Risk Assessment (e.g., security-aware hazard analysis and risk assessment (SAHARA)) [154]. In 2021, the ISO/SAE 21434 standard was published for Road Vehicles—Cybersecurity Engineering, which included EVITA, HEAVENS, and TVRA in recommendations for automotive threat modeling. In Fig. 2.17, steps of a threat modeling from ISO/SAE21434 standard are shown based on clause 9 (Concept) and clause 15 (TARA methods) of the standard [23] and short descriptions for each of these steps are provided in Table 2.2. It can be noted that protecting assets is the primary focus of this approach. Hence, the risk is determined based on impact scenarios and attack analysis on the assets.

Protection Techniques: Automotive cyber-protection in its current scope, primarily involves protecting the hardware and software in ECUs, communication devices and the data being exchanged inside and outside the vehicle boundary. In addition to cybersecurity prin-

Table 2.2: Expected Results of the ISO/SAE 21434 TARA Approach Based on Different Steps

ISO/SAE 21434 TARA Steps	Expected outcomes
Item definition	Item of interest, its operation environment and their interaction in context of cyber-security are defined.
Asset identification	Damage scenarios and assets with cyber-security properties that leads to potential damage if compromised are identified.
Impact rating	Impact on safety, financial, operational and privacy (S, F, O, P) of road users is assessed for damage scenarios.
Threat scenario identification	Targeted asset and cause of compromises are identified.
Attack path analysis	For each threat scenario, associated attack paths are identified.
Attack feasibility rating	Each attack path is ranked as very low or low or medium or high in terms of the effort to accomplish the attack.
Risk value determination	Risk value is determined for each threat scenario based on the related impact and associated attack feasibility.
Risk treatment decision	Risk values are assessed to determine if the risk should be avoided/reduced/shared/retained or all of them.

ciple for confidentiality, integrity and availability, also known as CIA, operational and safety aspect of the cars important consideration for vehicle cybersecurity [155]. The main pillar of the protection strategy is cryptographic methods. The cryptographic strategies: hashing algorithms, symmetric key encryption, asymmetric key encryption in combination with cryptographic accelerators, hardware trust anchor and chain of trust infrastructure [156, 157]. In [156], Sharma et al. has summarized parametric details of various cryptography techniques. Hashing a cryptography technique is typically used for data integrity and less computational and memory requirement than encryption methods. Symmetric encryption is use for confidentiality of the data and use the same key for encryption and decryption. The Advanced Encryption Standard (AES) algorithm with key length of 128 bits and 256 bits

are widely used for symmetric key encryption. Asymmetric key algorithms use a public and private key pair to encrypt the data with one and decrypt the data with another. As two different keys are involved in asymmetric method, it is considered more secure than symmetric one. However, asymmetric key cryptography requires more computational power and execution time than symmetric key cryptography. For example, one of the widely used asymmetric algorithms today were described by RivestShamirAdleman in 1977, known as RSA algorithm use larger key size of 1048 bits. In recent years, elliptical curve based cryptography (ECC) which is a newer asymmetric cryptography technique with key size of 160 bits has been offered as more efficient alternative of RSA. Other than cryptography methods hardware ports, networks and critical memory are also protected by implementing access control and firewalls techniques. In [158], El-Rewini et al. discussed cyber challenges of in-vehicle and V2X communication protocols and various approaches of countermeasures proposed by other researchers. To protect in-vehicle communication, a symmetric key encryption method was proposed by Nowdehi et. al in 2017 which was adapted for secure on-board communication (SecOC) component by AUTOSAR standard in its basic software stack (BSW) stack [159]. As automotive ethernet is becoming a popular choice for in-vehicle communication to meet the demand of large amount of data transfer, AUTOSAR standard has adapted the IEEE 802.1AE standard for ethernet with media Access Control Security (MACsec), internet protocol security (IPSec) for securing in-vehicle communication over ethernet [160]. For V2X communication various organizational bodies including NIST, IEEE, SAE and ETSI provides standards and guidelines to secure the communication over bluetooth, Wi-Fi, DSRC and cellular [161, 162, 146, 163]. As 5G cellular based communication is considered as a strong solution to support future demand of V2X communication, in [164], Chen at al. has capture a detailed review and discussion on 5G security for intra-vehicular communication. Also, ETSI ITS and IEEE 1609.2 standards recommend public key infrastructure (PKI) based cryptography approaches for V2X communication related to safety applications [165, 166]. Further, these standards recommend the ECC based digital signature algorithm (ECDSA) for authentication method to have a low computation cost and communication delay [167]. However, evaluation of PKI based solution for a secured V2X approach are still limited to testbed and simulation under limited operating condition. Real-world model and experimental assessment of V2X application for mission-critical are still an open area for research.

IDS and VSOC: Several automotive communities and researchers have considered automotive specific intrusion detection system (IDS) as a fundamental solution for vehicle cyber incidents detection and reporting which has the potential to be extended to intrusion detection and prevention system (IDPS) [168, 169, 170]. AUTOSAR (AUTomotive Open System

Architecture) organization has released a specification in 2020 for vehicle intrusion detection system that provides a standardize interface to report on-board security events for a vehicle ECU and network environment [171]. Fundamentally IDS methods in cyber space are of three types signature-based, behavior-based and anomaly-based [172, 173]. Other IDS methods are inspired by these basic methods or a combination of them. In automotive, IDS are typically software components deployed in the network, host or as a distributed system. These types of IDS in mainly focus on network parameters such as data identifier, frequency, interval, frame and entropy, bus voltage for vehicle network protocols such CAN, automotive Ethernet [174, 175, 176] and lack in utilizing the application specific knowledge. Other than IDS, anomaly detection is also used in other application of automotive. Sensor anomaly detection [177, 178], vehicle traffic anomaly detection [179, 180], in-vehicle monitoring for autonomous vehicle [181] are few of the examples. With the transformation of automotive to connected cars and requirement of monitoring and logging security incident for automotive cybersecurity type approval by UN regulation R155 and R156, automotive industry has realized the need of vehicle security operations center (VSOC), a concept adapted from IT security operations center and tailored to protect the CAV from emerging threats [182]. The VSOC architecture can be viewed as a combination of four components, sensors to collect data from vehicle and traffic infrastructure, a log management component to process, normalize and prioritize these data, a correlation engine for analyzing the events using the cyber attack information detected by anomalies and alert information from Information and communication technology (ICT) devices, and a response system to take action when security incidents are detected [183]. At current stage several industry partners of automotive have proposed VSOC solution however it is still at very early stage of supporting full-scale of V2X [184, 185, 186].

2.7 ML Review

ML is considered a subbranch of artificial intelligence (AI). In recent years, several market research groups published reports that show the global market of ML is growing rapidly in many applications including automotive, transportation and security [187, 188]. In 1956 by John McCarthy, who was an MIT computer scientist coined the term “Artificial Intelligence” at a workshop at Dartmouth College [189]. In general, AI involves advanced computing techniques that aims to mimic various cognitive functions like human. In 1959, the term ML was first coined by Arthur Samuel, an eminent researcher of AI from IBM [189]. Unlike other knowledge-based or rule-based and symbolic approaches of AI methods, the focus of ML is to replace the explicit programming with automatic learning ability of the computer from the

provided dataset [190]. The recent surge in ML research and application can be attributed to two primary factors. One of them is the ability to create and store large datasets digitally. The other important enabler is the availability of affordable high-computing device to process these large datasets. Such dataset are typically created for specific applications such as forecasting, recognition, recommender, and language processing [191]. At a high-level, ML algorithms are categorized as supervised, unsupervised, semi-supervised and reinforcement learning based on the learning method [189]. For supervised learning methods, dataset is prepared with various pairs of inputs (or features) and the outputs (or labels) for the target system. These training pairs are then provided to the ML algorithm to produce a trained model that can predict the output for new inputs. Supervised learning methods are further divided into classification and regression methods to solve two different categories of problems. Classification method predicts the output from labeled discrete classes. Spam classification from email, image classification to detect cancerous cell, object detection on roads for AV are some examples of classifiers [191, 192]. On the other hand, regression methods predict the output as continuous value from the input. Weather prediction, financial forecasting, and drug response modeling are few examples prediction using regression methods [191]. Unsupervised learning methods do not have any directly associated response variables for the given set of features, rather the goal is to explore if there are some patterns and have an insight of the system from the given dataset [193]. Semi-supervised learning method is a hybrid approach where model is typically trained with a small set of labeled data and large set of unlabeled data. Semi-supervised learning method is applications like image and speech analysis, fraud detection in banking and insurance claims [191]. Reinforcement learning method use the concept of software agent and environment [191]. The software agent observes the state of environment and determines the reward or penalty when it executes an action. Using these inputs, the reinforcement learning algorithm updates the policy for the next action. Reinforcement learning is considered a powerful AI tool to automate and optimize efficiency of operation in many applications such as supply chain logistics, manufacturing, and autonomous driving. The working principles of these four types of ML methods are founded with mathematics and statistics. However, a different approach known as artificial neural network (ANN) introduced a paradigm shift in ML. Instead of using only computational methods, ANN uses the concept of connectionism inspired by the neurons in human brain for cognitive ability [194]. Foundation of ANN can be traced back to perceptron, a model proposed in 1950s and 1960s with very few layers for simple pattern classification and regression tasks. Early ANN models were not effective to capture nonlinear relationships from features and could not solve real-world problems with complex data. The modern era of ANN started during 1980s and 1990s, when multilayer

perceptron (MLP) and the backpropagation algorithm boosted the ANN with ability to deduce linear and nonlinear relations. As depicted in Fig. 2.12, ANN structure consists of an input layer, an output layer and one or multiple hidden layers with node(s). The nodes in

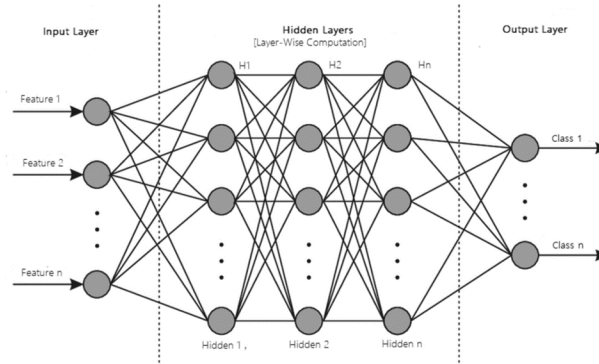


Figure 2.12: ANN Generic Architecture [191]

input layer represent features (inputs) and have connections to target nodes in hidden layer. Each connection is assigned with a value known as weight to indicate the importance of the feature to the target node. Each target node is configured with a bias to add adaptability and it combines all the weighted inputs and the bias as an input to activation function. The value of the activation function determines the node is considered active or dormant in the network. This process repeats for each hidden layers and finally ends at output layer with predictions. This is called forward propagation. In Fig. 2.13, four most common activation functions used in ANN are shown. It can be noted, that linear function is typically used for

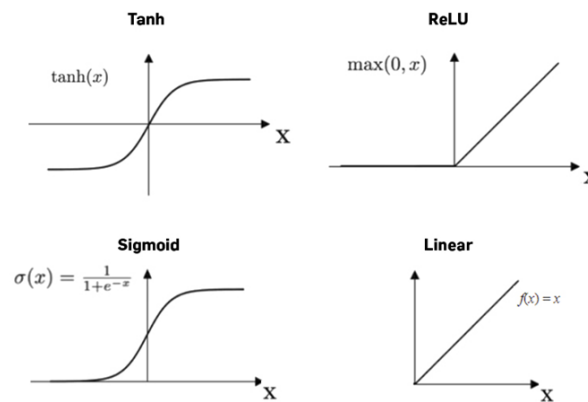


Figure 2.13: Common Activation Function in ANN [195]

simple linear regression model whereas sigmoid, tanh and ReLU introduce non-linearity to neural network [196, 197]. However, there are some key differences between them. Sigmoid

function normalize the output between 0 and 1, tanh function normalize the output between -1 and 1. Both of these functions have saturation problem when output reaches to minimum and maximum value which cause the gradient to vanish and adversely effect the learning process. ReLu function has no saturation for any positive value and computationally more efficient than sigmoid and tanh. It should be noted that the activation function for output layer depends on the type of prediction is expected from the trained model. The other significant milestone in ANN is back propagation techniques such as calculating loss and gradient descent enabled ANN to evaluate the accuracy of the result and improve the predictions for future epochs. The backpropagation technique also paved the path for deep neural network (DNN) and deep learning (DL) method which are used to learn from high-dimensional data. In early 1990s, Yann LeCun suggested a new architecture named LeNet-5 which applied convolutional layer and achieved 99% accuracy for a well-known computer vision problem called MNIST digit classification to classify handwritten digits from 0 to 9 [198]. This motivated the scientific community to propose several convolutional neural networks (CNN) to address more challenging visual recognition problem from real world. AlexNet, RCNN, VGG are some of important CNN models that are used to address various computer vision problem including semantic segmentation and object detection for AVs [199, 200, 201]. As shown in Fig. 2.14, input layer, convolution layer, pooling layer and fully connected layer and output layer are basic components of a generic CNN architecture [191]. The input layer

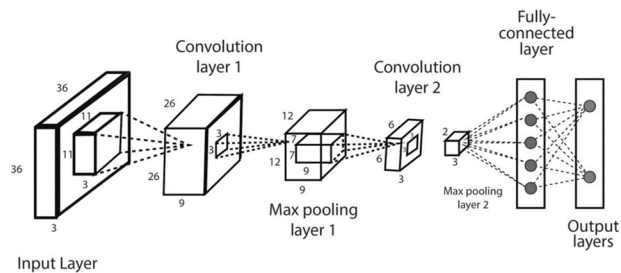


Figure 2.14: CNN Generic Architecture [191]

receives the raw input such as an image and then convolution layer(s) applies kernel (or filters) sliding over the input image to create feature maps for the entire image. Pooling layer typically applies average pooling or max pooling method to reduce the size of the image for faster and memory efficient computation while ensuring important features of the image are maintained. Output of pooling layer is passed to fully connected layer in vector format where a linear transformation is added with a weighted matrix followed by a non-linear transformation using the activation function. In the output layer, a logistic functions like sigmoid or softmax is applied to obtain the probability distribution score of output clas-

sification [197, 199]. While CNN architectures primarily focus on spatial structure of the data, another variant of neural network called, recurrent neural network (RNN) was created to learn from sequential data [202]. In 1980s RNN became useful architecture for speech recognition, natural language processing, financial forecasting. However, when RNN-based models get trained to learn long-range dependencies in a sequence with gradient descent optimization method, the gradient can become significantly small and not effective. This is known as “vanishing gradient” problem. In 1997, Hochreiter and Schmidhuber invented a special type of RNN known as long short-term memory (or LSTM) that solved the vanishing gradient problem of RNN [203]. To overcome limitations of RNN, the LSTM model introduced a special memory unit to learn long-term dependencies in sequential data. LSTM also features forward and backward direction during training. In Fig. 2.15, an architecture for a typical vanilla LSTM block is presented. As shown in this diagram, a LSTM unit

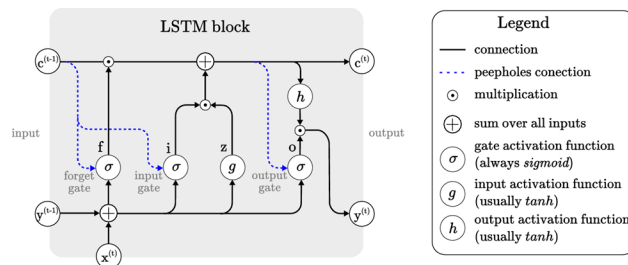


Figure 2.15: LSTM Vanilla Architecture [203]

consists of a cell, an input gate, a forget gate and an output gate. The cell in LSTM was introduced to store the values over time intervals. The forget gate takes the input x^t at current iteration and hidden states from the previous iteration y^{t-1} sometimes represented by h^{t-1} to determine which information from previous cell state c^{t-1} to retain or discard. To achieve this, a sigmoid function is applied as forget gate activation function on x^t and y^{t-1} with a weight matrix and bias. The output f^t is a vector with values between 0 and 1 which is then multiplied with c^{t-1} . The input gate has two main functions, input gate activation and candidate memory cell creation. At input gate the input x^t and y^{t-1} are passed to a sigmoid function where an input gate weight matrix and input gate bias are applied to produce modulated input i^t . For candidate memory cell \bar{c}^t creation, an activation function (typically hyperbolic tangent function, tanh) is applied on x^t and y^{t-1} with a candidate cell state specific weight matrix and bias. The final new cell state c^t is created by combining the dot product of i^t and \bar{c}^t with the dot product f^t and c^{t-1} . The output gate of LSTM block decides which hidden states to provide as output. Output gate also applies a sigmoid function with output gate specific weight matrix and bias on x^t and y^{t-1} and produce values between 0 and 1 o^t . Finally, the new hidden states y^t is derived by the dot-product of o^t and

modulated cell state c^t with tanh activation function. Since 2007, LSTM became popular as it demonstrated higher performance than other RNNs for various application with complex sequential data including speech recognition, machine translation, language modeling, stock pricing and weather forecasting. For real world application generally LSTM layer needs to be combined with an input layer at the beginning, an output layer at the end and variant of other layers such as activation layers, normalization layers, dropout layers, fully connected layers [204, 199, 205]. It should be noted, that DL techniques are still evolving in research and there are new models being proposed and evaluated by AI and ML community [206].

- Naive Bayes: Use Bay's theorem to calculate the probability of each class for a given value of feature. It assumes each feature is independent from each other.
- Decision Tree: This is a top-down approach which starts with the root at top and use the concept of entropy and information gain or Gini impurity index at each decision node to split out into smaller subsets of data and feature to form sub-nodes and branches. The final prediction or classification is made at terminal nodes, also known as leaf nodes.
- SVM: SVM starts by mapping the input data into high-dimensional feature space to make datapoints separable. The transformation function is known as kernel and can be liner or non-linear depending on the dataset. After applying kernel, boundary is defined by the support vectors for the datapoints. While training, SVM tries to maximize the distance (or margin) between decision boundary and the nearest support vectors to have a generalized decision boundary (or hyperplane).
- KNN: KNN use Euclidean distance function to create new datapoints based on similarity measures. A simple majority vote of k nearest neighbors of each point classifies the data.

2.8 Cyber-physical Challenges of AV and ToD

In Fig. 2.16, a report published by Upstream in 2021 is presented which breaks down the top attack vectors for automotive applications from 2010 to 2020 [2]. It can be noted from this figure that attack vectors for modern vehicles has a dense attack surface that stretches beyond the attacks on the in-vehicle network and ECUs. The attack surface extends to communication between vehicle to cloud, keyfob, blue and wi-fi connection to personal portable devices such as phone, laptop, connected vehicle software applications and various sensors in and around the vehicle. Cyber-physical attacks are special types of security breach that im-

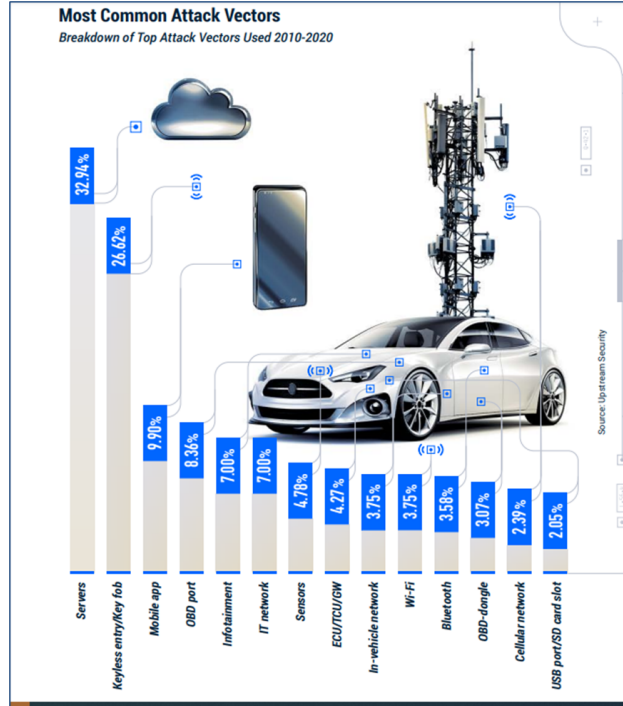


Figure 2.16: Automotive Attack Vectors 2010-2020 [2]

pacts beyond traditional cyber space domain IT environment [207]. These types of attack can target any components of a cyber-physical system which typically consists of operating interface, compute environment, network and the physical processes to sense and actuate. Unlike conventional cars, AVs are highly dependent on perception sensors, localization sensors, AI-based algorithms, and vehicle-to-everything (V2X) communication for driving capability without a driver [11, 12]. All of these areas affect the attack surface, software vulnerabilities, and the severity of the impact. In [13], researchers were successful in manipulating Tesla’s autopilot system by using split-second light projections on roads. Sensor jamming, blinding, spoofing, distributed denial-of-service (DDoS) attacks, manipulation of communication devices, and adversarial ML techniques on AI-driven algorithms are some of these attack methods demonstrated by researchers in this area [14, 15, 16, 17, 18, 19]. These kinds of cyber-physical attacks are specifically targeted, posing potential threats to AVs and objects in ODD. As AVs are still in the early stages of delivering base functionality and real-life testing, cyber-physical threats to AVs are slowly emerging. However, with more AVs, on the road in the future, threats will also increase and can compromise safety of passenger and other road users, cause damage to property, disrupt mobility service and destroy the trust on AVs.

AV Perception: A typical architecture of an ADS includes *perception* to detect and rec-

ognize traffic signs, objects, and other road users in its ODD, *localization* to determine its position in an environment, *planning* to handle the mission, trajectory, and motion, and *decision making* to take an intelligent, safe, and optimal decision in complicated and dynamic driving scenarios [208, 209, 210]. In the AV perception domain, there are primarily four sensor technologies that are included camera, radar, Lidar, and ultrasonic [211]. For many years, radar, camera, and ultrasonic sensors have been used in automobiles for advanced driver assistance system (ADAS) while Lidar has gained recent attention from the AV community because of its 3D mapping capability of the scene. Several studies on the advantages and disadvantages of these sensors show that radar is a good choice for distance and velocity measurement of moving objects even in adverse weather conditions, but it has poor static object detection and cannot classify the objects. Also, ultrasonic sensors detect only the objects within a short range and cannot classify the objects [212]. For optics-based sensors, the camera captures the image with the necessary visual details to classify and recognize them, but the accuracy of distance and speed measurement is challenging [212]. Lidar is suitable for 3D mapping of the scene and can detect lanes by measuring intensity variation, but the classification process via Lidar is poor in comparison with that of a camera. Also, Lidar cannot interpret the detailed visual information from traffic signs [212, 213]. Both Lidar and the camera’s performances are limited by the weather conditions, visibility, occlusion, and reflectivity of objects. It can be represented that multi-modal sensor technology may be a realistic solution for an AV application, keeping the camera as a primary sensor for classification and recognition by advanced ML algorithms that traffic sign recognition (TSR) can be another algorithm for recognizing the traffic signs [214, 213, 215]. Table 2.3 summarizes some of the recent research in vision-based perception with advanced ML algorithms for an AV application. With significant advancements in computation power, neural network-based ML algorithms are showing promising results to address the challenges of vision-based AV perception to detect objects, pedestrians, lanes, traffic lights, and traffic signs on and around drivable roads.

An advanced deep learning system, incorporating a faster region-based CNN (R-CNN), has been created in [216] to detect and classify on-road obstacles. To ensure its efficiency in AVs driving on highways, it was tested to deliver at least 10 frames/second with VGA resolution images. The operation of the system was unaffected by the form and viewpoint of the objects, as well as variations in illumination and environmental circumstances. In contrast to classifier-based methods, YOLO considers object detection as a prediction problem and trains on a loss function that correlates directly to detection performance with the overall model trained. Compared to other detection approaches (e.g., deformable parts model (DPM) and R-CNN), scholars in [217] demonstrated better performance when extrapolating

Table 2.3: A Literature Survey on ML Algorithms for an AV Perception System

Author	AV perception type	ML algorithm	Contributions
Prabhakar <i>et al.</i> [216]	Obstacle detection and classification	Region-based convolutional neural network (R-CNN)	A deep learning system using a faster R-CNN trained with PASCAL VOC image dataset is developed for the detection and classification of on-road obstacles (e.g., vehicles, pedestrians, and animals). At least 10 frames per second for a VGA resolution image frame using a Titan X GPU demonstrated the suitability of the system for highway driving of AVs. The detection and classification results on images from KITTI and iRoads, and also Indian roads showed the performance of the system invariant to object's shape and view, and different lighting and climatic conditions.
Redmon <i>et al.</i> [217]	Object detection	YOLO	YOLO can be trained directly on full images. Unlike classifier-based approaches, YOLO frames object detection as a regression problem and is trained on a loss function that directly corresponds to detection performance, and the entire model is trained jointly. It outperforms other detection methods, including DPM and R-CNN, when generalizing from natural images to other domains (e.g., artwork).
Li <i>et al.</i> [218]	Structural Prediction and Lane Detection in Traffic Scene	CNN, RNN	A multi-task deep CNN is developed to detect the presence of the object and geometric attributes (location and orientation) simultaneously with respect to the region of interest (ROI). In the second approach, an RNN is used its internal status memory to infer the presence/absence of a lane over a sequence of image areas.
Raturaj <i>et al.</i> [219]	Traffic Light Detection and Recognition	Faster R-CNN Inception-V2 model via transfer learning	A DNN-based model for reliable detection and recognition of traffic lights in realtime was proposed.
Wang <i>et al.</i> [220]	Pedestrian detection	Repulsion loss with Fast R-CNN	A robust detection for pedestrians in a populated area outperformed all the state-of-the-art methods on both CityPerson and Caltech benchmarks.
Lin <i>et al.</i> [221]	TSR	CNN	Since the nature of TSR is the collection and image processing to capture deep visual features from images, a CNN is used to extract important frames from images. Convolutional layers capture features, and then these are utilized for training an SVM classifier.

from realistic images to other contexts. To concurrently identify the presence of objects and their geometric properties, a multi-task deep CNN was developed in [218]. Then, the authors used the recurrent neural network (RNN) algorithm for inferring the presence or absence of a lane over a set of image regions. Additionally, a model using deep neural networks (DNNs) was proposed for accurate, real-time traffic light recognition and detection. To do this, a CNN was utilized to extract important frames from images, and the resulting system outperformed state-of-the-art algorithms on a variety of benchmarks for pedestrians detection in densely populated areas. In another study, support vector machine (SVM) classifiers were trained using feature acquisition performed by convolutional layers [219, 220, 221]. However, these AI-based algorithms do not guarantee the desired levels of performance and safety in all scenarios [222, 223]. These limitations can produce undesired outcomes when new abnormal or adversarial scenarios occur in run-time during autonomous driving [224].

The scholars employed the German Traffic Sign Recognition Benchmarks (GTSRB) dataset to train their prediction method on a subset of 43 classes; this strategy involved an integrated implementation of an artificial neural network (ANN) and histograms of oriented gradients (HOG) and achieved an accuracy of 80% [225]. Min *et al.* [226] suggested using an LW-RefineNet to divide the scene and acquire the details concerning the spatial positioning at the pixel level. After that, the constraint model was developed to define the search regions. Experiments have demonstrated that this strategy reduces the likelihood of incorrectly detecting small traffic signs. Nevertheless, it has limitations in situations where detection is inefficient on both sides of the roadway or in other situations (e.g., intersections). Zhan *et al.* [227] introduced multi-headed self-attention YOLOv3 (MSA-YOLOv3), which is using mix up visual enhancements and incorporated a multi-scale spatial pyramid pooling component to acquire deeper features, and address the challenges of high-precision real-time classification of road signs in naturalistic environments.

Cyber-physical attack on AV perception: As explained in the previous section, an AV perception system has cyber-physical properties. Comprising these cyber-physical properties can cause potential hazards to automated driving. These attacks can be divided into two categories. First, attacks are purely physical and relatively simple to change the objects and traffic signs in ODD. Latter, those that are artificially created adversarial attacks where the targets are perception sensors and AI-based algorithms for AV perception systems and usually look normal to human eyes. This section investigates the challenges that AVs have while interacting with traffic signs and other objects (e.g., pedestrians, vehicles, and animals) on the road that are subjected to adversarial activities. These adversarial attacks may be generated, then put in any landscape, and then applied to image classifiers afterward. They cause the classification process to ignore the other items in the scene and merely re-

port the category that they are trying to identify. These intrusive activities might not seem like a problem for people to deal with under normal circumstances; nevertheless, this is a potentially catastrophic obstacle for AVs. The challenge of effectively creating an accurate TSR system is complicated since the system must be trained to detect traffic signs that are partially obstructed by objects, in bad conditions resulting in insufficient maintenance, and barely visible in severe weather circumstances. There is a variety of factors that can contribute to anomalies, including the climate, environment, visibility, and location [228]. Research in this area shows digital/pixel perturbation on traffic signs, point-wise perturbation on object classification algorithm, poster-printing attack with I-FGSM, C&W, Deepfool, JSMA [229, 230] attackers can exploit the vulnerabilities in AV algorithms to attack the system.

Threat Modeling for CPS: Other industries (e.g., mining, power grid, shipping, and aviation) have studied a system-theoretic approach of threat modeling for analyzing the security of CPSs [231, 232, 233, 234]. This approach focuses on the mission of the control system or process and functional model instead of being focused on assets. It guides to analyze the system and technical interactions as well as, non-technical interactions (e.g., human, social) rather than being focused on component failure merely. However, these methods were not designed for AV-specific TARA. In [235], Chattopadhyay *et al.* have argued that the current AV security is poorly understood and presented security by framework design to analyze the security of AVs as a CPS with a systems engineering approach. Also, the authors have conducted a few experiments to fail AV’s missions. They were performed by manipulating tire pressure and sensor data, creating a software update attack on the infotainment system to maliciously update the weight and labels of the object detection algorithm, and introducing a DoS attack for AVs. In [236], Khatun *et al.* presented a scenario-based threat modeling and assessment for over-the-air updates for an AV. For risk assessment metrics specific to AVs, Li *et al.* studied various methods and classified them into time-based, kinematics-based, statistics-based, potential-based, and unexpected driving behavior-based metrics [237]. Some researchers have analyzed automotive security threats as a physical system. In [238], Guo *et al.* have shown a physics-driven approach to map DoS, replay, and deception attacks to model the predictive control-based system that optimizes the instantaneous driving velocity and torque allocation to reduce energy consumption. One of the new approaches to evaluate the security of complex CPSs is STPA-Sec. Unlike conventional threat models that originated from the IT domain, the STPA-Sec process is a system theory-based approach. It is an extension of STPA that is tailored to include security analysis.

Cyberphysical Challenges of ToD for road vehicles: Connected services offered in modern vehicles typically include cabin pre-heating, vehicle locator, mileage report, battery

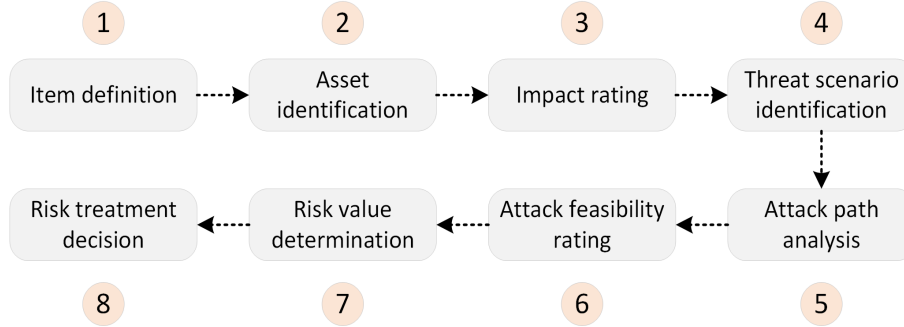


Figure 2.17: TARA Steps of ISO/SAE 21434 Standard

health status monitoring and some other functions. In general, these services do not control the driving in real-time. Unlike these services, ToD for road vehicles depends on V2I connectivity to remotely control the motion of a vehicle. Porting the driving task from in-vehicle, closed environment to external world using wi-fi or cellular network makes the driving service and experience heavily dependent on quality of service (QoS) of the communication channel. Further, QoS of such network is susceptible to various challenges including electromagnetic disturbance, latency and jitters in communication network, channel availability. As of today, a standard for QoS of communication channel required for safe and comfortable ToD on public road is not established yet. However, in [239], authors have conducted some experiments to provide an initial requirement of an up-link of 3 MBit/s, a down-link of 0.25 MBit/s, network latency of 250 ms, and a jitter less than 150 ms while performing DDT for safe ToD operation. To mitigate such challenges unmanned vehicles for military applications use military grade communication. For an example, military UAVs are operated using ultra-high frequency military-grade air-to-ground communications and direct data links and satellites are used for modulation schemes for different ranges [240]. However, using such technologies is not feasible for ToD of road vehicles. This is due to the number of vehicles on public roads expected to use connected services at a particular time are significantly higher as compare to military applications [125]. It can be noted that in case of military ground vehicle, the mission typically involves some type of tactical mission [241] where as for teleoperated road vehicles, the mission is to provide safe and convenient transportation [5]. Unlike a remotely operated military vehicles in a battle zone, ODD for road vehicles involves public roads with civilians and public property. Though information on cyberattack on military vehicle is not available publicly, a recent article published in October, 2013 from University of South Australia claims that an algorithm has been developed by Australian researchers that can intercept a man-in-the-middle (MitM) cyberattack on an unmanned military robot [242]. ToD communication is a type of V2X communication an in section 2.6 it was reviewed that

real-world model and experiments are not studied in detailed for security of mission-critical application with V2X connectivity. Hence, security aspect of V2X for ToD application to be rigorously studied. It should be noted that for ToD, vehicle control command is transmitted outside vehicle's physical space. Hence, an asymmetric key cryptography approach may be preferred over symmetric key cryptography. Further, asymmetric cryptography methods including PKI-based approach need to be evaluated for computation and communication overhead in a real-world model of connected car ecosystem.

2.9 Anomaly Detection in CPS

In science, anomaly is described when there is a difference between actual observation and expected outcome developed based on the original scientific idea [243]. In statistics and data mining field, outliers in the data set are considered as anomaly. Presently AD is used in various industries including information theory, finance, manufacturing, health monitoring and medical device, fraud detection, IoT security and many others. For physical systems, detecting anomalies in AV sensors, aerial systems, smart grids and intelligent traffic systems are examples of some important applications. AD for IDS was introduced in 1980s to detect security violations by recognizing abnormal patterns in system logs [244]. In Table 2.4 recent research work on cyber-physical attack detection with AD are reviewed. It can be noted from Table X, that current AD techniques for automotive IDS primarily focus on finding anomalies based on a data-driven analysis of network and less consideration on physical behavior of the vehicle. However Table 2.4 shows that, research on other CPS systems found that for detecting cyber-physical attacks, hybrid approaches by combining data-driven model and physics-based model have some benefits.

Table 2.4: A Literature Survey on Anomaly Detection in CPS

Author	Method	Application	Contributions
Rahul <i>et al.</i> [245]	Physics Guided ML Techniques	cyber-physical systems in general	<ol style="list-style-type: none"> 1.classified the hybrid models into physics-based preprocessing, physics-based network architectures, physics-based regularization, and miscellaneous categories based on the way the Model-based is brought into the hybrid architecture. 2. proposed five metrics for all-round performance evaluation of a hybrid CPS model.
Cody <i>et al.</i> [246]	Hybrid physics model-based data-driven framework	Smart grid real-time monitoring	<ol style="list-style-type: none"> 1. Presented hybrid framework with physics-based and data-driven ECD algorithm. 2. Tested the result on IEEE 118-bus system which shows 6.75% improvement from physic-based solution.
Faris <i>et al.</i> [247]	Statistical Learning and Kinematic Model	Adaptive cruise control for autonomous vehicle	<ol style="list-style-type: none"> 1. Propose Generalized Extreme Studentized Deviate with Sliding Chunks (GESD-SC) approach, which is applied at each vehicle in the platoon to detect anomalies in real-time based on the vehicle’s own speeding decisions.
Jie <i>et al.</i> [248]	Spatio-temporal correlation based long short-term memory (LSTM) method	Unmanned Aerial Vehicle	Proposed a STC-LSTM and shown this method can accurately locate the anomalies of UAV flight data and provide high-precision recovery prediction values.
Bin <i>et al.</i> [249]	Physics-based Neural Networks	Power System	Several paradigms of PINN (e.g., PI loss function, PI initialization, PI design of architecture, and hybrid physics-DL models) are summarized

Table 2.5: Parametric Variations of SAE J3016 Automation Level

SAE J3016 Automation Level						
Parameters	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Automation	None	Driver-assistance	Partial	Conditional	High	Full
ODD perception	Frontal coverage	Coverage in front, rear and four corners of the vehicle	Same as L1	Increase in corner coverage from L1, L2 Nearby surround view coverage	Increase in surround view like human driver is recommended	Similar to L4
ODD connectivity	Not required	Not required	Not required	Not required	Connectivity is recommended to communicate with V2X	Increase in connectivity from L4 to connect from remote areas
DDT scope of DAS	None	Longitudinal or lateral control at a time (sustained basis)	Longitudinal and lateral control at the same time (sustained basis)	Complete DDT (OEDR+ tactical+ operational)	Complete DDT (OEDR+ tactical+ operational)	Complete DDT (OEDR+tactical+ operational)
DDT fallback	Driver	Driver	Driver	Driver	DAS	DAS
Monitor DDT performance system failure	N/A	Driver	Driver	Driver	DAS	DAS
Monitor DAS performance	N/A	Driver	Driver	DAS	DAS	DAS
Minimal risk condition	N/A	N/A	N/A	Not mandatory, user decides final action	must	must
Failure mitigation	N/A	N/A	N/A	Recommended	Recommended	Recommended
Misuse or abuse	N/A	No significant evidence	Important	Important	N/A	N/A
Response to user request	N/A	N/A	N/A	Relinquish DDT upon request by DDT fallback-ready user	ADS may delay relinquishing DDT for performance or hazard prevention	ADS may delay relinquishing DDT for performance or hazard prevention
Standards regulations	ISO 26262 UNECE-WP.29	ISO 26262 ISO/ SAE 21434 UNECE WP.29	ISO 26262 ISO/ SAE 21434 UNECE WP.29	ISO 26262 ISO/ SAE 21434 ISO/PAS 21448 UN Reg 157 UNECE WP.29	ISO 26262 ISO/ SAE 21434 ISO/PAS 21448 UN Reg 157 UNECE WP.29	ISO 26262 ISO/ SAE 21434 ISO/PAS 21448 UN Reg 157 UNECE WP.29
Functional system architecture	Distributed [250]	Domain-centric [250]	Domain-centric [250]	Domain-centric [250]	Centralized [250]	Centralized [250]
DDT sensors (#)	Radar (1) [251],[252],[253]	RADAR (1-3) SONAR (1-12) Camera (1-2) IMU (1) [251],[252],[253], [254]	RADAR (3-5) SONAR (up to 17) Camera (2-6) IMU (1) GNSS/GPS (1) [251],[252],[253], [254]	RADAR (8) SONAR (up to 12) Camera (6-20) Lidar (1-5) IMU (i1) GNSS/GPS (i1) [251],[252],[253], [254],[82]	RADAR (8) SONAR (up to 12) Camera (6-20) Lidar (1-5) IMU (i1) GNSS/GPS (i1) [251],[252],[253], [254],[82]	RADAR (8) SONAR (up to 12) Camera (6-20) Lidar (1-5) IMU (i1) GNSS/GPS (i1) [251],[252],[253], [254],[82]
Connector bandwidth	1 MB [80]	1 GB [80]	1 GB [80]	6 GB - 12 GB [80]	6 GB - 12 GB [80]	6 GB - 12 GB [80]
Data generation (per day)	N/A	0.3 TB [77]	0.3 TB [77]	5 TB - 32 TB [82],[77],[76]	5 TB - 32 TB [82],[77],[76]	5 TB - 32 TB [82],[77],[76]
Data storage technology	SLC NAND e.MMC UFS [78]	SLC NAND e.MMC UFS [78]	SLC NAND e.MMC UFS [78]	e.MMC UFS Embedded SSD [78]	e.MMC UFS Embedded SSD [78]	e.MMC UFS Embedded SSD [78],[255]
Vehicle to cloud data (per hour)	N/A	10 GB	25 GB [256]	300 GB	400 GB	500 GB [256]
AI processor throughput (Trillion operations per second)	N/A	1	2 [257]	24 [257]	320 [257]	4000+ [257]
RAM bandwidth	500 MB/s [258]	60 GB/s [258]	60 GB/s [258]	512 - 1024 GB/s [258]	512 - 1024 GB/s [258]	1024 GB/s [258]
Lines of code	10 million [259]	100 millions [259]	100 million [259]	300 - 500 million [259]	300 - 500 million [259]	300 - 500 million [259]
AI compute energy (% total energy consumed in car)	N/A	1-4% [260]	1-4% [260]	13%-20% [261] [262]	40%	40%-50%

CHAPTER 3

Threat Modeling of Automated and Teleoperated Vehicles

In previous chapter 2, current practices in automotive cybersecurity are discussed in section 2.6 which highlights the importance of threat identification in automotive cybersecurity framework. A threat modeling, also referred to as TARA model, is generally viewed as the starting point for designing a cyber-secure system. Further, in section 2.8, emerging cyber-physical challenges in automotive because of various elements of AV and teleoperated technology including sensor, AI/ML algorithms, cyber-physical interaction, and connectivity are discussed in detail. Due to lack of AV and ToD specific threat analysis available in research, threat analysis that specifically focus on AV and ToD system are performed as part of this dissertation. This threat modeling work is presented in this chapter in two parts. In section 3.1 a thorough analysis of threats to AV perception system is conducted which resulted in proposing a novel threat modeling approach for such system. In section 3.2, the threat modeling of ToD system for road vehicle is performed. The result from ToD threat analysis is an important step that motivated this research to propose a novel anomaly detection approach for ToD system that uses context awareness and knowledge of vehicle physical parameters. This anomaly detection method is presented in chapter 4 and experiments with a LMD case study with this method is discussed in chapter 5.

3.1 Threat Modeling for AV Perception System

In 2021, ISO/SAE 21434 standard was published that provides a threat analysis and risk assessment (TARA) guideline for E/E systems within road vehicles. Most of these threat modeling approaches have the foundation of IT-based threat models with some modifications relevant to E/E systems. However, an ADS has a different kind of operating environment and requires a stricter real-time response to changes in that environment than devices in an

IT environment. Moreover, ADS requires more cyber-physical interactions with the environment, higher software complexity, and real-time decision-making abilities than a conventional vehicle. Following an inappropriate method may provide incorrect metrics of cyber-assurance and cause safety hazards or disruption of mobility services in reality. Hence, it is critical to analyze the effectiveness of these threat models for AV cyber-physical attacks with a holistic approach.

3.1.1 Assumptions and Scope

- This study is focused on the camera as an AV perception sensor.
- Perception algorithms are assumed to be AI-based, and the main focus is on the theoretical framework, mathematical model with a preliminary example for an AV perception system.
- TARA model is for object classification functionally of an AV perception system.
- The values shown in impact rating, attack feasibility rating, and risk mitigation factor are used as examples to demonstrate a comparison between TARA and integrated threat modeling approaches. In some cases, these values are based on preliminary guidance from ISO/SAE 21434 [23] and in other cases, they are merely a suggestion and may vary depending on various factors (e.g., the applications, organizational needs, and cyber-security goals).

3.1.2 Problem Formulation

Safe autonomous driving requires appropriate real-time detection and classification of the objects in ODD. Hence, the OC algorithm is chosen for this comparative analysis of threat models for AV perception systems. Based on a detailed literature study, two threat modeling methods were down-selected to evaluate their effectiveness for AV perception systems. The first method is the ISO/SAE 21434 standard, which is used in vehicle cybersecurity. The second method is STPA-Sec, which focuses on missions and system interactions, both internal and external. As the AV perception environment is highly dynamic, these properties of STPA-Sec make it a potential choice for this study. Hence, the problem is formulated:

- With object classification functionally of AV perception system and its impact on cyber-physical interaction of AV in its ODD.

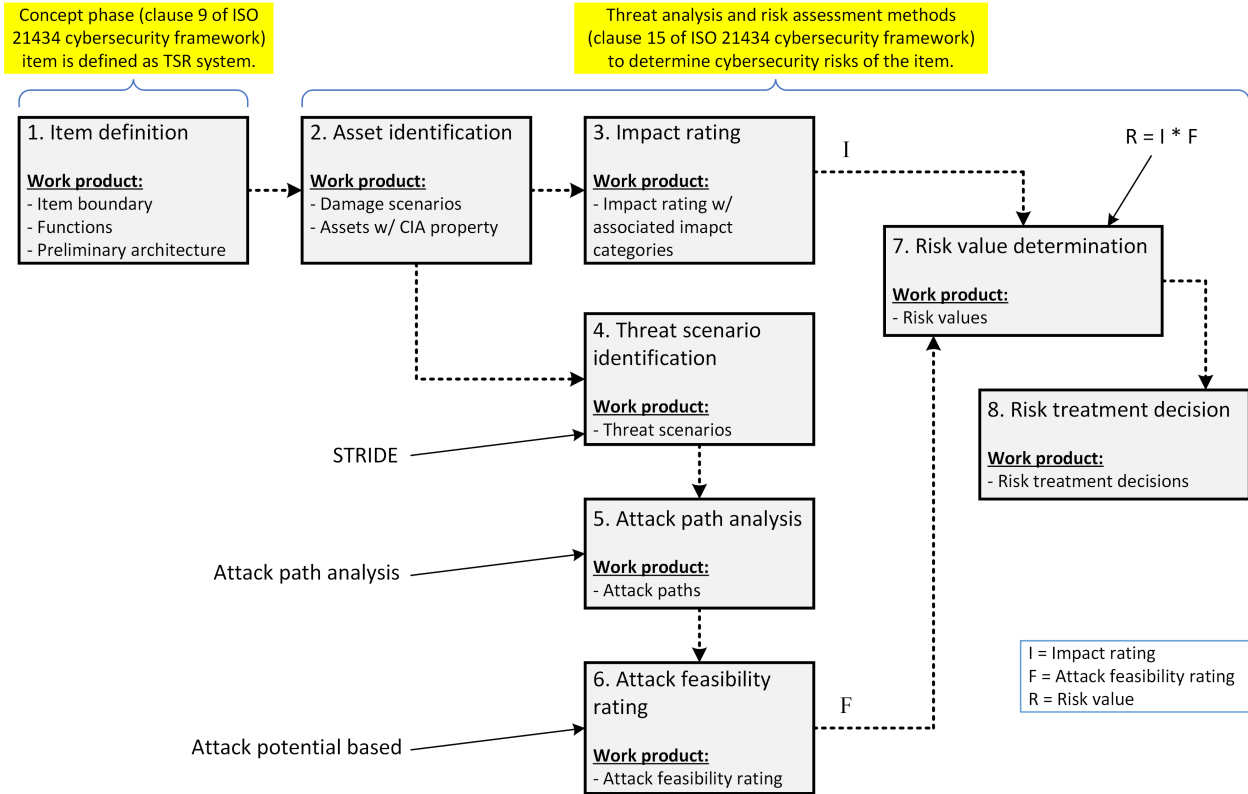


Figure 3.1: A Detailed Representation of ISO/SAE 21434 TARA Steps Considering the Work Products

- Next, the logical architecture of typical ADS is adapted for service-oriented architecture and AUTOSAR.
- A comparative study is performed between traditional threat modeling approaches using ISO/SAE 21434 guidelines and systems theory-based STPA-Sec for ML applications.

3.1.3 ISO/SAE 21434 Approach

The guidelines provided in the example of ISO/SAE 21434 - *Annex H* is used for this case study. Fig. 3.1 shows the specific methods used in various steps of the ISO/SAE 21434 approach.

3.1.3.1 Item Definition

Item boundary: OC is an important subsystem of a vision-based object detection/recognition system for automated driving functions. In Fig. 3.2, a conceptual block diagram is

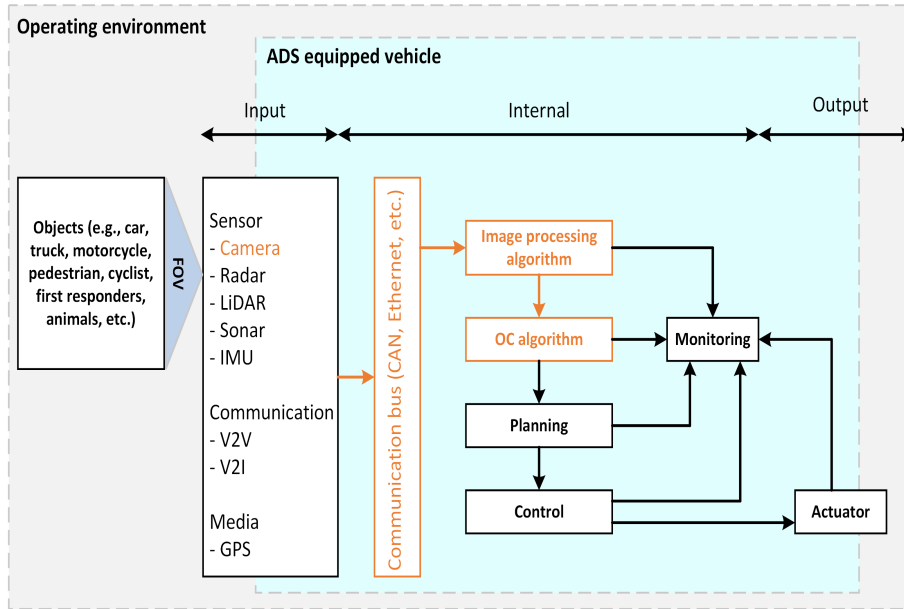


Figure 3.2: An OC Concept Level Block Diagram with Different Objects

shown for OC process as a part of ADS and examples of scenes with off-nominal situations.

Item functions: The purpose of an OC subsystem is to classify the objects that are detected on and near a drivable road by the cameras mounted in an AV. The input of the OC system is image data after image processing. Object detection and bounding box estimation tasks are performed on the image captured by the vehicle’s camera. The output of the OC system can provide useful information about the objects in an ROI to assist the driver in L1/L2 SAE levels and to plan and monitor the vehicle motion in L3, L4, and L5 SAE levels.

Preliminary architecture: Preliminary architecture is the same block diagram that is mentioned in the **Item** boundary.

3.1.3.2 Asset Identification

Prerequisite: Item definition.

Work product: Damage scenarios, and assets with cyber-security properties. **Method:**

- Based on the item definition of an OC system, assets that are exploitable in a cyber-physical domain and damages due to attacks on these assets are identified in Table 3.1.

Table 3.1: An OC Asset Identification along with Damage Scenarios due to Attacks Considering the CIA Characteristics

Asset	CIA Property			Damage Scenarios
	C	I	A	
A.1: Camera Vision.	-	x	x	D.1: Physical injury to occupants as well as other road users (e.g., pedestrians, workers, occupants in another vehicle). D.2: Public/personal property damage. D.3: Traffic rule violation (e.g., school bus and emergency vehicle misclassification, object misclassification at a 4-way STOP sign or pedestrian crossing, vehicles in a controlled/restricted zone). D.4: Traffic issue (e.g., AV platooning diversion/congestion). D.5: Compromised OC IP and performance. D.6: Sensitive images (e.g., images captured in restricted access zone, or personally identifiable information (PII) principal) may become publicly available to the criminals.
A.2: Raw image captured by the camera.	x	x	x	
A.3: Image sent by the camera (communication).	x	x	x	
A.4: H/W which is running image processing and OC.	x	x	x	
A.5: Image processing algorithm/code.	x	x	x	
A.6: Interface b/w image processing and OC code.	-	x	x	
A.7: OC code.	-	x	x	

- Assets are classified with basic cyber-security properties, including the CIA.

3.1.3.3 Impact Rating

Prerequisite: Damage scenarios.

Work product: Impact ratings along with impact categories.

Method:

- In Table 3.2, damage scenarios identified in the previous steps, (D.1 to D.6) are classified into safety, financial, operational, and privacy. The impact of damage is rated following the guidelines in ISO 21434, Annex F.
- As per this guideline, ratings are divided into four categories, including severe, major, moderate, and negligible.
- If one damage can cause multiple impacts, only the impact category with the root cause is considered.

3.1.3.4 Threat Scenario Identification

Prerequisite: Item definition, damage scenarios, and assets with cyber-security properties.

Work product: Threat scenarios.

Method:

- In Table 3.3, threat scenarios (T.x) are identified for the assets, A.1 to A.7, that were identified in earlier steps.

Table 3.2: OC Impact Categories and Rating Levels with Consequences for Different Scenarios

Damage Scenarios	Impact Rating		
	Impact Category	Rating	Relevant Guide Criteria (ISO 21434)
D.1	Safety	Severe	Life-threatening injuries (survival uncertain), fatal injuries (Note: S3 as per ISO 26262).
D.2	Finance	Major	The financial damage leads to substantial consequences which the affected road user will be able to overcome.
D.3	Finance	Moderate	The financial damage leads to inconvenient consequences which the affected road user will be able to overcome with limited resources.
D.4	Operation	Severe	The operational damage leads to the loss or impairment of a core vehicle function.
D.5	Finance	Major	The financial damage leads to substantial consequences which the affected road user will be able to overcome.
D.6	Privacy	Moderate	<p>The privacy damage leads to inconvenient consequences for the road user. The information regarding the road user is:</p> <ul style="list-style-type: none"> • Sensitive but difficult to link to PII principle, • Not sensitive but easy to link to the PII principle.

- These threats are identified using the STRIDE method.
- None of the assets in the scope have repudiation or elevation of privilege-related applications. Hence, these two threat classes are not shown in the table.

3.1.3.5 Attack Path Analysis

Prerequisite: Threat scenarios.

Work product: Attack paths.

Method:

- In this step, attack paths for each threat (T.1 to T.23) are identified.
- Attack paths could be via physical or remote attacks on physical elements, hardware, and software in this analysis.
- In Table 3.4, a few examples from work on attack path analysis are shown along with the attack feasibility rating assessed in the next step.

3.1.3.6 Attack Feasibility Rating

Prerequisite: Attack paths.

Work product: Attack feasibility ratings.

Method:

- Attack feasibility rating is performed following attack potential-based approaches as per the guideline in ISO 21434, Annex G [23] in this analysis.
- Attack potential relies on five core factors, including elapsed time (ET), specialist expertise (SE), knowledge of the item or component (KoIC), window of opportunity (WoO), and equipment (Eq).
- The value for each of these factors is assigned for the attack paths of each threat.
- These values correspond to the various levels for the corresponding factor based on ISO 21434, Annex G.
- The levels are determined based on the understanding of attack path feasibility from the perspective of these factors. For example, putting a tape on a traffic sign or putting an object of interest can be done quickly in one day (ET) by a layman (SE) with publicly available knowledge (KoIC) and unlimited opportunity (WoO) without

Table 3.3: OC Threat Scenarios Identified by Different Classes of Attacks Including Spoofing, Tampering, Information Disclosure, and DoS

Damage scenarios	Attack class	Threat scenarios for each Asset						
		A.1	A.2	A.3	A.4	A.5	A.6	A.7
D.1	Spoofing	T.2	T.4	T.8	T.12	T.16	T.18	T.21
	Tampering	T.1	T.5	T.9	T.13	T.17	T.19	T.22
	Information Disclosure	-	-	-	-	-	-	-
	DoS	T.3	T.6	T.10	T.14	-	T.20	T.23
D.2	Spoofing	T.2	T.4	T.8	T.12	T.16	T.18	T.21
	Tampering	T.1	T.5	T.9	T.13	T.17	T.19	T.22
	Information Disclosure	-	-	-	-	-	-	-
	DoS	T.3	T.6	T.10	T.14	-	T.20	T.23
D.3	Spoofing	T.2	T.4	T.8	T.12	T.16	T.18	T.21
	Tampering	T.1	T.5	T.9	T.13	T.17	T.19	T.22
	Information Disclosure	-	-	-	-	-	-	-
	DoS	T.3	T.6	T.10	T.14	-	T.20	T.23
D.4	Spoofing	T.2	T.4	T.8	T.12	T.16	T.18	T.21
	Tampering	T.1	T.5	T.9	T.13	T.17	T.19	T.22
	Information Disclosure	-	-	-	-	-	-	-
	DoS	T.3	T.6	T.10	T.14	-	T.20	T.23
D.5	Spoofing	T.2	T.4	T.8	T.12	T.16	T.18	T.21
	Tampering	T.1	T.5	T.9	T.13	T.17	T.19	T.22
	Information Disclosure	-	-	-	-	-	-	-
	DoS	T.3	T.6	T.10	T.14	-	T.20	T.23
D.6	Spoofing	-	T.4	T.8	T.12	T.16	T.18	T.21
	Tampering	T.1	T.5	T.9	T.13	T.17	T.19	T.22
	Information Disclosure	-	T.7	T.11	T.15	-	-	-
	DoS	T.3	T.6	T.10	T.14	-	T.20	T.23

Table 3.4: Attack Feasibility Rating Considering the Parameters Defined in Accordance with ISO/IEC 18045 Standard

Threat ID#	Attack path	Attack Feasibility Assessment							Aggregated Attack Feasibility Rating	
		ET	SE	KoIC	WoO	Eq	Value	AFR	Max of the individual AF for each threat	Numeric value for Feasibility
T.1	1. Physical access (Sticker on Lens),	0	0	0	4	0	4	High	High	2
	2. Remote Auto-Control Attack.	1	6	0	4	4	15	High	High	2
T.2	Remote Lens flare/ Ghost effect attack	17	6	0	4	7	34	Medium	Medium	1.5
T.22	1. Physical access to in-vehicle n/w or ECU,	4	6	3	10	4	27	Very-low	Medium	1.5
	2. Malware attack	4	6	3	1	4	18	Medium	Medium	1.5

any special equipment (Eq). For instance, a malware attack on OC code may take approximately a month (ET = 4) for an expert (SE = 6), to gain some restricted knowledge (KoIC = 3). An easy opportunity considering can be carried out remotely (WoO = 1) and a computer with good programming ability connected to the internet (Eq = 4).

- An attack feasibility rating for each attack path is generated by adding values of these core factors for a particular attack path, and based on the range of the final value, it is classified into one of these four classes: High = 0 – 13, Medium = 14 – 19, Low = 20 – 24, Very low ≥ 25 .
- Finally, an aggregated attack feasibility rating associated with each threat scenario is calculated by choosing the maximum ratings of the attack feasibility, corresponding to attack paths, e.g., if one attack path is Medium and another attack path is High for the same threat scenario, then the aggregated feasibility rating is High.

3.1.3.7 Risk Value Determination

Prerequisites: Threat scenarios, impact ratings, and attack feasibility ratings.

Work product: Risk values.

Method:

Table 3.5: A Risk Value Determination for Different Attacks on Camera Vision

Threat ID	AAFR	Impact Rating						Risk Value					
		D.1:S	D.2:F	D.3:F	D.4:O	D.5:F	D.6:P	D.1:S	D.2:F	D.3:F	D.4:O	D.5:F	D.6:P
T.1	2	2	1.5	1	2	1.5	1	5	4	3	5	4	3
T.2	1.5	2	1.5	1	2	1.5	0	4	3.25	2.5	4	3.25	1
T.22	1.5	2	1	1.5	2	1.5	1	4	2.5	3.25	4	3.25	2.5

- Risk values are calculated for each threat scenario corresponding to each damage scenario impacted by the threat, using equation (3.1) [263]. In order to accurately determine the risk level, a comprehensive risk assessment must be conducted by taking into account the impact level of potential damage scenarios and the attack feasibility level of possible attack paths. This ensures that a precise evaluation can be made regarding the feasibility of each threat that may occur [264].

$$R = 1 + I \times F \quad (3.1)$$

where

- $R = Risk\ value$,
 - $I = Impact\ rating: Negligible = 0, Moderate = 1, Major = 1.5, Severe = 2$,
 - $F = aggregated\ attack\ feasibility\ rating: Very\ Low = 0, Low = 1, Medium = 1.5, High = 2$.
- As per ISO 21434, if a threat scenario corresponds to more than one damage scenario and/or an associated damage scenario has impacts in more than one impact category, a separate risk value can be determined for each of those impact ratings.
 - The risk value of threat scenarios is between 1 and 5, where a value of 1 represents the minimal risk.

In Table 3.5, some of the threats with the analyzed risk values are shown.

3.1.3.8 Risk Treatment Decision

Prerequisite: Item definition, threat scenarios, risk values.

Work product: Risk treatment decisions.

Method: Following threats have 3-5 risk values in most of the impact categories.

- T.1 Camera Vision Tampering,
- T.2 Camera Vision Spoofing,

- T.22 Camera Vision DoS.

A robust AI/ML framework can be considered to improve the accuracy of camera-based OC, resulting a reduction of risk of the threats T.1, T.2, and T.3 as an example of a risk treatment option.

3.1.4 STPA-SEC Approach

This section captures the threat modeling and risk analysis on an OC algorithm with an STPA-Sec approach. Fig. 3.3 shows the steps of STPA-Sec used in this case study. Steps with dark red fonts indicate the customization of an STPA-Sec specific to this case study. The rest of this section shows the analysis with an example from each step shown in this diagram.

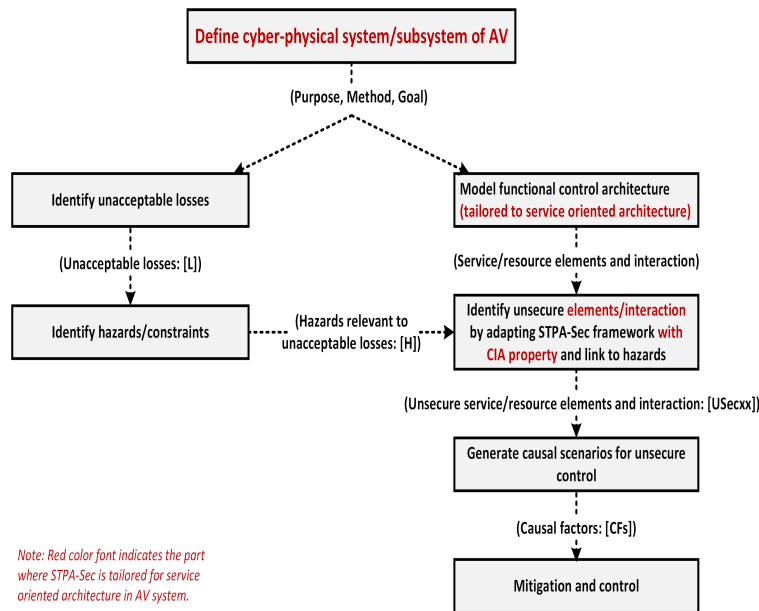


Figure 3.3: A STPA-Sec TARA for an AV Perception System Regarding the Loss, Hazards, and CFs

3.1.4.1 Cyber-physical System/Subsystem of AV

The first step for an STPA-Sec analysis is to elicit the goals and methods of the system. In Table 3.6, an OC subsystem for an AV perception system is defined by the guide words from an STPA-Sec method.

Table 3.6: An OC System Description with a STPA-Sec Format for an AV Perception System

A system to do (What = Purpose)	By means of (How = Method)	In order to contribute to (Why = Goal)
An OC subsystem classifies the object detected around AV	by using camera and AI-based algorithms	for AV to drive following the traffic rules.

Table 3.7: Different OC Unacceptable Losses Identified for the Mission (Example)

Level	Losses
L-1	Loss of life or injury.
L-2	Damage of the vehicle.
L-3	Damage of public property.
L-4	Legal consequence.
L-5	Reduction in vehicle sell.
L-6	Negative impact on investment.
L-7	Loss of intellectual property.
L-8	Loss of intellectual property.

3.1.4.2 Identify Unacceptable Losses

In this step, unacceptable losses for the problem or missions are identified and shown in Table 3.7.

3.1.4.3 Identify System Hazards

After identifying unacceptable losses for an AV system, the possible hazards relevant to OC algorithm are mapped that may lead to a loss.

3.1.4.4 Model Functional Control Structure

An STPA-Sec analysis does not require a physical control structure of the system, instead, a model of functional control structure is used to analyze unsecured control action. As the automotive software design is shifting from monolithic architecture to service-oriented architecture (SOA) [265], this step is tailored to model OC in SOA environment with AU-

Table 3.8: Sample OC Hazards Description with Relevant Losses (Example)

Hazard No.	Hazard Description	Related Loss
H-1	An AV does not stop or maneuver appropriately when an object is in its path.	L-1, L-2, L-3, L-4, L-5, L-6, L-8
H-2	An AV reacts to an object in its path that either does not exist or is insignificant.	L-1, L-2, L-3, L-4, L-5, L-6, L-8
H-3	A design/implementation detail is exposed to the outside world.	L-5, L-6, L-7

TOSAR [266]. This is done to align with the significant demand for advanced computation, re-usability, and ease of scalability of software and hardware components in connected and automated vehicles. In Fig. 3.4, an example of a concept-level architecture of vehicle autonomy in SOA is provided where the elements are grouped into three categories:

- Feature Elements (FE): Features that help to accomplish various scenarios of ADS (e.g., highway autopilot, city driving, pedestrian protection).
- Service Elements (SEL): Software units designed to perform a specific task that can be used by software units via a service interface-based contract; image processing, object detection, motion planning, and lateral control are some of the services in this model.
- Resource Elements (RE): These elements are mainly sensors, actuators, communication buses, memory, and computation nodes to capture environmental and system inputs, process and execute algorithms, and actuate controls accordingly.

Finally, a category called CPS elements is added to capture the cyber-physical interaction of an AV in its operating environment to complete the functional model for an STPA-Sec analysis. Furthermore, plausible services and interactions with an automated driving feature and resources for object detection/classification are identified in this diagram. Square heads indicate the publisher (for services) or the source for physical elements, and the circular end is the subscriber (for services) or sink (for physical elements). As an OC process is the target subsystem for the TARA analysis in this case study, the elements of interest for OC service are highlighted with the red boundary and red arrow. This concept-level model is used to identify unsecure elements in subsequent steps.

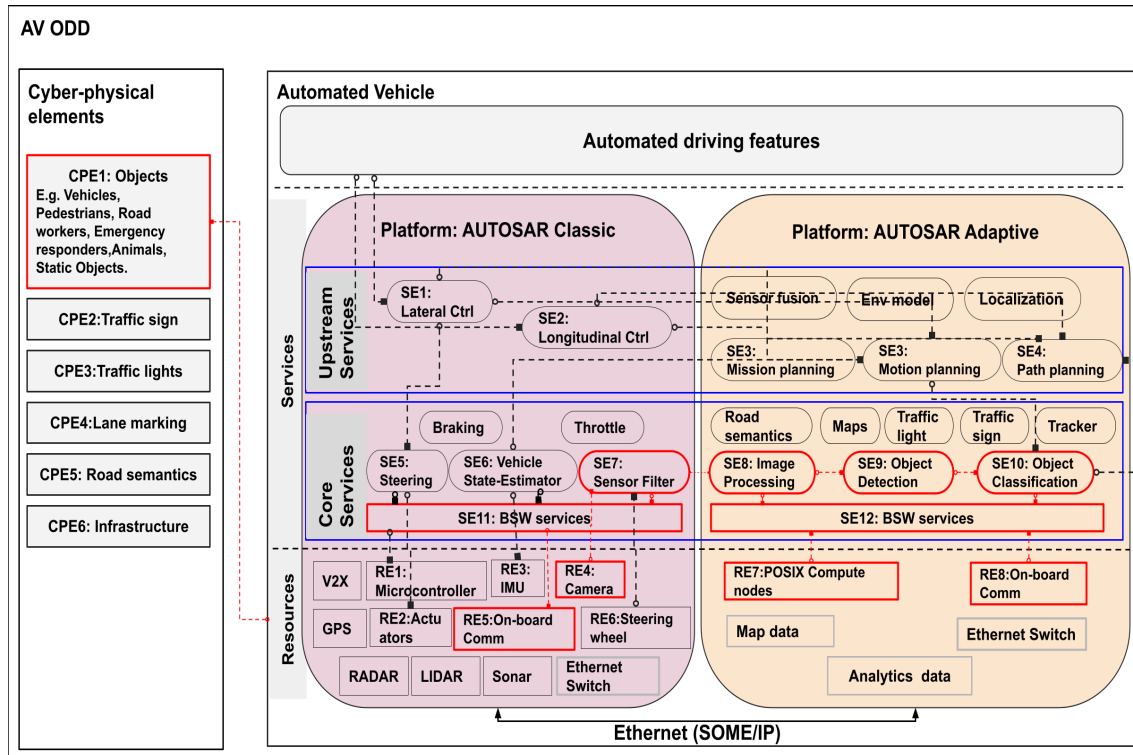


Figure 3.4: A Sample Vehicle Autonomy SOA Architecture

3.1.4.5 Identify Unsecure Elements

To Identify unsecure Elements, the STPA format of guide words is adapted in this step, but the actual guide words are created based on the CIA principle of security engineering as shown in Table 3.9.

3.1.4.6 Causal Factor

As per STPA-Sec, this step is followed to generate the CFs for unsecured control. In an SOA framework, systems behavior is the result of service interactions between elements. For this purpose, a specific set of guide words are created in this paper to classify the associated causes of the unsecure elements in the SOA framework. In Table 3.10, these guide words are listed to identify the “what” is the cause and “how” it can happen. In Table 3.11, examples are captured with possible CFs (“what” and “how”) for the unsecure element identified in the previous step.

Table 3.9: An Identification of Unsecure Element Guide Words Based on the CIA Characteristic

Element	Confidentiality	Integrity		Availability
	Accessible to inappropriate element causes hazards (UsecC)	Providing Incorrect Content causes hazards (UsecIC)	Providing at Incorrect Timing causes hazards (UsecIT)	Not availability causes hazards (UsecA)
SE10: OC	UsecC-1 (Providing OC to unsubscribed services) Causes: H-3	UsecIC-1 (Incorrectly classified object) Causes: H-1, H-2	UsecIT-1 (Delayed) Causes: H-1 UsecIT-2 (Early) Causes: H-2	UsecA-1 (Not availability of OC service) Causes: H-1
RE4: Camera	-	UsecIC-2 (Corrupted raw data provided) Causes: H-1, H-2	UsecIT-3 (Delayed) Causes: H-1 UsecIT-4 (Providing early can be missed by consumer) Causes: H-1, H-2	UsecA-2 (Not having Camera raw data transmission) Causes: H-1
CPE1: Objects in ODD	-	UsecIC-3 (Object's incorrect visual property) Causes: H-1, H-2	-	UsecA-3 (Object visual property cannot be perceived/disappeared) Causes: H-1

Table 3.10: A Chart for CF Identification Guide Words

“What” can cause unsecure interaction	high-level classification of “How” can it happens
- Feature application	- Algorithm/Logic vulnerability (LV) - I/O vulnerability (I/OV) - O/S vulnerability (OV) - Memory vulnerability (MV) - Process vulnerability (PV) - Database vulnerability (DV) - Network vulnerability (NV) - Cyber-physical vulnerability (CPV) - Human vulnerability (HV)
- Feature interface	
- Service interface	
- Service logic/data	
- Service repository	
- Optical	
- Temperature	
- Electromagnetic	
- Mechatronics	
- Temporal	
- Off-board communication	
- On-board communication	
- Power and energy	

Table 3.11: An Identification of CFs Based on What-How (WH) Method (Examples)

Unsecure Elements	CF	
	What can cause it	How can it occur
USecA-1	CF1: Blocked Service Interface CF2: Not executed service logic/algorithm CF3: Corrupted service registry CF4: Unsuccessful service find CF5: Failure to perform service call	NV, OV, PV OV, PV MV, DV OV, PV OV, PV
USecC-1	CF6: Spoofed service interface CF7: Easy access to program location service logic/algorithm CF8: Altered service registry CF9: Spoofed service find CF10: Aliasing service call	NV, PV MV, PV MV, DV NV, OV, PV NV, OV, PV
USecIC-1	CF11: Corrupted service interface CF12: Manipulated service logic/algorithm CF13: Manipulated service data CF14: Altered service registry CF15: Spoofed service find CF16: Aliasing service call	NV, OV, PV LV DV, MV DV, MV NV, OV, PV NV, OV, PV
USecIT-1	CF17: Busy service interface CF18: Delayed execution of service logic/algorithm CF19: Delayed service call	NV, OV, PV OV, PV OV, PV
USecIT-2	CF20: Old transaction data in service interface CF21: Replay transaction in service interface	MV, PV NV, PV
USecIC-3	CF22: Physical damage to the object CF23: Physical damage to camera lens CF24: Altering visual appearance (e.g., tape, paint, mask) CF25: Artificial projection on object CF26: Projection on camera lens CF27: Adversarial AI-based image	CPV CPV CPV, LV CPV CPV CPV, LV

3.1.4.7 Mitigation and Control

In this step, STPA-Sec mitigation and control strategies are provided to eliminate or avoid the cause of an unsecured control action (e.g., firewall) to handle NV, an access control for MV, an encrypted message for DV, and a robust algorithm for LV. In this paper, the primary focus is on a TARA method, hence, detailed risk mitigation strategies are not captured here.

3.1.5 Comparison Between Two Threat Models

Comparing both of the threat models for an CO algorithm, it is observed that STPA-Sec can provide some advantages with its system-based approach over the asset-centric approach in the ISO/SAE 21434. On the other hand, the attack feasibility rating and risk determination of the ISO/SAE 21434 are more appropriate to transfer the analysis to a traditional cybersecurity framework. Hence, the advantages of STPA-Sec can be mentioned as follows:

- STPA-Sec captures malicious cyber-physical interactions in an AV perception environment, such as objects in the road and other road users, as well as distributed service interactions between various elements inside the system. Nevertheless, ISO/SAE 21434 is intended for E/E assets with cyber-security properties in a road vehicle and not for CPE in an operating environment.
- AVs are expected to deliver certain missions, hence, STPA-Sec is advantageous by utilizing a functional model rather than an asset that helps to capture the critical paths for delivering the missions/goals.
- AVs are dynamic systems on the road with complex and computation-intensive software. Hence, optimizing run-time energy, latency, and computing hardware resources is critical. Associating the threats to CFs of unsecured actions/services instead of whole assets, adds more granularity which allows using the cyber-defense and protection resources, optimally.

The advantages of ISO/SAE 21434 approach can be considered as follows:

- STPA-Sec does not have an in-built risk assessment method, whereas a risk assessment in the ISO/SAE 21434 standard helps to determine the risk value of OC process based on the impact and attack feasibility of a threat.
- STPA-Sec does not provide a software-centric perspective of the CFs for the threats, but using STRIDE as recommended in the ISO/SAE 21434, guidelines help to identify the threats of an OC algorithm from a software oriented approach.

- ISO/SAE 21434 provides a practical approach to assess the attack feasibility based on ET, SE, KoIC, WoO and Eq which is applicable to OC processes for an AV perception system.

3.1.6 Proposed Method: An Integrated Approach of Threat Analysis for AV

From the case study illustrated in the problem statement section, it is observed that STPA-Sec approach provides a relevant approach to identify and analyze threats for AV perception systems and ISO/SAE 21434 provides benefits of an automotive specific risk analysis framework. But individually, they lack in providing a complete framework for AV perception systems. Moreover, none of them specifically provide a comprehensive framework to address the threats on AI algorithms in AV perception systems and evaluate the risk based on various object types in an AV ODD. This section presents an integrated TARA framework and the associated mathematical model to address this gap.

The proposed novel approach covers the following:

- An integrated threat modeling framework that combines system-centric and asset-centric approaches to analyze the threats of perception from system interaction with the environment and from attacks on the hardware and software components.
- A mathematical model where the AI robustness factor is incorporated as an additional attack potential factor for attack feasibility assessment, along with other factors from ISO/IEC 18045.
- Object-centric risk evaluation model where impacts are rated for depending on the types of objects and corresponding unacceptable losses in AV ODD.

3.1.7 Framework

As AVs are real-time CPSs with a complex interaction with the environment and subsystems within the AV system, it is critical to find out the unsecured interaction that can result in hazards and unaccepted losses. The risk assessment should consider the differences between the object types in ODD and the impact. Thus, the resources to defend and protect from attacks, can be focused on relevant interactions rather than any asset. Also, threat modeling limited by the focus on assets may miss the vulnerable system interactions. An AV perception system is heavily integrated with the environment with various sensors and

driven by complex software and AI-driven algorithms on high-performing computing hardware from the design and implementation perspective. Hence, the threat modeling for an AV perception system requires mapping the CFs to appropriate attack classes with some well-established threat modeling approaches in the software industry (e.g., STRIDE). Also, it covers various adversarial attacks on AI algorithms and cyber-physical attacks. This helps to present the threat and risk analysis of an AV perception system in a known format to cyber-security engineers and take advantage of a holistic cyber-security mechanism evolved in various industries. Based on the observations from the threat modeling in this study, an integrated approach is proposed to address the needs mentioned above:

- Figure 7 shows an integrated approach to TARA adapted from STPA-Sec and the ISO/SAE 21434 standard. This approach starts by analyzing an AV perception system as a CPS and utilizes STRIDE to transform the CFs of unsecured control actions in the AV perception system into an attack class. This helps to perform the rest of the threat and risk analysis in a cyber-security domain by utilizing the attack analysis method from ISO/SAE 21434.
- As the AV perception system is implemented using ML algorithms and other complex software components, algorithm robustness factor (RF) is added as one of the parameters, along with other factors presented in the ISO/SAE 21434 standard to assess the attack feasibility and include the knowledge of CPE in the ODD, and KoIC is replaced with KT.
- For an AI algorithm-specific RF, a cumulative performance of the AI algorithm with typical scenarios abnormal scenarios, and against various adversarial attacks (e.g., perturbation attack, poisoning attack, and model inversion) is proposed while conventional software elements (e.g., O/S, network, and memory) can utilize common vulnerability scoring system (CVSS) ranking system.
- The impact of an attack is expressed in terms including severity, occurrence, duration, and the cost of recovery from the losses caused by the attack. For OC-related loss in the AV perception system, these parameters are proposed based on various types of objects (e.g., humans, bicyclists, and vehicles in the ODD of an AV).
- Finally, the risk value determination is proposed by augmenting the ISO/SAE 21434 risk formula with the updated formula for impact as per

the previous bullet and risk mitigation factors to contain the controllability and detectability of an unsecured control action/attack for the risk evaluation.

3.1.8 Mathematical Model

As per ISO/SAE 21434 recommendation, attack potential relies on five core factors, including elapsed time (ET), specialist expertise (SE), knowledge of the item or component (KoIC), window of opportunity (WoO), and equipment (Eq) following the attack potential values as per ISO/IEC 18045 standard for an automotive sector. However there is no recommendation to address the robustness of the AI algorithm and the influence of the object type in AV ODD. In this section, a novel mathematical model is presented in equation (3.2) for assessing the risk value in the context of AI vulnerability analysis, specifically for USecX (R_{USecX}). This model, distinct from previous approaches, incorporates a mitigation factor (M_{USecX}) that accounts for the controllability (C_{USecX}) and detectability (D_{USecX}) of attacks, assigning values from 0 to 2 to various levels of these parameters, as illustrated in equation (3.2) [267, 268]. The model’s innovation lies in its consideration of the mitigation factor, a critical aspect often overlooked in prior research. This factor plays a pivotal role in gauging the extent to which attacks can be detected and managed, thereby linking the concepts of attack types, their controllability and detectability, and overall risk assessment in a comprehensive framework.

$$R_{USecX} = \frac{1 + I_{USecX} \times F_{USecX}}{1 + M_{USecX}} \quad (3.2)$$

$$M_{USecX} = C_{USecX} + D_{USecX}$$

This approach also prioritizes various road elements (e.g., humans, animals, and vehicles) based on factors such as their damage severity ($S_{L,USecX}$), presence rating ($O_{H,USecX}$), average recovery time ($T_{L,USecX}$), and financial loss ($\Gamma_{L,USecX}$). Additionally, the impact rating (I_{USecX}) ranges from 0 to 3 (low to severe levels, respectively), encompassing the overall impact of cyberattacks, which can vary across environmental, financial, and operational safety aspects, defined as equation (3.3):

$$I_{USecX} = S_{L,USecX} \times O_{H,USecX} + T_{L,USecX} + \Gamma_{L,USecX} \quad (3.3)$$

This method highlights the heightened risk and necessity for effective risk management strategies. The approach categorizes risk levels into four intuitive groups, aiding in easier interpretation and application in risk assessments, in which low, moderate, high, and severe

impact ratings can be assigned. The framework, based on the sum of attack potential values, establishes a link between these values and the attack feasibility rating (F_{USecX}), as outlined in equation (3.4) and depicted in Fig. 5.1.

SE		KoIC		Eq		RF	
Layman	0	Public	0	Standard	0	Performance: Normal scenarios = Poor Abnormal scenarios = Poor Adversarial attacks = Poor	0
Proficient	1	Restricted	1	Specialized	1	Performance: Normal scenarios = Good Abnormal scenarios = Poor Adversarial attacks = Poor	1
Expert	2	Sensitive	2	Custom-built	2	Performance: Normal scenarios = Good Abnormal scenarios = Good Adversarial attacks = Poor	2
Multiple Experts	3	Critical	3	Multiple Custom-built	3	Performance: Normal scenarios = Good Abnormal scenarios = Good Adversarial attacks = Good	3

ET		WoO	
< a day	0	Unlimited	0
< a week	1	Easy	1
< a month	2	Moderate	2
> a month	3	Difficult	3

Parameter (ϕ)	Attack potential description and value (V)
----------------------	--

Figure 3.5: Evaluation of Attack Potential in Compliance with ISO/IEC 18045 Parameters

The attack potential values, determined by parameters in equation (3.5), range from 0 to 18 and are categorized into three groups (i.e., 0-6, 7-12, and 13-18) for better comprehension of attack feasibility.

$$F_{USecX} = \max(F_{USecX}^{\eta_i}) \quad (3.4)$$

$$\sum V_{\eta_i} = V_{\eta_i}^{SE} + V_{\eta_i}^{KoIC} + V_{\eta_i}^{Eq} + V_{\eta_i}^{ET} + V_{\eta_i}^{WoO} + V_{\eta_i}^{RF} \quad (3.5)$$

for $i = 1, 2, 3, \dots, n.$

equation (3.5) delineates the correlation among attack potential parameters, highlighting that basic attack paths (utilizing standard tools, unskilled attackers, and public information) have higher possibility of success due to their simplicity. The complexity and feasibility of an attack path inversely correlate with the required attack potential degree. The novel index, $V_{\eta_i}^{RF}$ measures the resilience of ML algorithms (i.e., object classification) against typical, abnormal, and adversarial scenarios. This index effectively assesses the performance of AVs under attacks, regarding different objects, reflecting the AVs' environmental dependence.

3.2 Threat Model and Attack Model for ToD

In chapter 2, it was reviewed that ToD of road vehicles on public roads is an emerging technology for future mobility solutions with LMD, corss-border transport and elderly mobility

Table 3.12: Functions and Dataflows for Various ToD

		Data flow		Function						
		Vehicle To Operating Station	Operating Station to vehicle	Sensing	Perception	Localization	Planning	Decision	Control	Actuation
Direct control		Sensor data	Control command via steering, brake, acceleration pedal operation by remote operator.	Vehicle	OPS	OPS	OPS	OPS	Hi level:OPS Lo level:OPS	Vehicle
Shared control		Object list or a representation of the free space	Desired control command via steering, brake, acceleration pedal operation by remote operator.	Vehicle	Vehicle	Vehicle	OPS	Vehicle and OPS	Hi level:Vehicle/ OPS Lo level:Vehicle	Vehicle
Indirect Control	Trajectory guidance	Sensor data	Control command as trajectory	Vehicle	Vehicle/ OPS	Vehicle/ OPS	OPS	OPS	Hi level:OPS Lo level:Vehicle	Vehicle
	Waypoint guidance	Sensor data	discrete waypoints	Vehicle	Vehicle/ OPS	Vehicle/ OPS	OPS	OPS	Vehicle	Vehicle
	Interactive path planning	Object list and a grid map	Optimized path	Vehicle	Vehicle	Vehicle	Vehicle and OPS	OPS	Vehicle	Vehicle
	Perception Modification	Object list and a grid map	Bounding box	Vehicle	Vehicle and OPS	Vehicle	Vehicle	Vehicle	Vehicle	Vehicle

service as two of the potential applications. ToD involves monitoring, controlling or providing guidance to the driving function of a vehicle from a remote operating station. Further, the high-level concept of ToD system and communication flow were illustrated in section 2.5. According to this review, for a typical ToD system, the perception information sent by the vehicle to the operating station via cloud and fog infrastructure using wireless or cellular network. Similarly, control commands from the operating station are sent to the vehicle. This makes the teleoperated vehicle a cyber-physical system and poses a potential exposure of perception data and control commands outside vehicle boundaries. This means various digital devices at operator station, cloud infrastructure, vehicle sensors, in-vehicle network and the ECUs are also part of potential attack surface. An attacker can target communication channels and other components of vehicle ToD system. Hence, threat modeling for teleoperated vehicles with its potential use case on public roads is crucial. Further, deeper analysis with teleoperated vehicle system models and attack models is necessary to understand real world feasibility of such threats. However, as per current literature survey threat analysis in this area has not been explored in depth. For this dissertation, an attack-tree based threat modeling for a ToD followed by an attack model for LMD are performed, this work is presented in this section.

Given the extensive and dispersed attack surface of vehicle tele-operation, an attack-tree based method is employed for the threat analysis. In this study, TARA of the ToD system is carried out with following steps. The first step involves identifying the components of a ToD system. From the literature review discussed in section 2.5, ToD functions can be distributed in three categories of components (e.g., operator station, IoT infrastructure and vehicle) as categorized in Table 3.12. An operator station must include human operator, operator terminal, server and local communication network. It might also have artificial intelligence

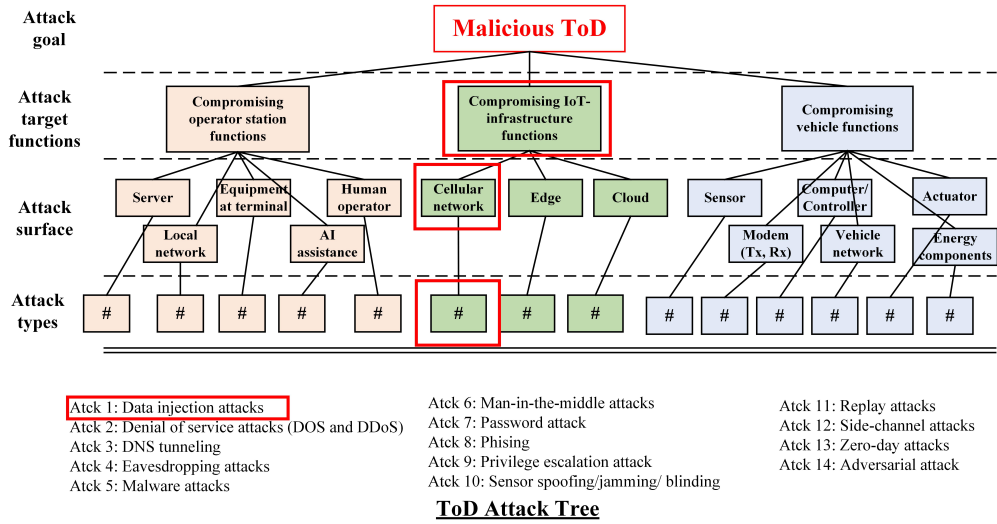


Figure 3.6: An Attack Tree for a ToD Event

(AI) assistance to the terminal. An IoT infrastructure can be divided into three primary sub-components including cellular network, cloud and edge. From the ToD perspective, the vehicle needs to have sensing devices for perception, localization, inertia and vehicle diagnostics. A vehicle also requires an in-vehicle communication network to communicate between multiple ECUs and modem to communicate using cellular channels. For vehicle motion, it needs the drive-train, controller and actuators. In the second step, all of these components are organized in a tree structure as shown in Fig. 3.6. According to this tree, ToD operation is the root and operator station functions, IoT infrastructure functions and vehicle functions are added as its children or leaf nodes. The components involved to deliver each of these three functions are further listed as the third layer of leaf nodes. For example, the server and other equipment at the terminals are example of leaf nodes of operator station functions. Cellular network, edge computing device and back-end cloud are are components to deliver IoT infrastructure functions. Vehicle function require sensor, actuator, computing device, controller, modem, in-vehicle network, energy providing components. In the third step, this tree is analyzed with with potential attacks on ToD system. According to this attack tree, if attacker’s goal is to maliciously take control of ToD, the layer 3 nodes of the tree (components) can be exploited as attack surface to compromise the target functions at layer 2 which are leaf nodes of the root node. Further, to exploit the attack surface attackers can use several attack types which make the fourth layer of the tree. For an example, as marked with red rectangles in Fig. 3.6, “data injection attacks” on cellular network can alter the intended communication between the operator station and vehicle, which can cause unintended driving maneuver for the teleoperated vehicle. Though a comprehensive database

of attacks on ToD is not available, the attacks on AV and other IoT devices were reviewed in detail. Such attacks are then analyzed for ToD context as shown in Table 3.13 to derive the list of attack types. As per this attack tree analysis, 14 types of attacks are identified for a malicious ToD. Further, it can be argued that operator station and vehicle which can enforce certain level of physical security to bolster cybersecurity solution. However, ToD for road vehicles use publicly available wireless or cellular networks for V2X connectivity which increase the attack feasibility.

Table 3.13: Potential Attack Types for ToD System

Attack Type	Vehicle					IoT Infrastructure			Operator Station				
	Vehicle Sensor	Vehicle Processing Unit	Vehicle N/W	Vehicle Tx/Rx	Vehicle Actuator	Cellular N/W	Edge	Cloud	Server	Local N/W	Equipment at Terminal	Human Operator	AI
Data Injection Attacks							x	x	x	x	x		x
Denial of Service Attacks (DOS and DDoS)		x	x	x		x	x	x	x	x	x		
DNS Tunneling				x		x	x	x	x	x			
Eavesdropping Attacks			x	x		x	x	x	x	x	x		
Malware		x					x	x	x		x		x
Man-in-the-middle Attacks	x		x	x		x	x	x	x	x			
Password Attack								x	x	x	x	x	
Phishing													
Privilege Escalation Attack								x	x	x	x		
Sensor Spoofing/ jamming/ blinding	x												
Replay Attacks	x		x	x		x	x	x	x	x	x		
Side-Channel Attacks		x				x	x	x	x	x	x		
Zero-day Attacks	x	x	x	x	x	x	x	x	x	x	x		
Adversarial Attacks													x

Note: This table is created based on the literature review of [269, 270, 271, 272, 273, 25, 274, 275, 276, 277, 278, 13, 14, 15, 16, 17, 18, 19]

In the 4th step, most promising applications of ToD is analyzed for an impact on safety, finance and legality due to malicious ToD, as illustrated in Fig. 3.7. This analysis is carried out with a subjective approach considering that malicious ToD can disrupt lateral and longitudinal motions, and suspension control of tele-operated vehicle. Such incidents can interrupt ToD service and even jeopardize the safety of passengers and other road users. In [279, 280, 281, 282], researchers have discussed various consequences of disrupting cross border transportation, LMD and mobility services. According to these papers, disruption of these applications have major adverse effects on road safety and regional economy. As these are the potential applications for ToD, it can be argued that a malicious ToD event can inflict serious harm to these applications. Finally, in the 5th step of the TARA, a risk is assessed based on the likelihood of attacks causing a malicious ToD and the impact on the ToD application. At present, ToD for public roads is still a developing technology. However,

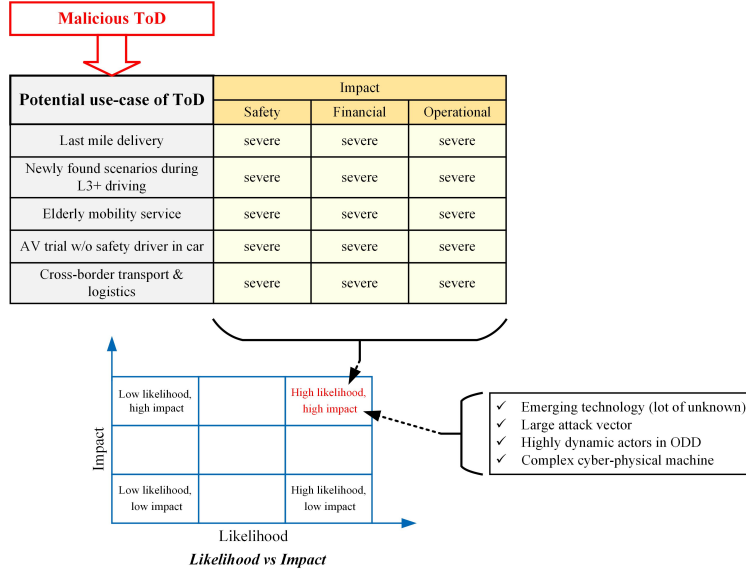


Figure 3.7: A Teleoperated Vehicle Attack Likelihood vs Impact

when ToD is implemented on public roads, attack surface and the number of impacted users will expand. As a result, the risk will also escalate, which is demonstrated as a high risk in Fig. 3.7.

3.2.1 Attack Model for LMD

According to the attack tree analysis, an attacker can cause malicious ToD event by compromising the IoT infrastructure. In this section, firstly, an attack model is developed for one of the potential use-cases of ToD event on public roads, known as LMD. Secondly, an attack formulation is implemented for an FDI attack on steering wheel angle command from tele-operator. The LMD represents the concluding stage in a business-to-customer (B2C) delivery process where the package is transported to the recipient, either directly to their home or to a designated pickup location [283]. The FDI attack scenario of the teleoperated LMD vehicle can be illustrated with Fig. 3.8. As shown in this diagram, sensors on the vehicle collect the data around the vehicle and send it to the operator terminal using a cellular/wireless communication. A human operator makes the driving decision based on the digital perception at the terminal and sends the driving command to the vehicle using the cellular channel. When the vehicle receives the driving control command, the control system, drive-train and the actuators deliver the desired driving actions. This diagram also shows the FDI attack targeted to the vehicle steering control command to manipulate the driving maneuver. As LMD typically involves city and urban locations, a delivery vehicle may need to make a turn at an intersection while following its route. However, an attack on steering

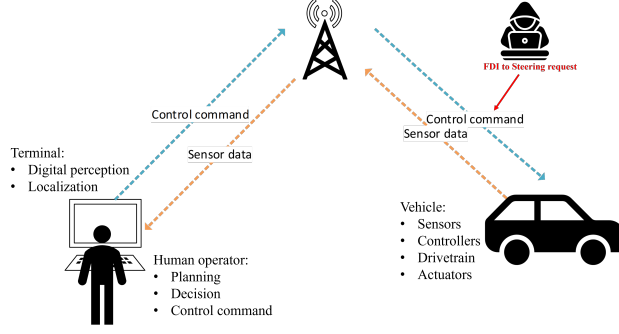
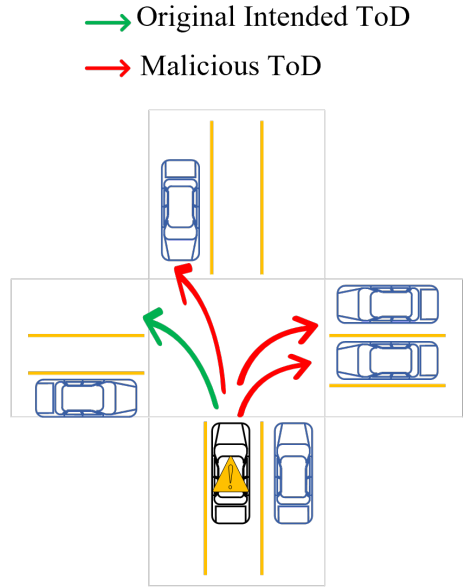


Figure 3.8: An FDI Attack on Communication Between Remote Operator and the Vehicle

command can execute an undesired driving action and trajectory causing an accident that is depicted in Fig. 3.9. According to this diagram, the normal trajectories for vehicle A is shown with green arrows but the vehicle follows the path shown in red arrows under a cyber-attack. This malicious behavior can be a potential cause of frontal or angled collision with other stationary and moving road users. Based on US NSC data 2020, angled collision and head on collision are the top two reasons for deaths and fatal crashes in the U.S. [99]. The analysis of damaged pattern and severity of impact for passenger cars presented by Kurebwa *et. al* shows that the probability of damage and severity is significantly higher at the front and front corner zones as compared to other point of impact on a vehicle [98]. Hence, an FDI attack on steering command from tele-operator is selected for case study of the attack model. An attack model designed for this study is presented in Fig. 3.10. As depicted, driver inputs for steering wheel angle, accelerator pedal and brake pedal determines the motion control logic of tele-operated vehicle. Furthermore, motion control signals determine the vehicle heading angle and vehicle dynamics. Therefore, it can be derived that an FDI attack on driver input for steering wheel angle will impact the vehicle heading angle and dynamics. In order to create this attack, an attack formula is developed for the FDI on steering wheel angle. For this purpose, ISO/SAE 21434 is reviewed for recommended core factors to assess the attack feasibility. The attack generation and formulation can be yielded from Fig. 3.11 and equation (3.6):

$$\hat{\alpha} = f_{atk}(\alpha, \epsilon, \bar{\omega}) \quad (3.6)$$

Where, f_{atk} is the attack generation function, $\hat{\alpha}$ is the false data injected steering wheel angle command, α is the original steering wheel angle command, ϵ is the injected fault, $\bar{\omega}$ is the window of opportunity which is $f_w(\partial, \rho)$. Also, ∂ and ρ show the duration of the fault injected and the point of injection, respectively. According to equation (3.6), an FDI steering wheel angle is a result of original steering wheel angle signal injected noise with a specific window of opportunity (WoO). From an attacker perspective, it is crucial to inject the false



A ToD left turn at a traffic intersection.

Figure 3.9: A Traffic Light Intersection Attack Scenario

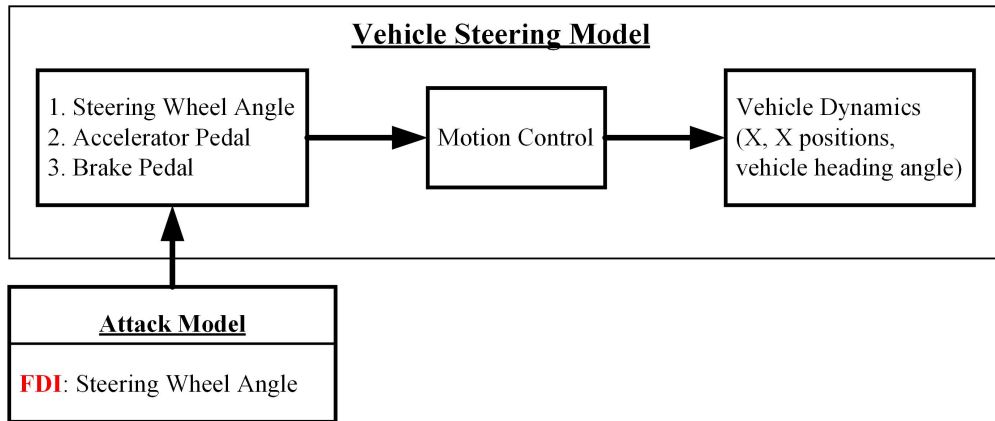


Figure 3.10: A System Model for the Vehicle's Steering Angle Under Attacks

data at appropriate *WoO* to create a desired adverse effect. Hence, *WoO* is created by choosing the point of noise injection to the signal and duration of the noise. This is further illustrated in Fig. 3.11 with examples. As shown in **Example 1**, the point of injection in this case is when the original steering wheel angle starts to change for the desired turn whereas the point of injection starts ahead of such maneuver in **Example 2**. Also, the duration of the attack is relatively for a small duration as compared to **Example 2**.

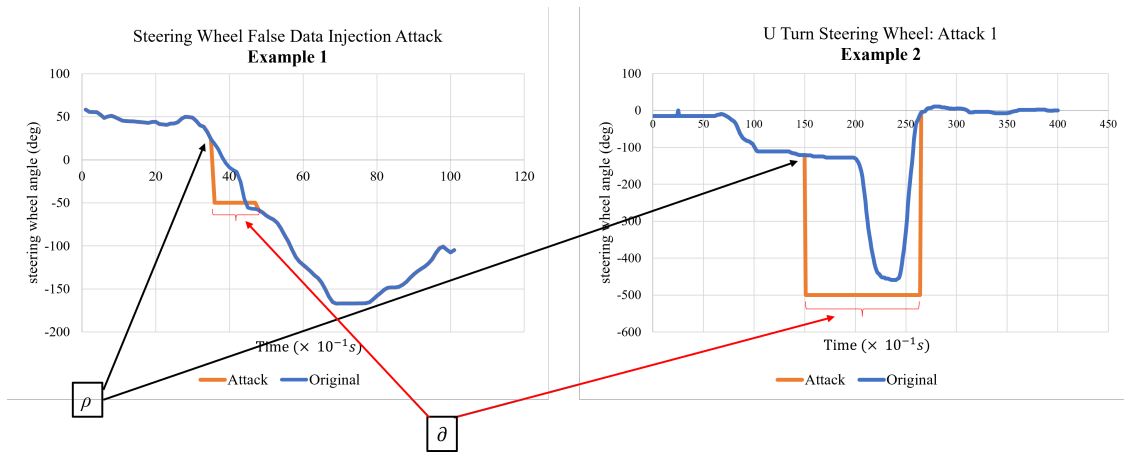


Figure 3.11: An FDI in the Steering Wheel Angle

CHAPTER 4

Anomaly Detection for Teleoperated LMD

In section 3.2 of chapter 3, an attack tree based TARA was presented for ToD road vehicles on public road. As per this TARA, ToD system has large attack surface and there are various types of potential attacks that can cause the threat of a malicious ToD. The TARA also shows the threat of malicious ToD has risk with high impact for potential ToD applications including LMD of goods from depot to home or business. In this chapter, first the current limitation of automotive cybersecurity strategy to protect against malicious ToD is highlighted. Next, a novel method is proposed to detect such malicious ToD by analyzing the context of ToD application and physical parameter of the vehicle under ToD. It can be noted, the anomaly detection method proposed in this dissertation is based LMD application as described in assumptions and scope below. However, in future this concept can be extended to other application of ToD or road vehicles.

4.1 Problem Statement

The problem statement of detecting malicious ToD in this chapter is described as follows:

- With evolving cyber threats relying on traditional cybersecurity methods (e.g., cryptography, root of trust, chain of trust, access control) cannot guarantee protection from all potential attacks.
- Moreover, teleoperated vehicles are a specific type of cyber-physical system with dynamic operating environment. Hence, defense-in-depth principle for teleoperated vehicles must be explored beyond traditional cybersecurity solutions.
- UN R155 compliance requires securing vehicles by design and reporting security incidents specially for vehicle fleets. As LMD is a potential use case of ToD, this application falls under the same requirements.

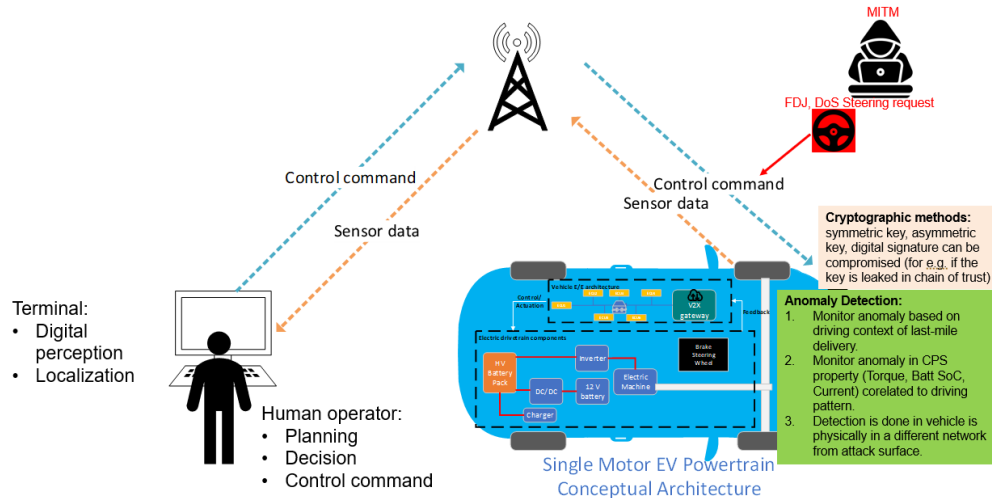
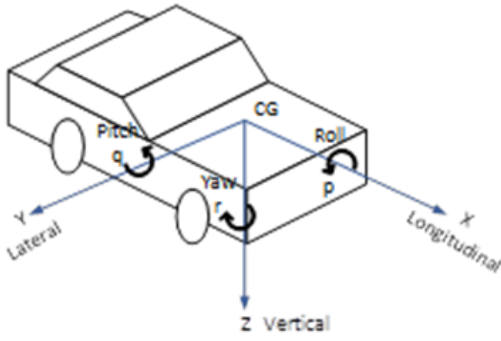


Figure 4.1: Cyber-physical Anomaly Detection of ToD at High-level

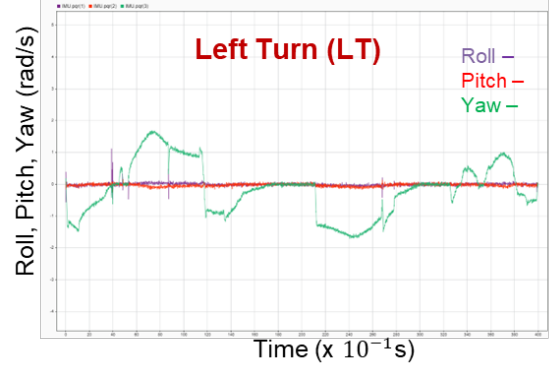
- Further, in teleoperated vehicles there is no human driver physically present to monitor and control in case of a cyberattack. Hence, anomaly detection is crucial for incident reporting and road safety.
- Current anomaly detection techniques in automotive primarily focus on in-vehicle network behavior and limited consideration of physical behavior.

However, research on other CPS systems found that for detecting cyber-physical attacks, hybrid approaches by combining data-driven model and physics-based model have some benefits. Driving behavior of a teleoperated vehicle can depend on various dynamic factors. Road condition, weather, location, and time of the day, priority of the business or mission can be classified as context of the ToD. Based on this knowledge, teleoperated driver's next intended maneuvers at a particular location can be predicted. However, the actual driving maneuver and trajectory during a turn depends on the driver inputs, design of vehicle-propulsion and vehicle-dynamics. In this work, PCADS for teleoperated LMD vehicle is proposed when steering wheel angle command from teleoperated driver is injected with false data during maneuvering at left turn, right and U-turn. The proposed method requires the knowledge of driving context of the delivery and time series pattern of vehicle's physical parameters during the above mentioned maneuvers. High-level concept of cyber-physical anomaly detection based on vehicle physical parameter is illustrated in Fig. 4.1.

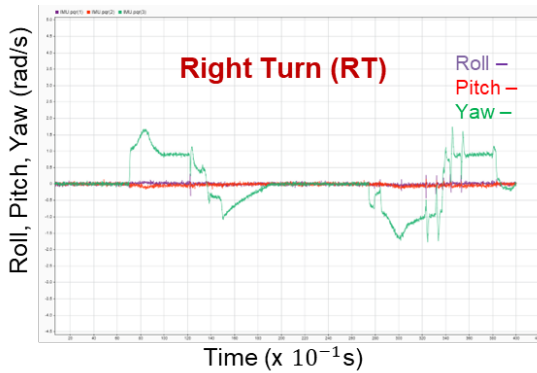
A single motor based electric vehicle (EV) architecture is shown as an example. Depending on the EV architecture including the number and type of traction motors, ESS and vehicle's mechanical design value of vehicle physical parameters can vary during the vehicle maneuver. Roll, pitch, yaw, wheel angle, battery current, motor torque are some of the parameters which



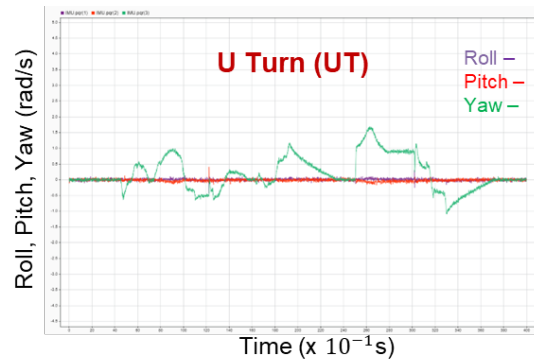
(a) SAE Vehicle Coordinate System



(b) Roll, Pitch and Yaw during LT



(c) Roll, Pitch and Yaw during RT



(d) Roll, Pitch and Yaw during UT

Figure 4.2: Example of Vehicle Physical Parameter Variation with Left Turn (LT), Right Turn (RT), U Turn (UT)

realize the difference. For an example as shown in Fig. 4.2, time series value of roll, pitch and yaw measured by vehicle IMU sensor for the same vehicle configuration is different for left turn, right turn and u-turn maneuvers. For known vehicle configuration, PCADS method monitors these vehicle parameters to detect anomaly in trajectory during left turn, right turn and u-turn. The detailed of the method is discussed in section 4.2 methodology.

4.1.1 Assumption and Scope

The assumption and scope of the anomaly detection methodology proposed in this chapter are as follows:

- This work is focused on a specific use case of ToD which is LMD.
- The primary goal of this method is to detect the anomalies for cyber incident analysis. Altering the driving action autonomously based on this detection is not in scope of

this work.

- For driving context, solving vehicle routing plan (VRP) to find optimal route for fleet of vehicles is not in scope and it is assumed the VRP is accurate and robust to address real-time traffic density, road condition, weather, service time, vehicle maintenance schedule.
- Dynamic alert generation is out of scope, in this work it is simulated as a binary flag.
- For physical parameter learning, left turn, right turn and U-turn maneuvers are considered.
- Experimental results are based on the dataset mentioned in the experiment section.
- Proposed method assumes vehicle configuration and vehicle physical parameter value for left turn, right turn and U-turn maneuvers of the target vehicle is known to anomaly detection system.

4.2 Methodology

In this section, a PCADS method is proposed to detect the anomaly during left turn, right turn and U-turn of LMD vehicles. The scope of this method is focused on the FDI attack on steering wheel angle in this paper. In order to detect the anomalies, the PCADS method requires the knowledge of DCs for the delivery vehicle and time-series patterns of vehicle's physical parameters during the left, right and U-turn maneuvers. The general framework of the proposed method is represented in Fig. 4.3. As depicted in this diagram, this proposed method has two stages of AD process including

- Context-aware anomaly detection (PCADS-CA).
- Physics-based anomaly detection (PCADS-PB).

At a high-level view, the PCADS-CA method uses two inputs to compare and detect anomalies. One input is intended the maneuver at each intersection which is concluded from DCs and the second input is the actual driving command received from tele-operated driver at each intersection. On the other hand, the PCADS-PB method monitors the pattern of the vehicle's physical parameter time-series values during a specific turn and compares it with the learned patterns for the same type of turns for any deviation. In the next section, PCADS-CA and PCADS-PB models are presented with detail of detection methodology, algorithm and mathematical modeling.

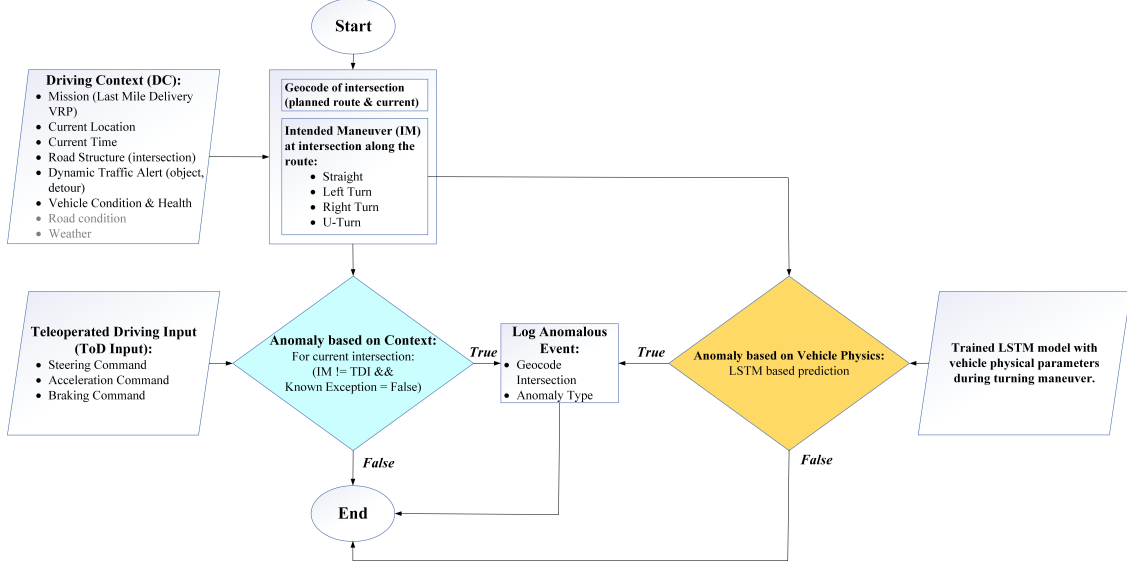


Figure 4.3: An LMD ToD Anomaly Detection Framework

4.2.1 Stage 1: PCADS-Context-aware Anomaly Detection

Driving behavior of a tele-operated vehicle can depend on various dynamic factors. Road conditions, weather, location, and time of the day and the priority of the business or mission can be classified as DCs of a ToD event. Hence, the next intended maneuvers (IMs) of a tele-operated driver at a particular location can be predicted. However, the actual driving maneuver during a turn depends on the driver inputs, design of the vehicle’s propulsion and dynamics. These factors are the foundation of the PCADS-CA method. This is computationally expressed with Eqs. (4.1), (4.2), and (4.3). As per these set of equations, tele-operated driver’s input, D_I , correlates to the IM D_M and D_M correlates to the DC, D_C . Based on this relevancy, PCADS-CA methods presented in algorithm 1, 2, and 3. Algorithm 1 detects the wrong turn at intersections, algorithm 2 detects the vehicle at intersection turning outside the expected time window and the intention of algorithm 2 is to reduce the false positive (FP) for known dynamic alerts.

$$D_C = f_1(m, \gamma, t, \omega, \tau, l, \varepsilon) \quad (4.1)$$

Where,

m = Mission (e.g., emergency vehicle, LMD, cross border transport, ride share).

γ = Road conditions (e.g., wet, dry, ice/snow, construction).

t = Traffic congestion (i.e., light, moderate, heavy).

ω = Weather conditions (i.e., clear, rain, fog, snow).

Algorithm 1: An anomalous maneuver detection at intersection – incorrect maneuver

Data: m, R, G, l, t, D_I, V
Result: A'_C
if m *is TRUE* **for** V **then**
 | $V(R, G) \leftarrow m(R, G)$;
 | initialize $D_{I_{Lat}}, D_{I_{Long}}, D_{I_{Mnvr}}$ for V ;
end
while $R \neq 0$ **do**
 | find Geo-code for all G ;
 | create data store E for V with: $D_{E_{Lat}}, D_{E_{Long}}, D_{E_{Mnvr}}$;
end
while $V \neq 0$ **do**
 | $D_{I_{Lat}}, D_{I_{Long}}, D_{I_{Mnvr}} \leftarrow l_{Lat}, l_{Long}, D_I$;
 | find $D_{I_{Lat}}, D_{I_{Long}} = D_{E_{Lat}}, D_{E_{Long}}$;
 | **if** $D_{I_{Mnvr}}$ *at* $D_{I_{Lat}}, D_{I_{Long}} \neq D_{E_{Mnvr}}$ *at* $D_{E_{Lat}}, D_{E_{Long}}$ **then**
 | set $A'_C = TRUE$ in E ;
 | **end**
end

τ = Current time.

l = Location of the vehicle.

ε = Dynamic factors (e.g., other road users and objects in the path, road blocks).

R = Planned route of the target vehicle for LMD (e.g., map data for depot, drop-off locations, directions, time window).

G = A list of all intersections for region of interest with geo-coding (i.e., latitude and longitude).

$$[D_M \in \{st, lt, rt, ut\}] = f_2(D_C) \quad (4.2)$$

Where,

st = Go straight, lt = Make left turn, rt = Make right turn, ut = Make U-turn.

$$[D_I \in \{Cmd_{str}, Cmd_{accl}, Cmd_{Brk}\}] = f_3(D_M) \quad (4.3)$$

Where,

Cmd_{str} = A steering command from ToD.

Cmd_{accl} = An acceleration control command from ToD.

Cmd_{Brk} = A brake control command from ToD.

\hat{H} denotes the vehicle health.

A'_C denotes the anomaly based on DCs.

Algorithm 2: An anomalous maneuver detection at intersection - incorrect time window

Data: m, R, G, l, t, D_I, V

Result: A'_C

while $V \neq 0$ **do**

$D_{I_{Lat}}, D_{I_{Long}}, D_{I_{Mnvr}} \leftarrow l_{Lat}, l_{Long}, D_I;$

find $D_{I_{Lat}}, D_{I_{Long}} = D_{E_{Lat}}, D_{E_{Long}};$

if $D_{I_{Mnvr}} \text{ at } D_{I_{Lat}}, D_{I_{Long}}, \neq D_{E_{Mnvr}} \text{ at } D_{E_{Lat}}, D_{E_{Long}}, D_{E_{Time}}$ **then**

set $A'_C = TRUE$ in $E;$

end

end

Algorithm 3: An anomalous maneuver detection at intersection – filtering dynamic alert

Data: $m, R, G, l, \epsilon, t, D_I, V, \hat{H}$

Result: A'_C

while $V \neq 0$ **do**

$D_{I_{Lat}}, D_{I_{Long}}, D_{I_{Mnvr}} \leftarrow l_{Lat}, l_{Long}, D_I;$

find $D_{I_{Lat}}, D_{I_{Long}} = D_{E_{Lat}}, D_{E_{Long}};$

if $D_{I_{Mnvr}} \text{ at } D_{I_{Lat}}, D_{I_{Long}}, \text{ tao} \neq D_{E_{Mnvr}} \text{ at } D_{E_{Lat}}, D_{E_{Long}}, D_{E_{Time}}$ **then**

if $\epsilon = NULL$ & $\hat{H} = OK$ **then**

set $A'_C = TRUE$ in $E;$

end

end

end

4.2.2 Stage 2: PCADS-Physics-based Anomaly Detection

The vehicle motion in tele-operated vehicles can be divided into two categories including cyber and physical elements. A driving maneuver command for steering, braking and acceleration received by vehicle falls under the cyber elements. On the other hand, a transfer of power from energy source to wheel, vehicle motion and dynamics is a part of physical elements. The working principle of these physical elements is the core of PCADS-PB method. The proposed framework of PCADS-PB model is outlined in Fig. 4.4. As illustrated in this

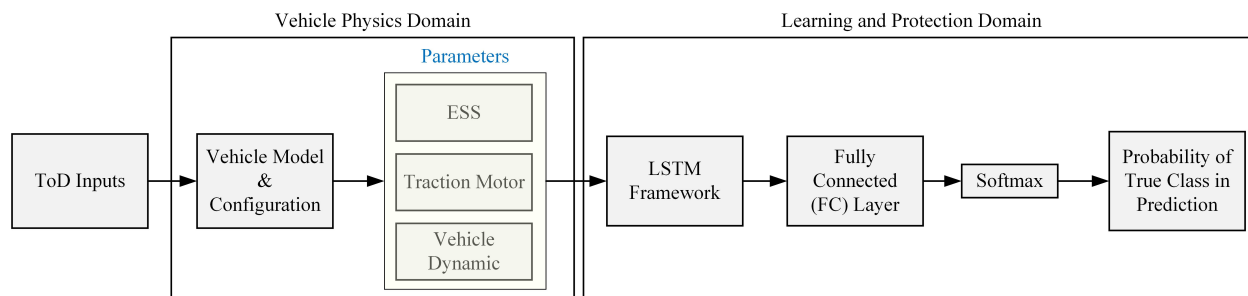


Figure 4.4: A Vehicle Physics-based Anomaly Detection Framework

diagram, the detection mechanism is divided into two domains including the vehicle physics domain and learning and prediction domain. When PCADS-PB algorithm receives the ToD input, it first enters the vehicle physics domain. Steering wheel angle, accelerator pedal and brake pedal are provided to the vehicle model and the output of vehicle’s model is passed on to the learning and prediction domain. In this domain, an ML algorithm is used to learn the correlation between output of vehicle physics domain to left turn, right turn and U-turn maneuvers. With an appropriate learning, the proposed method is intended to predict the anomaly in a time-series sequence of the vehicle physical parameters for the corresponding turning maneuver. LSTM algorithm is a type of RNN architectures that has proven to be very efficient to learn from complex sequential data to solve ML tasks [284, 285]. Thus, this algorithm has chosen as a base model for the learning and prediction domain. It should be noted that, vehicle’s models should be configured with power-train and vehicle dynamics of the target vehicle. For this research, drive-train is modeled as a full-electric vehicle; hence, the selected parameter for drive-train is from ESS and traction motor. In the following section, the mathematical model for each component of the PCADS-PB method is described in detail.

4.2.2.1 Proposed Mathematical Modeling

The proposed framework for the PCADS-PB process can be illustrated in Fig. 4.4.

Inputs As can be seen, the first step is the time-series ToD inputs including the acceleration-pedal-position (APP), steering-wheel-angle (SW), and the brake-pedal-status (BP) which can be defined as Eqs. (4.4) - (4.6):

$$\text{Acceleration-pedal-position (APP)} \rightarrow \{APP_{t-N}, \dots, APP_t\} \quad (4.4)$$

$$\text{Steering-wheel-angle (SW)} \rightarrow \{SW_{t-N}, \dots, SW_t\} \quad (4.5)$$

$$\text{Brake-pedal-status (BP)} \rightarrow \{BP_{t-N}, \dots, BP_t\} \quad (4.6)$$

Where N is the number of time steps, and t is the current time. Also, APP can be changed from 0 to 100% based on the discrete values, SW has an interval between -450 to 450 degrees, and BP is a binary (i.e., 0 or 1) input. Ultimately, the general input can be mentioned in equation (4.7):

$$\text{Inputs} = \{APP_{t-N}, SW_{t-N}, BP_{t-N}, \dots, APP_t, SW_t, BP_t\} \quad (4.7)$$

Vehicle Model & Configuration The vehicle's model and its configuration can influence how these inputs are translated into the motion and can be described as follows:

- Drivetrain Configuration: D with $D \in \{S, D, Q\}$ for single, dual, and quad motor configurations, respectively.
- Steering System: Assuming a kinematic model for simplicity.
- Tire Specification: Fixed for this model.

Drivetrain Dynamics: The drivetrain configuration influences the torque distribution to the wheels. For simplicity, we will consider a linear model where the APP linearly maps to torque output, modulated by the drivetrain configuration.

$$T_{output} = f_{trq}(APP_t, D) \quad (4.8)$$

Where T_{output} is the torque output and $f_{trq}()$ is a function that depends on APP and the drivetrain configuration D .

Steering Dynamics: SW_t can be directly related to the vehicle's turning radius or steering angle at the wheels through the kinematic steering model.

$$\theta_{steer} = g(SW_t) \quad (4.9)$$

Where θ_{steer} is the effective steering angle at the wheels, and $g(\cdot)$ represents a function mapping the SW to the wheel steering angle, considering factors such as steering ratio.

Braking Dynamics: The braking dynamics can be modeled as a binary effect on the vehicle's deceleration, considering BP.

$$a_{deceleration} = h(BP_t) \quad (4.10)$$

Where $a_{deceleration}$ is the deceleration due to braking, and $h(\cdot)$ is a function that maps the BP to deceleration force. This could be a simple binary model or a more complex one incorporating brake system dynamics.

- **Integration Into the Vehicle Motion:** The overall vehicle motion can then be determined by integrating these inputs and configurations into the equations of motion, considering both longitudinal and lateral dynamics. This involves solving differential equations that describe how the vehicle's velocity, position, and orientation change over time based on the inputs and configurations.

$$\frac{d(\text{Vehicle State})}{dt} = \Psi(T_{output}, \theta_{steer}, a_{deceleration}, \text{Vehicle Configuration}) \quad (4.11)$$

Where $\Psi(\cdot)$ shows the system of differential equations of vehicle dynamics.

Model Parameters Integrating the output of the “Vehicle Model and Configuration” with the “Vehicle Physical Parameters” requires a detailed mathematical model that encompasses ESS, motor characteristics, and vehicle dynamics (VD). This model will bridge the inputs related to vehicle control (i.e., APP, SW, BP) and the physical responses of the vehicle, taking into account the complexity added by different motor configurations. A summary of inputs along with the vehicle physical parameters are as follows:

- Accelerator Pedal Position (APP_t)
- Steering Wheel Angle (SW_t)
- Brake Pedal Status (BP_t)
- Drivetrain Configuration (D)
- ESS Parameters: Current (A), and power (W)
- Motor (M) Parameters: Torque (Nm), and Speed (rad/s)

- Vehicle Dynamic (VD) Parameters: Wheel Angle (WA), Roll (R), Pitch (PT), Yaw, and Acceleration in x, y, a directions (a_x, a_y, a_z)

ESS Dynamics: The ESS's dynamics can be modeled based on the power required by the motors:

$$P_{battery} = \sum_{n=1}^{N_m} (T_M \times \omega_M) \quad (4.12)$$

Where N_M is the number of motors (1 for single, 2 for dual, and 4 for quad), T_{Mi} is the torque output of motor i , and ω_{Mi} is the rotational speed of motor i . The battery current $I_{battery}$ can be calculated by dividing $P_{battery}$ by the battery voltage $V_{battery}$.

Motor Dynamics: Motor torque and speed are functions of the accelerator pedal position and the vehicle's current state. For each motor configuration:

$$T_{Mi} = f_{Torque}(APP_t, D) \quad (4.13)$$

$$\omega_{Mi} = f_{Speed}(V_{vehicle}, D) \quad (4.14)$$

Vehicle Dynamics: Vehicle dynamics incorporate the effects of steering, braking, and acceleration inputs on the vehicle's orientation and position:

- WA is directly influenced by SW_t .
- R, PT, Yaw dynamics can be derived from the vehicle's motion, considering gravitational forces, lateral forces during turns, and acceleration/deceleration.
- Acceleration (a_x, a_y, a_z) is influenced by the forces generated by the motors (forward/backward), lateral forces (during turning), and vertical forces (from road surface).

$$VD = \Psi_{VD}(T_{output}, \theta_{steer}, a_{deceleration}, ESS, \text{Motor Dynamics}) \quad (4.15)$$

LSTM Framework The parameters from the previous step can be defined as follows:

- $VD_t = [WA_t, R_t, PT_t, Yaw_t, a_{x,t}, a_{y,t}, a_{z,t}]$.
- Traction Motor: $M_t = [T_M, \omega_M]$ multiplied by the number of motors based on the configuration.
- ESS: $E_t = [I_{battery}, P_{battery}]$.

Hence, we can find the $x_t = [E_t, M_t, VD_t]$. We will maintain the LSTM cell equations but elaborate on the input vector:

1. Input Gate: $i_t = \sigma(W_{xi} \cdot x_t + W_{hi} \cdot h_{t-1} + b_i)$
2. Forget Gate: $f_t = \sigma(W_{xf} \cdot x_t + W_{hf} \cdot h_{t-1} + b_f)$
3. Cell State: $g_t = \tanh(W_{xg} \cdot x_t + W_{hg} \cdot h_{t-1} + b_g)$, & $c_t = f_t \cdot c_{t-1} + i_t \cdot g_t$
4. Output Gate: $o_t = \sigma(W_{xo} \cdot x_t + W_{ho} \cdot h_{t-1} + b_o)$, & $h_t = o_t \cdot \tanh(c_t)$

As described, a monitoring of vehicle physical parameters over time during turning maneuver is considered as a sequence to the class relation. While performing the classification process for a given set of time-series sequential data, the LSTM model calculates the probability scores corresponding to each class. In this case, the class indicates the left turn, right turn and U-turn. The PCADS-PB model assesses the probability score assigned to each of turns for a given set of vehicle physical parameters in sequence, as shown in Algorithm 4. If the probability score does not satisfy the criteria for the known expected turn, then an

Algorithm 4: The physics-based anomaly detection Score

Data: $Turn_{Expected}, \log P(Turn_{All})$
Result: A'_P
if $\log P(Turn_{Expected}) < \log P(Turn_{Other})$ **then**
 | A'_P is TRUE;
end

anomaly is reported. A discussion of the experimental results will be presented in the next section.

CHAPTER 5

Experiments and Result

In chapter 5, experimental set up, steps and results conducted for this research are discussed. There are two main sections in this chapter. In the first part, case study and results proposed integrated TARA approach for AV perception is presented. This includes the impact rating calculation with a object-focused risk evaluation utilizing real traffic crash data and usability of proposed AI robustness factor for holistic evaluation AI based perception system for AV during normal, abnormal and adversarial scenarios. In the second part, false data injection (FDI) to steering wheel angle for ToD and proposed PCADS method for anomaly detection for LMD application are presented.

5.1 Case Study: Integrated Approach of Threat Analysis for AV

A case study with the proposed method of integrated approach of threat analysis for AV is presented in this section. Impact rating with this framework is demonstrated with real data from traffic crashes where the most important objects are impacted. Also, the effect of the robustness of the detection algorithm on attack feasibility assessment is illustrated with some AI/ML-based state-of-the-art detection algorithms used in AVs.

5.1.0.1 Impact Rating for Different Objects from Traffic Crash Data

This section presents the real traffic crash data along with the calculations for impact ratings for different objects. Table 5.1 demonstrates the different parameters in impact rating (I_{USecX}) considering humans, bicyclists & motorcyclists, animals, and vehicles involved in car crashes. The real data was extracted from the Michigan Traffic Crash Facts (MTCF) and National Safety Council – Injury Facts [286, 287] for crashes in December 2022 in Michigan State. This data is categorized based on four groups, including fatal injury, suspected serious injury, suspected minor & possible injury, and no injury, to calculate the parameters

Table 5.1: Impact Rating Parameters for Different Objects on the Road Based on Real Traffic Crash Data

Objects	Severity ($S_{L,U\text{Sec}X}$)	Occurrence ($O_{H,U\text{Sec}X}$)	Recovery time (months) ($T_{L,U\text{Sec}X}$)	Financial loss (M\$) ($\Gamma_{L,U\text{Sec}X}$)
Human (i.e., Pedestrian)	1.298	0.0253	4.65	259.9
Bicyclist & Motorcyclist	0.788	0.00663	2.15	25.3
Animal	0.0208	0.753	0.044	22.9
Vehicle	0.191	0.2147	0.48	204.8

involved in equation (3.3). The severity levels are considered severe (3), high (2), moderate (1), and low (0), respectively, for different objects involved in crashes. The first parameter, severity, can be calculated for the pedestrians involved in crashes based on different levels of injuries as follows:

$$\begin{aligned}
 \text{Severity} &= \\
 &\left(\text{Severe} \times \frac{\text{Fatal Injury}}{\text{Total Crash Count}} + \text{High} \times \frac{\text{Suspected Serious Injury}}{\text{Total Crash Count}} \right. \\
 &\left. + \text{Moderate} \times \frac{\text{Suspected Minor \& Possible Injury}}{\text{Total Crash Count}} + \text{Low} \times \frac{\text{No Injury}}{\text{Total Crash Count}} \right) \\
 &= 3 \times \frac{23}{198} + 2 \times \frac{37}{198} + 1 \times \frac{114}{198} + 0 \times \frac{24}{198} = 1.298
 \end{aligned}$$

Similarly, other severity values can be found for different objects on the road. Occurrence can be found according to the total crash count (i.e., 198) for pedestrians divided by the total crash count (i.e., $198 + 52 + 5907 + 1683 = 7840$) for all objects (e.g., $\frac{198}{7840} = 0.0253$) to show the presence of objects according to the traffic crashes on the road. This is the same procedure to find other *Occurrence* values for different objects. Assume a range of recovery times within each category including fatal (9 – 12 months), serious (6 – 9 months), minor/possible (1 – 3 months), and no injury (0). The average recovery time for each category using the midpoint can be found. A sample calculation of the average recovery time (months) for pedestrians can be $\frac{23 \times 10.5 + 37 \times 7.5 + 114 \times 2 + 24 \times 0}{198} = 4.65$ months, and a similar process can be carried out for bicyclists and motorcyclists, animals, and vehicle items. Regarding the average costs per injury category, it is necessary to define the average costs for each injury category. These can vary significantly depending on factors (e.g., location, healthcare costs, legal settlements, and lost wages). Some rough estimates can be mentioned as follows:

- Fatal Injury: \$10,000,000 (assuming high cost of life, medical expenses, and lost wages)
- Suspected Serious Injury: \$500,000 (assuming moderate cost of medical treatment and lost wages)
- Suspected Minor Injury & Possible Injury: \$100,000 (assuming lower cost of medical treatment)
- No Injury: \$0 (assuming no immediate financial loss)

An example of the financial loss calculations based on the pedestrian object can be represented as follows:

- Fatal Injury: 23 pedestrians \times \$10,000,000/pedestrian = \$230,000,000
- Suspected Serious Injury: 37 pedestrians \times \$500,000/pedestrian = \$18,500,000
- Suspected Minor Injury & Possible Injury: 114 pedestrians \times \$100,000/pedestrian = \$11,400,000
- No Injury: 24 pedestrians \times \$0/pedestrian = \$0

Total Estimated Cost: \$230,000,000 + \$18,500,000 + \$11,400,000 + \$0 = \$259,900,000

According to Table 5.1, human object category demonstrates the highest impact rating among objects, according to real traffic crash data. I_{USecX} index can be advantageous in terms of different parameters including damage severity, presence of different objects on the road, average recovery time after damage occurrence, and financial loss. According to real crash data in Michigan State, a thorough analysis of different objects considering indexes can be carried out. For instance, even though the occurrence index ($O_{H,USecX}$) for animals is significantly higher than other objects, this object category has lower average values for severity, recovery time, and the loss. Also, different level of injuries considered which the most vulnerabilities have been obtained to humans and vehicles, respectively.

5.1.1 Attack Feasibility Assessment with AI Robustness Factor

The section details three case studies that utilize a modified formula incorporating an AI robustness factor to assess attack feasibility. Currently, in the absence of a standardized robustness metric, the prevailing practice is to gauge AI's resilience based on conventional performance metrics amidst defensive scenarios. ROC curve, accuracy, precision, recall, and F1-score are some of the common metrics that are used for evaluating AI performance. In this paper, the performance metrics provided by the authors are translated to RF factor as per Fig. 5.1 along with other parameters. For the first two cases, it is assumed that performance of the perception algorithm is good in normal and abnormal scenarios to highlight the effect on RF and attack feasibility due to adversarial

attacks. First example is for speed limit sign detection with same defense model for multiple attacks and the second one is for object detection under the same attack with multiple defense methods [229, 230]. These case studies are shown with attack type, defense method, attack potential and attack feasibility values in Table 5.2. The third case is presented to show the comparison of attack feasibility ratings when the defense method is completely missing for AI perception algorithm under adversarial attack and performance is poor for abnormal scenarios. This example is crafted based on the performance of traffic cone detection in abnormal scenarios [288] and then assumed perception will be poor under adversarial attack. In Fig. 5.2, a comprehensive risk assessment approach with an AI robustness factor from our proposed integrated TARA method is presented.

SE		KoIC		Eq		RF	
Layman	0	Public	0	Standard	0	Performance: Normal scenarios = Poor Abnormal scenarios = Poor Adversarial attacks = Poor	0
Proficient	1	Restricted	1	Specialized	1	Performance: Normal scenarios = Good Abnormal scenarios = Poor Adversarial attacks = Poor	1
Expert	2	Sensitive	2	Custom-built	2	Performance: Normal scenarios = Good Abnormal scenarios = Good Adversarial attacks = Poor	2
Multiple Experts	3	Critical	3	Multiple Custom-built	3	Performance: Normal scenarios = Good Abnormal scenarios = Good Adversarial attacks = Good	3

ET		WoO	
< a day	0	Unlimited	0
< a week	1	Easy	1
< a month	2	Moderate	2
> a month	3	Difficult	3

Parameter (ϕ)	Attack potential description and value (V)
----------------------	--

Figure 5.1: Evaluation of Attack Potential in Compliance with ISO/IEC 18045 Parameters

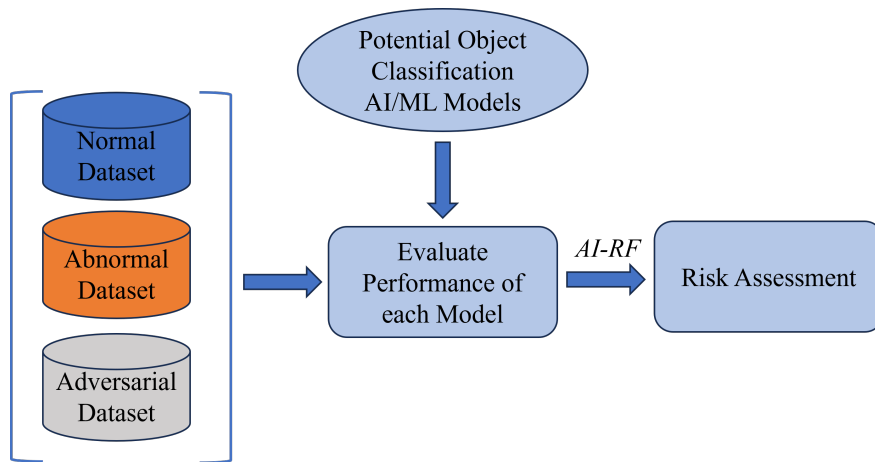


Figure 5.2: A Comprehensive Risk Assessment Based on the AI Robustness Factor for AV Perception Datasets

In this approach, potential AI/ML models for AV perceptions systems can be evaluated against normal, abnormal and adversarial dataset. For each model AI RF can be assigned based on Fig. 5.1 and provided to risk assessment formula according to equation 3.2.

Table 5.2: Attack Feasibility Calculations for Different AI Algorithms’ Robustness for Perception Systems

#	Attack feasibility assessment							Attack feasibility
	\mathbf{V}^{ET}	\mathbf{V}^{SE}	\mathbf{V}^{KoIC}	\mathbf{V}^{WoO}	\mathbf{V}^{Eq}	\mathbf{V}^{RF}	$\sum \mathbf{V}$	
1.	4	3	3	0	4	3	17	Low
2.	1	3	3	0	0	2	9	Moderate
3.	1	3	3	0	0	1	8	High

Case 1 - Attack: poster-printing attack I-FGSM, C&W, Deepfool, JSMA.
Defense method: SVD-based optimal approximation with 5G.
Performance: accuracy score (80%–90%). hence determined as good performance.

Case 2 - Attack: a patch on the back of a truck placed in front of the camera.
Defense method: FPDA, Z-mask, HyperNeuron.
Performance: 0.5–0.6 AUROC. hence determined as poor performance.

Case 3 - Performance for the abnormal scenario is 65.8%.

Assumption 1: For Cases 1 and 2, performance is good in normal and abnormal scenarios.
Assumption 2: For Case 3, performance is good in normal but there is no defense against adversarial scenarios.

As per our analysis, a decrease in AI RF enables lower values of SE , ET , and Eq for a successful attack. As a result, the attack feasibility is high when AI RF is low. When this is combined with abnormal scenarios, as shown in Case 3, the cumulative attack feasibility also increases. It can be interpreted as a higher risk according to equation 3.2. In Fig. 5.3, an AI/ML model performance for normal, abnormal and adversarial scenarios based on different case studies from Table 5.2 is shown as a bar chart for a comparative view.

A prediction value near to 0 represents model performance is not evaluated or shown poor performance and 1 and 2 values represent moderate and good performance, respectively. It can be noted that these models have not shown the comprehensive good results against normal, abnormal and adversarial scenarios as shown in an hypothetical example of ideal robust AI/ML model on the right side of the chart.

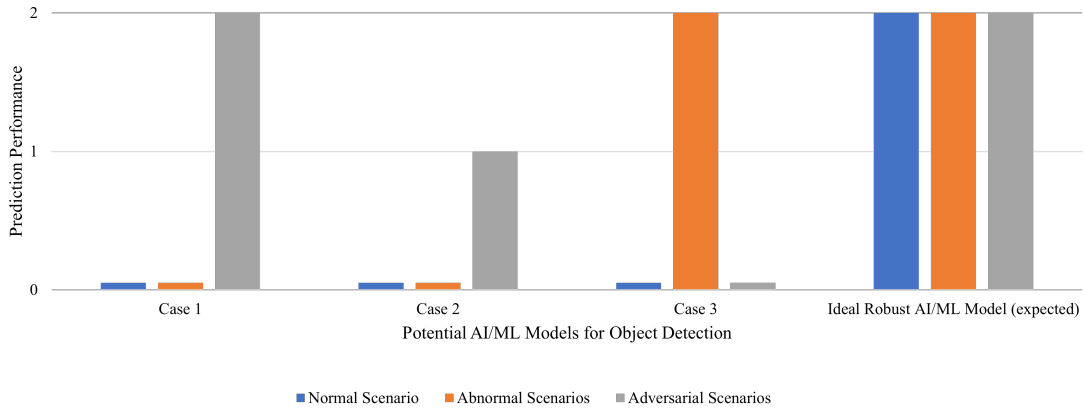


Figure 5.3: A Comparative Example of an AI Robustness Factor Evaluation Considering Case Studies from Table II for Normal, Abnormal, and Adversarial Scenarios

5.2 Case Study: PCADS for Detecting FDI Attacks on Steering Command in LMD Application

In this section, the experimental set up to evaluate the proposed anomaly detection method, PCADS is presented. Experimental steps are broadly divided into two parts. In first part, experiments focus is on context-ware anomaly detection of PCADS. For this, a teleoperated vehicle delivery scenario is created using open source route planner and then original route plan for the delivery is manipulated with false data to create attack. It should be noted for this experiment it is assumed the delivery vehicles follows the planned route and the estimated time window at each location. The original route plan and manipulated route plan is used as input to context-aware anomaly detection subsystem. In the second part, the focus is on physics-based anomaly detection in trajectory of the teleoperated vehicle during the left turn, right turn and u-turn. For this experiemnt, a real dataset known as D2CAV (by Behrad et al.) [289] was selected as good data and attack data is created by injecting false data using the attack formulation described in section 3.2.1. Original data and attack data are used to evaluate proposed physics-based anomaly detection.

5.2.1 Original Dataset for Driving Maneuver

A real dataset known as D2CAV (by Behrad et al.) was selected as Good Data. This data is collected with Ford vehicle during left turn, right turn and U-turn. Dataset contains time series value of steering wheel angle, accelerator position and brake pedal status at sample rate of 100 ms. Minimum 65 observations for each type of turn are selected as good dataset for this research.

5.2.2 Context-aware Anomaly Detection

The experiment steps for context-aware part of PCADS is as follows:

- creation of example data for teleoperated delivery route with turns at multiple intersection.
- manipulating intended turn action to create mismatch in turning maneuver from the original route.
- manipulating the time of the intended turn at a particular location.
- adding a dummy dynamic alert signal.
- applying context-aware anomaly detection algorithm 1, 2 and 3, to above created original data and false data.

First, an original route plan for a delivery vehicle is created with web-based route planning service from *MyRouteOnline* [290]. This provides the IM at each intersection along the delivery route derived from DCs. This corresponds to IM and DC processes in Fig. 4.3. Secondly, the ToD input is created by altering the original route which includes the expected turn at certain intersection along the route and the modification of the expected time window of the turn. Additionally, an input is added to indicate if there is any dynamic alert on a particular intersection. In the final step, IM from step 1 and altered ToD input and dynamic alert from step 2 are passed to the PCADS-PB algorithm proposed in Section 4. This algorithm is written in MATLAB scripting language and executed with MATLAB version 2023a in Microsoft Windows 10 environment. The plots are generated using `plotPosition`, `ploteroute` and `geoplayer` functions in MATLAB. For hardware, a computer with a 12th Gen Intel(R) Core(TM) i7-12850HX, 2100 Mhz, 16 Core(s), 24 Logical Processor(s) and 64 GB RAM. Results from the above experiments are presented in three steps as with Fig. 5.4 , 5.5 and 5.6. In Fig. 5.4, the focus is to detect the anomaly in driving action at a particular location (intersection). In this figure, the snapshot of original route plan for the teleoperated delivery vehicle is provided in a table on the left side and the map is shown on the right side. The table captures the geocodes from start to stop with intersection and the expected ToD action from original route plan. On the map the expected route and ToD action is marked as solid blue line. The red line on the map represents when the driving action at certain intersection was altered to simulate an attack. The second experiment is to detect the anomaly in ToD action with respect to the time-window and this is shown in Fig. 5.5. In addition to geocode information the ETA and actual arrival times are also shown in the tabular part of this figure. On the map the blue dots mean the actual ToD action at those intersections met the expected action and time-window. However, the the red dots mean the ToD action at those intersections happened outside the expected time-window. The third part of the experiment is shown in Fig. 5.6 which

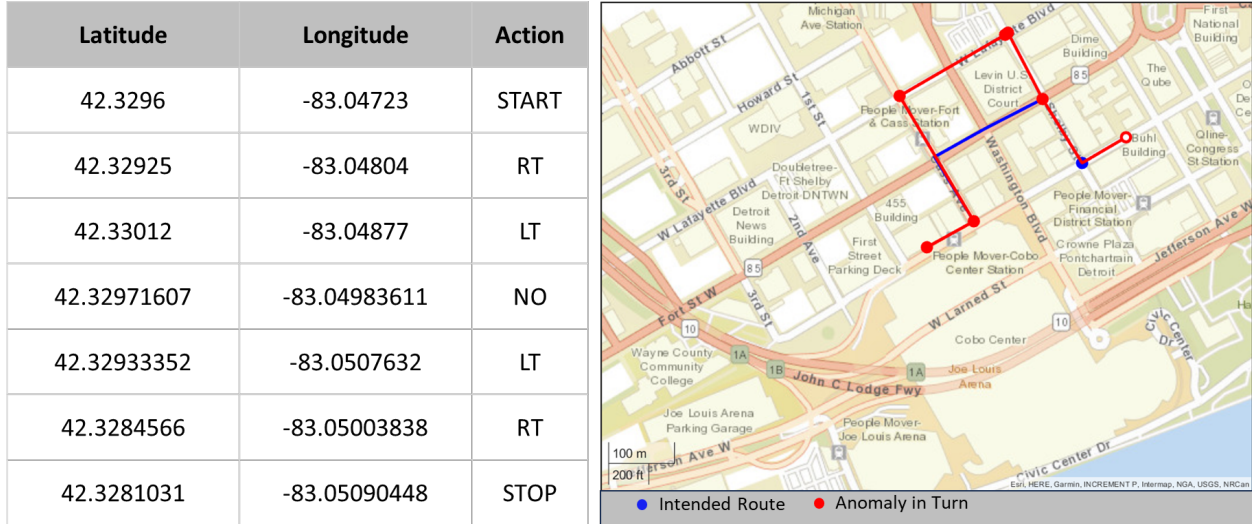


Figure 5.4: Context-aware Anomaly Detection - Incorrect Turn

shows that the proposed algorithm can filter out if a dynamic alert notification is provided by an in-vehicle or external alert system. According to this figure, the table shows the DC including the original intended maneuvering action for intersections along the selected delivery route. The right most column shows the dynamic alert for an intersection. The map shows the results of combined PCADS-CA detection. According to this diagram, the blue line indicates the original route and blue dots denotes the intersection along the route. The red dots indicate that PCADS-CA method’s detected anomalies in an actual maneuver from the intended action. However, the results also notify about the dynamic alerts at intersections along the route with yellow dots. Generally, the results illustrate that the PCADS-CA model can detect the first stage of anomalies based on the DC. Further, it also provides notification dynamic alerts to reduce FPs due to some obstruction or emergency has been received by the vehicle. It can be noted that robustness of this method requires the delivery vehicle routing plan to be efficient and vehicle has the ability to receive real-time update of dynamic situations.

5.2.3 Physics-based Anomaly Detection

This section elaborates the experiment and results with physics-based AD stage of the PCADS model. The flow of the experiments is described as follows, 1) data selection and generation, 2) training the model with data without injected noise and 3) anomaly detection when noise is injected. MATLAB classification learner application and deep learning toolbox in MATLAB 2023a version are used for training and testing of the ML models for PCADS-PB experiments. Each of these three steps is discussed with the results below.

Latitude	Longitude	ETA	Actual Arrival Time
42.32931441	-83.04636048	910	910
42.329258237	-83.04742661	915	915
42.3283979	-83.05016232	921	921
42.32825425	-83.05051565	926	922
42.33012383	-83.0487764	932	932
42.33013	-83.0487645	937	941

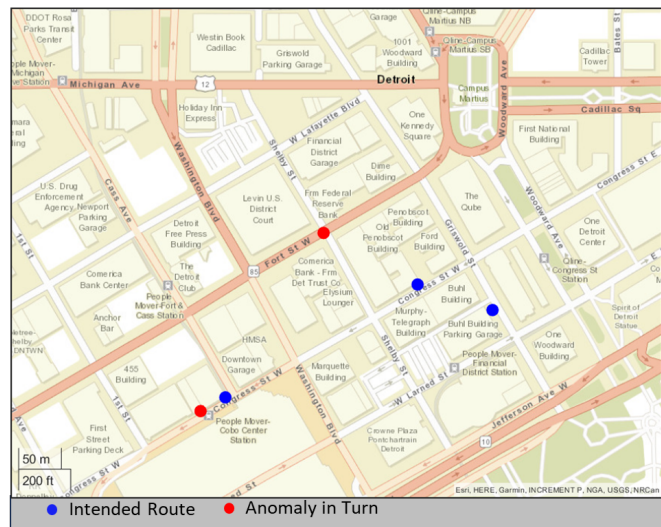


Figure 5.5: Context-aware Anomaly Detection - Incorrect Time

Latitude	Longitude	Action	Alert
42.3296	-83.04723	START	NULL
42.32925	-83.04804	RT	NULL
42.33012	-83.04877	LT	NULL
42.32971607	-83.04983611	NO	DETOUR
42.32933352	-83.0507632	LT	VEH_HEALTH
42.3284566	-83.05003838	RT	NULL
42.3281031	-83.05090448	STOP	OBJECT

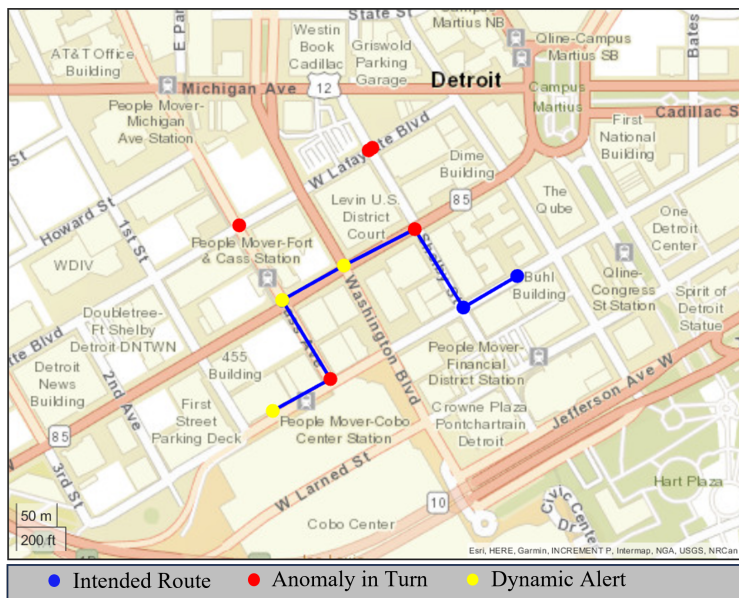


Figure 5.6: Context-aware Anomaly Detection - Filtering Dynamic Alert

5.2.3.1 Data Selection and Generation

An dataset to experiment with PCADS-PB model is generated based on the real dataset known as “D2CAV.” The dataset contains of 75 left turn, 78 right turn, 62 U-turn scenarios. As per the scope of this paper, steering wheel angle, accelerator pedal and brake pedal signals are extracted from this dataset. The signals are recorded every 100 ms. This dataset is used as a good ToD input dataset. In the next step, 31 observations are randomly selected from the left turn, right turn and U-turn scenarios and a FDI attack dataset is created by injecting noise to the steering wheel angle in these 31 observations. The noise is injected using the attack formula, shown in equation (3.6) and is implemented using MATLAB. As illustrated in Fig. 5.7, an attack dataset consists two points of injection in the steering wheel angle command and the duration of the injected noise is 2 seconds. The points of injection are close to the beginning of turns and around the mid-point of turning. These two datasets are termed as P1 noise real data, and P2 noise real data. In the final step, a virtual vehicle model is used to generate dataset for vehicle physical parameters. The virtual vehicle model is selected as an electric drive train with six degrees of freedoms. Vehicle physical parameters are selected from three subsystems including ESS, traction motor and vehicle dynamics. Virtual vehicle model is configured and simulated using virtual vehicle composer application in MATLAB MATLAB/SIMULINK software. One dataset of the vehicle physical parameters is created with the good ToD input dataset and two datasets are created for the attack dataset with P1 and P2 noise injection, these are named as P1 noise virtual vehicle data, and P2 noise virtual vehicle data.

5.2.3.2 Model Training and Testing with Real Data

In section 4.2.2 it was discussed that the proposed PCADS-PB formulates the anomaly detection problem in trajectory patterns during turning maneuvers as a sequence to a classification problem. However, before detecting the anomaly in turning maneuver, the model needs to be trained with the known normal observations of right turn, left turn and u-turn. The dataset with steering wheel angle, accelerator pedal, brake pedal, vehicle speed and heading angle for aforementioned maneuvers from the real data are used to train the ML models in this experiment. Moreover, for a sequence to classification training approach, it is important to compare and select the appropriate region of the sequence in each observation. For this reason, the first set of experiments for PCADS-PB is conducted with two set of sequences from the original real dataset described in the section 5.2.3.1. The first set of sequence is chosen as the entire sequence of 40 seconds for each observation and the other set of the training sequence is a shorter duration where the actual turning maneuver happens. The performance of testing with these two set of sequences for real data are presented in Tables 5.3 and 5.4.

Table 5.3 represents the result from first set which is the entire 40 seconds of sequence and Table 5.4 represents the sequence narrowed down to the duration of the maneuvers. The left most column in both of tables show the ML algorithms used for training. Based on the literature review in section 2.7, for this classification problem, three types of ML algorithms are chosen. First one is

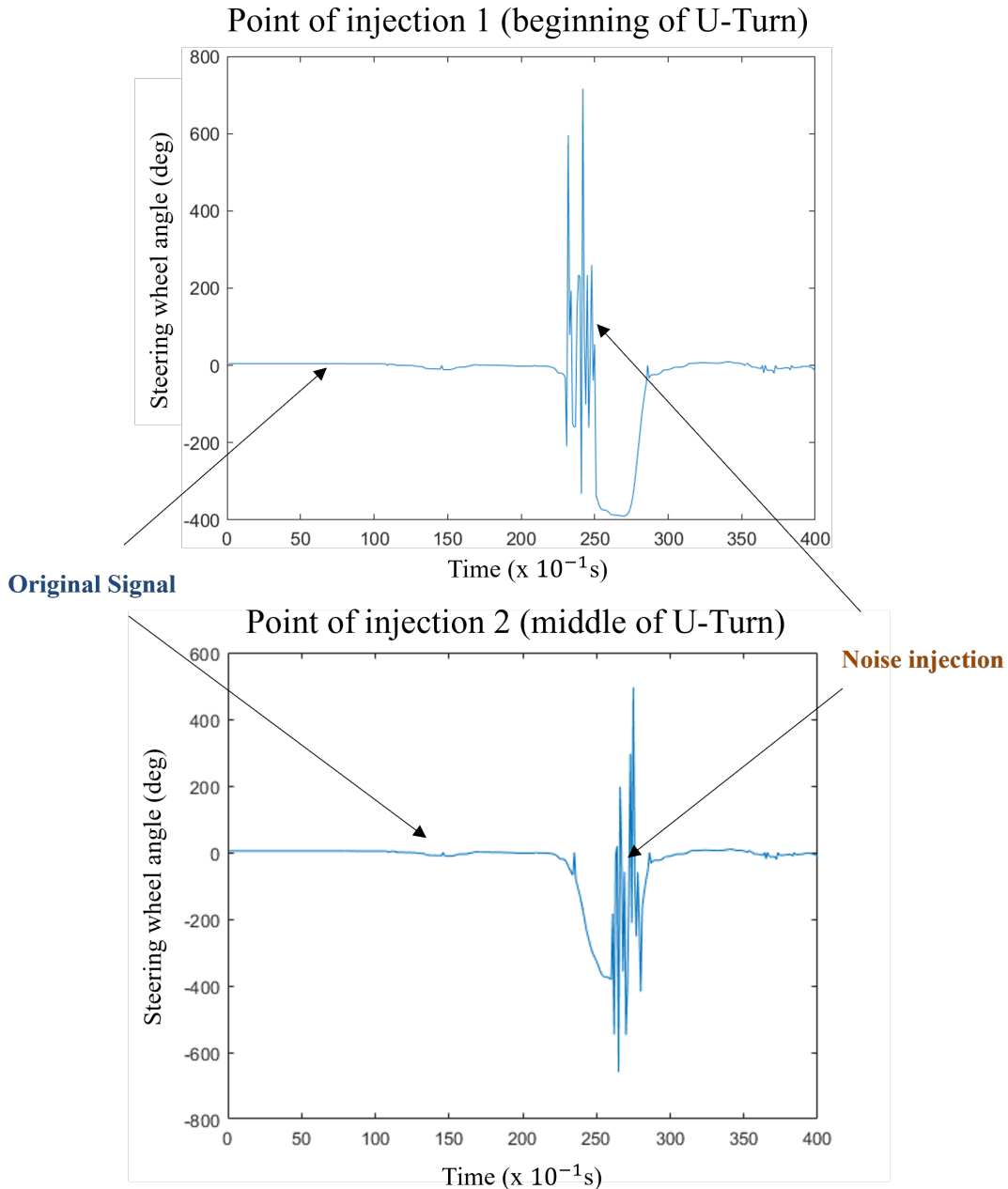


Figure 5.7: An Example of Attack on Steering Wheel Command by Noise Injection

a tree based classifier which is a popular method of classification in tradition ML. The second set of algorithms are neural network (NN) based architecture of various depth and the third one is LSTM which is DL based approach widely popular for sequence to classification problem. The columns, “Accuracy,” “Precision,” “Recall,” and “F1-score” represent the commonly used ML metric that to evaluate ML performance. The values in these columns correspond to the type of maneuver mentioned in the column “Class”. These values range from 0 to 1, where a higher value represents

Table 5.3: A Comparison of ML Algorithms for Good Dataset with Entire Sequence

Classifier Type	Class	Accuracy	Precision	Recall	F1-score
Tree	Left Turn	0.85	0.78	0.83	0.80
	Right Turn	0.94	0.92	0.92	0.92
	U-Turn	0.89	0.84	0.77	0.81
Narrow NN	Left Turn	0.80	0.73	0.68	0.70
	Right Turn	0.89	0.83	0.88	0.86
	U-Turn	0.86	0.76	0.76	0.76
Medium NN	Left Turn	0.87	0.88	0.75	0.81
	Right Turn	0.92	0.84	0.97	0.90
	U-Turn	0.91	0.85	0.82	0.84
Wide NN	Left Turn	0.87	0.86	0.75	0.80
	Right Turn	0.91	0.82	0.97	0.89
	U-Turn	0.93	0.91	0.84	0.87
Bi-layered NN	Left Turn	0.81	0.74	0.69	0.72
	Right Turn	0.89	0.82	0.88	0.85
	U-Turn	0.88	0.80	0.79	0.80
Tri-layered NN	Left Turn	0.82	0.75	0.72	0.73
	Right Turn	0.87	0.83	0.82	0.83
	U-Turn	0.86	0.74	0.79	0.77
LSTM	Left Turn	0.99	0.99	0.99	0.99
	Right Turn	0.95	0.99	0.89	0.94
	U-Turn	0.95	0.83	0.99	0.91

better ML performance. It should be noted that accuracy for ML classification problem provides the measure of correctness of the model. It is calculated as total number of true positives (TP) and true negatives (TN) divided by total number of observations. The precision is a measurement of positive predictions, and it is calculated as TP predictions divided by the total of TP and false positive (FP) predictions. The recall focus on the quality of negative predictions and it is calculated as TP divided by the sum of TP and false negatives (FN). F1 Score is a popular metric to have a comprehensive evaluation of classification models. F1-score helps to interpret ML performance to

Table 5.4: A Comparison of ML Algorithms for Good Dataset with Sequence Focused at Maneuvering Duration

Classifier Type	Class	Accuracy	Precision	Recall	F1-score
Tree	Left Turn	0.97	1.00	0.91	0.95
	Right Turn	1.00	1.00	1.00	1.00
	U-Turn	0.97	0.91	1.00	0.95
Narrow NN	Left Turn	0.94	0.85	1.00	0.92
	Right Turn	0.97	1.00	0.90	0.95
	U-Turn	0.97	1.00	0.90	0.95
Medium NN	Left Turn	0.97	0.92	1.00	0.96
	Right Turn	1.00	1.00	1.00	1.00
	U-Turn	0.97	1.00	0.90	0.95
Wide NN	Left Turn	0.94	0.85	1.00	0.92
	Right Turn	0.97	1.00	0.90	0.95
	U-Turn	0.97	1.00	0.90	0.95
Bi-layered NN	Left Turn	0.97	1.00	0.91	0.95
	Right Turn	1.00	1.00	1.00	1.00
	U-Turn	0.94	0.90	0.90	0.90
Tri-layered NN	Left Turn	0.94	0.85	1.00	0.92
	Right Turn	0.97	1.00	0.90	0.95
	U-Turn	0.97	1.00	0.90	0.95
LSTM	Left Turn	1.00	1.00	1.00	1.00
	Right Turn	1.00	1.00	1.00	1.00
	U-Turn	1.00	1.00	1.00	1.00

have a balance between high precision and high recall. By comparing the metric values between Tables 5.3 and 5.4, it can be derived that for the known normal observations of left-turn, right and u-turn from the real dataset the performance is better when ML model is trained with the sequence focused on the duration rather than the entire duration of the observation. Also, it can argued that a narrower sequence can reduce the model computation load. Based on this comparative analysis the model corresponding to Table 5.4 is used for further experiments in this research. The next set

of experiments focus on the anomaly detection with this trained model when noise injected in real data.

5.2.3.3 Anomaly Detection in Real Data with Noise

This section presents the experiments and result for anomaly detection in real data with PCADS-PB approach. While reviewing the ML approaches in section 2.7, it was discussed that softmax function is commonly used in the output layer of NN for classification problem with multi-class in the dataset. The softmax function assigns decimal probabilities to each class in a multi-class during prediction. The output of softmax function was used in section 4.2.2 while defining the anomaly detection framework, mathematical model and algorithm for PCADS-PB. Therefore, as a first step the probability density score (the output of softmax function) were analyzed for observations with true and false predictions. important to elaborate the concept NN architecture reviewed with a perspective of this experiment. An example of this analysis is presented in Table 5.5. It might be

Table 5.5: Example of Prediction Probability Score with Softmax Function

Left Turn	Right Turn	U-Turn	Prediction	Test	Status
0.05	0.92	0.03	‘RT’	‘RT’	TRUE
0.86	0.08	0.07	‘LT’	‘LT’	TRUE
0.05	0.03	0.91	‘UT’	‘UT’	TRUE
0.10	0.85	0.04	‘RT’	‘UT’	FALSE
0.05	0.93	0.02	‘RT’	‘UT’	FALSE
0.94	0.01	0.05	‘LT’	‘RT’	FALSE

noted that the probability score ranges from 0 to 1. As shown in Table 5.5, the highest probability score observed by an ML classifier for a particular class reported as a predicted class. When the predicted class matches the true class provided in a test sample, the prediction is TRUE (shown with a green color) while the prediction is FALSE, when the probability score of the true class is not the highest one (shown with a red color). This observation supports the hypothesis proposed in Algorithm 4.

As next step, the ML models trained as part of Table 5.4 are tested with the two noise injected datasets termed as “P1,” and “P2” in section 5.2.3.1. The results are presented in Table 5.6. According to this table, for noise injected datasets “P1 noise real data,” and “P2 noise real data” tree-based method could detect 1 out of 31 FDI samples for each datasets. LSTM based approach could detect 10 anomaly for “P1 noise real data,” and 7 anomalies for “P2 noise real data.” The neural network based approach detected approximately 20 anomalies out of 31 FDI for “P1,” and “P2” point of noise injection combined.

Table 5.6: Anomaly Detection in Real Data with Noise

Classifier Type	P1 noise real data		P2 noise real data	
	No. of FDI Tested	No. of Anomaly Detected	No. of FDI Tested	No. of Anomaly Detected
Tree	31	1	31	1
Narrow NN	31	21	31	20
Medium NN	31	21	31	20
Wide NN	31	21	31	20
Bilayered NN	31	18	31	21
Trilayered NN	31	20	31	21
LSTM	31	10	31	7

It may be noted, that the model used for anomaly detection in this part of the experiment is directly from the real dataset which contains steering wheel angle, accelerator pedal, brake pedal signals, vehicle speed and heading angle. Vehicle physical parameters for vehicle dynamics such as yaw, roll, pitch and parameters for traction motor and energy storage are not part of real dataset. Therefore, the next part of the experiment is conducted with the virtual vehicle dataset generated with the inputs from real dataset as described in section 5.2.3.1.

5.2.3.4 Experiment with Virtual Vehicle Data

In this part of the experiment, the proposed PCADS-PB approach is applied on the virtual vehicle dataset. As described in the data generation part before, the input from real dataset was used as input to a virtual vehicle created in MATLAB/Simulink environment. This virtual vehicle is configured as BEV with a single traction motor. From the simulation of this virtual vehicle with inputs from real dataset the vehicle physical parameters for vehicle dynamics, traction motor and HV battery are recorded to create the good dataset for virtual vehicle. Further, similar to experiment with real data, this virtual vehicle dataset is used to train the ML algorithms focusing on the sequence around the maneuver labeled for each observation. The same set of ML algorithms used in training with real data are chosen to train the models with virtual vehicle data. For ease of comparison, the result of with testis presented in Table 5.7 in a similar format of Table 5.4 for real data. From a comparative analysis of Table 5.7 and Table 5.4, it may be noted that the overall performance to predict the correct maneuver from the vehicle physical parameters of virtual vehicle good dataset is in the higher range and similar to performance of models trained with

real data. Therefore, as a next step these trained models with virtual vehicle dataset are used for anomaly detection experiment with virtual dataset. It is important to mention the “P1 noise

Table 5.7: A Comparison of ML Algorithms for Virtual Vehicle Good Dataset with Sequence Focused at Maneuvering Duration

Classifier Type	Class	Accuracy	Precision	Recall	F1-score
Tree	Left Turn	0.94	0.91	0.91	0.91
	Right Turn	1.00	1.00	1.00	1.00
	U-Turn	0.97	1.00	0.91	0.95
Narrow NN	Left Turn	0.90	0.90	0.82	0.86
	Right Turn	0.97	1.00	0.90	0.95
	U-Turn	0.94	0.83	1.00	0.91
Medium NN	Left Turn	0.94	0.91	0.91	0.91
	Right Turn	1.00	1.00	1.00	1.00
	U-Turn	0.94	0.90	0.90	0.90
Wide NN	Left Turn	0.90	0.83	0.91	0.87
	Right Turn	0.97	1.00	0.90	0.95
	U-Turn	0.94	0.90	0.90	0.90
Bi-layered NN	Left Turn	0.94	0.91	0.91	0.91
	Right Turn	1.00	1.00	1.00	1.00
	U-Turn	0.94	0.90	0.90	0.90
Tri-layered NN	Left Turn	0.94	0.91	0.91	0.91
	Right Turn	1.00	1.00	1.00	1.00
	U-Turn	0.94	0.90	0.90	0.90
LSTM	Left Turn	1.00	1.00	1.00	1.00
	Right Turn	1.00	1.00	1.00	1.00
	U-Turn	1.00	1.00	1.00	1.00

virtual vehicle data,” and “P2 noise virtual vehicle data” datasets are generated by simulating the same set of sequence of inputs in “P1 noise real data,” and “P2 noise real data” respectively. The anomaly detection results for virtual vehicle “P1,” and “P2” noise data are presented in Table 5.8. According to this table, the tree based classifier could detect 2 out of 31 FDI in virtual vehicle dataset for “P1,” and “P2” noise. Narrow NN and wide NN could detect 13 and 19 samples as anomaly for “P1” noise where as medium NN detected only 1. For “P2” noise injection narrow NN identify 21 of 31 as anomaly which is more than detected by medium and wide NN with 16 and 13 respectively. Between bi-layered and tri-layered NN, for “P1” noise tri-layered NN performed better than bi-layered NN with 16 and 4 respectively however, for “P2” noise bi-layered detected 21 anomaly which is better than tri-layered with 13 detection. For this particular experiment LSTM could detect all of the anomalies.

Table 5.8: Anomaly Detection in Virtual Vehicle Data with Noise

Classifier Type	P1 noise virtual vehicle data		P2 noise virtual vehicle data	
	No. of FDI Tested	No. of Anomaly Detected	No. of FDI Tested	No. of Anomaly Detected
Tree	31	2	31	2
Narrow NN	31	13	31	21
Medium NN	31	1	31	16
Wide NN	31	19	31	13
Bilayered NN	31	4	31	21
Trilayered NN	31	16	31	13
LSTM	31	31	31	31

5.2.3.5 Discussion

The observations from the above experiments conducted for the proposed PCADS-PB anomaly detection method can be summarized as follows. The result from the first experiment highlights the importance of selecting the appropriate training sequences from each observations of the original real dataset to correctly train the model. Result from training and testing of ML model, suggest that the performance of the selected ML algorithms are better when the training is focused on the sequence around the specific maneuver labeled for that observation instead of training the entire sequence. The second experiment was to evaluate the performance of anomaly detection

with these trained model when noise is injected real dataset. The result of this experiment show that none of the selected algorithms could detect all of the FDI as anomaly. The tree based classifier has the worst performance amongst all. NN based classifiers performed the best with approximately 65% the anomaly detected in average. LSTM was able to detect around 30% of the anomaly. This result suggested the need of a dataset with features that capture the other important information including vehicle dynamics. As the real dataset did not have the parameter for comprehensive information on vehicle dynamics and no information for propulsion, the third experiment was conducted with virtual dataset. This virtual dataset was created by simulating a BEV virtual vehicle model with the driver inputs for steering wheel angle, acceleration and brake pedal from real dataset. Result from model trained with this virtual dataset with more features relevant to vehicle dynamics show that LSTM performed better than the other selected ML approaches to detect anomaly for “P1 noise virtual vehicle data,” and “P2 noise virtual vehicle data,” the two types of noise dataset created for this experiment. These preliminary results and observations made during the experiments suggest that the proposed PCADS-PB has the potential to contribute in further research in the area of anomaly detection for ToD application. It may be noted that the aim of proposed PCADS method is to detect inconsistencies in ToD in correlation to vehicle energy flow, vehicle propulsion, and vehicle dynamics. However, the case study in this dissertation is focused on anomaly detection during turning maneuver, hence vehicle dynamics related parameters are relevant features. For extended scope of PCADS, feature analysis of ESS and traction motor is an important step. As future work this dissertation recommend experiments with various training sequence, feature analysis of relevant vehicle physical parameter according to the vehicle configurations for ToD applications, various point of noise injections and comparative analysis with other anomaly detection methods.

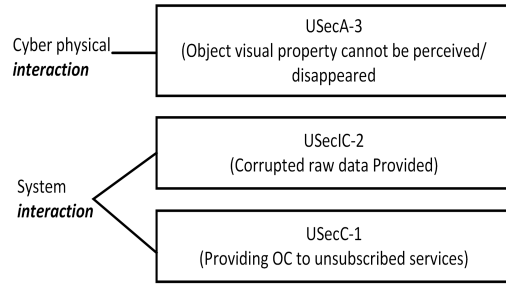
CHAPTER 6

Conclusions and Future Work Recommendation

Autonomous driving is one of the key enablers for transforming mobility solutions into safe, secure, and convenient modes. Current state-of-the-art technology for automated driving has limitations in real life scenarios scenarios, hence ToD has emerged as human-in-the-loop solution. Both autonomous driving and teleorpated driving poses cyber-physical threats that increase concerns for the safety and security of the riders, other road users, and in some cases, the protection of public property.

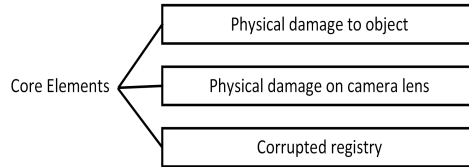
With many actors and their dynamic interactions in the AV's operating environment cyber-physical threats for AVs are not limited to IT cyber-threats. Conventional threat modeling approaches are intended for E/E components of the vehicle and are not focused on AV missions and cyber-physical interactions in AV ODD that heavily affect the performance of an AI-based algorithm for ADS. In this work, recent research on the AV security topic is reviewed. The findings from the literature reviews are presented in three categories. First, a common practice in automotive threat modeling (ISO/SAE 21434) is summarized, along with its limitations and recent progress in an AV-specific security approach from other researchers. Next, the advantages and limitations of an AI algorithm for a vision-based AV perception systems are discussed. Lastly, the latest research in cyber-physical attacks on the vision system is reviewed. To address the need for AV perception-specific threat modeling, this paper proposes an integrated approach that unifies the mission-centric threat analysis method for CPSs considering ISO/SAE 21434 standard. First, a comparative TARA on OC process from the AV perception system is performed with an asset-centric approach and STPA-Sec, which focuses on the interaction and mission of the system. Accordingly, the authors have introduced a transformation step between causal scenarios for unsecured interaction of STPA-Sec and attack class using the STRIDE model. The proposed method can identify threats of AV missions abstracted from platform-level core security resources, as well as the threats to core components of the platform.

In Fig. 6.1, a snapshot of the threat analysis is shown. It can be noted that the proposed method has identified threats in cyber-physical and system interactions, which are critical and



1. Tight coupling with AV mission related interaction (with physical environment and service). Loose coupling with Electrical and electronics (E/E) resource.
2. Secure-by-design of AV feature.
3. Efficient and dynamic (run-time) utilization of use of Security-as-a-service (SaaS) based on mission priority and criticality on demand as atomic as interaction level.
4. Abstraction between application need and platform level cybersecurity resources.

(a)



1. Loose coupling with AV mission related interaction. Tight coupling with E/E resource.
2. Less flexible to support dynamic utilization of use of Security-as-a-service (SaaS).
3. Dedicated security resource guaranteed for pre-defined all time critical threats and core elements.

(b)

Figure 6.1: Key Observations from Results with Proposed Threat Analysis

tightly coupled with AV missions. This allows a security-by-design approach to be followed by the concept level of AV feature design. On the other hand, this analysis has also identified threats to core elements that require dedicated resources. With this ability to identify threats to AV missions abstracted from platform-level core security resources, the security-as-a-service (SAAS) strategy can be decided dynamically based on mission priority and the criticality of AV on demand, as can be observed in Fig. 6.2. On the left side, (a) shows two missions, including M1 for a highway driving scenario and M2 for a city driving scenario, with different needs and types of cyber-physical and system interactions. Depending on the current mission during AV driving, security resources (S1, S2, and S3) are repurposed to secure interactions I4, I5 from I1, I3 for efficient utilization of security resources when AV switched from M1 to M2. At the bottom, (b) shows security S4 to S8 are dedicated to secure core elements that need the resources all the time.

The TARA model presented here incorporates the effect of objects on the road and the robustness

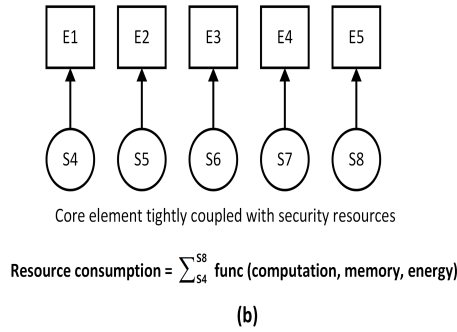
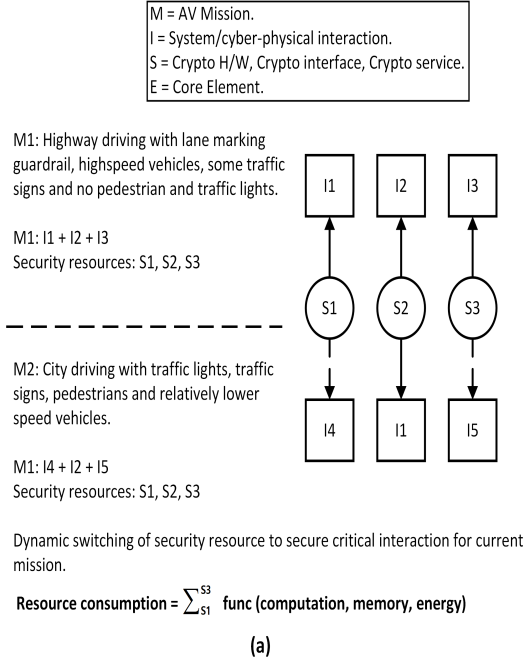


Figure 6.2: An Illustration of Resource Consumption for AV Security

of AV perception algorithms. A case study with humans, cyclists, animals, and vehicles from traffic crash data demonstrates that the proposed model embeds object-level granularity while evaluating the risk of every perception system under an attack. This case study shows that an assessment of attack feasibility augmented with an AI robust factor captures the holistic performance of the perception algorithm under normal, abnormal, and adversarial scenarios with attack and defense methods. We believe that both of these enhancements are useful tools to assess the risk of the AV perception system and evaluate potential solutions to mitigate the threat. As future scope, object-focused impact rating model needs to be with traffic data for various scenarios and other combinations of attack and defense methods. Secondly, the enhancement of risk assessment with AI RF factor needs to be evaluated with a exhaustive list of AI/ML models for AV scenarios.

ToD (ToD) system for public road is in its early stage of evaluation, limited research is available for cyber-physical threats of ToD. Threat modeling in this work shows the risk of ToD is high for

FDI attack on driving control signal from teleoperator to teleoperated vehicle. Also, FDI dataset for ToD driving control signal is not available. Hence, in this research an attack formulation is developed by introducing noise with various window of opportunity. To detect such attack Physics-based Context-aware Anomaly Detection System (PCADS) is presented. Based on the observation and analysis from this research, addressing the following gaps is necessary for future research in to develop a cyber-physical security framework for ToD:

- An exhaustive dataset for false data injection on ToD control is necessary for robust evaluation of anomaly detection method against such attacks.
- Attack formulation shown in this work needs to be extended to various combination of noise, point of injection and duration of attack.
- For anomaly detection the experimental results show that successful detection of anomaly with proposed Physics-based Context-aware Anomaly Detection System (PCADS) depends on the combination of multiple factors including selection of the training sequence, availability and quality of vehicle physical parameter dataset for the specific application, point of noise injection. Therefore, rigorous experiment with such variations is recommended for further evaluation of the performance.
- Proposed PCADS method is formulated based on sequence to classification problem. However, other approach of anomaly detection with the knowledge of physical system needs to be explored and compared with this approach.
- In this research attack creation and anomaly detection is focused on false data injection attack, however as shown in attack tree analysis in section 3.2, ToD has potential threats from other types of attack vectors. Hence, further research with other attack types and mitigation methods is critical for safe and reliable operation of ToD.

APPENDIX

MATLAB Scripts

```
%% PCADS-CA plot positions and route
    geoplayer(data.latitude(1),data.longitude(1),zoomLevel);
    plotPosition(player,data.latitude(i),data.longitude(i));
    plotRoute(player,data.latitude,data.longitude);

%% PCADS-PB train and test data separation
    index_train = randsample(1:height(Dataset_T), 180);
    index_test =
        [3,10,18,26,31,40,57,58,59,67,68,80,85,93,98,102,110,
         121,127,139,150,157,166,176,184,198,201,205,208,211,212];

    T_Train = T(index_train,:);
    T_Test = T(index_test,:);

%% PCADS-PB noise injection
    T_Noise_P1_Test = T_Test;
    T_Noise_P1_Test(:,141:160) = T_Noise_P1_Test(:,141:160).*
        randn(1,20);
    T_Noise_P2_Test = T_Test;
    T_Noise_P2_Test(:,161:180) = T_Noise_P2_Test(:,161:180).*
        randn(1,20);

%% PCADS-PB LSTM model training
    layers = [ ...
        sequenceInputLayer(inputSize)
        %selfAttentionLayer(10,200)
        bilstmLayer(numHiddenUnits1,OutputMode="last")
        batchNormalizationLayer
        leakyReluLayer
        fullyConnectedLayer(numClasses)
        softmaxLayer
        classificationLayer]
```

```

options = trainingOptions("adam", ...
    ExecutionEnvironment="cpu", ...
    GradientThreshold=1, ...
    MaxEpochs=10, ...
    MiniBatchSize=miniBatchSize, ...
    SequenceLength="longest", ...
    Shuffle="never", ...
    Verbose=1, ...
    ValidationData={XValidation,YValidation}, ...
    ValidationFrequency=30, ...
    Plots="training-progress");
[net,info] = trainNetwork(XTrain,YTrain,layers,options);

%% PCADS-PB LSTM model normal scenario test
[YPred,Scores] = classify(net,XTest, ...
    MiniBatchSize=miniBatchSize, ...
    SequenceLength="longest")

%% LSTM attack scenario test
index_lstm_test = index_test;
XTest_lstm = obs_data_new(index_lstm_test);
YTest_lstm = obs_class(index_lstm_test);
YTest_lstm_noise_P1 = YTest_lstm;
YTest_lstm_noise_P2 = YTest_lstm;
XTest_lstm_noise_P1 = XTest_lstm;
for i_randn=1:31
    XTest_lstm_noise_P1{i_randn}(2,40:59) = XTest_lstm{
        i_randn}(2,40:59)*randn(20);
end
XTest_lstm_noise_P2 = XTest_lstm;
for i_randn=1:31
    XTest_lstm_noise_P2{i_randn}(2,60:79) = XTest_lstm{
        i_randn}(2,60:79)*randn(20);
end
[YPred_lstm_noise_P2,Scores] = classify(net,
    XTest_lstm_noise_P2, ...
    MiniBatchSize=miniBatchSize, ...
    SequenceLength="longest")

```

BIBLIOGRAPHY

- [1] Verified Market Research. Global automotive cyber security market size by security (end-point security, application security), by application (telematics system, body control comfort system), by form (in-vehicle and external cloud services), by vehicle (passenger car and commercial vehicle), by geographic scope and forecast. Technical Report 5157, Lewes, Delaware 19958, 2021.
- [2] Upstream. Upstream 2021 global automotive cybersecurity report., 2021.
- [3] Synopsys and SAE International. Securing the modern vehicle a study of automotive industry cybersecurity practices., 2019.
- [4] NHTSA and USDOT. Automated driving systems: A vision for safety, Sep., 2017.
- [5] Sidi Lu, Ren Zhong, and Weisong Shi. Teleoperation technologies for enhancing connected and autonomous vehicles. In *2022 IEEE 19th International Conference on Mobile Ad Hoc and Smart Systems (MASS)*, pages 435–443, 2022.
- [6] NIST cybersecurity framework v1. National Institute of Standards and Technology website, Accessed on Aug 08, 2022.
- [7] Jin Ye et al. Cyber-physical security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges, and future visions. *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 9(4):4639–4657, 2021.
- [8] Hang Zhang, Bo Liu, and Hongyu Wu. Smart grid cyber-physical attack and defense: A review. *IEEE Access*, 9:29641–29659, 2021.
- [9] J. Johnson. Annual number of malware attacks worldwide from 2015 to 2020. Technical report, Statista, Hamburg, Germany, 2021.
- [10] Kate Kochetkova. Shock at the wheel: your jeep can be hacked while driving down the road, Jul. 2015.
- [11] Yao Deng, Tiehua Zhang, Guannan Lou, Xi Zheng, Jiong Jin, and Qing-Long Han. Deep learning-based autonomous driving systems: A survey of attacks and defenses. *IEEE Transactions on Industrial Informatics*, 17(12):7897–7912, 2021.
- [12] Xuting Duan, Hang Jiang, Daxin Tian, Tianyuan Zou, Jianshan Zhou, and Yue Cao. V2i based environment perception for autonomous vehicles at intersections. *China Communications*, 18(7):1–12, 2021.

- [13] Eu agency for cybersecurity says autonomous vehicles highly vulnerable to various cybersecurity challenges. *CPO*. Accessed on Aug 08, 2022.
- [14] Chawin Sitawarin, Arjun Nitin Bhagoji, Arsalan Mosenia, Prateek Mittal, and Mung Chiang. Rogue signs: Deceiving traffic sign recognition with malicious ads and logos. *arXiv preprint arXiv:1801.02780*, 2018.
- [15] Jonathan Petit, Bas Stottelaar, Michael Feiri, and Frank Kargl. Remote attacks on automated vehicles sensors: Experiments on camera and lidar. *Black Hat Europe*, 11(2015):995, 2015.
- [16] Slight street sign modifications can completely fool machine learning algorithms. *IEEE Spectrum*. Accessed on Aug 08, 2022.
- [17] Christopher DiPalma, Ningfei Wang, Takami Sato, and Qi Alfred Chen. Demo: Security of camera-based perception for autonomous driving under adversarial attack. In *2021 IEEE Security and Privacy Workshops (SPW)*, pages 243–243, 2021.
- [18] Neha Yadav, Syed Anas Ansar, and Pawan Kumar Chaurasia. Review of attacks on connected and autonomous vehicles (cav) and their existing solutions. In *2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, pages 1–6, 2022.
- [19] Kyounggon Kim, Jun Seok Kim, Seonghoon Jeong, Jo-Hee Park, and Huy Kang Kim. Cybersecurity for autonomous vehicles: Review of attacks and defense. *Computers Security*, 103:102150, 2021.
- [20] Tao Zhang. Toward automated vehicle teleoperation: Vision, opportunities, and challenges. *IEEE Internet of Things Journal*, 7(12):11347–11354, 2020.
- [21] Van Sy Mai, Richard J. La, Tao Zhang, and Abdella Battou. End-to-end quality-of-service assurance with autonomous systems: 5g/6g case study. In *2022 IEEE 19th Annual Consumer Communications Networking Conference (CCNC)*, pages 644–651, 2022.
- [22] Chuanjie Cai, Yijun Zhang, and Qian Chen. Adaptive control of bilateral teleoperation systems with false data injection attacks and attacks detection. In *2022 41st Chinese Control Conference (CCC)*, pages 4407–4412, 2022.
- [23] Road Vehicles - Cybersecurity Engineering ISO/SAE21434, 2021.
- [24] System-theoretic process analysis for security (STPA-Sec): Cyber security and STPA. MIT Partnership for Systems Approaches to Safety and Security (PSASS), March 27, 2017.
- [25] Mitre attck® matrices.
- [26] Brett Smith, Adela Spulber, Shashank Modi, and Terni Fiorelli. Technology roadmaps: Intelligent mobility technology, materials and manufacturing processes, and light duty vehicle propulsion. *Report of Center for Automotive Research, Ann Arbor, MI*, 2017.
- [27] Top 10 automotive industry trends & innovations in 2021, 2022.
- [28] Strategy and PwC. Digital auto report 2021 – volume 1, 2021.

- [29] Shatad Purohit, Ayesha Madni, Arun Adiththan, and Azad M. Madni. Digital twin integration for software defined vehicles: Decoupling hardware and software in automotive system development. In *2023 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pages 1259–1264, 2023.
- [30] Ziran Wang, Xishun Liao, Xuanpeng Zhao, Kyungtae Han, Prashant Tiwari, Matthew J. Barth, and Guoyuan Wu. A digital twin paradigm: Vehicle-to-cloud based advanced driver assistance systems. In *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, pages 1–6, 2020.
- [31] Liang Zhao, Guangjie Han, Zhuhui Li, and Lei Shu. Intelligent digital twin-based software-defined vehicular networks. *IEEE Network*, 34(5):178–184, 2020.
- [32] Göran Smith and David A. Hensher. Towards a framework for mobility-as-a-service policies. *Transport Policy*, 89:54–65, 2020.
- [33] Alex Davies. Self-driving cars have a secret weapon: remote control. *Wired*, Feb, 2018.
- [34] Teleoperation expanding the solution space for automated driving, 2022. Online: <https://www.nist.gov/news-events/news/2022/09/teleoperation-expanding-solution-space-automated-driving>.
- [35] 5g-blueprint forum on teleoperation. Online:<https://www.5gblueprint.eu/5g-blueprint-forum-on-teleoperation-event-highlights/>.
- [36] A. Drivelink® and teleassist® enable a pragmatic approach toward the future of self-driving vehicles, 2023.
- [37] Driveu.auto solution in level 4 autonomous shuttle operations.
- [38] Ottopia and hyundai mobis team for automotive grade teleoperation platform.
- [39] Julia Horowitz. Amazon’s zox robotaxi drives on public roads in california for the first time, 2023.
- [40] Reza N. Jazar. *Vehicle dynamics: theory and applications*. Springer, London;New York;, 2008.
- [41] M. Abe and W. Manning. Chapter 3 - fundamentals of vehicle dynamics. In M. Abe and W. Manning, editors, *Vehicle Handling Dynamics*, pages 47–118. Butterworth-Heinemann, Oxford, 2009.
- [42] Shaopu Yang, Yongjie Lu, and Shaohua Li. An overview on vehicle dynamics. *International Journal of Dynamics and Control*, 2013.
- [43] Philip Polack, Florent Altché, Brigitte d’Andréa Novel, and Arnaud de La Fortelle. The kinematic bicycle model: A consistent model for planning feasible trajectories for autonomous vehicles? In *2017 IEEE Intelligent Vehicles Symposium (IV)*, pages 812–818, 2017.
- [44] Xiang Liu, Min Xu, and Mian Li. New ta index-based rollover prevention system for electric vehicles. *Energies*, 8:2008–2031, 03 2015.

- [45] Lekshmi S. and Lal Priya P.S. Mathematical modeling of electric vehicles - a survey. *Control Engineering Practice*, 92:104138, 2019.
- [46] Inc Society of Automotive Engineers and Global Info Centre Canada. *Vehicle Dynamics Terminology: SAE J670e*. Global Info Centre Canada, 1978.
- [47] Uwe Kiencke. Automotive control systems. In Robert A. Meyers, editor, *Encyclopedia of Physical Science and Technology (Third Edition)*, pages 839–855. Academic Press, New York, third edition edition, 2003.
- [48] Bilin Aksun Guvenc, Tilman Bunte, Dirk Odenthal, and Levent Guvenc. Robust two degree-of-freedom vehicle steering controller design. *IEEE Transactions on Control Systems Technology*, 12(4):627–636, 2004.
- [49] Junnian Wang, Fei Teng, Jing Li, Liguozang, Tianxin Fan, Jiayu Zhang, and Xingyu Wang. Intelligent vehicle lane change trajectory control algorithm based on weight coefficient adaptive adjustment. *Advances in Mechanical Engineering*, 13:168781402110033, 03 2021.
- [50] Longxi Liu, Zihao Wang, Yunqing Zhang, and Jinglai Wu. Trajectory planning of autonomous vehicles based on parameterized control optimization for three-degree-of-freedom vehicle dynamics model. Technical report, SAE Technical Paper, 2024.
- [51] David C Forbes, Gary J Page, Martin A Passmore, and Adrian P Gaylard. A fully coupled, 6 degree-of-freedom, aerodynamic and vehicle handling crosswind simulation using the driver model. *SAE International Journal of Passenger Cars-Mechanical Systems*, 9(2016-01-1601):710–722, 2016.
- [52] Syed M Hur Rizvi, Muhammad Abid, Abdul Qayyum Khan, Shaban Ghias Satti, and Jibrán Latif. H control of 8 degrees of freedom vehicle active suspension system. *Journal of King Saud University-Engineering Sciences*, 30(2):161–169, 2018.
- [53] *Longitudinal Vehicle Dynamics*, pages 95–122. Springer US, Boston, MA, 2006.
- [54] Rajesh Rajamani. *Lateral Vehicle Dynamics*, pages 15–46. Springer US, Boston, MA, 2012.
- [55] James Balkwill. Chapter 5 - cornering. In James Balkwill, editor, *Performance Vehicle Dynamics*, pages 95–179. Butterworth-Heinemann, 2018.
- [56] Min Yu, Simos A. Evangelou, and Daniele Dini. Advances in active suspension systems for road vehicles. *Engineering*, 33:160–177, 2024.
- [57] Yannik Weber and Stratis Kanarachos. The correlation between vehicle vertical dynamics and deep learning-based visual target state estimation: A sensitivity study. *Sensors*, 19(22), 2019.
- [58] Moad Kissai, Bruno Monsuez, Xavier Mouton, Didier Martinez, and Adriana Tapus. Importance of vertical dynamics for accurate modelling, friction estimation and vehicle motion control. In *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, pages 1370–1377, 2018.

- [59] Xiangping Wu, Yongjun Pan, Gengxiang Wang, and Liang Hou. Pitch motion suppression of electric vehicle active suspensions based on multibody dynamics. *Mechanism and Machine Theory*, 198:105667, 2024.
- [60] Kamil Çağatay Bayindir, Mehmet Ali Gözükküçük, and Ahmet Teke. A comprehensive overview of hybrid electric vehicle: Powertrain configurations, powertrain control techniques and electronic control units. *Energy Conversion and Management*, 52(2):1305–1313, 2011.
- [61] Sergio Manzetti and Florin Mariasiu. Electric vehicle battery technologies: From present state to future systems. *Renewable and Sustainable Energy Reviews*, 51:1004–1012, 2015.
- [62] Wei Liu, Tobias Placke, and K.T. Chau. Overview of batteries and battery management for electric vehicles. *Energy Reports*, 8:4058–4084, 2022.
- [63] Ahmad Faraz, A. Ambikapathy, Saravanan Thangavel, K. Logavani, and G. Arun Prasad. *Battery Electric Vehicles (BEVs)*, pages 137–160. Springer Singapore, Singapore, 2021.
- [64] Gopal K. Dubey. *Fundamentals of electrical drives*. 1994.
- [65] Ahmed T. Hamada and Mehmet F. Orhan. An overview of regenerative braking systems. *Journal of Energy Storage*, 52:105033, 2022.
- [66] Shugang Jiang. Vehicle e/e architecture and its adaptation to new technical trends. Technical report, SAE Technical Paper, 2019.
- [67] Hadi Askaripoor, Morteza Hashemi Farzaneh, and Alois Knoll. E/e architecture synthesis: Challenges and technologies. *Electronics*, 11(4), 2022.
- [68] Glen J Drellishak. An overview of automotive electronics, 1977. In *IEEE 1977 Region Six Conference Record, 1977.*, pages 41–48. IEEE, 1977.
- [69] Dingwang Wang and Subramaniam Ganesan. Automotive domain controller. In *2020 International Conference on Computing and Information Technology (ICCIIT-1441)*, pages 1–5, 2020.
- [70] Weiyang Zeng, Mohammed A. S. Khalid, and Sazzadur Chowdhury. In-vehicle networks outlook: Achievements and challenges. *IEEE Communications Surveys Tutorials*, 18(3):1552–1571, 2016.
- [71] Andrea Reindl, Daniel Wetzels, Norbert Balbierer, Meier Hans, Michael Niemetz, and Sangyong Park. Comparative analysis of can, can fd and ethernet for networked control systems. 10 2021.
- [72] Siddhartha .V, Naveen Kalappa, and Sitaram Yaji. Comparison of can, lin, flex ray and most in-vehicle bus protocols. 04 2019.
- [73] Nicholas Rocchi, Andrea Toscani, Giovanni Chiorboli, Daniel Pinardi, Marco Binelli, and Angelo Farina. Transducer arrays over a²b networks in industrial and automotive applications: Clock propagation measurements. *IEEE Access*, 9:118232–118241, 2021.

- [74] Aurélien Francillon, Boris Danev, and Srdjan Capkun. Relay attacks on passive keyless entry and start systems in modern cars. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. Eidgenössische Technische Hochschule Zürich, Department of Computer Science, 2011.
- [75] Stephen Mason. Vehicle remote keyless entry systems and engine immobilisers: Do not believe the insurer that this technology is perfect. *Computer Law Security Review*, 28(2):195–200, 2012.
- [76] Simon Wright. Autonomous cars generate more than 300 tb of data per year, Jul. 2021.
- [77] Chris Mellor. Data storage estimates for intelligent vehicles vary widely, Jan. 2020.
- [78] Aman Madhok. Autonomous vehicles to boost memory requirement, Feb. 2021.
- [79] Sreeraj Arole. From monolith to service-oriented architecture: A model-based design approach towards software-defined vehicles. In *2023 5th International Conference on Electrical, Control and Instrumentation Engineering (ICECIE)*, pages 1–9. IEEE, 2023.
- [80] Connection Supplier . Automotive connectivity evolves to meet demands for speed bandwidth, Nov. 2019.
- [81] Valery A. Kokovin, Alexander A. Evsikov, Saygid U. Uvaysov, Aida S. Uvaysova, and Viktor I. Nefedov. Scanning network for solving navigation problems of autonomous vehicles. In *2020 International Conference on Electrotechnical Complexes and Systems (ICOECS)*, pages 1–6, 2020.
- [82] Chris Mellor. Autonomous vehicle data storage: We grill self-driving car experts about sensors, clouds . . . and robo taxis, Feb. 2020.
- [83] Amrita Ghosal, Subir Halder, and Mauro Conti. Secure over-the-air software update for connected vehicles. *Computer Networks*, 218:109394, 2022.
- [84] Joshua E. Siegel, Dylan C. Erb, and Sanjay E. Sarma. A survey of the connected vehicle landscape—architectures, enabling technologies, applications, and development areas. *IEEE Transactions on Intelligent Transportation Systems*, 19(8):2391–2406, 2018.
- [85] Alaa Mourad, Siraj Muhammad, Mohamad Omar Al Kalaa, Hazem Refai, and Peter Hoehner. On the performance of wlan and bluetooth for in-car infotainment systems. *Vehicular Communications*, 09 2017.
- [86] Thomas Fügen, Jürgen von Hagen, and Werner Wiesbeck. Wireless in-car communication with bluetooth. *ATZ worldwide*, 104(7):25–28, Jul 2002.
- [87] Valerian Mannoni, Vincent Berg, Stefania Sesia, and Eric Perraud. A comparison of the v2x communication systems: Its-g5 and c-v2x. In *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, pages 1–5, 2019.
- [88] Pierre Roux, Stefania Sesia, Valerian Mannoni, and Eric Perraud. System level analysis for its-g5 and lte-v2x performance comparison. In *2019 IEEE 16th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, pages 1–9, 2019.

- [89] Road deaths and injuries hold back economic growth in developing countries, 2018.
- [90] Road safety report 2021: Japan. Technical report, International Transport Forum, 2021.
- [91] A García-Altés and K Pérez. Injury prevention : journal of the international society for child and adolescent. *International Journal of Dynamics and Control*, 2017.
- [92] Road safety in the western pacific, World Health Organization. Online: <https://www.who.int/westernpacific/health-topics/road-safety>.
- [93] Road safety, Pan American Health Organization. Online: <https://www.paho.org/en/topics/road-safety>.
- [94] Road safety initiative, United Nations Institute for Training and Research. Online: <https://unitar.org/sustainable-development-goals/people/our-portfolio/road-safety-initiative>.
- [95] Road safety annual report 2022, International Transport Forum. Online: <https://www.itf-oecd.org/sites/default/files/docs/irtad-road-safety-annual-report-2022.pdf>.
- [96] Car crash deaths and rates between 1913 and 2022.
- [97] Overview of motor vehicle traffic crashes in 2021, NHTSA. Online: <https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/813435>.
- [98] L. Fortuna, Joseph Kurebwa, and Tawanda Mushiri. A study of damage patterns on passenger cars involved in road traffic accidents. *Journal of Robotics, Hindawi*, 2019.
- [99] Motor-vehicle deaths, injuries, and number of crashes by type of crash, 2022, National Safety Council. Online: <https://injuryfacts.nsc.org/motor-vehicle/overview/type-of-crash/>.
- [100] Jennifer Shuttleworth. Sae and iso refine the levels of driving automation. 2021.
- [101] UNECE. All you need to know about automated vehicles. Technical report, UNECE, Geneva 10, Switzerland, 2021.
- [102] NHTSA and USDOT. Framework for automated driving system safety, Dec., 2020.
- [103] California Department of Motor Vehicle. California autonomous vehicle regulations, Jun., 2020.
- [104] Iso/pas 21448:2019, road vehicles — safety of the intended functionality. Technical report, International Organization for Standardization, Geneva, CH, Jan. 2019.
- [105] ISO/DIS 34501, Road vehicles — Terms and definitions of test scenarios for automated driving systems. Technical report, International Organization for Standardization, Geneva, CH.
- [106] ISO/DIS 34502, Road vehicles — Scenario-based safety evaluation framework for Automated Driving Systems. Technical report, International Organization for Standardization, Geneva, CH.

- [107] ISO/DIS 34503, Road vehicles — Taxonomy for operational design domain for automated driving systems. Technical report, International Organization for Standardization, Geneva, CH.
- [108] UL4600, evaluation of autonomous products. Technical report, Underwriters Laboratories (UL) Standards, Geneva, CH.
- [109] ASAM. ASAM publishes concept for a new autonomous vehicle safety standard enabling testing for road readiness, Feb., 2022.
- [110] Kichun Jo, Junsoo Kim, Dongchul Kim, Chulhoon Jang, and Myoungho Sunwoo. Development of autonomous car—part i: Distributed system architecture and development process. *IEEE Transactions on Industrial Electronics*, 61(12):7131–7140, 2014.
- [111] Mitchell L Cunningham and Michael A Regan. Driver distraction and inattention in the realm of automated driving. *IET Intelligent Transport Systems*, 12(6):407–413, 2018.
- [112] Oliver Jarosch, Hanna Bellem, and Klaus Bengler. Effects of task-induced fatigue in prolonged conditional automated driving. *Human factors*, 61(7):1186–1199, 2019.
- [113] Huansheng Ning, Rui Yin, Ata Ullah, and Feifei Shi. A survey on hybrid human-artificial intelligence for autonomous driving. *IEEE Transactions on Intelligent Transportation Systems*, 2021.
- [114] SAE j3016 taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles. Technical report, SAE, Geneva, CH, Apr. 2021.
- [115] Claytex techblog . Understanding operational design domain to create informed safety in autonomous vehicles deployment, Jul. 2021.
- [116] Mansi Girdhar, Yongsik You, Tai-Jin Song, Subhadip Ghosh, and Junho Hong. Post-accident cyberattack event analysis for connected and automated vehicles. *IEEE Access*, 10:83176–83194, 2022.
- [117] Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles. Technical report, SAE, Apr. 2021.
- [118] Road traffic act (related to automated driving).
- [119] Bringing autonomous driving into the realm of practice, 2021.
- [120] Daniel Bogdoll, Stefan Orf, Lars Töttel, and J. Marius Zöllner. Taxonomy and survey on remote human input systems for driving automation systems. *arXiv*, 2022.
- [121] Code of practice: automated vehicle trialling, UK. Online: <https://www.gov.uk/government/publications/trialling-automated-vehicle-technologies-in-public/code-of-practice-automated-vehicle-trialling>.
- [122] 5g-blueprint project. Online:<https://www.5gblueprint.eu/about/>.
- [123] Teleoperation consortium. Online:<https://www.teleoperation.org/>.

- [124] NIST supports teleoperation forum on concepts and standardization. Online: <https://www.nist.gov/news-events/news/2021/12/nist-supports-teleoperation-forum-concepts-and-standardization>.
- [125] Oscar Amador, Maytheewat Aramrattana, and Alexey Vinel. A survey on remote operation of road vehicles. *IEEE Access*, 10:130135–130154, 2022.
- [126] Jai Prakash, Michele Vignati, Edoardo Sabbioni, and Federico Cheli. Vehicle teleoperation: Human in the loop performance comparison of smith predictor with novel successive reference-pose tracking approach. *Sensors*, 22(23), 2022.
- [127] Adrian Smith. The estonian startup using teleoperation to deliver driverless last-mile deliveries - clevon ceo sander sebastian agur, Feb 2023.
- [128] Scelsi Fabrizio Ugo and Hartmann Volker. Vay’s teledriving-first approach.
- [129] Cybersecurity of vehicle teleoperation, QA Consultants.
- [130] Connected automated mobility 2025: Realising the benefits of self-driving vehicles in the UK.
- [131] Alon Podhurst. Teleoperation: accelerating autonomous vehicle deployment.
- [132] Teleoperation: Safety principles and indirect methods of control.
- [133] Sean O’Neill. How zoox vehicles “find themselves” in an ever-changing world, 2022.
- [134] Announcing the formation of the teleoperation consortium, 2021. Online: <https://www.teleoperation.org/press-releases>.
- [135] NIST vehicle teleoperation forum event 2020. Online: <https://www.nist.gov/news-events/events/2020/11/nist-vehicle-teleoperation-forum>.
- [136] 5g blueprint remote stations for teleoperated driving. Online: <https://5g-ppp.eu/5g-blueprint-remote-stations-for-teleoperated-driving/>.
- [137] Domagoj Majstorovic, Simon Hoffmann, Florian Pfab, Andreas Schimpe, Maria-Magdalena Wolf, and Frank Diermeyer. Survey on teleoperation concepts for automated vehicles, 2022.
- [138] Julia Orlovska, Fjollë Novakazi, Bligård Lars-Ola, MariAnne Karlsson, Casper Wickman, and Rikard Söderberg. Effects of the driving context on the usage of automated driver assistance systems (adas) -naturalistic driving study for adas evaluation. *Transportation Research Interdisciplinary Perspectives*, 4:100093, 2020.
- [139] Sobhan Moosavi, Behrooz Omidvar-Tehrani, R. Bruce Craig, Arnab Nandi, and Rajiv Ramnath. Characterizing driving context from driver behavior. In *Proceedings of the 25th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems, SIGSPATIAL ’17*, New York, NY, USA, 2017. Association for Computing Machinery.
- [140] Andy Greenberg. A new wireless hack can unlock 100 million volkswagens. *Retrieved July*, 6:2019, 2016.
- [141] Andy Greenberg. Tesla responds to chinese hack with a major security upgrade. *Wired*, 2016.

- [142] Mohammad Ali Sayed, Ribal Atallah, Chadi Assi, and Mourad Debbabi. Electric vehicle attack impact on power grid operation. *International Journal of Electrical Power Energy Systems*, 137:107784, 2022.
- [143] Mathy Vanhoef and Frank Piessens. Denial-of-service attacks against the 4-way wi-fi handshake. In *Proceedings of the 9th International Conference on Network and Communications Security*. Academy & Industry Research Collaboration Center (AIRCC), 2017.
- [144] Hirofumi Onishi, Kelly Wu, Kazuo Yoshida, and Takeshi Kato. Approaches for vehicle cybersecurity in the us. *International Journal of Automotive Engineering*, 8(1):1–6, 2017.
- [145] Mujahid Muhammad and Ghazanfar Ali Safdar. Survey on existing authentication issues for cellular-assisted v2x communication. *Vehicular Communications*, 12:50–65, 2018.
- [146] Christine Laurendeau and Michel Barbeau. Threats to security in dsrc/wave. In *International Conference on Ad-Hoc Networks and Wireless*, pages 266–279. Springer, 2006.
- [147] Jin Cao, Maode Ma, Hui Li, Yueyu Zhang, and Zhenxing Luo. A survey on security aspects for lte and lte-a networks. *IEEE communications surveys & tutorials*, 16(1):283–302, 2013.
- [148] Cybersecurity best practices for the safety of modern vehicles. Technical report, NHTSA, 2022.
- [149] Geib, Jeremy and Santos, Brittany and Berry, David and Baldwin, M. and Kess, Barbara. Microsoft threat modeling tool threats, 2022.
- [150] Data integrity: Identifying and protecting assets against ransomware and other destructive events. <https://www.nccoe.nist.gov/publication/1800-25/VolA/index.html>. Accessed: 2022-10-30.
- [151] Jingjing Hao and Guangsheng Han. On the modeling of automotive security: A survey of methods and perspectives. *Future Internet*, 12(11), 2020.
- [152] Olaf Henniger, Alastair Ruddle, Hervé Seudié, Benjamin Weyl, Marko Wolf, and Thomas Wollinger. Securing vehicular on-board it systems: The evita project. In *VDI/VW Automotive Security Conference*, page 41, 2009.
- [153] Aljoscha Lautenbach and M Islam. Heavens–healing vulnerabilities to enhance software security and safety. *The HEAVENS Consortium (Borås SE)*, 2016.
- [154] Georg Macher, Harald Sporer, Reinhard Berlach, Eric Armengaud, and Christian Kreiner. Sahara: A security-aware hazard and risk analysis method. 03 2015.
- [155] Ahmad M. Nasser. *Automotive Cybersecurity Engineering Handbook: The Automotive Engineer’s Roadmap to Cyber-Resilient Vehicles*. Packt Publishing, Limited, Birmingham, 1 edition, 2023.
- [156] Dilip Kumar Sharma, Ningthoujam Chidananda Singh, Daneshwari A Noola, Amala Nirmal Doss, and Janaki Sivakumar. A review on various cryptographic techniques algorithms. *Materials Today: Proceedings*, 51:104–109, 2022. CMAE’21.

- [157] Carson Labrado and Himanshu Thapliyal. Hardware security primitives for vehicles. *IEEE Consumer Electronics Magazine*, 8(6):99–103, 2019.
- [158] Zeinab El-Rewini, Karthikeyan Sadatsharan, Daisy Flora Selvaraj, Siby Jose Plathottam, and Prakash Ranganathan. Cybersecurity challenges in vehicular communications. *Vehicular Communications*, 23:100214, 2020.
- [159] Nasser Nowdehi, Aljoscha Lautenbach, and Tomas Olovsson. In-vehicle can message authentication: An evaluation based on industrial criteria. In *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, pages 1–7, 2017.
- [160] Berardino Carnevale, Luca Fanucci, Samson Bisase, and Harman Hunjan. Macsec-based security for automotive ethernet backbones. *Journal of Circuits, Systems and Computers*, 27(05):1850082, 2018.
- [161] John Padgette, John Bahr, Mayank Batra, Marcel Holtmann, Rhonda Smithbey, Lily Chen, and Karen Scarfone. Guide to bluetooth security. Technical report, National Institute of Standards and Technology, 2017.
- [162] D. Johnston and J. Walker. Overview of ieee 802.16 security. *IEEE Security Privacy*, 2(3):40–48, 2004.
- [163] Jeffrey Cichonski, Joshua Franklin, and Michael Bartock. Guide to lte security. Technical report, National Institute of Standards and Technology, 2016.
- [164] Huimin Chen, Jiajia Liu, Jiadai Wang, and Yijie Xun. Towards secure intra-vehicle communications in 5g advanced and beyond: Vulnerabilities, attacks and countermeasures. *Vehicular Communications*, 39:100548, 2023.
- [165] ITS Communications Security Architecture and Security Management, 2021.
- [166] IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages, 2016.
- [167] Roshan Sedar, Charalampos Kalalas, Francisco Vázquez-Gallego, Luis Alonso, and Jesus Alonso-Zarate. A comprehensive survey of v2x cybersecurity mechanisms and future research paths. *IEEE Open Journal of the Communications Society*, 4:325–391, 2023.
- [168] Vehicle cybersecurity current research, NHTSA. Online: <https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity#the-topic-cybersecurity-protection-methods>.
- [169] ESCRYPT intrusion detection and prevention solution. Online: <https://www.etas.com/en/products/intrusion-detection-and-prevention-solution.php>.
- [170] Research into defending automobiles via intrusion detection systems (ids), pg 21-40, Auto-ISAC community call,feb 2022. Online: https://automotiveisac.com/s/2022_02_02_Auto-ISAC_02Feb22_CC_FINAL-1.pdf.
- [171] Specification of intrusion detection system protocol AUTOSAR, R20-11. Online: https://www.autosar.org/fileadmin/standards/R20-11/F0/AUTOSAR_PRS_IntrusionDetectionSystem.pdf.

- [172] Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36(1):16–24, 2013.
- [173] Aleksandar Milenkoski, Marco Vieira, Samuel Kounev, Alberto Avritzer, and Bryan D. Payne. Evaluating computer intrusion detection systems: A survey of common practices. *ACM Comput. Surv.*, 48(1), sep 2015.
- [174] Clinton Young, Joseph Zambreno, Habeeb Olufowobi, and Gedare Bloom. Survey of automotive controller area network intrusion detection systems. *IEEE Design Test*, 36(6):48–55, 2019.
- [175] Yang L. Zhong F. Xiao, J. Robust anomaly-based intrusion detection system for in-vehicle network by graph neural network framework. *Applied Intelligence*, 2023.
- [176] Sampath Rajapaksha, Harsha Kalutarage, M. Omar Al-Kadri, Andrei Petrovski, Garikayi Madzudzo, and Madeline Cheah. Ai-based intrusion detection systems for in-vehicle networks: A survey. *ACM Comput. Surv.*, 55(11), feb 2023.
- [177] Sivaramakrishnan Rajendar and Vishnu Kaliappan. Sensor data based anomaly detection in autonomous vehicles using modified convolutional neural network. *Intelligent Automation Soft Computing*, 32:859–875, 01 2022.
- [178] Franco van Wyk, Yiyang Wang, Anahita Khojandi, and Neda Masoud. Real-time sensor anomaly detection and identification in automated vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 21(3):1264–1276, 2020.
- [179] Armstrong Aboah. A vision-based system for traffic anomaly detection using deep learning and decision trees. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, pages 4207–4212, June 2021.
- [180] Selim S. Sarikan and A. Murat Ozbayoglu. Anomaly detection in vehicle traffic with image processing and machine learning. *Procedia Computer Science*, 140:64–69, 2018. Cyber Physical Systems and Deep Learning Chicago, Illinois November 5-7, 2018.
- [181] Francisco Caetano, Pedro Carvalho, and Jaime Cardoso. Deep anomaly detection for in-vehicle monitoring—an application-oriented review. *Applied Sciences*, 12(19), 2022.
- [182] Jenny Hofbauer, Kevin Gomez, and Hans-Joachim Hof. From soc to vsoc: Transferring key requirements for efficient vehicle security operations. 10 2023.
- [183] Vita Barletta, Danilo Caivano, Mirko De Vincentiis, Azzurra Ragone, Michele Scalera, and Manuel Serrano. V-soc4as: A vehicle-soc for improving automotive security. *Algorithms*, 16:112, 02 2023.
- [184] The connected car security operations center (SOC). Online: <https://upstream.auto/resources/the-connected-car-soc/>.
- [185] ESCRYPT vehicle security operations center. Online: <https://www.etas.com/en/products/vehicle-security-operations-center.php>.

- [186] Vehicle-soc service overview, fujitsu and upstream. Online: <https://www.fujitsu.com/jp/solutions/business-technology/future-mobility-accelerator/mobility-security/en/>.
- [187] Machine learning - worldwide market size, statista. Online: <https://www.statista.com/outlook/tmo/artificial-intelligence/machine-learning/worldwide#market-size>.
- [188] Global machine learning (ml) market size 2022, fortune business insights. Online: <https://www.fortunebusinessinsights.com/machine-learning-market-102226>.
- [189] Hui Jiang. *Introduction*, page 1–18. Cambridge University Press, 2021.
- [190] James A Nichols, Hsien W Herbert Chan, and Matthew AB Baker. Machine learning: applications of artificial intelligence to imaging and diagnosis. *Biophysical reviews*, 11:111–118, 2019.
- [191] Iqbal H. Sarker. Machine learning: Algorithms, real-world applications and research directions. *SN Computer Science*, 2(3):160, Mar 2021.
- [192] Sampo Kuutti, Richard Bowden, Yaochu Jin, Phil Barber, and Saber Fallah. A survey of deep learning applications to autonomous vehicle control. *IEEE Transactions on Intelligent Transportation Systems*, 22(2):712–733, 2020.
- [193] Gareth James, Daniela Witten, Trevor Hastie, Robert Tibshirani, and Jonathan Taylor. *Unsupervised Learning*, pages 503–556. Springer International Publishing, Cham, 2023.
- [194] Lyndon White, Roberto Togneri, Wei Liu, and Mohammed Bennamoun. *Introduction to Neural Networks for Machine Learning*, pages 1–21. Springer Singapore, Singapore, 2019.
- [195] AI Wiki. Activation function. Online: <https://machine-learning.paperspace.com/wiki/activation-function>.
- [196] Tomasz Szandała. *Review and Comparison of Commonly Used Activation Functions for Deep Neural Networks*, pages 203–224. Springer Singapore, Singapore, 2021.
- [197] Chigozie Nwankpa, Winifred Ijomah, Anthony Gachagan, and Stephen Marshall. Activation functions: Comparison of trends in practice and research for deep learning. *arXiv preprint arXiv:1811.03378*, 2018.
- [198] Yann LeCun, Larry Jackel, Leon Bottou, A Brunot, Corinna Cortes, John Denker, Harris Drucker, Isabelle Guyon, Urs Muller, Eduard Sackinger, et al. Comparison of learning algorithms for handwritten digit recognition. In *International conference on artificial neural networks*, volume 60, pages 53–60. Perth, Australia, 1995.
- [199] Zhang J. Humaidi A. J. Al-Dujaili A. Duan Y. Al-Shamma O. Santamaría J. Fadhel M. A. Al-Amidie M. Farhan L. Alzubaidi, L. Review of deep learning: concepts, cnn architectures, challenges, applications, future directions. *Journal of big data*, page 132306, March 2021.
- [200] Anamika Dhillon and Gyanendra K. Verma. Convolutional neural network: a review of models, methodologies and applications to object detection. *Progress in Artificial Intelligence*, 9(2):85–112, Jun 2020.

- [201] Hongbo Gao, Bo Cheng, Jianqiang Wang, Keqiang Li, Jianhui Zhao, and Deyi Li. Object classification using cnn-based fusion of vision and lidar in autonomous vehicle environment. *IEEE Transactions on Industrial Informatics*, 14(9):4224–4231, 2018.
- [202] Alex Sherstinsky. Fundamentals of recurrent neural network (rnn) and long short-term memory (lstm) network. *Physica D: Nonlinear Phenomena*, 404:132306, March 2020.
- [203] Greg Van Houdt, Carlos Mosquera, and Gonzalo Nápoles. A review on the long short-term memory model. *Artificial Intelligence Review*, 53(8):5929–5955, Dec 2020.
- [204] Runze Zuo, Zhanfeng Zhou, Binbin Ying, and Xinyu Liu. A soft robotic gripper with anti-freezing ionic hydrogel-based sensors for learning-based object recognition. In *2021 IEEE International Conference on Robotics and Automation (ICRA)*, pages 12164–12169, 2021.
- [205] T.N. Ghorsad, A.V Zade, Jianqiang Wang, Keqiang Li, Jianhui Zhao, and Deyi Li. Hybrid cnn+lstm deep learning model for intrusions detection over iot environment. *International Journal on Recent and Innovation Trends in Computing and Communication*, 2023.
- [206] Iqbal H. Sarker. Deep learning: A comprehensive overview on techniques, taxonomy, applications and research directions. *SN Computer Science*, 2(6):420, Aug 2021.
- [207] Insurance definiton: Cyber-physical attack, IRMI. Online: <https://www.irmi.com/term/insurance-definitions/cyber-physical-attack>.
- [208] Gustavo Velasco-Hernandez, De Jong Yeong, John Barry, and Joseph Walsh. Autonomous driving architectures, perception and data fusion: A review. In *2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP)*, pages 315–321, 2020.
- [209] C. Badue et al. Self-driving cars: A survey. *Expert Systems with Applications*, 165:113816, 2021.
- [210] Wenhao Zong, Changzhu Zhang, Zhuping Wang, Jin Zhu, and Qijun Chen. Architecture design and implementation of an autonomous vehicle. *IEEE Access*, 6:21956–21970, 2018.
- [211] Sean Campbell, Niall O’Mahony, Lenka Krpalcova, Daniel Riordan, Joseph Walsh, Aidan Murphy, and Conor Ryan. Sensor technology in autonomous vehicles : A review. In *2018 29th Irish Signals and Systems Conference (ISSC)*, pages 1–4, 2018.
- [212] Jessica Van Brummelen, Marie O’Brien, Dominique Gruyer, and Homayoun Najjaran. Autonomous vehicle perception: The technology of today and tomorrow. *Transportation research part C: emerging technologies*, 89:384–406, 2018.
- [213] Lipu Zhou and Zhidong Deng. Lidar and vision-based real-time traffic sign detection and recognition algorithm for intelligent vehicle. In *17th International IEEE Conference on Intelligent Transportation Systems (ITSC)*, pages 578–583, 2014.
- [214] Felix Nobis, Maximilian Geisslinger, Markus Weber, Johannes Betz, and Markus Lienkamp. A deep learning-based radar and camera sensor fusion architecture for object detection. In *2019 Sensor Data Fusion: Trends, Solutions, Applications (SDF)*, pages 1–7, 2019.

- [215] Qiping Chen, Yinfei Xie, Shifeng Guo, Jie Bai, and Qiang Shu. Sensing system of environmental perception technologies for driverless vehicle: A review of state of the art and challenges. *Sensors and Actuators A: Physical*, 319:112566, 2021.
- [216] Gowdham Prabhakar, Binsu Kailath, Sudha Natarajan, and Rajesh Kumar. Obstacle detection and classification using deep learning for tracking in high-speed autonomous driving. In *2017 IEEE Region 10 Symposium (TENSymp)*, pages 1–6, 2017.
- [217] Joseph Redmon, Santosh Divvala, Ross Girshick, and Ali Farhadi. You only look once: Unified, real-time object detection. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2016.
- [218] Jun Li, Xue Mei, Danil Prokhorov, and Dacheng Tao. Deep neural network for structural prediction and lane detection in traffic scene. *IEEE Transactions on Neural Networks and Learning Systems*, 28(3):690–703, 2017.
- [219] Ruturaj Kulkarni, Shruti Dhavalikar, and Sonal Bangar. Traffic light detection and recognition for self driving cars using deep learning. In *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, pages 1–4, 2018.
- [220] Xinlong Wang, Tete Xiao, Yuning Jiang, Shuai Shao, Jian Sun, and Chunhua Shen. Repulsion loss: Detecting pedestrians in a crowd. In *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pages 7774–7783, 2018.
- [221] Feng Lin, Yan Lai, Lan Lin, and Yuxin Yuan. A traffic sign recognition method based on deep visual feature. In *2016 Progress in Electromagnetic Research Symposium (PIERS)*, pages 2247–2250. IEEE, 2016.
- [222] Jinshan Liu and Jung-Min Park. Seeing is not always believing”: Detecting perception error attacks against autonomous vehicles. *IEEE Transactions on Dependable and Secure Computing*, 18(5):2209–2223, 2021.
- [223] Jasmin Breitenstein, Jan-Aike Termöhlen, Daniel Lipinski, and Tim Fingscheidt. Systematization of corner cases for visual perception in automated driving. In *2020 IEEE Intelligent Vehicles Symposium (IV)*, pages 1257–1264, 2020.
- [224] Adnan Qayyum, Muhammad Usama, Junaid Qadir, and Ala Al-Fuqaha. Securing connected autonomous vehicles: Challenges posed by adversarial machine learning and the way forward. *IEEE Communications Surveys & Tutorials*, 22(2):998–1026, 2020.
- [225] Abdulrahman Kerim and Mehmet Önder Efe. Recognition of traffic signs with artificial neural networks: A novel dataset and algorithm. In *2021 International Conference on Artificial Intelligence in Information and Communication (ICAIIIC)*, pages 171–176. IEEE, 2021.
- [226] Weidong Min, Ruikang Liu, Daojing He, Qing Han, Qingting Wei, and Qi Wang. Traffic sign recognition based on semantic scene understanding and structural traffic sign location. *IEEE Transactions on Intelligent Transportation Systems*, 23(9):15794–15807, 2022.
- [227] Huibing Zhang, Longfei Qin, Jun Li, Yunchuan Guo, Ya Zhou, Jingwei Zhang, and Zhi Xu. Real-time detection method for small traffic signs based on yolov3. *IEEE Access*, 8:64145–64156, 2020.

- [228] Angelica F Magnussen, Nathan Le, Linghuan Hu, and W Eric Wong. A survey of the inadequacies in traffic sign recognition systems for autonomous vehicles. *International Journal of Performability Engineering*, 16(10), 2020.
- [229] Limin Xiao, Limin Xiao, Wenxue Yang, and Jinbin Zhu. Defense against adversarial attacks in traffic sign images identification based on 5g. *EURASIP Journal on Wireless Communications and Networking*, pages 1687–1499, 2020.
- [230] Federico Nesti, Giulio Rossolini, Gianluca D’Amico, Alessandro Biondi, and Giorgio Buttazzo. Carla-gear: a dataset generator for a systematic evaluation of adversarial robustness of vision models, 2022.
- [231] Ivo Friedberg, Kieran McLaughlin, Paul Smith, David Laverty, and Sakir Sezer. STPA-SafeSec: Safety and security analysis for cyber-physical systems. *Journal of information security and applications*, 34:183–196, 2017.
- [232] Amardeep Singh Sidhu. *Application of STPA-Sec for analyzing cybersecurity of autonomous mining systems*. PhD thesis, Massachusetts Institute of Technology, 2018.
- [233] Meriam Chaal, Osiris A Valdez Banda, Jon Arne Glomsrud, Sunil Basnet, Spyros Hirdaris, and Pentti Kujala. A framework to model the stpa hierarchical control structure of an autonomous ship. *Safety Science*, 132:104939, 2020.
- [234] Daniel Patrick Pereira, Celso Hirata, and Simin Nadjm-Tehrani. A stamp-based ontology approach to support safety and security analyses. *Journal of Information Security and Applications*, 47:302–319, 2019.
- [235] Anupam Chattopadhyay, Kwok-Yan Lam, and Yaswanth Tavva. Autonomous vehicle: Security by design. *IEEE Transactions on Intelligent Transportation Systems*, 22(11):7015–7029, 2021.
- [236] Marzana Khatun, Michael Glaß, and Rolf Jung. An approach of scenario-based threat analysis and risk assessment over-the-air updates for an autonomous vehicle. In *2021 7th International Conference on Automation, Robotics and Applications (ICARA)*, pages 122–127, 2021.
- [237] Yang Li, Keqiang Li, Yang Zheng, Bernhard Morys, Shuyue Pan, and Jianqiang Wang. Threat assessment techniques in intelligent vehicles: A comparative survey. *IEEE Intelligent Transportation Systems Magazine*, 13(4):71–91, 2021.
- [238] Lulu Guo, Bowen Yang, Jin Ye, Hong Chen, Fangyu Li, Wenzhan Song, Liang Du, and Le Guan. Systematic assessment of cyber-physical security of energy management system for connected and automated electric vehicles. *IEEE Transactions on Industrial Informatics*, 17(5):3335–3347, 2021.
- [239] Stefan Neumeier, Ermias Andargie Walelgne, Vaibhav Bajpai, Jörg Ott, and Christian Facchi. Measuring the feasibility of teleoperated driving in mobile networks. In *2019 Network Traffic Measurement and Analysis Conference (TMA)*, pages 113–120, 2019.
- [240] Wahab Khawaja, Ismail Guvenc, David W. Matolak, Uwe-Carsten Fiebig, and Nicolas Schneckeburger. A survey of air-to-ground propagation channel modeling for unmanned aerial vehicles. *IEEE Communications Surveys & Tutorials*, 21(3):2361–2391, 2019.

- [241] Jordan A Whitson, David Gorsich, Vladimir V Vantsevich, Michael Letherwood, Oleg Sarpunkov, and Lee Moradi. Military unmanned ground vehicle maneuver: A review and formulation. 2023.
- [242] University of South Australia. New cyber algorithm shuts down malicious robotic attack., 2023.
- [243] Definition of anomaly - understanding science glossary, UC Berkley. Online: <https://undsci.berkeley.edu/glossary/anomaly/>.
- [244] D.E. Denning. An intrusion-detection model. *IEEE Transactions on Software Engineering*, SE-13(2):222–232, 1987.
- [245] Rahul Rai and Chandan K. Sahu. Driven by data or derived through physics? a review of hybrid physics guided machine learning techniques with cyber-physical system (cps) focus. *IEEE Access*, 8:71050–71073, 2020.
- [246] Cody Ruben, Surya Dhulipala, Keerthiraj Nagaraj, Sheng Zou, Allen Starke, Arturo Bretas, Alina Zare, and Janise McNair. Hybrid data-driven physics model-based framework for enhanced cyber-physical smart grid security. *IET Smart Grid*, 3(4):445–453, 2020.
- [247] Faris Alotibi and Mai Abdelhakim. Anomaly detection for cooperative adaptive cruise control in autonomous vehicles using statistical learning and kinematic model. *IEEE Transactions on Intelligent Transportation Systems*, 22(6):3468–3478, 2021.
- [248] Jie Zhong, Yujie Zhang, Jianyu Wang, Chong Luo, and Qiang Miao. Unmanned aerial vehicle flight data anomaly detection and recovery prediction based on spatio-temporal correlation. *IEEE Transactions on Reliability*, 71(1):457–468, 2022.
- [249] Bin Huang and Jianhui Wang. Applications of physics-informed neural networks in power systems - a review. *IEEE Transactions on Power Systems*, 38(1):572–588, 2023.
- [250] Srinivas Bangalore. Timing in Autonomous Vehicles, Mar. 2019.
- [251] Aptiv - Mobility Insider. What are the levels of automated driving?, Nov. 2020.
- [252] Mobility Foresights. Global automotive ultrasonic sensors market 2021-2026.
- [253] Abdullahi Chowdhury, Gour Karmakar, Joarder Kamruzzaman, Alireza Jolfaei, and Rajkumar Das. Attacks on self-driving cars and their countermeasures: A survey. *IEEE Access*, 8:207308–207342, 2020.
- [254] Ed Brown Sensor Technology . The sensing systems that make adas work, Mar. 2021.
- [255] Bogdan Popa. Next-gen cars will need 11tb of storage to handle the data we throw at them, Nov. 2020.
- [256] Molex Staff. High-speed data and connected cars, May 2021.
- [257] Manouchehr Rafie. Edge ai computing advancements driving autonomous vehicle potential, Oct. 2021.
- [258] Sven Evers. Cinco-play: Memory is that critical to autonomous driving, Nov. 2017.

- [259] Automotive World . Bosch: Did you know...facts and figures about electronics and software in vehicles, Jul. 2020.
- [260] Jarosław Mamala, Michał Śmieja, and Krzysztof Praznowski. Analysis of the total unit energy consumption of a car with a hybrid drive system in real operating conditions. *Energies*, 14(13), 2021.
- [261] Oliver Mitchell. Self-driving cars have power consumption problems, Feb. 2018.
- [262] Nick Harris. Light is the key to long-range, fully autonomous evs, May. 2021.
- [263] Yunpeng Wang, Yinghui Wang, Hongmao Qin, Haojie Ji, Yanan Zhang, and Jian Wang. A systematic risk assessment framework of automotive cybersecurity. *Automotive Innovation*, 4(3):253–261, 2021.
- [264] Seunghyun Park and Hyunhee Park. Pier: cyber-resilient risk assessment model for connected and autonomous vehicles. *Wireless Networks*, pages 1–15, 2022.
- [265] Marcel Rumez, Daniel Grimm, Reiner Kriesten, and Eric Sax. An overview of automotive service-oriented architectures and implications for security countermeasures. *IEEE Access*, 8:221852–221870, 2020.
- [266] Marcelino Varas. Service-oriented software architectures: Bridging the gap between autosar classic and adaptive systems, Nov. 2019.
- [267] Ian J Goodfellow, Jonathon Shlens, and Christian Szegedy. Explaining and harnessing adversarial examples. *arXiv preprint arXiv:1412.6572*, 2014.
- [268] Fei Wu, Limin Xiao, Wenxue Yang, and Jinbin Zhu. Defense against adversarial attacks in traffic sign images identification based on 5g. *EURASIP Journal on Wireless Communications and Networking*, 2020(1):1–15, 2020.
- [269] Rongxing Lu, Lan Zhang, Jianbing Ni, and Yuguang Fang. 5g vehicle-to-everything services: Gearing up for security and privacy. *Proceedings of the IEEE*, 108(2):373–389, 2020.
- [270] Yash Shah and Shamik Sengupta. A survey on classification of cyber-attacks on iot and iiot devices. In *2020 11th IEEE Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON)*, pages 0406–0413, 2020.
- [271] Derui Ding, Qing-Long Han, Yang Xiang, Xiaohua Ge, and Xian-Ming Zhang. A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing*, 275:1674–1683, 2018.
- [272] Upinder Kaur, Haozhe Zhou, Xiabin Shen, Byung-Cheol Min, and Richard M. Voyles. Robomal: Malware detection for robot network systems. In *2021 Fifth IEEE International Conference on Robotic Computing (IRC)*, pages 65–72, 2021.
- [273] Keywhan Chung, Xiao Li, Peicheng Tang, Zeran Zhu, Zbigniew T. Kalbarczyk, Ravishankar K. Iyer, and Thenkurussi Kesavadas. Smart malware that uses leaked control data of robotic applications: The case of Raven-II surgical robots. In *22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2019)*, pages 337–351, Chaoyang District, Beijing, September 2019. USENIX Association.

- [274] James Jin Kang, Kiran Fahd, Sitalakshmi Venkatraman, Rolando Trujillo-Rasua, and Paul Haskell-Dowland. Hybrid routing for man-in-the-middle (mitm) attack detection in iot networks. In *2019 29th International Telecommunication Networks and Applications Conference (ITNAC)*, pages 1–6, 2019.
- [275] Mahmood A. Al-Shareeda, Mohammed Anbar, Selvakumar Manickam, and Iznan H. Hasbullah. Password-guessing attack-aware authentication scheme based on chinese remainder theorem for 5g-enabled vehicular networks. *Applied Sciences*, 12(3), 2022.
- [276] Chien-Ming Chen, King-Hang Wang, Kuo-Hui Yeh, Bin Xiang, and Tsu-Yang Wu. Attacks and solutions on a three-party password-based authenticated key exchange protocol for wireless communications. *Journal of Ambient Intelligence and Humanized Computing*, 10(8):3133–3142, Aug 2019.
- [277] Luca Crocetti, Luca Baldanzi, Matteo Bertolucci, Luca Sarti, Bernardino Carnevale, and Luca Fanucci. A simulated approach to evaluate side-channel attack countermeasures for the advanced encryption standard. *Integration*, 68:80–86, 2019.
- [278] Joseph Gravellier, Jean-Max Dutertre, Yannick Teglia, Philippe Loubet Moundi, and Francis Olivier. Remote side-channel attacks on heterogeneous soc. In Sonia Belaïd and Tim Güneysu, editors, *Smart Card Research and Advanced Applications*, pages 109–125, Cham, 2020. Springer International Publishing.
- [279] Shahryar Sorooshian et al. Toward a modern last-mile delivery: Consequences and obstacles of intelligent technology. *Applied System Innovation*, 5(4):82, 2022.
- [280] Bill Anderson, Marta Leardi-Anderson, and Laurie Tannous. Automated trucking and border crossings. *Cross-Border Institute*, 2018.
- [281] Juan E Muriel et al. Assessing the impacts of last mile delivery strategies on delivery vehicles and traffic network performance. *Transportation Research Part C: Emerging Technologies*, 144:103915, 2022.
- [282] Praveena Penmetsa, Pezhman Sheinidashtegol, Aibek Musaev, Emmanuel Kofi Adanu, and Matthew Hudnall. Effects of the autonomous vehicle crashes on public perception of the technology. *IATSS research*, 45(4):485–492, 2021.
- [283] Noppakun Tiwapat, Choosak Pomsing, and Peerapop Jomthong. Last mile delivery: Modes, efficiencies, sustainability, and trends. In *2018 3rd IEEE International Conference on Intelligent Transportation Engineering (ICITE)*, pages 313–317. IEEE, 2018.
- [284] Xuan Li and Fei-Yue Wang. Scenarios engineering: Enabling trustworthy and effective ai for autonomous vehicles. *IEEE Transactions on Intelligent Vehicles*, 2023.
- [285] Hongqing Chu, Hejian Zhuang, Wenshuo Wang, Xiaoxiang Na, Lulu Guo, Jia Zhang, Bingzhao Gao, and Hong Chen. A review of driving style recognition methods from short-term and long-term perspectives. *IEEE Transactions on Intelligent Vehicles*, 2023.
- [286] Michigan traffic crash facts (MTCF). <https://www.michigantrafficcrashfacts.org/>. Accessed on Nov. 2023.

- [287] National Safety Council - Injury Facts. <https://injuryfacts.nsc.org/>. Accessed on Nov. 2023.
- [288] Hong Zhu, Thi Minh Tam Tran, Aduen Benjumea, and Andrew Bradley. A scenario-based functional testing approach to improving dnn performance. In *2023 IEEE International Conference on Service-Oriented System Engineering (SOSE)*, pages 199–207, 2023.
- [289] Behrad Toghi, Divas Grover, Mahdi Razzaghpour, Rajat Jain, Rodolfo Valiente Romero, and Yaser P. Fallah. A maneuver-based urban driving dataset and model for cooperative vehicle applications, 2020.
- [290] MyRouteOnline. <https://www.myrouteonline.com>, 2009. Accessed: 2024-03-20.